



UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACSISTEL

INGENIERÍA EN TELECOMUNICACIONES

TRABAJO DE INTEGRACIÓN CURRICULAR

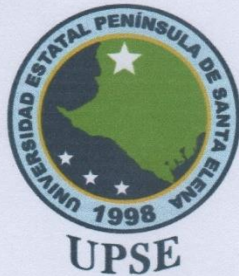
**Implementación de un sistema IDS para la gestión y
seguridad para redes WISP**

Jerick Tobías Guerrero Yagual

Dirigido por:

Ing. Luis Miguel Amaya Fariño, Mgtr.

LA LIBERTAD – 2026



**UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por **Guerrero Yagual Jerick Tobías**, como requerimiento para la obtención del título de Ingeniero en telecomunicaciones.

La Libertad, a los 03 días del mes de agosto del año 2026

TUTOR

Ing. Luis Miguel Amaya Fariño, Mgtr.



**UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

AUTORIZACIÓN

Yo, Guerrero Yagual Jerick Tobías

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de artículo profesional de alto nivel con fines de difusión pública, además apruebo la reproducción de este artículo académico dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

La Libertad, a los 03 días del mes de agosto del año 2026

EL AUTOR


Guerrero Yagual Jerick Tobías



UPSE

**UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

TRIBUNAL DE SUSTENTACIÓN

Ing. Ronald Rovira Jurado, Ph.D.
DIRECTOR DE LA CARRERA

Ing. Luis Amaya Fariño, Mgtr.
DOCENTE TUTOR

Ing. Fernando Chamba, Mgtr.
DOCENTE ESPECIALISTA

Ing. Corina Gonzabay De La A, Mgtr.
SECRETARIA



**UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

DECLARACIÓN DE RESPONSABILIDAD

Yo, Guerrero Yagual Jerick Tobías

DECLARO QUE:

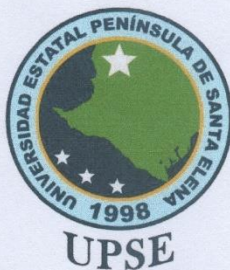
El trabajo de Titulación, **Implementación de un sistema IDS para la gestión y seguridad para redes WISP** de un previo a la obtención del título en Ingeniero en Telecomunicaciones, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 03 días del mes de agosto del año 2026

EL AUTOR


Guerrero Yagual Jerick Tobías



**UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado **Implementación de un sistema IDS para la gestión y seguridad para redes WISP**, presentado por el estudiante, **Guerrero Yagual Jerick Tobías** fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 05%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.

 **Certificado de análisis**
Compilatio Magister+ | UPSE-ECU

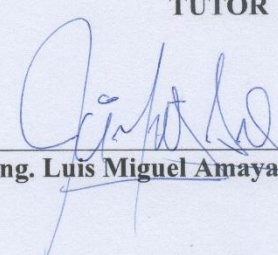
JERICK
ID : 5e17f2aaed9d7679bce70d62174d474985addf8c

 **5%**
Textos sospechosos

Nombre del fichero : JERICK.txt
Tamaño del archivo original : 33.18 MB
Número de palabras : 35.639

Depositante : AMAYA FARIÑO LUIS MIGUEL
Fecha de depósito : 31 de julio de 2026
Tipo de carga : interface
Fecha de fin de análisis : 31 de julio de 2026

TUTOR


Ing. Luis Miguel Amaya Fariño, Mgtr.

AGRADECIMIENTO

En primer lugar, agradezco a Dios por brindarme la vida, la salud, la sabiduría y la fortaleza necesarias para culminar esta etapa académica. Su guía ha sido fundamental en cada momento de este proceso, permitiéndome superar dificultades y mantener la perseverancia para alcanzar este objetivo.

A mi familia Guerrero Yagual, por ser mi principal apoyo durante toda mi formación profesional. Gracias por su amor, paciencia, comprensión y confianza, por acompañarme en cada decisión y por motivarme a seguir adelante incluso en los momentos más difíciles. Este logro también es fruto de su esfuerzo, sacrificio y respaldo incondicional.

A mi novia Elizabeth, por su apoyo constante, paciencia y motivación durante el desarrollo de este trabajo. Gracias por estar presente en este proceso, por brindarme palabras de aliento y por acompañarme en los momentos de mayor exigencia académica y personal.

A mis compañeros del grupo WISP, conformado por Natanael, Jeffry y Elvin, por el trabajo en equipo, el compromiso y la colaboración durante el desarrollo del proyecto. Su aporte fue importante para fortalecer el proceso práctico, compartir conocimientos y avanzar de manera conjunta en la implementación de la infraestructura propuesta.

A mis amigos de carrera, como Mayrin, Angie, Jorge, Bryan, Santiago, Diana y demás colegas, por las experiencias compartidas, el apoyo mutuo y los aprendizajes obtenidos a lo

largo de la vida universitaria. Cada etapa recorrida junto a ellos contribuyó a mi crecimiento académico, personal y profesional.

Al Ing. Luis Amaya, al Ing. Fernando Chamba, al Ing. Carlos Andrade y al Ing. Daniel Jaramillo por sus orientaciones, guía y acompañamiento durante el desarrollo de este trabajo de titulación y por el aprendizaje a lo largo de esta carrera. Sus experiencias, recomendaciones y apoyo académico fueron fundamentales para la culminación de esta investigación.

A la rama IEEE UPSE y al Capítulo Técnico AP-S UPSE, por contribuir a mi formación académica, liderazgo y crecimiento profesional, brindándome espacios de aprendizaje, participación y desarrollo dentro del ámbito de la ingeniería y las telecomunicaciones.

Finalmente, agradezco a todas las personas que, de una u otra manera, formaron parte de este proceso y aportaron con su apoyo, consejos y motivación para la culminación de esta meta académica.

Jerick Tobías Guerrero Yagual

DEDICATORIA

Dedico este trabajo de titulación, en primer lugar, a Dios, por ser mi guía, mi fortaleza y mi apoyo en cada etapa de mi vida. Gracias a su voluntad he podido superar los desafíos presentados durante mi formación académica y alcanzar esta meta tan importante.

A mi familia Guerrero Yagual, por ser el pilar fundamental de mi vida, por su amor, sacrificio, paciencia y apoyo incondicional. Cada logro alcanzado es también reflejo del esfuerzo y confianza que siempre depositaron en mí.

A mi novia Elizabeth, por acompañarme con amor, comprensión y motivación durante este proceso. Su apoyo constante fue fundamental en los momentos de dificultad y cansancio, recordándome siempre la importancia de seguir adelante.

Dedico también este logro a todas las personas que creyeron en mí y me brindaron palabras de aliento a lo largo de este camino universitario. Este trabajo representa no solo el cierre de una etapa académica, sino también el resultado de perseverancia, esfuerzo y dedicación.

Jerick Tobías Guerrero Yagual

ÍNDICE GENERAL

DECLARACIÓN DE DOCENTE TUTOR.....	2
DECLARACIÓN AUTORÍA DEL ESTUDIANTE.....	3
TRIBUNAL DE SUSTENTACIÓN	4
DECLARACIÓN DE RESPONSABILIDAD.....	5
CERTIFICACIÓN DE ANTIPLAGIO	6
AGRADECIMIENTO	7
DEDICATORIA.....	9
ÍNDICE GENERAL	10
ÍNDICE DE FIGURAS.....	15
ÍNDICE DE TABLAS	17
ÍNDICE DE ECUACIONES	18
ÍNDICE DE ANEXOS.....	18
CAPÍTULO 1: GENERALIDADES DEL PROYECTO.....	19
1.1. Resumen.....	19
1.2. Abstract.....	21
1.3. Introducción	23
1.4. Antecedentes	24
1.5. Descripción del proyecto	27
1.5.1. Fases de implementación	31
1.6. Objetivos	35
1.6.1. Objetivo general.....	35
1.6.2. Objetivos específicos	35
1.7. Justificación	37
1.8. Alcance del proyecto.....	40
1.9. Metodología	44
CAPÍTULO 2: MARCO TEÓRICO Y TECNOLÓGICO.....	45
2.1. Redes inalámbricas de proveedores de servicio WISP	45
2.1.1. Arquitectura típica de una red WISP.....	45
2.1.1.1. Núcleo de red (PoP).....	47
2.1.1.2. Nodos de distribución	47
2.1.1.3. Equipos en las instalaciones del cliente	49
2.1.1.4. Sistemas de gestión y monitoreo.....	50

2.2. Arquitectura y seguridad en redes WISP	51
2.2.1. Arquitecturas de seguridad perimetral en redes inalámbricas WISP	51
2.2.2. Control de accesos en entornos segmentados entre VLAN y listas de control.....	53
2.2.3. <i>Firewalls</i> como mecanismo de control y seguridad en redes WISP	55
2.2.4. Aplicación de políticas y priorización de tráfico en plataformas de congestión de red para filtrado	59
2.3. Seguridad en redes WISP.....	62
2.3.1. Amenazas y vulnerabilidades comunes	62
2.3.2. Tipos de ataques detectables por un IDS en una red WISP	62
2.3.2.1. Ataques de denegación de servicio	62
2.3.2.2. Ataques de suplantación de identidad	63
2.3.2.3. Amenazas de <i>software</i> malicioso	63
2.3.2.4. Detección de intrusiones y actividades no autorizadas.....	63
2.3.3. Seguridad interna en redes WISP	64
2.3.3.1. Amenazas y vulnerabilidades internas específicas de redes WISP	64
2.3.4. Estrategias de defensa en profundidad.....	65
2.4. <i>Firewall</i> como herramienta de seguridad.....	66
2.4.1. Definición y evolución del <i>firewall</i>	66
2.5. Sistemas de detección de intrusos, IDS	69
2.5.1. Fundamentos de Snort y Suricata en redes inalámbricas.....	69
2.5.2. <i>Port Mirroring</i> y análisis pasivo en entornos segmentados.....	71
2.5.3. Reglas de detección y actualización de firmas IDS	72
2.5.4. Integración del IDS con perfiles diferenciados de usuarios en WISP	74
2.6. Herramientas de monitoreo y análisis de tráfico.....	76
2.6.1. Herramientas de análisis de tráfico y evaluación de IDS	76
2.6.1.1. iPerf en entornos de laboratorio	76
2.6.1.2. Wireshark en entornos de laboratorio	77
2.6.1.3. Validación del impacto de sistemas IDS y <i>firewalls</i> sobre el rendimiento de red ...	77
2.6.2. Gestión y monitoreo en redes WISP	80
2.6.2.1. Supervisión de redes inalámbricas con herramientas de monitoreo de código abierto	80
2.6.2.2. Gestión remota segura y monitoreo visual en tiempo real.....	81
2.6.2.3. Arquitectura de monitoreo distribuido para entornos WISP simulados.....	83

2.7. Métricas y evaluación del rendimiento de red	84
2.7.1. Latencia.....	84
2.7.2. <i>Jitter</i>	85
2.7.3. <i>Throughput</i>	86
2.7.4. Tasa de pérdida o error de paquetes	86
2.7.5. Tasa de generación de alertas y falsos positivos del IDS.....	87
2.8. Simulación de ataques y validación de sistemas IDS	90
2.8.1. <i>Port Scanning</i> , DoS y <i>Spoofing</i> : técnicas reproducibles en laboratorio	90
2.8.2. Herramientas de ofensiva ética: Nmap, hping3 y Ettercap.....	92
2.8.3. Modelos de ataque y análisis de respuesta del IDS	94
CAPÍTULO 3: PROPUESTA TECNOLÓGICA Y METODOLOGÍA DE IMPLEMENTACIÓN	96
3.1. Fase 1: Diagnóstico y planificación técnica.....	96
3.1.1. Análisis de requerimientos de red	96
3.1.1.1. Requerimientos de segmentación lógica y gestión	96
3.1.1.2. Requerimientos de monitoreo y captura pasiva	96
3.1.1.3. Requerimientos de infraestructura inalámbrica	97
3.1.1.4. Requerimientos de rendimiento y conectividad física	97
3.1.2. Especificaciones técnicas y justificación del <i>hardware</i> seleccionado	98
3.1.2.1. Nodo de enrutamiento y gestión: MikroTik hEX (RB750Gr3)	99
3.1.2.2. Nodo de conmutación y captura: TP-Link (TL-SG3428).....	100
3.1.2.3. Infraestructura de distribución inalámbrica: Ubiquiti airMAX AC	100
3.1.2.4. Accesorios de protección y conectividad.....	101
3.2. Fase 2: Diseño lógico y físico del sistema	102
3.2.1. Plan de direccionamiento IP y segmentación VLAN	102
3.2.1.1. Definición de segmentos y roles de red	103
3.2.1.2. Justificación técnica de la segmentación	104
3.2.1.3. Representación física de la infraestructura	104
3.2.1.4. Implementación física de la infraestructura de red	105
3.2.2. Alcance técnico de la propuesta	106
3.2.3. Enfoque de seguridad adoptado	107
3.3. Fase 3: Implementación del entorno de red y arquitectura general propuesta.....	109
3.3.1. Arquitectura general de la red WISP propuesta	109

3.3.2. Ubicación del IDS dentro de la arquitectura.....	113
3.3.3. Flujo general del tráfico	115
3.3.4. Escenario de validación controlada del IDS	116
3.3.5. Modelo funcional de análisis, clasificación y generación de alertas del IDS	118
3.4. Fase 4: Aplicación de seguridad, monitoreo y criterios de evaluación del IDS	120
3.4.1. Indicadores técnicos de evaluación del IDS	120
3.4.2. Matriz de validación mediante eventos controlados.....	123
3.5. Fase 5: Evaluación, pruebas y documentación del entorno IDS.....	125
3.5.1. Entorno de prueba utilizado	125
3.5.1.1. Preparación e instalación del sistema operativo base	127
3.5.2. Generación de eventos controlados	131
3.5.3. Visualización de alertas en Kibana	133
3.5.4. Integración del IDS con la infraestructura de red	136
3.5.5. Configuración del sistema de notificación por correo electrónico	140
3.5.5.1. Configuración inicial del servicio de correo	140
3.5.5.2. Configuración de autenticación segura en Gmail	142
3.5.5.3. Configuración del cliente de correo msmtpt	144
3.5.5.4. <i>Script</i> de monitoreo y envío de notificaciones.....	146
CAPÍTULO 4: RESULTADOS Y ANÁLISIS DEL SISTEMA IDS IMPLEMENTADO	149
4.1. Resultados de la implementación del IDS	149
4.1.1. Verificación del funcionamiento del IDS.....	149
4.1.2. Integración con ELK Stack.....	152
4.1.3. Visualización general del <i>dashboard</i> del IDS.....	154
4.2. Resultados de detección mediante escenarios controlados.....	156
4.2.1. Prueba de escaneo de puertos con Nmap.....	156
4.2.2. Análisis técnico de las alertas registradas por Suricata IDS	158
4.2.3. Escenario de ataque controlado y análisis de tráfico en la infraestructura IDS WISP .	161
4.2.4. Escenario de saturación de tráfico y comportamiento anómalo en la red WISP	164
4.3. Validación del sistema de notificación por correo electrónico	166
4.3.1. Notificación por actividad DNS detectada	166
4.3.2. Notificación de alerta IDS detectada	167
4.3.3. Resumen de validación del sistema de notificación	169

4.4. Análisis de métricas de red	171
4.4.1. Distribución de alertas por dirección IP de origen.....	171
4.4.2. Distribución de protocolos detectados por el IDS	173
4.4.3. Análisis de las principales firmas de alerta detectadas	175
4.4.4. Análisis de consultas DNS registradas por el IDS	177
4.4.5. Comportamiento del tráfico de red en la infraestructura WISP	179
4.4.6. Caracterización de eventos predominantes del IDS.....	180
4.4.7. Comparación del comportamiento del tráfico en la vista general y con filtrado de alertas IDS	183
4.5. Correlación y validación integral del sistema IDS	186
4.5.1. Correlación global del comportamiento del sistema IDS en la red WISP	186
4.5.2. Validación funcional de la captura de tráfico.....	188
4.5.3. Resultado global de la validación del sistema IDS	193
Conclusiones	197
Recomendaciones	200
Anexos	202
Bibliografía	207

ÍNDICE DE FIGURAS

Figura 1: Fases propuestas para la implementación del IDS para la red WISP	34
Figura 2: Software para gestión y tráfico de datos	41
Figura 3: Software para IDS y firewall	41
Figura 4: Bosquejo de etapas para red WISP con IDS	43
Figura 5: Arquitectura típica de una red WISP	46
Figura 6: Zonas lógicas de la arquitectura de seguridad perimetral de entornos WISP	52
Figura 7: Arquitectura de seguridad perimetral de una red WISP	53
Figura 8: Beneficios de las redes VLAN asumiendo tres tipos diferentes de VLAN como abonados	54
Figura 9: Arquitectura de firewall perimetral en redes WISP de baja escala	56
Figura 10: Arquitectura de seguridad perimetral escalable en redes WISP	57
Figura 11: Línea de tiempo de evolución del firewall	67
Figura 12: Características de iPerf	76
Figura 13: Características de Wireshark	77
Figura 14: Arquitectura distribuida de red WISP	84
Figura 15: Proceso de implementación de modelos reproducibles	95
Figura 16: Arquitectura física de la red WISP con sistema IDS integrado para monitoreo del tráfico	99
Figura 17: Arquitectura lógica de la red WISP con segmentación VLAN e implementación del IDS mediante Port Mirroring	102
Figura 18: Arquitectura física de conexión desde el cliente (CPE) hacia el switch de agregación en la red WISP	105
Figura 19: Conexión física de la infraestructura de red WISP	106
Figura 20: Arquitectura general de la red WISP propuesta con integración del sistema IDS	109
Figura 21: Arquitectura detallada con integración del sistema IDS	110
Figura 22: Núcleo de red	111
Figura 23: Criterios técnicos de la ubicación del IDS	114
Figura 24: Escenario de validación controlada del sistema IDS en la red WISP	117
Figura 25: Modelo funcional de análisis, clasificación y generación de alertas del IDS	118
Figura 26: Panel conceptual de métricas de evaluación del IDS en la red WISP	122
Figura 27: Matriz visual de trazabilidad del sistema IDS en la red WISP	124
Figura 28: Configuración del almacenamiento durante la instalación de Ubuntu Server	127
Figura 29: Configuración del perfil del servidor IDS durante la instalación	128
Figura 30: Finalización de la instalación de Ubuntu Server en la laptop IDS	129
Figura 31: Verificación inicial del sistema operativo Ubuntu Server instalado	130
Figura 32: Dashboard preliminar de alertas IDS visualizadas en Kibana	134
Figura 33: Distribución de alertas por dirección IP de origen	135
Figura 34: Configuración del Port Mirroring en el switch TP-Link TL-SG3428	136
Figura 35: Configuración inicial de Postfix para el envío de correo desde el servidor IDS	141
Figura 36: Definición del nombre del sistema de correo del servidor IDS	142
Figura 37: Configuración de autenticación segura para el envío de alertas IDS	143

Figura 38: Creación de contraseña de aplicación para el sistema IDS	144
Figura 39: Configuración del cliente msmtpt en el servidor IDS	146
Figura 40: Lógica de monitoreo de eventos.....	147
Figura 41: Verificación del funcionamiento del servicio Suricata del sistema IDS.....	150
Figura 42: Verificación del funcionamiento del servicio Elasticsearch del sistema IDS.....	150
Figura 43: Verificación del funcionamiento del servicio Kibana del sistema IDS	151
Figura 44: Verificación del funcionamiento del servicio puerto 5601 para el acceso web a Kibana del sistema IDS	151
Figura 45: Acceso remoto a Kibana desde un equipo cliente	152
Figura 46: Dashboard general del sistema IDS implementado en Kibana	154
Figura 47: Ejecución del escaneo de puertos mediante Nmap	156
Figura 48: Visualización de alertas generadas tras el escaneo con Nmap	157
Figura 49: Detalle técnico de alertas registradas por Suricata IDS	159
Figura 50: Línea de tiempo de alertas generadas por Suricata IDS.....	160
Figura 51: Ejecución de escaneo y generación de tráfico controlado mediante Nmap	162
Figura 52: Visualización de eventos generados por Suricata IDS tras el ataque controlado	163
Figura 53: Generación de tráfico continuo hacia el servicio Kibana mediante saturación HTTP	164
Figura 54: Comportamiento del tráfico y eventos generados durante el escenario de saturación	165
Figura 55: Notificación por actividad DNS detectada en la red WISP.....	167
Figura 56: Notificación de alerta IDS detectada en la red WISP.....	168
Figura 57: Distribución de alertas por dirección IP de origen	172
Figura 58: Distribución de protocolos de red identificados por el IDS	174
Figura 59: Principales firmas de alerta detectadas por Suricata IDS.....	176
Figura 60: Análisis de consultas DNS generadas en la red monitoreada.....	178
Figura 61: Análisis del comportamiento del tráfico de red en la infraestructura WISP	179
Figura 62: Correlación general del tráfico y eventos generados por el IDS en la infraestructura WISP	181
Figura 63: Visualización general del tráfico de red en Kibana	183
Figura 64: Visualización filtrada de alertas generadas por Suricata IDS.....	184
Figura 65: Mapa de correlación del sistema IDS en la red WISP.....	186
Figura 66: Generación de tráfico ICMP mediante prueba de conectividad.....	189
Figura 67: Comportamiento del tráfico capturado por el sistema IDS mediante Kibana.....	190
Figura 68: Distribución de firmas de alerta detectadas por Suricata IDS	192
Figura 69: Distribución de eventos detectados por Suricata IDS	193

ÍNDICE DE TABLAS

Tabla 1: Evaluación del desempeño de los sistemas de detección de intrusos con un análisis de 10 archivos	28
Tabla 2: Elementos de un punto de presencia	47
Tabla 3: Tipos de enlaces de backhaul	48
Tabla 4: Tipos de AP de distribución	48
Tabla 5: Comparativa de plataformas de administración de red para filtrado y QoS	60
Tabla 6: Estrategias en niveles de la red	65
Tabla 7: Comparación entre tipos de firewalls	68
Tabla 8: Características de Snort y Suricata	70
Tabla 9: Reglas y detección en red WISP	73
Tabla 10: Perfiles de usuario	75
Tabla 11: Herramientas de monitoreo de código abierto	81
Tabla 12: Tasa de generación de alertas y falsos positivos	87
Tabla 13: Interpretación de los resultados de detección del IDS	89
Tabla 14: Técnicas reproducibles y sus códigos	90
Tabla 15: Comparación de técnicas reproducibles.....	92
Tabla 16: Características comparativas de herramientas de ofensiva ética	94
Tabla 17: Matriz de requerimientos frente a objetivos técnicos	98
Tabla 18: Matriz de segmentación lógica y direccionamiento.....	103
Tabla 19: Componentes principales de la arquitectura general propuesta	113
Tabla 20: Justificación técnica de la ubicación del IDS	115
Tabla 21: Secuencia funcional del proceso	119
Tabla 22: Indicadores técnicos de evaluación del sistema IDS	121
Tabla 23: Componentes utilizados en la validación preliminar del entorno IDS	126
Tabla 24: Etapas de preparación del sistema operativo base	131
Tabla 25: Eventos controlados considerados en la validación preliminar del IDS	132
Tabla 26: Visualizaciones configuradas en Kibana para la validación preliminar del IDS	133
Tabla 27: Configuración de puertos para Port Mirroring en el switch	137
Tabla 28: Paneles incluidos en el dashboard general del IDS.....	155
Tabla 29: Resumen de la prueba de escaneo de puertos	158
Tabla 30: Herramienta utilizada para inspeccionar los eventos almacenados	160
Tabla 31: Resumen del escenario de ataque controlado	163
Tabla 32: Resumen de la validación del sistema de notificación por correo electrónico	169
Tabla 33: Interpretación de la métrica de alertas por IP de origen.....	173
Tabla 34: Parámetros utilizados para el análisis de protocolos.....	175
Tabla 35: Interpretación de las principales firmas de alerta detectadas	177
Tabla 36: Resumen cuantitativo de firmas detectadas	182
Tabla 37: Distribución de severidad observada	182
Tabla 38: Parámetros obtenidos durante la prueba de tráfico ICMP	189
Tabla 39: Resumen de validación integral del sistema IDS implementado	194

ÍNDICE DE ECUACIONES

Ecuación 1: Cálculo de la latencia de transmisión del paquete	85
Ecuación 2: Cálculo del jitter mediante la variación del retardo	85
Ecuación 3: Cálculo del throughput.....	86
Ecuación 4: Tasa de error de paquetes (PER)	86
Ecuación 5: Precisión del IDS	88
Ecuación 6: Tasa de falsos positivos del IDS	88
Ecuación 7: Tasa de detección del IDS	88
Ecuación 8: Tasa de falsos negativos del IDS.....	88

ÍNDICE DE ANEXOS

Anexo 1: Montaje y ajuste de la antena sectorial Ubiquiti en la infraestructura WISP	202
Anexo 2: Conexión del inyector o switch PoE para la alimentación del equipo inalámbrico	202
Anexo 3: Conexión del cableado Ethernet/PoE hacia el equipo inalámbrico de la red WISP ...	203
Anexo 4: Conexión física del puerto 9 destinado al IDS en el switch TP-Link Omada, identificada mediante un recubrimiento negro en el cable Ethernet.	203
Anexo 5: Generación adicional de tráfico para visualización del IDS en fase preliminar	204
Anexo 6: Validación visual del sistema	204
Anexo 7: Validación de Kibana en conjunto con toda la infraestructura WISP	205
Anexo 8: Validación del ancho de banda en la infraestructura WISP en tiempo real con varios usuarios usando los servicios de la red	205
Anexo 9: Verificación del servidor IDS y visualización de eventos en Kibana	206

CAPÍTULO 1: GENERALIDADES DEL PROYECTO

1.1. Resumen

En un ambiente controlado, el presente trabajo desarrolló una simulación de una red WISP centrada en la administración y la seguridad de la red a través de un IDS. La solución consistió en la implementación de un *router* MikroTik con funciones de *firewall* y control de acceso, y de equipos MikroTik, TP-Link y Ubiquiti, los cuales permitieron la segmentación lógica del tráfico y la aplicación de políticas diferenciadas para distintos tipos de usuarios: VIP, empresarial y residencial.

Se implementó una topología punto a multipunto (PtMP), en la cual una antena sectorial fue el transmisor central y tres antenas CPE representaron los clientes simulados. El hEX RB750Gr3 de MikroTik realizó funciones de enrutamiento, control de tráfico, gestión de VLAN, autenticación de usuarios y aplicación de reglas de *firewall*. El *switch* gestionable TL-SG3428 permitió separar el tráfico entre los diferentes servicios, mientras que un servidor adicional actuó como sistema de monitoreo e IDS, utilizando Suricata integrado con herramientas de almacenamiento y visualización como Filebeat, Elasticsearch y Kibana.

La metodología se organizó en cinco etapas: planificación, diseño lógico y físico, implementación, aplicación de seguridad y monitoreo, y evaluación de los resultados. En cada fase se establecieron condiciones técnicas mínimas que debían cumplirse para pasar a la siguiente, lo que permitió verificar un avance escalable y riguroso del desarrollo del sistema.

Con ello se logró un entorno de laboratorio funcional y replicable, que fue capaz de emular el comportamiento de una red WISP real, con sus controles administrativos y de seguridad respectivos. Esta puesta en práctica constituye un recurso pedagógico que facilitará el

reforzamiento del aprendizaje práctico en telecomunicaciones y contribuirá a disminuir la brecha existente entre la formación académica y las necesidades del entorno laboral.

1.2.Abstract

Wireless Internet Service Provider (WISP) networks have become an important alternative for providing connectivity in areas where traditional infrastructure is limited. However, due to their open wireless nature and distributed architecture, these networks face security challenges related to traffic monitoring, unauthorized access attempts, and the identification of anomalous activities. This research presents the implementation of an Intrusion Detection System (IDS) integrated into a controlled WISP network environment, with the objective of improving traffic visibility, event analysis, and security monitoring capabilities.

The proposed solution was developed through the integration of a MikroTik router as the network core, a managed switch for traffic segmentation through VLANs, and an IDS server based on Suricata. The system uses Port Mirroring technology to perform passive traffic analysis without affecting the normal operation of the network. Additionally, the IDS was integrated with Filebeat, Elasticsearch, and Kibana to enable event storage, processing, visualization, and security alert analysis through interactive dashboards.

The implementation methodology consisted of five phases: technical planning, logical and physical design, infrastructure implementation, security monitoring integration, and system evaluation. Validation tests were performed through controlled traffic generation, including port scanning and abnormal traffic scenarios, allowing the analysis of Suricata's detection capability and the visualization of generated events in Kibana. Furthermore, an email notification mechanism was implemented to automatically inform the administrator about relevant detected events.

The results demonstrated that the implemented IDS was able to capture replicated network traffic, detect security-related events, generate alerts, and provide technical evidence through logs and graphical dashboards. The proposed architecture provides a practical and scalable approach

for WISP network monitoring and security event analysis, strengthening the application of telecommunications and network security technologies in controlled environments.

Keywords: Intrusion Detection System, WISP Networks, Suricata, Port Mirroring, VLAN, Network Security, Kibana.

1.3.Introducción

En el entorno actual de las telecomunicaciones, las redes inalámbricas WISP (Wireless Internet Service Provider) han surgido como una solución eficaz para llevar la conectividad a zonas urbanas y rurales de difícil acceso. No obstante, la formación práctica sobre este tipo de redes es escasa en el ámbito académico, lo que genera una brecha entre los conocimientos teóricos impartidos en las aulas y las competencias técnicas que exige el mercado laboral. Esta situación se refleja especialmente en el desconocimiento de la gestión administrativa, el control de accesos y las medidas de seguridad en infraestructuras inalámbricas reales.

Ante esta problemática, el presente trabajo de titulación propone el diseño e implementación de un entorno de laboratorio que simule una red WISP real, enfocado en la administración, la segmentación de servicios y la aplicación de políticas de seguridad mediante las funciones de *firewall* del *router* MikroTik y mecanismos de control de accesos. El proyecto se desarrolló en un laboratorio académico, utilizando equipos accesibles como *routers* MikroTik, antenas TP-Link y Ubiquiti, un *switch* gestionable y un servidor para pruebas de IDS, lo cual permitió a los estudiantes interactuar con tecnologías empleadas en el entorno profesional.

La propuesta tiene como objetivo no solo reforzar el aprendizaje técnico, sino también fomentar competencias prácticas como el monitoreo de tráfico, la autenticación de usuarios, la segmentación por perfiles (VIP, empresarial, residencial) y la respuesta ante eventos de seguridad. De este modo, se busca ofrecer un instrumento didáctico efectivo que aporte al fortalecimiento de la educación en telecomunicaciones y a la preparación de profesionales listos para afrontar situaciones operativas reales.

1.4. Antecedentes

En los últimos años, las redes inalámbricas de proveedores de servicios de Internet (WISP, por sus siglas en inglés) se han convertido en una solución efectiva para brindar conectividad en zonas rurales, periurbanas e incluso en sectores urbanos donde el acceso a la infraestructura de fibra óptica es difícil. [1]

Alejandro Augusto Andrade Mafla diseñó e implementó un entorno de gestión basado en políticas en redes WISP, con el objetivo de elevar la calidad del servicio mediante una gestión técnica más eficiente. En su estudio, el autor se refiere a los fundamentos teóricos de la gestión de redes y a la terminología establecida en el RFC 3198, así como a los modelos de información PCIM (Policy *Core* Information Model) y PCELS (Policy *Core* Extensions LDAP Schema). Estos modelos sirven de guía para una mejor administración en la futura implementación de este proyecto. [2]

Estas redes se caracterizan por su escalabilidad y rápida instalación, lo que las convierte en una alternativa atractiva para reducir la brecha digital. Sin embargo, al igual que cualquier otra red, las WISP tienen desafíos críticos en relación con su administración, seguridad, calidad de servicio y gestión del ancho de banda, lo cual requiere que quien las opere cuente con una preparación técnica muy sólida.

Los estudiantes de la carrera de Telecomunicaciones presentan una brecha entre la formación teórica adquirida y las competencias prácticas que necesitan para el trabajo, sobre todo en las tecnologías usadas en redes WISP, y más aún cuando se trata de poner en marcha medidas de seguridad avanzadas como los sistemas de detección de intrusos (IDS).

Estas redes son una alternativa clave para la expansión del acceso a Internet, pero su correcta administración y seguridad son todavía un reto para los futuros profesionales.

Emanuel Adrián Arias desarrolló el proyecto “Infraestructura de Red de Datos para WISP”, cuyo objetivo es establecer una red de conectividad eficiente y escalable que permita brindar servicios de Internet, datos, voz y video en cinco regiones metropolitanas previamente identificadas como prioritarias por su alta demanda. Este trabajo es un ejemplo claro de cómo la planificación estructural y técnica de redes WISP puede combinarse con esquemas modernos de administración, sirviendo de base y referencia directa para la propuesta de implementación de sistemas IDS en entornos de laboratorio de telecomunicaciones. [3]

A nivel internacional, universidades y academias técnicas han creado entornos WISP en laboratorio para la formación práctica, como el proyecto WISP Lab de la Universidad de Zaragoza (España), que emplea MikroTik y Ubiquiti para enseñar seguridad en redes inalámbricas.

En Ecuador existen experiencias aisladas de formación en redes, pero son pocas las iniciativas que han incorporado esquemas completos de administración de red, uso de dispositivos *firewall* y segmentación de clientes en un entorno académico controlado.

Una de las principales dificultades que enfrentan los estudiantes es la ausencia de prácticas formativas que les permitan experimentar con las tecnologías de gestión de redes y seguridad en tiempo real, lo cual dificulta una preparación completa para el mundo laboral.

Esta iniciativa resulta aún más relevante a la luz de investigaciones anteriores en las que se demostró que la utilización de sistemas IDS en escenarios educativos no solo posibilitó la detección de ataques como escaneos de puertos, DoS y tráfico sospechoso, sino que también favoreció el aprendizaje práctico de los estudiantes al interactuar con configuraciones reales de

seguridad. Esta referencia demuestra que el uso de tecnologías como Snort, Suricata y herramientas de administración de red puede convertirse en un recurso pedagógico de gran valor.

[3]

Los proveedores de servicios WISP necesitan ingenieros con experiencia en la configuración y el mantenimiento de dispositivos físicos como *routers*, sistemas de autenticación y mecanismos de control de acceso, así como conocimientos sobre segmentación de red, calidad de servicio (QoS) y detección de eventos asociados a ataques. [3]

1.5.Descripción del proyecto

El presente proyecto de tesis consiste en la implementación de un sistema IDS para la gestión y la seguridad de redes WISP en un ambiente controlado. Se busca generar un ámbito de aprendizaje práctico en el cual los estudiantes de la carrera de Telecomunicaciones puedan desarrollar competencias reales en la configuración, gestión y protección de redes inalámbricas, empleando herramientas y equipos que se utilizan en el día a día del mundo profesional. [4]

Debido a que los estudiantes de Telecomunicaciones pueden presentar limitaciones en cuanto a experiencia práctica previa, la presente propuesta proporciona una solución educativa que permite acercarlos a los escenarios técnicos que enfrentarán durante su ejercicio profesional.

Mediante el uso de dispositivos como un *router* MikroTik con funciones de *firewall* integradas, *switches* gestionables, puntos de acceso y un servidor de seguridad con Suricata como motor IDS seleccionado para la implementación, se permitirá que los estudiantes experimenten de forma directa con configuraciones avanzadas, tales como control de accesos, segmentación de red, gestión del ancho de banda y aplicación de reglas de seguridad; también permitirá emular incidentes reales de red como escaneos de puertos, intentos de acceso no autorizado, ataques DoS o tráfico malicioso.

José Eduardo Arteaga Pucha desarrolló una evaluación de las funcionalidades de los sistemas de detección de intrusos basados en red (NIDS) sobre plataformas de código abierto utilizando la técnica de detección de anomalías. En su investigación realizó una comparación entre diferentes sistemas IDS, incluyendo herramientas como Suricata y Snort, considerando escenarios virtuales de aprendizaje, simulación de ataques y evaluación de funcionamiento.

La Tabla 1 sirve de apoyo y base para el presente proyecto en lo referente a los tipos de IDS que se pueden emplear. [5]

Tabla 1: Evaluación del desempeño de los sistemas de detección de intrusos con un análisis de 10 archivos

Nº	Paquetes	Suricata		Snort	
		Paquetes perdidos	Tiempo de respuesta (s)	Paquetes perdidos	Tiempo de respuesta (s)
1	1492331	0%	40	0%	23
2	1237119	0%	24	0%	36
3	1726319	0%	10	63%	38
4	1947815	0%	32	0%	64
5	1483419	0%	16	74%	29
6	1362869	0%	10	53%	33
7	1157328	0%	12	0%	36
8	1616710	0%	12	0%	38
9	1807060	0%	8	38%	62
10	1349635	0%	10	0%	28
Σ	15180605	0%	174	22,8%	387

Fuente: <http://dspace.espoch.edu.ec/bitstream/123456789/8748/1/20T01065.pdf>

El sistema IDS no solo permite detectar amenazas, sino que también es una herramienta educativa muy valiosa, ya que permite a los estudiantes revisar registros, generar reportes y tomar decisiones basadas en datos reales, fortaleciendo sus habilidades técnicas y de análisis crítico.

Con el apoyo de prácticas guiadas y documentación técnica, se facilitará un aprendizaje estructurado, colaborativo y orientado a resolver problemas reales del sector.

Se configuró el sistema IDS, se implementaron políticas de seguridad en el dispositivo *firewall*, se segmentó la red mediante VLAN, se realizaron esquemas de control de acceso y se logró una gestión íntegra del entorno.

El proyecto no es solo una práctica técnica. También responde a una necesidad formativa apremiante: dar solución a la brecha existente entre la teoría que se imparte en las aulas y la práctica que se requiere en el campo profesional.

El entorno también permite al estudiante desarrollar habilidades transversales más allá del componente técnico, tales como la planificación de recursos, la documentación de procesos, el trabajo colaborativo y la toma de decisiones bajo presión. En un mundo cada vez más interconectado y digital, resulta indispensable que los profesionales no solo sepan configurar redes, sino que también comprendan el valor estratégico de protegerlas, administrarlas adecuadamente y adaptarlas a las exigencias del usuario final.

El objetivo no es únicamente proporcionar a los estudiantes habilidades técnicas, sino también otorgarles la confianza y experiencia requeridas para desempeñarse de manera competente en el ámbito de las telecomunicaciones, especialmente en empresas que funcionan con redes WISP.

El esquema de red implementado funciona de la siguiente manera:

- Desde el laboratorio, una antena sectorial (punto a multipunto) entregó la señal inalámbrica a tres clientes simulados que representaban a abonados con diferentes planes de servicio (VIP, empresarial y residencial), cada uno con su propia antena receptora.
- El *router* del laboratorio funcionó como núcleo de la red, gestionando el direccionamiento IP, la autenticación de clientes, la asignación de ancho de banda

y la aplicación de reglas del *firewall*. También se integraron VLAN para segmentar el tráfico por tipo de cliente y conseguir un aislamiento lógico entre servicios.

- Se implementaron métodos de autenticación por *Hotspot* o RADIUS que permitieron asignar perfiles personalizados con credenciales de acceso y políticas de navegación según el tipo de usuario.
- Las reglas del *firewall* definieron el tipo de tráfico permitido o bloqueado. El sistema pudo detectar comportamientos sospechosos mediante herramientas como el IDS o el análisis de tráfico en tiempo real. Como complemento, el *software* The Dude o Zabbix mostró de forma gráfica el estado de los dispositivos de red, su conectividad y rendimiento.
- Se realizaron pruebas funcionales con cada tipo de cliente para comprobar que las políticas de seguridad y administración se cumplieran correctamente. Se registró el comportamiento de la red y, cuando fue necesario, se propusieron ajustes para mejorar su desempeño o seguridad.

1.5.1. Fases de implementación

Fase 1: Diagnóstico y planificación técnica

El objetivo de esta fase fue sentar las bases técnicas y académicas para poder realizar la implementación del sistema WISP. Se realizó un diagnóstico inicial mediante el análisis de los requerimientos del entorno y la revisión de documentación técnica sobre redes inalámbricas, *firewall*, control de acceso y administración del tráfico. Se identificaron y eligieron los equipos adecuados (*router*, *switch*, antenas, servidor), comprobando su compatibilidad y funcionamiento en conjunto. También se definieron los perfiles de clientes (administración, VIP, empresarial y residencial) que serían simulados en el laboratorio y se elaboró un primer diseño lógico de la red. Esta fase permitió establecer una planificación estructurada para reducir posibles inconvenientes durante las etapas posteriores de implementación.

Fase 2: Diseño lógico y físico del sistema

Una vez definidos los recursos y los objetivos, en esta fase se diseñó la arquitectura de red a nivel lógico y físico. Se elaboraron los diagramas con la topología del sistema, se asignaron las direcciones IP a cada segmento de red, se definieron las VLAN y se establecieron las políticas de acceso, velocidad y seguridad para cada tipo de cliente. También se especificó el recorrido del tráfico de red, los enlaces inalámbricos y el flujo de comunicación entre el *router*, el *switch* y las antenas transmisoras y receptoras. Este diseño sirvió como guía técnica para la implementación física de la infraestructura y permitió validar la propuesta antes de continuar con las siguientes etapas.

Fase 3: Implementación del entorno de red

En esta fase se realizó la instalación física de los dispositivos en el laboratorio, incluidos el *router*, el *switch* gestionable, la antena sectorial transmisora y las antenas receptoras. Se configuraron los enlaces punto a multipunto, se realizó la segmentación por VLAN y se asignó a cada cliente su perfil correspondiente. Se montaron y comprobaron las colas de tráfico, de forma que el ancho de banda que recibe cada tipo de cliente fuera el estipulado. Esta fase tuvo como objetivo conseguir una red WISP funcional, con conectividad estable y el flujo de datos correctamente dirigido.

Fase 4: Aplicación de seguridad y monitoreo

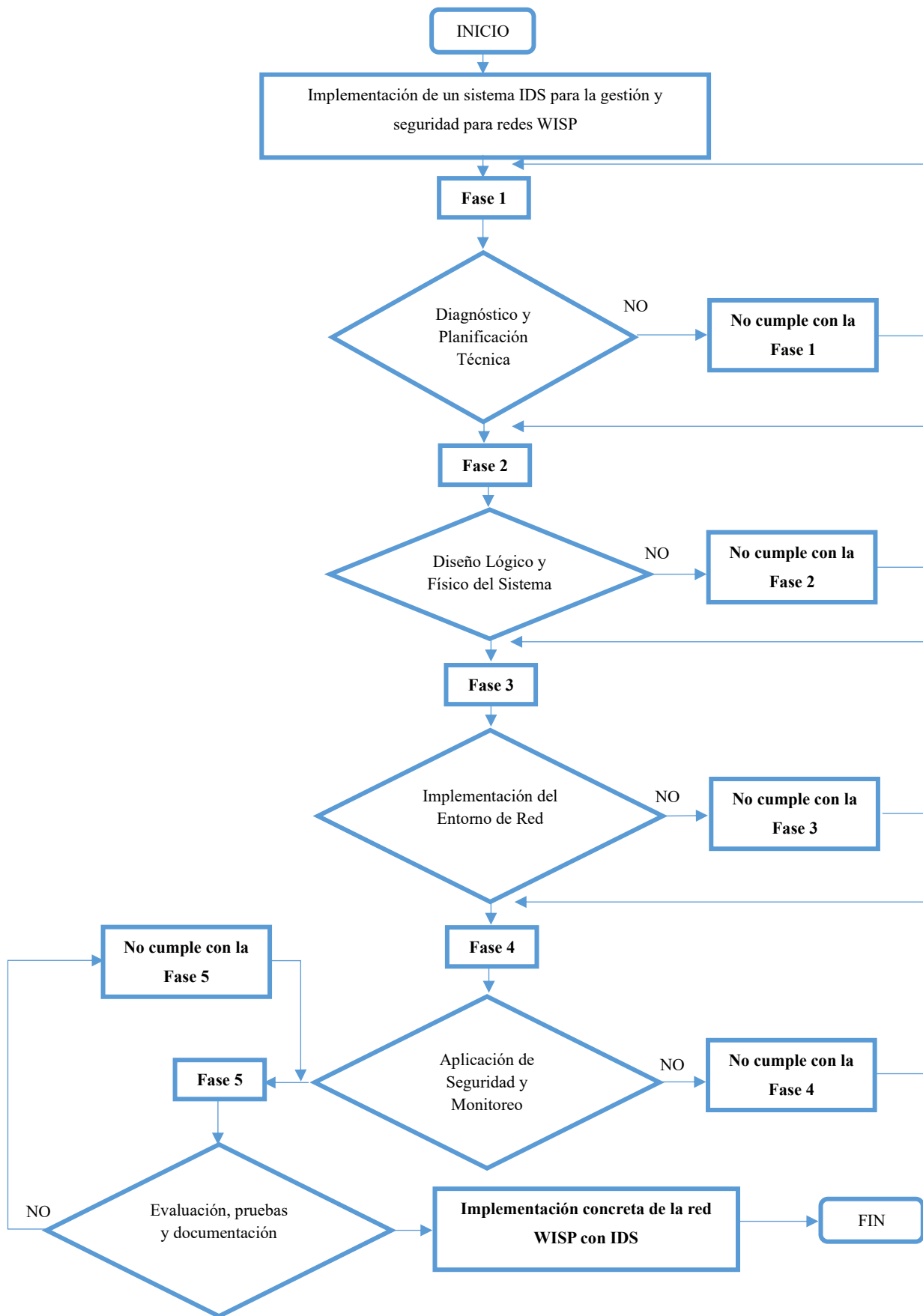
En esta etapa se consolidó la red con medidas de seguridad que protegieran los servicios y regularan el acceso de los usuarios. Se implementaron funciones de filtrado y *firewall* en el *router* MikroTik, así como control de puertos y detección de eventos asociados a ataques. De igual forma, se implementó un sistema de autenticación mediante *Hotspot* o un servidor RADIUS, mediante el cual se puede gestionar el acceso de los clientes en función de su perfil. De forma complementaria, se instaló un sistema IDS (como Suricata) en una máquina física y se configuró un *software* de monitoreo como The Dude o Zabbix, que permite visualizar y analizar el tráfico de red, generar alertas y registrar eventos de seguridad. Esta fase permitió verificar que el entorno simulado quedara protegido y totalmente controlado.

Fase 5: Evaluación, pruebas y documentación

La fase final tuvo como objetivo verificar que el sistema WISP implementado cumpliera con todos los requerimientos técnicos y pedagógicos planteados al inicio del proyecto. Se hicieron pruebas de velocidad, segmentación de tráfico, control de accesos y seguridad, evaluando el comportamiento del sistema con cada tipo de cliente simulado. Se documentaron los resultados

obtenidos, generando registros de *logs*, capturas del tráfico, configuraciones aplicadas y métricas de rendimiento. Finalmente, se redactó un informe técnico completo con recomendaciones para futuras mejoras o escalabilidad del entorno. La documentación resultante será útil tanto para reproducir el laboratorio como para servir de base a futuros trabajos académicos de telecomunicaciones.

Figura 1: Fases propuestas para la implementación del IDS para la red WISP



1.6. Objetivos

1.6.1. Objetivo general

Implementar un sistema IDS para la gestión y seguridad de una red WISP en un ambiente controlado, mediante Suricata integrado con herramientas de monitoreo y visualización como Filebeat, Elasticsearch y Kibana, con el fin de capturar, analizar, visualizar y notificar eventos relevantes de tráfico y seguridad en la infraestructura de red.

1.6.2. Objetivos específicos

- Diseñar la arquitectura lógica y física de una red WISP en un ambiente controlado, considerando segmentación de red, direccionamiento IP, flujo de tráfico y ubicación del sistema IDS.
- Configurar el mecanismo de *Port Mirroring* en el *switch* gestionable para permitir la captura pasiva del tráfico de red hacia el servidor IDS sin afectar la comunicación principal.
- Implementar un servidor IDS basado en Ubuntu Server y Suricata para analizar el tráfico capturado y registrar eventos relevantes dentro de la infraestructura WISP.
- Integrar el sistema IDS con Filebeat, Elasticsearch y Kibana para almacenar, procesar y visualizar eventos de tráfico y seguridad mediante *dashboards*.
- Simular escenarios controlados de tráfico, escaneo y saturación mediante herramientas como Nmap y hping3 para evaluar la respuesta del IDS.
- Evaluar los eventos registrados por el IDS mediante métricas de tráfico y seguridad como direcciones IP de origen, protocolos detectados, firmas de alerta, consultas DNS, volumen de tráfico y severidad.

- Configurar y validar un sistema de notificación por correo electrónico asociado al IDS, con el fin de alertar al administrador ante eventos relevantes detectados en la red monitoreada.

1.7. Justificación

La evolución constante de las tecnologías de comunicación y la creciente demanda de conectividad en zonas urbanas y rurales han impulsado la proliferación de redes WISP como una solución viable, accesible y flexible para brindar acceso a Internet donde la infraestructura tradicional no llega todavía. No obstante, este tipo de redes se distingue por operar en entornos expuestos y con recursos limitados, lo que las convierte en objetivos frecuentes de ataques, interferencias y vulnerabilidades.

La seguridad y la buena administración de la red pasan a ser aspectos críticos que requieren no solo equipos adecuados, sino también personal técnico idóneo que garantice la estabilidad, integridad y disponibilidad del servicio. [1]

Según Barrios y Castillo, los proveedores WISP, al trabajar en entornos abiertos y con recursos limitados, tienden a priorizar la cobertura sobre la seguridad, lo que crea brechas que pueden ser aprovechadas por actores maliciosos sin que los administradores lo detecten a tiempo. [14]

Frente a esta necesidad, se identifica una problemática académica relacionada con la falta de formación práctica especializada en el ámbito de la ciberseguridad dentro del área de redes inalámbricas, especialmente en el contexto de las redes WISP.

Asimismo, esta realidad tecnológica no siempre se refleja adecuadamente en la formación universitaria. Muchos programas de estudio de telecomunicaciones siguen centrándose en contenidos teóricos y no incluyen prácticas que simulen escenarios reales de amenazas o gestión avanzada de redes. [1]

Este trabajo se sustenta en la necesidad de reforzar la formación práctica en el ámbito de la ciberseguridad aplicada a redes WISP, introduciendo tecnologías de monitoreo tales como los sistemas de detección de intrusos (IDS). El objetivo es ofrecer a los estudiantes una experiencia práctica que acompañe y amplíe sus conocimientos teóricos en el campo de las telecomunicaciones.

Karen Scarfone y Peter Mell elaboraron una *Guide to Intrusion Detection and Prevention Systems (IDPS)*. El IDS es una parte fundamental de la red moderna, sobre todo en aquellas redes cuya infraestructura está expuesta a medios inalámbricos; su función no solo es detectar amenazas, sino también mejorar la visibilidad del tráfico y del comportamiento de los usuarios. [8]

El uso de un sistema IDS dentro de un ambiente controlado permitirá a los estudiantes aprender a identificar tráfico sospechoso, analizar patrones de comportamiento anómalo, aplicar políticas de seguridad y actuar frente a intentos de acceso no autorizados. Estas habilidades no solo son altamente demandadas en el mercado laboral, sino que resultan vitales para el diseño y mantenimiento de redes seguras y funcionales, especialmente en el sector WISP, donde la infraestructura suele ser más vulnerable a ataques externos.

Este trabajo no solo contribuye a la formación profesional de los estudiantes, sino que también mejora la infraestructura académica al ser ejecutado en los laboratorios de telecomunicaciones. La propuesta satisface una necesidad real del ámbito educativo y profesional, ofreciendo una solución concreta que potencia la preparación técnica de los futuros ingenieros en telecomunicaciones.

La utilización de herramientas de código abierto como Suricata, en conjunto con una arquitectura de red bien diseñada, permite detectar comportamientos maliciosos en tiempo real,

incrementa la capacidad de monitoreo y respuesta ante incidentes y, al mismo tiempo, constituye un recurso pedagógico muy efectivo. [5]

Existe una brecha entre la formación técnica y la aplicación práctica en entornos tecnológicos especializados. Esta limitación se hace especialmente patente en ámbitos como las telecomunicaciones y las redes, donde los laboratorios a disposición carecen de entornos realistas que posibiliten aplicar conceptos tales como la gestión del ancho de banda, la configuración de redes inalámbricas WISP o las políticas de seguridad en tiempo real.

En el país, el uso de servicios WISP ha tenido un crecimiento sostenido en los sectores rurales y en los barrios urbanos de difícil acceso. En provincias como Santa Elena, más del 35 % de las conexiones se realizaron mediante tecnologías inalámbricas tipo WISP, lo que refleja la demanda real de profesionales que dominan el tema. Sin embargo, la poca integración de tecnologías como MikroTik, Ubiquiti o servidores de monitoreo en los entornos académicos limita la preparación de los futuros técnicos para afrontar estos escenarios.

1.8. Alcance del proyecto

El alcance de este proyecto de tesis comprende la implementación de un sistema IDS (Intrusion Detection System) dentro de un esquema integral de gestión, administración y seguridad de redes WISP (Wireless Internet Service Provider). El sistema se desarrolló y probó en un ambiente controlado.

El sistema propuesto no solo pretende detectar amenazas y vulnerabilidades en tiempo real, sino que también busca fortalecer las capacidades prácticas de los estudiantes de Telecomunicaciones, disminuyendo la brecha existente entre los conocimientos teóricos adquiridos en el aula y los retos técnicos que enfrentan en el mundo laboral.

El proyecto es de aplicación directa en asignaturas como redes inalámbricas, seguridad de redes, gestión de telecomunicaciones y proyectos integradores. Puede ponerse en práctica en cursos de actualización profesional o capacitación técnica para estudiantes y docentes.

Se diseñó e implementó una red educativa WISP que constituye una representación realista de la arquitectura y de las operaciones más comunes en entornos laborales. Esto incluye la configuración de enlaces inalámbricos, *routers*, puntos de acceso, segmentación de red con VLAN y gestión de tráfico.

Figura 2: *Software* para gestión y tráfico de datos



Se incorporó un sistema IDS de código abierto (Snort o Suricata), integrado en un servidor dedicado o virtualizado, que permite capturar, analizar y monitorear el tráfico de red para identificar posibles intrusiones, accesos no autorizados, ataques DoS, escaneos y anomalías de comportamiento. [13]

Figura 3: *Software* para IDS y firewall



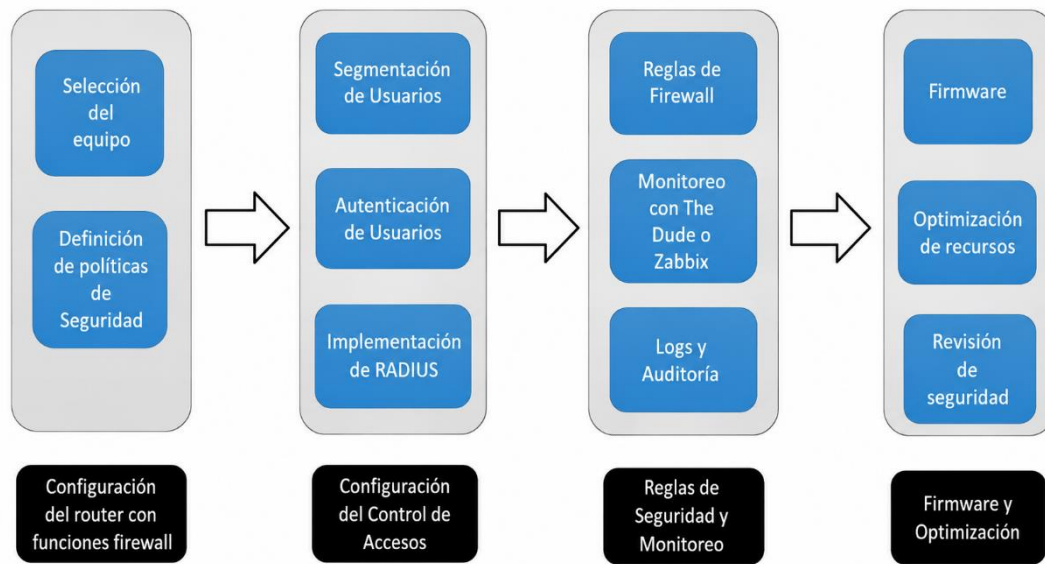
Se empleó equipamiento y *software* que reflejan herramientas reales del mundo laboral, como *routers*, *switches* gestionables y radios de acceso Ubiquiti. Esto permite que los alumnos conozcan marcas y tecnologías que encontrarán con frecuencia en su profesión.

Se realizaron simulaciones de ataques y tráfico malicioso utilizando herramientas como Kali Linux, Nmap, Metasploit o hping3 para evaluar la efectividad del sistema IDS en situaciones reales. Asimismo, se validó el sistema IDS mediante métricas como la detección de amenazas, el número de falsos positivos y negativos, el uso de recursos, la estabilidad de la red y los tiempos de respuesta. [3]

El sistema consideró la segmentación de la red por tipo de usuario (VIP, empresarial y residencial) y la aplicación de políticas diferenciadas de calidad de servicio (QoS), lo que facilitó la simulación de un entorno realista de gestión de prioridades de tráfico. Mediante reglas específicas y control de accesos se evaluó el comportamiento de la red ante distintas configuraciones, con y sin activación del sistema IDS, lo que permitió generar comparaciones útiles para validar su eficacia.

Se analizó el impacto educativo del proyecto, evaluando cómo este tipo de implementación contribuye a la formación profesional, al desarrollo de competencias prácticas y a la preparación de los estudiantes para insertarse en el mundo laboral con una visión más técnica, crítica y actualizada.

Figura 4: Bosquejo de etapas para red WISP con IDS



1.9. Metodología

Investigación Descriptiva

Su finalidad es caracterizar de manera detallada una situación o un sistema. En este trabajo se describe detalladamente el funcionamiento de una red WISP, los problemas habituales de administración, los tipos de ataques más comunes y las herramientas y protocolos que se utilizan para mejorar la seguridad de la red. Se describen asimismo los componentes físicos y lógicos utilizados, proporcionando una clara comprensión del sistema y sus capacidades.

Investigación Documental

Se sustenta en el análisis de fuentes bibliográficas, normativas técnicas y trabajos previos relacionados con el tema de estudio. Esta modalidad es indispensable para la construcción del marco teórico y el diseño del sistema, ya que permite fundamentar decisiones técnicas a partir de estándares de seguridad de redes, manuales de configuración, artículos científicos y experiencias de implementación de IDS en redes similares.

Investigación Experimental

Este tipo de investigación se utiliza para comprobar el comportamiento de una red WISP gestionada con un sistema IDS bajo diferentes configuraciones y ataques simulados. Se realizaron pruebas prácticas sobre dispositivos físicos (*routers* con funciones de *firewall*, puntos de acceso, *switches*); esto posibilitó modificar variables como el ancho de banda, el tráfico malicioso o el control de accesos y medir sus efectos sobre el rendimiento y la seguridad de la red. [14]

CAPÍTULO 2: MARCO TEÓRICO Y TECNOLÓGICO

2.1. Redes inalámbricas de proveedores de servicio WISP

2.1.1. Arquitectura típica de una red WISP

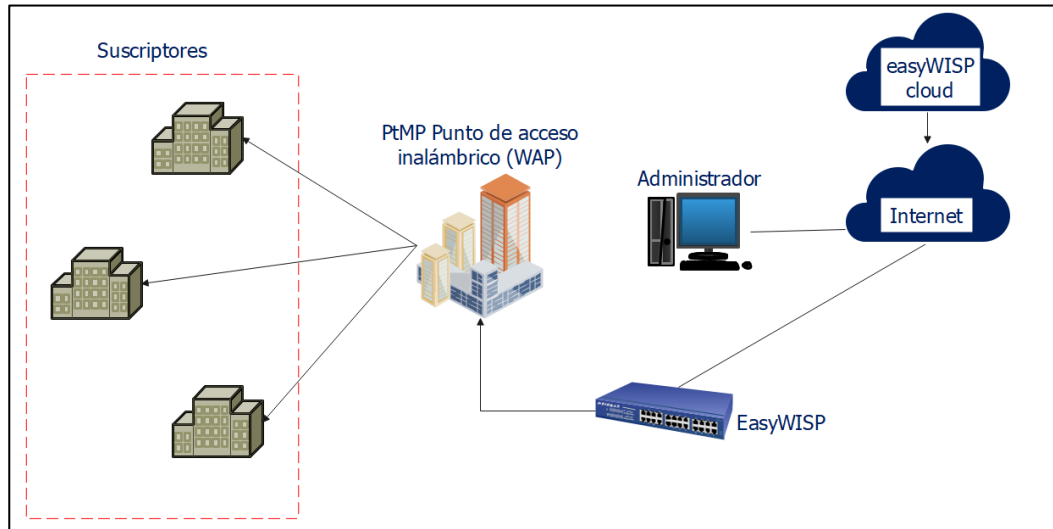
Para entender cómo una red WISP (Proveedor de Servicios de Internet Inalámbrico) lleva el servicio de Internet a los hogares y negocios, es fundamental visualizar su estructura básica. Una red WISP corresponde a una infraestructura de telecomunicaciones conformada por diferentes elementos físicos y lógicos que permiten la distribución inalámbrica del servicio de Internet.

El Punto de Presencia (PoP) constituye el nodo central de la arquitectura WISP. Aquí es donde el WISP establece su conexión principal con Internet, a menudo utilizando enlaces de fibra óptica robustos. En este nodo central de la red se encuentran los equipos más importantes: los *routers* que dirigen el tráfico, los *switches* que organizan la comunicación y los servidores que asignan las direcciones a cada dispositivo. Para la seguridad, es en este punto neurálgico donde se ubica el *firewall* principal. El *firewall* constituye el primer mecanismo de control del tráfico que ingresa y egresa de la red, segmentando y protegiendo la infraestructura interna.

Con base en la Figura 5 se evidencia el tipo de red y la distribución que se realiza en ella. Corresponde a una arquitectura típica y proporciona una base respecto al tipo de red WISP que se aplica en el presente proyecto. [15]

Para que una red sea robusta y libre de amenazas, se debe agregar un *firewall* interno y externo, además de un IDS correctamente configurado que detecte anomalías o intrusiones.

Figura 5: Arquitectura típica de una red WISP



Desde este centro, la conectividad se extiende a las torres o puntos de acceso remotos, que funcionan como los brazos del WISP. Los datos viajan a estas torres a través de enlaces de alta capacidad, ya sean potentes conexiones inalámbricas punto a punto o extensiones de fibra óptica. En estas torres se instalan las antenas y los puntos de acceso (AP) que emiten la señal de Internet a los sectores de cobertura, empleando distintas tecnologías inalámbricas que hacen posible llegar hasta los usuarios finales. [16]

El último equipo en las instalaciones de cada cliente es el CPE (Equipamiento del Cliente). Este dispositivo cumple la función de una antena exterior: es el que captura la señal de la torre más cercana y la convierte en una conexión que el *router* Wi-Fi del cliente puede llevar a los ordenadores, teléfonos y demás dispositivos.

Todo este complejo ecosistema es monitoreado y gestionado por sistemas especializados, que permiten al WISP mantener un control constante sobre el rendimiento de la red y la calidad del servicio, asegurando que los datos fluyan sin interrupciones y que la seguridad se mantenga vigilada.

2.1.1.1. Núcleo de red (PoP)

Constituye el nodo central de operación de la red WISP. Es el lugar físico donde el proveedor establece su conexión de alta capacidad con el resto de Internet.

Tabla 2: Elementos de un punto de presencia

Punto de presencia (PoP) o estación base principal	
Elementos	Descripción o función
Conexión troncal (Backbone Connection)	En el PoP, el WISP adquiere su ancho de banda de un proveedor de servicios de Internet de nivel superior (ISP mayorista). Esta conexión es el conducto principal de datos hacia y desde la red del WISP. Generalmente, se materializa a través de enlaces de fibra óptica de gran capacidad, que ofrecen alta velocidad y baja latencia.
Equipos de borde y agregación	Dentro del PoP, se ubican los equipos de red más potentes y críticos. Entre estos se incluyen <i>routers</i> de borde (<i>edge routers</i>) que gestionan el enrutamiento del tráfico entre la red interna e Internet.
Servicios centrales de red	El PoP también alberga servidores fundamentales para la operación. Entre ellos, el servidor DHCP (Dynamic Host Configuration Protocol) es clave para la asignación automática de direcciones IP a los dispositivos de los clientes, simplificando la gestión de la red.
Ubicación estratégica del firewall	El <i>firewall</i> principal de la red WISP se despliega estratégicamente en el PoP. Dada su posición como puerta de enlace entre la red interna y el Internet global, el <i>firewall</i> ejerce un control fundamental sobre el tráfico, aplicando políticas de seguridad para filtrar, bloquear y permitir la comunicación.

2.1.1.2. Nodos de distribución

Los nodos de distribución, comúnmente representados por torres o estructuras elevadas, son los puntos intermedios que extienden la conectividad desde el PoP hacia las áreas de cobertura de los clientes.

- Enlaces de *backhaul*: El tráfico de datos se transporta desde el PoP hasta estas torres mediante enlaces de *backhaul* [17]. Estos pueden ser:

Tabla 3: Tipos de enlaces de *backhaul*

Enlaces de <i>backhaul</i>	
Tipos de enlaces	Descripción
Inalámbricos punto a punto (PTP)	Utilizan equipos de radio de alta potencia y antenas direccionales para establecer conexiones de alta capacidad y baja latencia entre el PoP y cada torre. Operan en diversas bandas de frecuencia, incluyendo 5 GHz, 60 GHz o incluso bandas licenciadas, dependiendo de la distancia y el ancho de banda requerido.
Fibra óptica	En casos donde la infraestructura lo permite o la densidad de clientes lo justifica, se puede extender la fibra óptica directamente hasta las torres, ofreciendo la máxima capacidad y fiabilidad.

- *Access Point* (AP) de distribución: En la cima de estas torres se instalan los puntos de acceso (AP). Estos dispositivos emiten la señal inalámbrica que los clientes finales recibirán. [18]

Se utilizan principalmente dos tipos:

Tabla 4: Tipos de AP de distribución

Access Point de distribución	
Tipos de AP	Descripción
APs Sectoriales	Cuentan con antenas direccionales que cubren un sector específico (p. ej., 60°, 90°, 120°), permitiendo una mayor reutilización de frecuencias y una mejor gestión de la capacidad en áreas densas.
APs Omnidireccionales	Irradian la señal en 360 grados, siendo más adecuados para áreas de baja densidad de clientes o como puntos de acceso iniciales.

Se elige el tipo de AP y la tecnología inalámbrica (estándares 802.11ac/ax o soluciones de fabricantes especializados y propietarios como Ubiquiti, MikroTik o Mimosa) en función de factores como la distancia a los clientes, la interferencia ambiental y el ancho de banda deseado.

2.1.1.3. Equipos en las instalaciones del cliente

La capa final de la arquitectura WISP reside directamente en el lado del usuario.

- **Antenas/Radios CPE (Customer Premise Equipment):** Se requiere un CPE para cada cliente que se suscriba al servicio WISP. Este dispositivo, que normalmente es una antena direccional compacta con un radio incorporado, se coloca en el exterior de la casa o negocio del cliente, orientado hacia la torre WISP más cercana. Su función es recibir la señal inalámbrica y transformarla en una conexión de red estándar (generalmente Ethernet). La selección del CPE depende de la distancia a la torre y la línea de vista disponible. [19]
- **Conexión interna al cliente:** Desde el CPE, un cable de Ethernet se extiende dentro de la propiedad del cliente. Allí se conecta generalmente a un *router* Wi-Fi doméstico o de oficina. Este *router* se encarga de distribuir la conexión a todos los dispositivos internos del cliente (computadoras, smartphones, televisores inteligentes, etc.) a través de Wi-Fi o puertos Ethernet. [19]

2.1.1.4. Sistemas de gestión y monitoreo

Aunque no son componentes físicos que transmiten datos directamente, los sistemas de gestión son vitales para la operación eficiente de la red WISP.

- *Software* de gestión de red (NMS - Network Management System): Estas plataformas permiten a los administradores monitorear en tiempo real el estado de todos los equipos (AP, *routers*, *switches*), el tráfico de red, la calidad de la señal y la disponibilidad de los enlaces. Esto permite detectar problemas de manera proactiva y optimizar el rendimiento.
- Sistemas de control de acceso y facturación: Son herramientas que gestionan los perfiles de los clientes, los planes de servicio, el ancho de banda asignado a cada uno y el proceso de facturación.
- Monitoreo de seguridad: Es en esta capa de gestión donde se integra un sistema como el IDS (Intrusion Detection System), objeto del presente estudio. El IDS controla los flujos de tráfico y los eventos de seguridad que genera cada componente de la red, para así poder identificar actividades sospechosas que puedan ser señal de una amenaza o de un intento de intrusión. Los datos que recopila el IDS son de suma importancia para reforzar la protección proporcionada por el *firewall* y garantizar la integridad de la red WISP.

2.2. Arquitectura y seguridad en redes WISP

2.2.1. Arquitecturas de seguridad perimetral en redes inalámbricas WISP

Para los Proveedores de Servicios de Internet Inalámbrico (WISP), la seguridad perimetral es una de las principales líneas de defensa de la red frente a amenazas, tanto internas como externas.

Las redes que operan en entornos abiertos presentan un mayor riesgo de exposición a amenazas como el escaneo de puertos, los accesos no autorizados, la suplantación de identidad y los ataques DoS. Por ello, diseñar una adecuada defensa de seguridad perimetral es fundamental en el diseño de los recursos de red, la utilización del servicio y el mantenimiento de la infraestructura de sistemas.

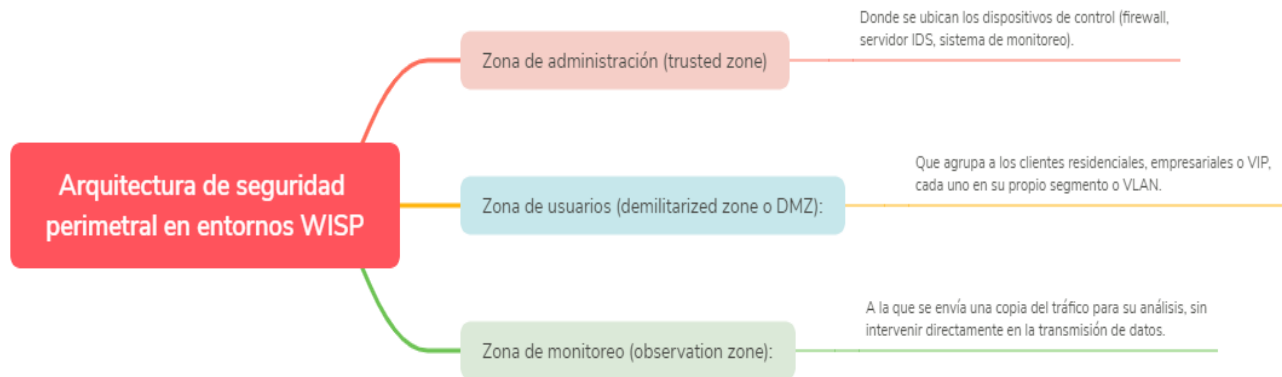
Un modelo de seguridad perimetral en ambientes WISP está formado por elementos tales como *firewalls*, enrutadores y conmutadores administrables, junto con lógica de segmentación mediante VLAN y sistemas de detección y respuesta ante intrusiones (IDS/IPS).

La delimitación del perímetro permite controlar y monitorear cada zona expuesta (cliente) para establecer políticas específicas de acceso y una gestión diferenciada por zona de confianza.

Para redes pequeñas y de laboratorio es habitual utilizar *routers* MikroTik en redes WISP por su bajo costo y gran flexibilidad. Estos dispositivos permiten aplicar reglas de *firewall* en los niveles 3 y 4, realizar NAT y monitorizar conexiones activas y listas de control por dirección MAC e IP. También pueden ser utilizados junto a *switches* gestionados con capacidad para VLAN 802.1Q, lo cual ayuda a mejorar la segmentación del tráfico evitando colisiones o acceso cruzado entre clientes. [3]

Como parte de la arquitectura del perímetro de la red, se recomiendan al menos tres zonas lógicas.

Figura 6: Zonas lógicas de la arquitectura de seguridad perimetral de entornos WISP

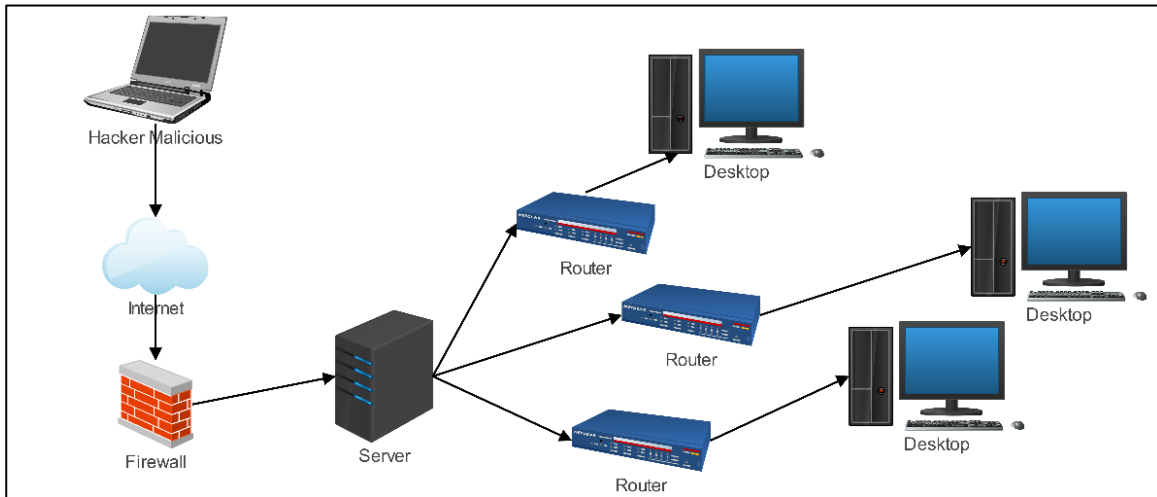


Estas arquitecturas están basadas en principios de mínimo privilegio y defensa en profundidad, lo que implica que ningún usuario debe tener acceso a más recursos de los estrictamente necesarios, y que cada capa (*switch*, *router*, IDS) debe tener controles redundantes para aumentar la capacidad de detección y contención de amenazas.

En la Figura 6 se muestra la forma en que se organiza la seguridad perimetral en una red WISP, dividiendo el entorno en zonas lógicas como la red pública, la red interna de clientes y la zona de administración.

Cada una de estas áreas está protegida por elementos como *routers*, *firewalls* y sistemas IDS que trabajan en conjunto para evitar accesos no autorizados y amenazas externas. La ilustración ayuda a entender cómo se construye una defensa en capas, donde cada segmento tiene funciones específicas de control y monitoreo para garantizar un entorno seguro.

Figura 7: Arquitectura de seguridad perimetral de una red WISP



2.2.2. Control de accesos en entornos segmentados entre VLAN y listas de control

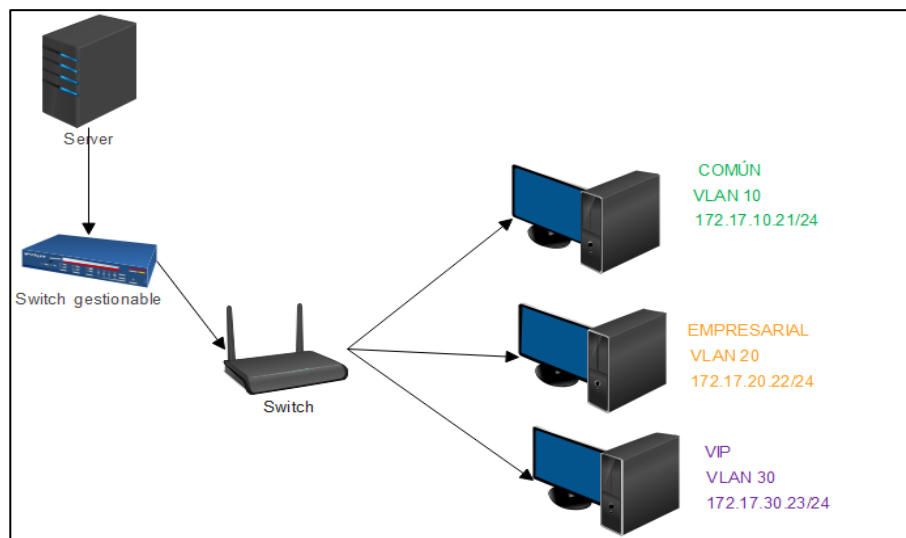
En las redes modernas, especialmente aquellas operadas por pequeños proveedores WISP o implementadas en entornos académicos, el control de accesos es una práctica indispensable para garantizar una administración eficiente y segura. Esta necesidad se acentúa cuando se debe gestionar el acceso de diferentes tipos de usuarios con niveles de prioridad distintos, como clientes residenciales, corporativos o de nivel VIP. Para responder a este reto, uno de los métodos más utilizados es la segmentación lógica a través de VLAN, combinada con listas de control de acceso (ACLs).

A través de las VLAN (Virtual Local Area Network), se puede dividir una red física en múltiples dominios virtuales. Esta estrategia permite separar el tráfico de red de manera lógica, independientemente del cableado o *hardware* compartido. [3]

En un escenario simulado o real, un proveedor puede asignar la VLAN 10 a la administración, la VLAN 20 a clientes empresariales, la VLAN 30 a clientes VIP y la VLAN 40 a clientes residenciales. Así, aunque todos los usuarios estén conectados al mismo *switch*, sus datos viajarán en canales virtualmente independientes, lo cual aporta orden, eficiencia y seguridad.

Por consiguiente, en la Figura 8 se puede observar cómo el uso de VLAN permite organizar a los usuarios de una red WISP según sus perfiles: VIP, empresarial y residencial. Esta segmentación facilita una administración más clara y ordenada, ya que cada grupo funciona dentro de su propio entorno lógico, aunque compartan el mismo *hardware* físico.

Figura 8: Beneficios de las redes VLAN asumiendo tres tipos diferentes de VLAN como abonados



Para complementar esta segmentación, se aplican listas de control de acceso (ACLs) desde dispositivos como *routers* o *firewalls* físicos. Estas listas funcionan como filtros inteligentes: definen exactamente qué tipo de tráfico está permitido o prohibido entre dispositivos o redes. De este modo, se pueden aplicar reglas como impedir que usuarios residenciales accedan a la VLAN de administración o restringir el uso de ciertos puertos o servicios por parte de usuarios no autorizados.

Esta arquitectura no solo mejora la seguridad, sino que también facilita la gestión de la red. Por ejemplo, si un usuario de la VLAN 30 intenta acceder a un recurso en la VLAN 10 sin permiso, la red simplemente lo bloquea sin necesidad de intervención del administrador. Asimismo, es

posible priorizar el tráfico de ciertos perfiles, garantizando que los clientes empresariales o VIP tengan mejor calidad de servicio en momentos de congestión. [6]

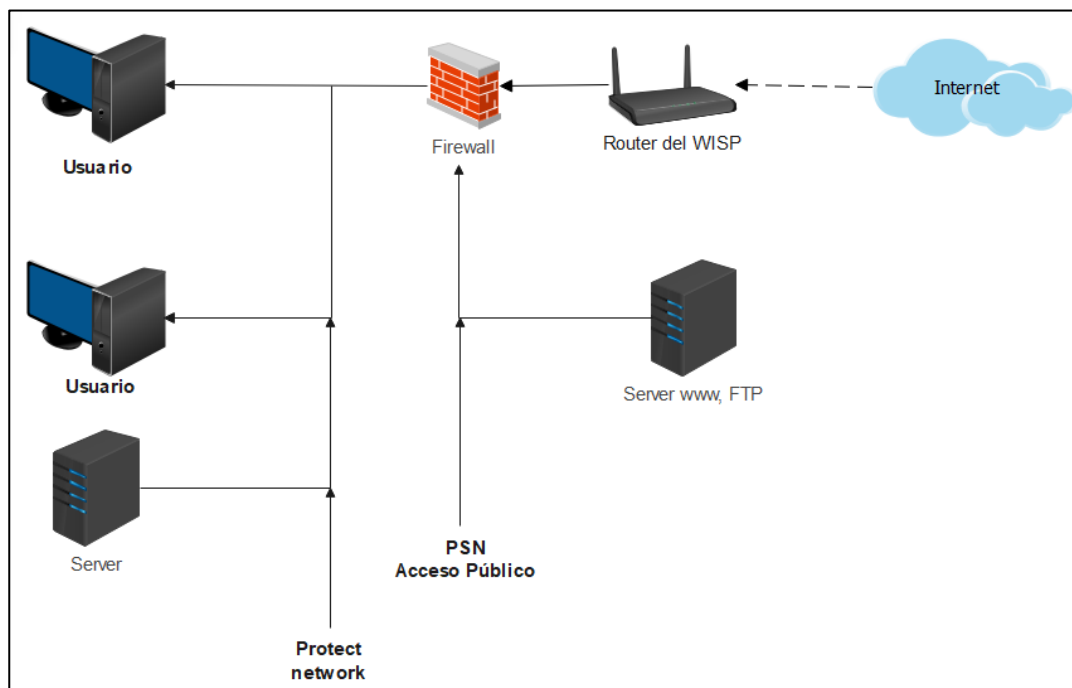
Para estudiantes de telecomunicaciones, trabajar con VLAN y ACL en entornos reales o simulados representa una oportunidad invaluable para comprender cómo se segmenta, protege y optimiza una red profesional. Estas herramientas no solo son estándar en la industria, sino que además ofrecen un enfoque práctico para aplicar los principios de diseño de redes seguras y eficientes.

2.2.3. *Firewalls* como mecanismo de control y seguridad en redes WISP

En redes de baja y mediana escala como las implementadas por pequeños proveedores de servicios inalámbricos (WISP), instituciones educativas o proyectos de laboratorio, la incorporación de un dispositivo *firewall* representa una solución efectiva para establecer un perímetro de seguridad robusto, flexible y fácil de gestionar. A través de estos dispositivos, es posible controlar qué tipo de tráfico entra o sale de la red, aplicar reglas personalizadas y proteger los recursos frente a amenazas comunes como accesos no autorizados, escaneos de puertos, ataques de denegación de servicio o propagación de malware.

En la Figura 9 se muestra cómo puede implementarse un dispositivo *firewall* en una red pequeña, como las que se encuentran en laboratorios o en proveedores WISP que recién inician operaciones. Este tipo de configuración permite controlar de manera efectiva qué tráfico puede ingresar o salir de la red, utilizando reglas simples y directas. Es una solución práctica y económica que, sin requerir equipos sofisticados, ayuda a reforzar la seguridad del entorno y a proteger los recursos disponibles.

Figura 9: Arquitectura de *firewall* perimetral en redes WISP de baja escala



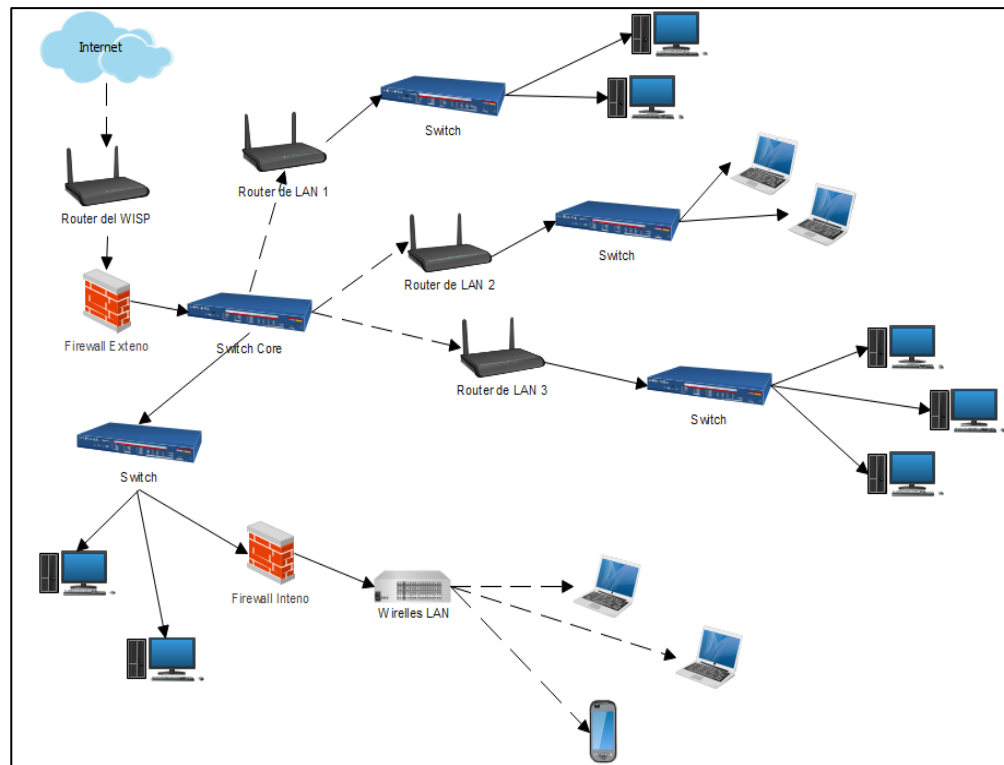
El dispositivo *firewall*, a diferencia del *firewall* embebido en *software*, opera de manera independiente del sistema operativo del servidor o de la red interna, lo que aporta mayor estabilidad y evita la sobrecarga de los dispositivos principales. [5]

Este tipo de dispositivo se instala generalmente entre la red interna y el punto de conexión a Internet o a una red de usuarios externos. Su función es actuar como un filtro de seguridad en tiempo real, inspeccionando los paquetes de datos y aplicando políticas de control basadas en la dirección IP, el puerto, el protocolo, el estado de la conexión e incluso el comportamiento del tráfico.

En la Figura 10 se ilustra un escenario más robusto, pensado para redes con una mayor cantidad de usuarios o tráfico, como las de una pequeña empresa o un WISP en crecimiento. El dispositivo *firewall* aquí no solo controla accesos, sino que también permite implementar funciones más avanzadas como VPN, reglas de calidad de servicio (QoS) y segmentación por

VLAN. La figura ayuda a visualizar cómo se puede escalar la seguridad en función del tamaño y complejidad de la red, sin perder de vista la eficiencia ni la facilidad de gestión.

Figura 10: Arquitectura de seguridad perimetral escalable en redes WISP



Existen múltiples plataformas disponibles para implementar *firewalls* físicos, cada una con sus características, beneficios y niveles de complejidad. Entre las más utilizadas en este tipo de entornos se encuentran pfSense, OPNsense, OpenWRT y soluciones comerciales basadas en Cisco, Ubiquiti o dispositivos integrados con EdgeOS. [5]

Estas plataformas permiten desde configuraciones básicas de filtrado hasta arquitecturas más avanzadas con NAT, QoS, VPN, listas de control de acceso (ACLs) y segmentación por VLAN.

Uno de los aspectos más valorados de estas soluciones es su capacidad de adaptación. Por ejemplo, un dispositivo *firewall* puede funcionar tanto en un entorno educativo como en un escenario real WISP, simplemente ajustando sus reglas de tráfico y capacidades de procesamiento.

Muchas de estas plataformas están disponibles bajo licencias de código abierto, lo que las hace ideales para la enseñanza, la práctica técnica y la replicación sin costos elevados.

Para los estudiantes o profesionales en formación, trabajar con *firewalls* físicos proporciona una experiencia directa con la gestión de la seguridad perimetral, lo que permite observar en tiempo real cómo una red reacciona frente a condiciones cambiantes de tráfico, amenazas o configuraciones erróneas.

Esta interacción fortalece no solo los conocimientos técnicos, sino también el criterio analítico y la toma de decisiones en el ámbito de las telecomunicaciones y la ciberseguridad.

2.2.4. Aplicación de políticas y priorización de tráfico en plataformas de congestión de red para filtrado

En redes inalámbricas como las operadas por pequeños proveedores WISP o en entornos de laboratorio académico, la gestión eficiente del tráfico no solo implica asegurar la conectividad, sino también establecer políticas de filtrado y priorización que mantengan el orden, la seguridad y el rendimiento del sistema.

Estas políticas permiten, por un lado, restringir el acceso a servicios o destinos no deseados y, por otro, garantizar que el tráfico más importante reciba preferencia en el uso del ancho de banda disponible. La aplicación de estas políticas puede llevarse a cabo a través de diversos sistemas operativos y plataformas de red que soporten funciones de *firewall* y calidad de servicio (QoS).

Entre las soluciones más comunes en proyectos de baja y mediana escala se encuentran pfSense, OpenWRT, RouterOS, EdgeOS e incluso soluciones embebidas en equipos de marcas como TP-Link, Ubiquiti o Cisco. Aunque cada plataforma tiene su propio enfoque, todas permiten gestionar el tráfico mediante reglas definidas por el administrador.

En la Tabla 5 se presenta una comparación de distintas plataformas utilizadas para la administración de red, específicamente en tareas de filtrado de tráfico y control de calidad de servicio (QoS). Se comparan opciones como pfSense, OpenWRT, RouterOS, entre otras, considerando su tipo de licencia, facilidad de uso y capacidades técnicas.

Tabla 5: Comparativa de plataformas de administración de red para filtrado y QoS

Plataformas de administración de red para filtrado y QoS						
Plataforma / SO	Tipo de licencia	Características destacadas	Nivel de dificultad	Soporte QoS	Soporte filtrado de tráfico	Adecuado para entorno WISP
pfSense	Código abierto	Interfaz web intuitiva, potente <i>firewall</i> , soporte multi-WAN	Medio	Avanzado (HFSC, PRIQ)	Completo (IP, puertos, protocolos)	Alta
OpenWRT	Código abierto	Muy flexible, apto para <i>routers</i> domésticos y comerciales	Medio/Alto	Avanzado (SQM, fq_codel)	Avanzado con <i>scripts</i> y módulos	Alta
EdgeOS (Ubiquiti)	Propietario	Basado en Vyatta, CLI potente, buen rendimiento	Medio	Medio (Smart Queue QoS)	Estándar (IP y puertos)	Alta
RouterOS	Licencia propietaria	Altamente personalizable, GUI + CLI, muy usado en MikroTik	Bajo/Medio	Completo (simple, trees, burst)	Completo	Muy alta
Cisco IOS (SMB)	Propietario	Estándar empresarial, comandos robustos vía CLI	Alto	Avanzado (CBWFQ, LLQ)	Muy completo	Alta
DD-WRT	Código abierto	Fácil de instalar en <i>routers</i> domésticos, GUI sencilla	Bajo	Limitado a intermedio	Básico	Media

Técnicamente, el filtrado del tráfico se hace mediante la creación de reglas que operan sobre los encabezados de red (IP, puertos, protocolos). Esto permite bloquear el acceso a puertos

específicos, impedir el tráfico de ciertos servicios (como P2P o juegos en línea) o restringir la comunicación entre segmentos de red. Estas reglas pueden aplicarse de forma general o segmentada por tipo de usuario, lo cual es útil en entornos con perfiles diferenciados (VIP, empresarial, residencial).

La priorización del tráfico, por su parte, se sustenta en los principios de calidad de servicio (QoS) que permiten clasificar los paquetes en función de su importancia. Dispositivos como pfSense y Ubiquiti EdgeOS, por ejemplo, disponen de herramientas para reconocer y marcar el tráfico sensible a la demora, como las videollamadas o el VoIP, y asignarle preferencia respecto de los flujos menos urgentes, como las actualizaciones de aplicaciones o las descargas. [7]

Esta clasificación se suele hacer mediante colas de tráfico, políticas de marcado y, en algunos casos, técnicas de *traffic shaping*. Lo que se busca es garantizar que los servicios esenciales funcionen sin contratiempos, aun cuando haya mayor demanda o cuando la red esté más congestionada.

En cuanto a la educación, el aprendizaje de la aplicación de estas políticas permite a los estudiantes comprender mejor cómo se estructura y se optimiza una red en situaciones del mundo real. Por otra parte, al trabajar con distintas plataformas, el estudiante se acostumbra a diferentes entornos de configuración, lo que le permite enriquecer su criterio técnico y tener herramientas para una gran variedad de contextos laborales.

2.3. Seguridad en redes WISP

2.3.1. Amenazas y vulnerabilidades comunes

Las redes de proveedores de servicios de Internet inalámbrico (WISP) funcionan en un entorno que, por su misma apertura, las expone a un conjunto importante de vulnerabilidades y amenazas. Los datos transmitidos por el aire son, por naturaleza, más susceptibles a ciertos riesgos que los transmitidos por redes cableadas. Estas redes son con frecuencia objeto de ataques, interferencias y explotación de vulnerabilidades. Entender estos riesgos es el primer paso para diseñar e implementar una estrategia de seguridad sólida.

2.3.2. Tipos de ataques detectables por un IDS en una red WISP

2.3.2.1. Ataques de denegación de servicio

El objetivo principal de un ataque de Denegación de Servicio (DoS) es interrumpir la disponibilidad de un recurso, como un servidor o una red, enviando un volumen de tráfico excesivo que lo sobrecargue. En un laboratorio se pueden simular estos ataques mediante herramientas específicas como hping3 o LOIC.

Es importante simular estos eventos para evaluar cómo reaccionan un sistema de detección de intrusos (IDS) y un *firewall*. La respuesta esperada del IDS es generar una alerta al detectar el volumen anómalo de paquetes, lo que podría llevar a un bloqueo temporal del tráfico del atacante para proteger el servicio. Por ejemplo, con hping3 se puede simular una saturación de peticiones a un servidor HTTP, esperando que el IDS genere una alerta por ataque “SYN *flood*” o por el volumen inusual de tráfico. Estas pruebas permiten validar la efectividad del sistema de seguridad implementado.

2.3.2.2. Ataques de suplantación de identidad

Este tipo de ataque, que se conoce como *Spoofing*, trata de hacer creer que el atacante es un usuario legítimo de la red. En entornos WISP, donde los usuarios se segmentan por perfiles (VIP, empresarial, residencial), un atacante que suplanta la identidad de un cliente privilegiado puede evadir las políticas de control y generar tráfico sospechoso sin levantar sospechas inmediatas.

Este tipo de amenaza pone a prueba la capacidad del IDS para identificar inconsistencias en los encabezados de paquetes y correlacionar el comportamiento de red con los perfiles establecidos.

2.3.2.3. Amenazas de *software* malicioso

Se identifica el malware como un tipo de ataque que supone una amenaza para las redes. Una de las funciones de un dispositivo *firewall* es proteger los recursos de la red frente a la propagación de este tipo de *software* malintencionado.

Un sistema de detección de intrusos (IDS) se programa con reglas basadas en firmas de amenazas conocidas para poder detectarlas. Así, por ejemplo, el sistema puede detectar que se descarga un archivo malicioso gracias a una firma de la base de datos de Emerging Threats Open (ET-Open). De igual forma, en la supervisión de perfiles de usuario, como el perfil residencial, se aplican reglas específicas para la detección de malware.

2.3.2.4. Detección de intrusiones y actividades no autorizadas

Las redes inalámbricas se encuentran expuestas a múltiples riesgos, entre los cuales se encuentran las intrusiones, que pueden tomar la forma de accesos no autorizados o escaneos de puertos, entre otros. Es por ello que un sistema de detección de intrusos (IDS) constituye la herramienta básica para la detección de este tipo de actividades.

Un IDS observa el tráfico de red para identificar patrones inusuales, posibles ataques, accesos no autorizados y alteraciones de los paquetes. El sistema examina los flujos de tráfico y los sucesos de seguridad con el fin de detectar cualquier actividad sospechosa que pueda ser señal de una amenaza o de una intrusión. Esto incluye la capacidad de identificar escaneos de puertos, intentos de acceso a la red de administración por parte de usuarios no autorizados o la suplantación de la identidad de un usuario con mayores privilegios.

2.3.3. Seguridad interna en redes WISP

2.3.3.1. Amenazas y vulnerabilidades internas específicas de redes WISP

Debido a su naturaleza compartida y su infraestructura de acceso inalámbrico, una red WISP es especialmente susceptible a una serie de amenazas internas que pueden comprometer su rendimiento y seguridad. Estas amenazas no siempre provienen de actores externos; muchas veces se originan desde el propio interior, de forma involuntaria o deliberada.

Entre las vulnerabilidades más comunes se encuentran las configuraciones incorrectas de equipos como *routers* y puntos de acceso, por ejemplo, cuando se mantienen las contraseñas predeterminadas o se utilizan protocolos abiertos. Otra amenaza habitual es el uso inadecuado de los privilegios administrativos. Por ejemplo, un técnico o miembro del personal con acceso elevado que no cuente con las restricciones adecuadas puede realizar cambios no autorizados o sin supervisión, lo que genera inestabilidad o brechas en la red.

Dispositivos internos comprometidos, como *laptops* o smartphones infectados, pueden ser puntos de entrada para ataques una vez conectados a la red, propagando malware o generando tráfico anómalo que afecta el desempeño del sistema. En casos donde la red no está bien segmentada, como ocurre en algunos WISP pequeños, una única estación comprometida puede tener acceso a varios servicios y nodos críticos, lo que empeora el problema.

2.3.4. Estrategias de defensa en profundidad

Frente a estas amenazas, la defensa no puede apoyarse en una sola herramienta o medida aislada. La estrategia más efectiva es la defensa en profundidad, un enfoque que consiste en implementar múltiples capas de seguridad que operen de manera complementaria para proteger todos los niveles de la red.

Tabla 6: Estrategias en niveles de la red

Niveles de la red	
Clasificación	Descripción
Segmentación interna	Mediante el uso de VLAN que separen a los clientes según su perfil (residencial, empresarial, VIP) y a los administradores de la red. Esta división lógica limita la propagación de incidentes y asegura que un problema en un segmento no afecte a toda la red.
Control de accesos	Esto implica establecer políticas claras sobre quién puede acceder a qué, desde qué dispositivo y en qué momento. Se deben implementar mecanismos de autenticación robustos, como contraseñas seguras, listas de control por MAC/IP y, en entornos más avanzados, autenticación mediante RADIUS o certificados digitales.
Funciones de firewall integradas en el router Mikrotik	Filtran el tráfico interno y externo. Aunque muchas veces se usan para detectar intrusos del exterior, estas también son clave para regular el tráfico dentro del entorno, evitando accesos cruzados indebidos o comunicaciones no autorizadas entre dispositivos internos.
Registro y monitoreo	Constituyen otro pilar de esta estrategia. A través de sistemas IDS, herramientas como Zabbix o Grafana, y análisis de <i>logs</i> , se pueden detectar comportamientos anómalos, generar alertas tempranas y reaccionar antes de que un problema se convierta en una amenaza seria.

2.4. Firewall como herramienta de seguridad

2.4.1. Definición y evolución del *firewall*

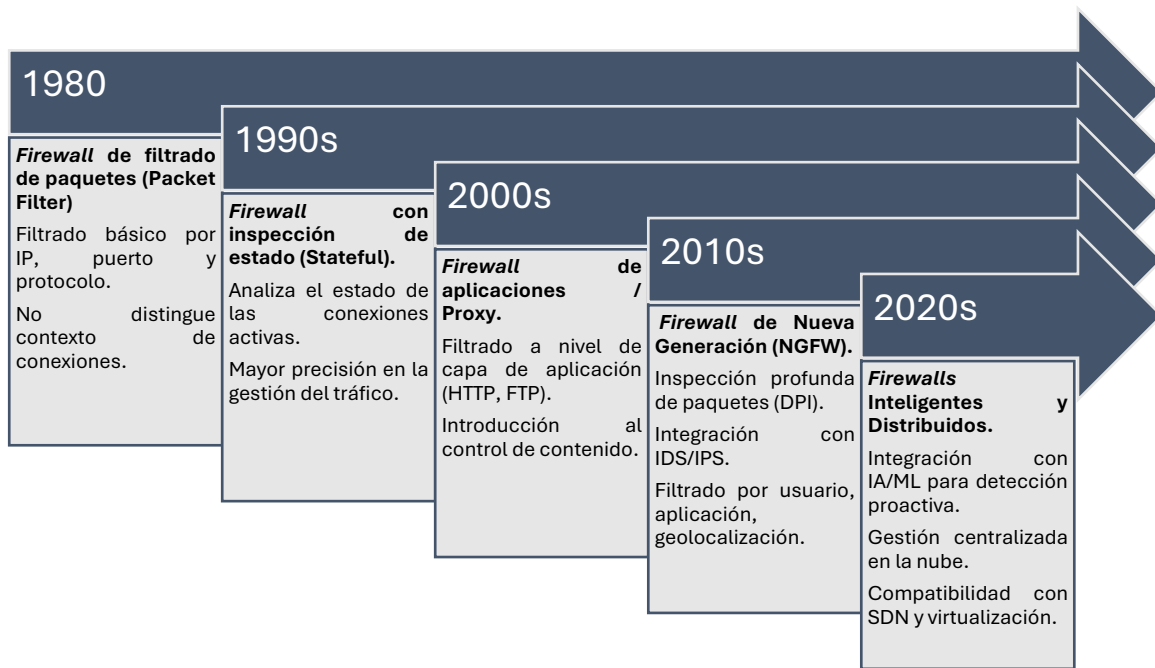
En el campo de las telecomunicaciones y la seguridad, el *firewall* se ha convertido en una de las herramientas básicas para proteger los recursos de red frente a accesos no autorizados, tráfico malicioso y ataques externos.

Su función principal es actuar como una barrera de control entre dos o más segmentos de red, generalmente entre una red interna de confianza (como la de un proveedor WISP) y una red externa no confiable, como Internet.

El *firewall* ha evolucionado significativamente desde su concepción inicial, adaptándose a los cambios en la arquitectura de red, la sofisticación de los ciberataques y la necesidad de una administración más granular.

Los *firewalls* en sus comienzos solo funcionaban como filtros de paquetes, donde cada decisión de permitir o bloquear tráfico se basaba en criterios simples como dirección IP, puerto y protocolo. Si bien fueron útiles en su momento, estos sistemas tenían limitaciones para detectar amenazas más sofisticadas que se camuflaban como tráfico legítimo.

Figura 11: Línea de tiempo de evolución del *firewall*



Con el tiempo, empezaron a aparecer los *firewalls* con inspección de estado (*stateful*), que podían reconocer el estado de las conexiones y tomar decisiones más inteligentes en función del contexto.

Esta mejora permitió que se filtraran las conexiones no solo por sus atributos estáticos, sino también por su comportamiento dentro de una sesión activa. Esta capacidad es muy útil en redes como las WISP, donde varios usuarios se conectan a la vez y de manera dinámica.

Tabla 7: Comparación entre tipos de *firewalls*

Tipos de <i>firewalls</i>			
Tipo de <i>firewall</i>	Características principales	Nivel OSI	Aplicación
Filtrado de paquetes	Revisa encabezados IP, puerto y protocolo.	Capa 3 y 4	Control básico del tráfico entrante/saliente. Ideal para enlaces WAN simples.
Inspección de estado	Monitorea el estado de las conexiones activas.	Capa 3 y 4	Útil para identificar sesiones completas. Mejora el control sobre usuarios activos.
Firewall de aplicación	Analiza tráfico a nivel de aplicación (HTTP, FTP).	Capa 7	Permite filtrar contenido web o acceso a servicios específicos.
NGFW (Next-Gen)	DPI, IPS, antivirus, control de aplicaciones, identificación de usuarios.	Capa 3 a 7	Ideal para WISP segmentados, perfiles diferenciados, integración con IDS.
Firewall basado en la nube / IA	Aprende patrones de tráfico, se adapta en tiempo real, escalable.	Multicapa	Apto para WISP en expansión con gestión centralizada y respuesta proactiva.

2.5. Sistemas de detección de intrusos, IDS

2.5.1. Fundamentos de Snort y Suricata en redes inalámbricas

En el campo de la ciberseguridad para redes, los IDS (sistemas de detección de intrusos) son fundamentales para identificar actividades maliciosas en el tráfico de red. Snort y Suricata son dos de los IDS de código abierto más utilizados, y ambos son ampliamente adoptados en entornos educativos, de investigación y productivos. Su integración con redes WISP permite monitorizar el tráfico segmentado, registrar eventos sospechosos y actuar como primera línea de defensa ante amenazas externas e internas.

Un IDS (Sistema de detección de intrusos) es un sistema que controla el tráfico de red para detectar patrones de comportamiento anómalo, posibles ataques, escaneos de puertos, intentos de acceso no autorizado o alteraciones de paquetes. [13]

Snort es un NIDS (Network Intrusion Detection System) creado por Cisco (anteriormente por Sourcefire) que trabaja mediante el análisis de paquetes de red en tiempo real. Funciona mediante un sistema de reglas definido por el usuario que permite reconocer patrones específicos de ataques o comportamientos anómalos.

Características:

- Compatible con redes de baja y mediana escala.
- Interfaz por línea de comandos, con gran control sobre las configuraciones.
- Comunidad activa y gran base de firmas de detección.
- Ideal para entornos de laboratorio con pocos recursos de *hardware*.

Suricata es una alternativa más moderna, desarrollada por la Open Information Security Foundation (OISF), que no solo actúa como IDS, sino que también puede funcionar como IPS (Intrusion Prevention System) y motor de captura de paquetes. A diferencia de Snort, está pensado para aprovechar arquitecturas multinúcleo, lo que lo hace más escalable y eficiente en redes donde circula más tráfico. [6]

Características clave:

- Soporte nativo para IPv6, TLS, HTTP/2, DNS y otros protocolos modernos.
- Captura de tráfico integrada y exportación en formatos como JSON.
- Procesamiento en paralelo para análisis más rápido.
- Ideal para redes con mayor carga de tráfico o entornos con múltiples segmentos.

En la Tabla 8 se presenta una comparación entre Snort y Suricata, considerando el tipo de análisis, rendimiento, soporte de protocolos, configuración y formato de registro de eventos.

Tabla 8: Características de Snort y Suricata

Característica	Sistema de detección de intrusos	
	Snort	Suricata
Tipo de análisis	Basado en firmas (reglas)	Basado en firmas y comportamiento
Rendimiento	Eficiente en entornos pequeños	Escalable para múltiples núcleos
Soporte de protocolos	Limitado	Ampliado y actualizado
Configuración	Más sencilla	Requiere mayor conocimiento
Registro de eventos	En texto	En JSON, EVE y más formatos

2.5.2. *Port Mirroring* y análisis pasivo en entornos segmentados

El *Port Mirroring* es la configuración de un *switch* gestionable para duplicar el tráfico de una o varias interfaces (como VLAN específicas, enlaces troncales o puertos de cliente) hacia un puerto espejo.

A este puerto se conecta el sistema IDS, que actúa como observador pasivo, es decir, analizará todo el tráfico, pero sin interactuar con él directamente.

Esta técnica es de gran utilidad en redes segmentadas, ya que permite al IDS recibir tráfico de múltiples zonas (VIP, empresarial, residencial) sin alterar la lógica de la red ni disminuir la velocidad de comunicación entre sus dispositivos.

El uso del *Port Mirroring* ofrece varias ventajas:

- Inspección simultánea de varios segmentos: El IDS puede recibir tráfico de todos los clientes sin necesidad de estar físicamente presente en cada nodo o VLAN.
- Menor carga en la red: Al operar de forma pasiva, no introduce retardos ni modificaciones en los paquetes transmitidos.
- Alta compatibilidad: La mayoría de los *switches* gestionables actuales (como TP-Link, Cisco o MikroTik) soportan esta función sin necesidad de licencias adicionales.
- Escalabilidad: Es posible modificar qué interfaces se espejan hacia el IDS a medida que cambia el diseño de la red o se segmentan nuevos perfiles de usuario.

Para que el análisis pasivo sea efectivo, es necesario asegurar que:

- El puerto espejo tenga suficiente capacidad (idealmente Gigabit Ethernet) para recibir el tráfico combinado sin pérdida de paquetes.
- El IDS tenga una interfaz dedicada para recibir el tráfico, sin compartir recursos con el tráfico de administración.
- El sistema operativo y la herramienta IDS estén configurados en modo promiscuo, de manera que puedan leer todos los paquetes sin descartarlos por pertenecer a otras direcciones MAC o VLAN.
- Se evite espejar tráfico innecesario para optimizar el rendimiento del IDS, especialmente en redes medianas o con múltiples clientes simultáneos.

2.5.3. Reglas de detección y actualización de firmas IDS

A diferencia de un *firewall*, que bloquea directamente el tráfico, un IDS trabaja con inspección profunda de paquetes (DPI) para descubrir amenazas sutiles que podrían pasar desapercibidas para los sistemas de filtrado tradicionales.

Por eso, son fundamentales la calidad, la actualización y la personalización de sus reglas.

En la Tabla 9 se describen reglas de detección aplicables a una red WISP, relacionando cada tipo de regla con su descripción, ejemplo de aplicación y herramienta IDS correspondiente.

Tabla 9: Reglas y detección en red WISP

Reglas y detección en red WISP			
Tipo de regla	Descripción	Ejemplo aplicado al WISP	Herramienta
Detección de escaneo	Reglas que identifican intentos de mapear puertos o servicios	Escaneo de puertos desde un cliente residencial a la red de administración	Snort / Suricata
Comportamiento anómalo	Detecta actividades inusuales en la red (frecuencia, tamaño, patrón)	Exceso de conexiones en corto tiempo desde un mismo cliente	Suricata
Intento de acceso no válido	Reglas que alertan sobre conexión a puertos o protocolos restringidos	Cliente empresarial intenta usar SSH hacia nodos internos no autorizados	Snort
Ataques conocidos	Reglas basadas en firmas de malware, exploits o patrones reconocidos	Descarga de un archivo malicioso detectado por firma ET-Open	Suricata + ET rules
Spoofing o falsificación	Detección de paquetes con IP o MAC falsificadas	Cliente residencial intenta suplantar a un usuario VIP	Snort
Política de uso	Reglas adaptadas a la segmentación y prioridad de perfiles	Usuario básico intenta consumir servicios de tráfico no habilitados	Reglas personalizadas

Para mantener la efectividad del sistema IDS, las firmas deben ser actualizadas periódicamente. Este proceso puede ser manual o automatizado, y generalmente se realiza a partir de fuentes como:

- Emerging Threats Open (ET-Open)
- Snort Community Rules
- Talos Intelligence (Cisco)
- Reglas locales personalizadas por el administrador

El IDS se puede configurar para que actualice estas reglas con herramientas como PulledPork, Suricata-Update o *scripts* automatizados en cron. La actualización periódica permite detectar nuevos vectores de ataque sin necesidad de volver a diseñar todo el sistema.

2.5.4. Integración del IDS con perfiles diferenciados de usuarios en WISP

Una de las principales ventajas de aplicar segmentación en redes WISP es la posibilidad de establecer políticas de seguridad y monitoreo diferenciadas según el tipo de cliente.

Esta segmentación no solo mejora el rendimiento de la red, sino que también permite al sistema IDS (Intrusion Detection System) funcionar con mayor precisión, ajustando su lógica de detección a las características propias de cada grupo de usuarios. [10]

En redes segmentadas mediante VLAN, subredes o SSID, es posible distinguir perfiles de usuario como:

- Clientes VIP, que requieren prioridad de tráfico y acceso a servicios especiales.
- Clientes empresariales, que demandan estabilidad, cifrado y control de aplicaciones.
- Clientes residenciales o estándar, cuyo uso es más variable y potencialmente desordenado.

La integración del IDS con perfiles diferenciados se basa en tres pilares:

- Visibilidad del tráfico segmentado: A través de *Port Mirroring*, el IDS puede recibir tráfico de múltiples VLAN. La interfaz de captura se configura para escuchar paquetes de todos los segmentos, permitiendo observar patrones específicos por grupo.

- **Aplicación de reglas diferenciadas:** El sistema IDS permite definir un conjunto de reglas para cada perfil de usuario, teniendo en cuenta las amenazas más comunes para su categoría. Así, por ejemplo, en el tráfico doméstico se monitorizan las descargas sospechosas, mientras que en el tráfico empresarial se prioriza la detección de conexiones persistentes o túneles no deseados.
- **Respuestas adaptativas y alertas específicas:** Las alertas generadas pueden clasificarse por tipo de cliente, permitiendo priorizar acciones. Una alerta en un segmento VIP puede escalar de inmediato, mientras que en segmentos residenciales puede dar lugar a una revisión de menor prioridad.

Tabla 10: Perfiles de usuario

Perfiles de usuario			
Perfil de usuario	Ejemplo de tráfico monitoreado	Tipo de regla aplicada	Respuesta esperada
Residencial	Descargas desde sitios de reputación baja	Detección de malware o P2P no permitido	Generación de alerta, análisis de comportamiento
Empresarial	Conexiones salientes a puertos inusuales (exfiltración)	Análisis de patrones persistentes y de túneles	Bloqueo de la IP de destino, escalamiento al administrador
VIP	Escaneo interno o intento de acceso lateral	Reglas de protección avanzadas y detección lateral	Alerta inmediata y cierre de sesión sospechosa

2.6. Herramientas de monitoreo y análisis de tráfico

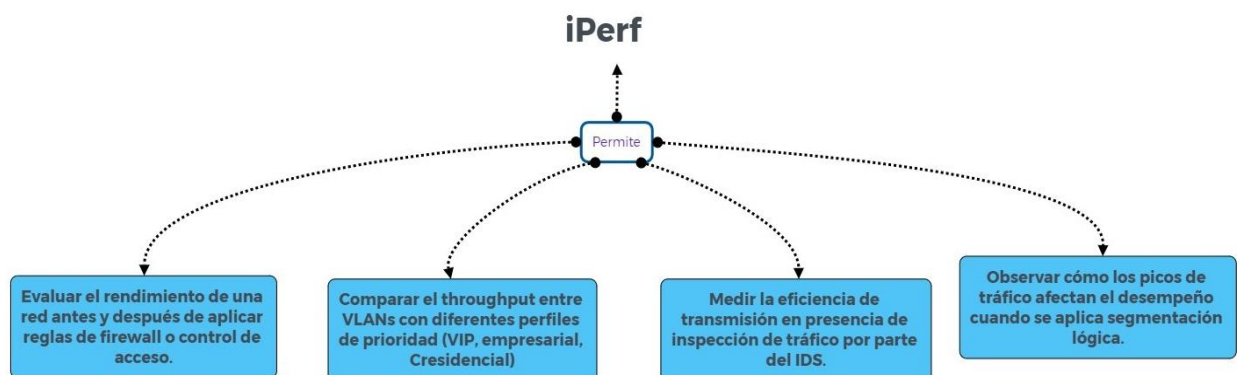
2.6.1. Herramientas de análisis de tráfico y evaluación de IDS

2.6.1.1. iPerf en entornos de laboratorio

iPerf es una herramienta de código abierto que permite medir el *throughput* entre dos puntos de red bajo distintas configuraciones y condiciones de carga. Su funcionamiento es sencillo pero eficaz: se configura un nodo como servidor y otro como cliente; se da inicio a una transmisión de datos controlada para medir el ancho de banda efectivo conseguido.

Con base en la Figura 12, se destacan las principales funciones de iPerf, herramienta ampliamente utilizada en laboratorios de redes para medir el rendimiento del tráfico entre dos puntos. Su capacidad para generar pruebas de velocidad en distintas condiciones la convierte en una opción ideal para observar el *throughput* real de la red. Esta herramienta permite a estudiantes y técnicos experimentar con parámetros tales como ancho de banda, duración de la prueba o número de flujos simultáneos, lo cual les da una perspectiva práctica del comportamiento del sistema.

Figura 12: Características de iPerf



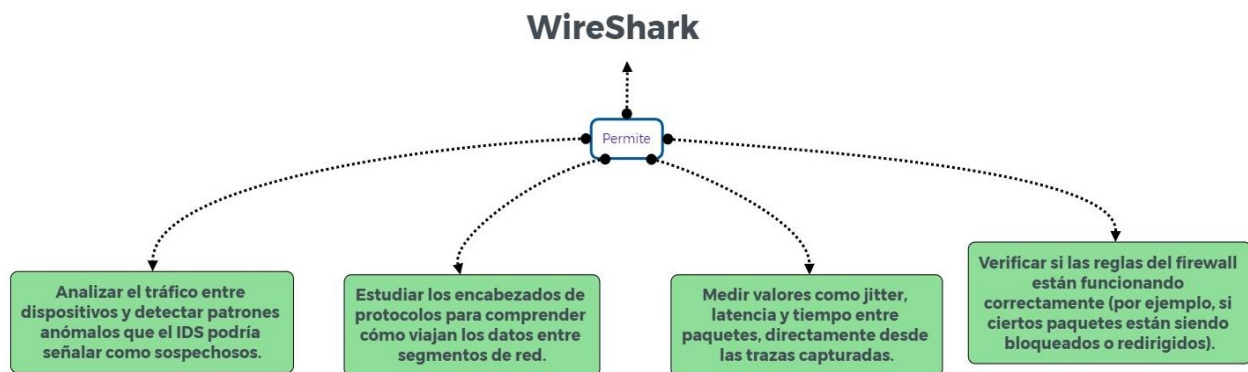
La ventaja de iPerf es que permite configurar parámetros como tamaño de los paquetes, número de flujos simultáneos, duración de la prueba, entre otros, lo que ofrece al estudiante un control total sobre las condiciones del experimento. [8]

2.6.1.2. Wireshark en entornos de laboratorio

Wireshark es un analizador de protocolos que captura y estudia el tráfico que circula por una interfaz de red en tiempo real. La interfaz gráfica permite filtrar, examinar, exportar y clasificar los paquetes capturados, lo cual es muy útil para fines educativos, de diagnóstico y de seguridad.

En la Figura 13 se presenta un analizador de protocolos que permite visualizar en detalle el tráfico que circula por una red. Esta figura muestra su capacidad para capturar, clasificar y analizar paquetes, una tarea esencial para el diagnóstico de problemas o la evaluación de la seguridad. Su interfaz amigable y sus potentes filtros hacen de ella una herramienta imprescindible para quien necesite conocer el comportamiento real de una red o comprobar configuraciones de IDS o *firewalls*.

Figura 13: Características de Wireshark



Wireshark resulta útil para comprobar que funciones como el *Port Mirroring* en *switches* donde el tráfico de una VLAN se duplica hacia el servidor IDS para su análisis pasivo funcionan correctamente. Esta capacidad permite simular entornos reales de monitoreo, sin interrumpir la operación normal de la red, lo que enriquece la experiencia de aprendizaje técnico. [8]

2.6.1.3. Validación del impacto de sistemas IDS y *firewalls* sobre el rendimiento de red

Cuando se introducen mecanismos de seguridad como un IDS y un *firewall* integrado en *hardware* en una red WISP segmentada, es esencial evaluar cómo estas herramientas afectan el

rendimiento general de la red. Ambos mecanismos son fundamentales para robustecer la protección y la gestión, pero su funcionamiento implica procesamiento adicional, análisis permanente del tráfico y, en ciertos casos, filtrado de datos en tiempo real. Por eso, su inclusión debe ir acompañada de una validación técnica que equilibre la seguridad con la eficiencia operativa.

La validación del impacto se basa en comparar el comportamiento de la red antes y después de activar el *firewall* o el IDS, empleando métricas específicas como:

- *Throughput* (tasa efectiva de transferencia): permite identificar si el flujo de datos se ve restringido significativamente al pasar por un sistema de inspección profunda (IDS) o al aplicar reglas de *firewall* complejas.
- Latencia y *jitter*: miden el tiempo de respuesta y la estabilidad del tráfico, fundamentales en servicios sensibles al tiempo como VoIP o videoconferencias.
- Pérdida de paquetes: detecta si las reglas de filtrado mal configuradas están descartando paquetes válidos, afectando la comunicación normal.
- CPU y uso de recursos en el IDS o *firewall*: un alto consumo de recursos podría ralentizar el procesamiento de paquetes o generar retrasos en la respuesta ante amenazas.

En el entorno experimental del presente proyecto, se realizó esta validación a través de pruebas controladas mediante herramientas tales como iPerf, Wireshark y registros del sistema IDS. Por ejemplo, iPerf permite comparar el *throughput* entre dos puntos de la red con y sin el IDS activo, mientras que Wireshark puede capturar retrasos o retransmisiones provocadas por reglas del *firewall*. [9]

El proceso de inspección de cada paquete que atraviesa una interfaz espejo o puerto en modo promiscuo por parte del IDS implica añadir una carga al sistema. Si está mal dimensionado o si las reglas de detección son demasiado numerosas, se puede producir congestión, falsos positivos o incluso se puede ralentizar la detección real.

Un *firewall* integrado en *hardware*, aunque realiza su tarea de enrutar o filtrar paquetes de forma muy eficiente, necesita estar configurado de forma óptima para que no se convierta en un cuello de botella. [10]

Por tanto, validar el impacto no solo implica verificar que la red “funciona”, sino demostrar que se mantiene eficiente, estable y segura bajo condiciones reales, incluso con mecanismos de defensa activos. En el mundo académico, este tipo de prácticas permite al estudiante comprender la relación entre rendimiento y seguridad, una habilidad fundamental para el diseño profesional de infraestructuras.

2.6.2. Gestión y monitoreo en redes WISP

2.6.2.1. Supervisión de redes inalámbricas con herramientas de monitoreo de código abierto

La supervisión continua es esencial en la administración moderna de redes, especialmente en entornos WISP, donde el tráfico de varios usuarios debe mantenerse fluido, seguro y bien distribuido.

Se incorporaron herramientas de monitoreo de código abierto con el fin de implementar una solución funcional, escalable y accesible que permita observar el comportamiento de la red y validar el funcionamiento del sistema IDS junto con otros mecanismos de seguridad.

En la Tabla 11 se presentan herramientas de monitoreo que permiten visualizar en tiempo real el estado de los dispositivos, detectar fallas, anticipar congestiones y generar alertas cuando se presentan comportamientos anómalos.

En entornos académicos o WISP en crecimiento, recurrir a plataformas abiertas permite además ajustar y personalizar el monitoreo de acuerdo con las necesidades del diseño implementado. [8]

Tabla 11: Herramientas de monitoreo de código abierto

Herramientas de monitoreo de código abierto	
Zabbix	Plataforma integral que permite recolectar datos de rendimiento (CPU, memoria, ancho de banda, estado de interfaces, etc.) y visualizar eventos mediante gráficos, mapas y alertas configurables. Es ideal para supervisar <i>switches</i> , <i>routers</i> , servidores y el propio IDS.
Nagios Core	Orientado a la supervisión de servicios y dispositivos. Su flexibilidad lo convierte en una excelente opción para monitorear disponibilidad de enlaces, latencia y servicios críticos dentro de la red WISP segmentada.
Grafana + Prometheus	Esta combinación permite recolectar métricas en tiempo real y presentarlas en paneles altamente personalizables. Es útil para representar visualmente el comportamiento del tráfico segmentado o el rendimiento del IDS con alertas basadas en condiciones específicas.

Estas herramientas permiten implementar monitoreo a través de protocolos como SNMP, ICMP, SSH o API REST, dependiendo del equipo y *software* a observar. Así, se puede, por ejemplo, supervisar la carga de un *firewall* integrado en *hardware*, el estado de enlaces inalámbricos entre nodos WISP, o las estadísticas de paquetes analizados por el IDS. [10]

Incluir este tipo de monitoreo en un laboratorio permite que el estudiante experimente con la observación del sistema en condiciones dinámicas, aprendiendo a reaccionar ante alertas, diagnosticar errores de red y correlacionar eventos.

Si un IDS genera muchas alertas por escaneos de puertos, el estudiante puede rastrear la fuente del ataque y verificar si el *firewall* lo bloqueó a tiempo, todo desde el sistema de monitoreo.

2.6.2.2. Gestión remota segura y monitoreo visual en tiempo real

En redes tales como las WISP, donde la infraestructura es normalmente distribuida geográficamente y el acceso físico a los equipos no siempre es posible o práctico, la gestión remota

segura se convierte en una necesidad operativa. Esta capacidad permite a los administradores de red controlar, configurar, monitorear y resolver incidentes sin necesidad de estar físicamente presentes, lo que reduce los tiempos de respuesta y aumenta la eficiencia del mantenimiento.

Entre los protocolos cifrados utilizados se encuentran:

- SSH (Secure Shell): para acceder a equipos como *routers*, *switches* y servidores de forma segura, sin exponer credenciales en texto plano.
- HTTPS: para el acceso a interfaces web de administración, evitando la interceptación de datos sensibles.
- VPNs (Virtual Private Networks): permiten establecer túneles seguros entre el administrador y la red WISP, lo cual resulta especialmente útil cuando se trabaja desde ubicaciones externas.

La implementación de estos protocolos se acompaña de mecanismos de autenticación robusta, como claves públicas/privadas, doble autenticación o restricción por dirección IP de origen.

Monitoreo visual en tiempo real

El uso de interfaces gráficas de monitoreo permite visualizar el comportamiento de la red en tiempo real, complementando la gestión remota. Estas interfaces presentan datos sobre el uso de ancho de banda, la actividad de los dispositivos, las alertas de seguridad, las tasas de paquetes inspeccionados por el IDS, entre otros datos, de manera clara y accesible. [11]

Herramientas como Grafana, Zabbix y Kibana (cuando se usan con sistemas como ELK Stack) permiten visualizar métricas en *dashboards* interactivos, facilitando la toma de decisiones

con base en evidencia visual. Es posible configurar alertas visuales o sonoras para eventos tales como la detección de ataques, caídas de enlaces o congestión del tráfico.

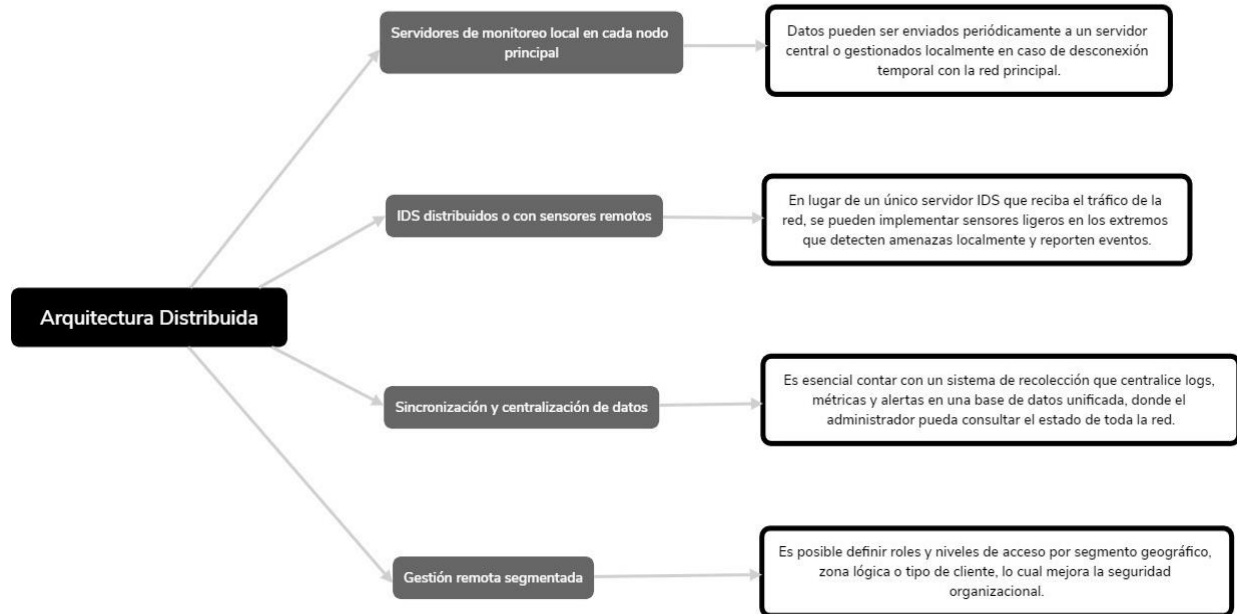
Desde el punto de vista educativo, este enfoque da al estudiante una experiencia realista sobre cómo se administra una red moderna. No solo aprende a configurar, sino también a interpretar el comportamiento de la red, a reaccionar ante fallas en tiempo real y a ajustar reglas del *firewall* o del IDS con base en la información que observa.

2.6.2.3. Arquitectura de monitoreo distribuido para entornos WISP simulados

Como las redes WISP están constituidas por numerosos nodos distribuidos geográficamente y atienden a diferentes tipos de usuarios, necesitan una arquitectura de gestión que no dependa únicamente de un punto de control. En este sentido, la arquitectura distribuida emerge como una solución eficiente, robusta y escalable que posibilita la supervisión, la gestión y el aseguramiento de la red de manera descentralizada, lo que se adapta mejor a la naturaleza dinámica de estas infraestructuras. [11]

La Figura 14 muestra una forma de organizar una red WISP bajo un enfoque distribuido, es decir, con múltiples nodos gestionados de forma descentralizada. Este esquema muestra cómo es posible supervisar y administrar una amplia red sin que todo dependa de un único punto de control. En entornos reales o simulados, esta arquitectura ofrece una mayor escalabilidad, flexibilidad y resistencia a los fallos, aspectos fundamentales para el éxito de redes en crecimiento o con alta demanda.

Figura 14: Arquitectura distribuida de red WISP



2.7. Métricas y evaluación del rendimiento de red

Para analizar el desempeño de una red WISP, sobre todo cuando se añaden mecanismos de seguridad como *firewalls* físicos e IDS, es indispensable disponer de métricas técnicas objetivas que permitan medir su eficiencia, estabilidad y capacidad de respuesta ante condiciones reales de tráfico. [1]

Estas métricas no solo proporcionan una visión cuantitativa del comportamiento de la red, sino que también guían las decisiones para mejorar la arquitectura, ajustar configuraciones y validar la efectividad de las políticas de seguridad implementadas.

2.7.1. Latencia

Representa el tiempo que tarda un paquete de datos en viajar desde el origen hasta el destino y regresar. En redes inalámbricas como las de un WISP, mantener una latencia baja es clave para asegurar una buena experiencia de usuario, especialmente en aplicaciones sensibles como videollamadas, transmisión en vivo o servicios en tiempo real.

$$L = \frac{P}{W}$$

Ecuación 1: Cálculo de la latencia de transmisión del paquete

Donde:

L: Latencia

P: Longitud en bytes del paquete

W: ancho de banda efectivo en Kilobytes por segundo

2.7.2. Jitter

El *jitter* es la variabilidad de la latencia entre paquetes sucesivos. Una red puede tener una latencia media aceptable, pero si el *jitter* es elevado, se generan cortes o interrupciones perceptibles en servicios multimedia. Esta métrica es especialmente importante al evaluar el comportamiento del tráfico en VLAN segmentadas y con control de calidad (QoS).

$$J = \sqrt{\frac{1}{N} \sum_{i=1}^N (D_i - \bar{D})^2}$$

Ecuación 2: Cálculo del *jitter* mediante la variación del retardo

Donde:

J: Jitter

$\frac{1}{N}$: Número total de paquetes medidos

D_i : el retraso del i – ésimo paquete

$\bar{D}$: el retraso promedio de todos los paquetes medidos

2.7.3. *Throughput*

Indica la velocidad efectiva con la que los datos se transfieren a través de la red. A diferencia del ancho de banda teórico, el *throughput* refleja el rendimiento real de la red, considerando pérdidas, congestión y priorización de tráfico. Medir este parámetro permite observar cómo afecta el uso de *firewalls* o reglas de IDS al flujo de datos.

$$\lambda = \frac{L}{W}$$

Ecuación 3: Cálculo del *throughput*

Donde:

λ : *Throughput*

L : *Concurrencia promedio*

W : *Promedio de duración de cada request*

2.7.4. Tasa de pérdida o error de paquetes

Una red confiable debe transmitir los paquetes de forma íntegra. Las pérdidas pueden estar relacionadas con interferencias, congestión o reglas de filtrado mal aplicadas.

Esta métrica permite verificar si las políticas de control y seguridad están afectando negativamente el servicio.

$$PER = \frac{\text{Número de paquetes con errores}}{\text{Número total de paquetes enviados}} * 100$$

Ecuación 4: Tasa de error de paquetes (PER)

2.7.5. Tasa de generación de alertas y falsos positivos del IDS

En una red segmentada, un IDS puede generar un gran número de alertas. Medir cuántas de ellas son relevantes y cuántas no es clave para validar la precisión del sistema. Este indicador permite ajustar reglas de detección y refinar el comportamiento del IDS sin comprometer el rendimiento.

Tabla 12: Tasa de generación de alertas y falsos positivos

	Hay incidente	No hay incidente
Hay alerta	Verdadero positivo (VP)	Falso positivo (FP)
No hay alerta	Falso negativo (FN)	Verdadero negativo (VN)

A partir de esta matriz de clasificación, se puede interpretar el desempeño del IDS frente a los eventos detectados en la red. Un verdadero positivo (VP) se produce cuando el sistema genera una alarma y, en efecto, hay un incidente o comportamiento anómalo. Se dice que existe un falso positivo (FP) cuando el IDS genera una alerta, pero el tráfico es el correspondiente a una actividad legítima de la red. Por otra parte, un falso negativo (FN) se produce cuando hay un incidente real, pero el sistema no lo detecta; en cambio, un verdadero negativo (VN) representa una condición normal, en la cual no hay incidente y el IDS tampoco genera alerta.

En un entorno WISP, esta clasificación es importante debido a que el tráfico de los usuarios puede variar constantemente por navegación web, consultas DNS, conexiones seguras, pruebas de conectividad o por consumo elevado de ancho de banda.

Por esto, un IDS mal ajustado puede producir muchas alertas irrelevantes, lo que afecta al análisis que hace el administrador y dificulta la identificación de amenazas reales. Pero si las reglas

son demasiado permisivas, el sistema podría pasar por alto eventos relevantes, produciendo falsos negativos.

Para evaluar la precisión del IDS se pueden emplear indicadores derivados de la matriz anterior. Entre los más relevantes se encuentran:

Precisión del IDS:

$$Precisión = \frac{VP}{(VP + FP)} \times 100$$

Ecuación 5: Precisión del IDS

Tasa de falsos positivos:

$$Tasa\ de\ falsos\ positivos = \frac{FP}{(FP + VN)} \times 100$$

Ecuación 6: Tasa de falsos positivos del IDS

Tasa de detección:

$$Tasa\ de\ detección = \frac{VP}{(VP + FN)} \times 100$$

Ecuación 7: Tasa de detección del IDS

Tasa de falsos negativos:

$$Tasa\ de\ falsos\ negativos = \frac{FN}{(FN + VP)} \times 100$$

Ecuación 8: Tasa de falsos negativos del IDS

Estos indicadores permiten determinar si el sistema IDS está generando alertas útiles o necesita ajustes en sus reglas de detección. El análisis de estos indicadores ayuda a mejorar la

configuración del IDS, reducir alertas innecesarias y aumentar la confiabilidad del monitoreo de seguridad en el contexto de una red WISP segmentada.

Tabla 13: Interpretación de los resultados de detección del IDS

Resultado	Interpretación en el IDS
Verdadero positivo (VP)	El IDS genera una alerta y realmente existe un incidente o tráfico anómalo.
Falso positivo (FP)	El IDS genera una alerta, pero el tráfico corresponde a una actividad legítima.
Falso negativo (FN)	Existe un incidente, pero el IDS no genera ninguna alerta.
Verdadero negativo (VN)	No existe incidente y el IDS no genera alerta.

2.8. Simulación de ataques y validación de sistemas IDS

2.8.1. *Port Scanning*, DoS y *Spoofing*: técnicas reproducibles en laboratorio

La formación práctica requiere el estudio no solo de herramientas defensivas, sino también de las técnicas más utilizadas por los atacantes. En este sentido, el laboratorio académico se convierte en un espacio seguro y controlado donde los estudiantes pueden simular ataques reales como *Port Scanning*, Denegación de Servicio (DoS) y *Spoofing*, con el fin de evaluar la efectividad de un sistema IDS implementado en redes segmentadas como las WISP.

En la Tabla 14 se presentan las distintas herramientas y sus respectivos comandos que pueden utilizarse para evaluar el comportamiento del IDS.

Tabla 14: Técnicas reproducibles y sus códigos

Técnicas reproducibles	
Herramientas	Código
<i>Port Scanning</i>	<code>nmap -sS -T4 -p- [IP objetivo]</code>
<i>Denial of Service (DoS)</i>	<code>hping3 --flood -S -p 80 [IP objetivo]</code>
Nmap (Network Mapper)	<code>nmap -sS -p 1-1000 -v [IP objetivo]</code>
Hping3	<code>hping3 --flood -S -p 80 [IP destino]</code>
Ettercap	<code>ettercap -T -M arp:remote /victima1/ /victima2/</code>

Técnicas reproducibles:

- ***Port Scanning* (Escaneo de puertos):** El escaneo de puertos es una técnica común usada para descubrir servicios activos en un equipo de red. Un atacante puede

identificar puertos abiertos, vulnerabilidades asociadas y sistemas mal configurados.

El IDS debe detectar esta actividad como sospechosa, generar una alerta de escaneo y registrar la IP de origen y el tipo de puerto objetivo.

- ***Denial of Service (DoS)***: El ataque de denegación de servicio busca interrumpir la disponibilidad de un recurso al enviar tráfico excesivo que sature la red o los dispositivos.

Con herramientas como hping3 o LOIC, es posible simular estos ataques.

En un entorno WISP segmentado, se puede observar cómo el IDS detecta el volumen anómalo de paquetes y cómo el *firewall* responde bloqueando o limitando el tráfico del atacante.

- ***Spoofing (suplantación de identidad)***: El *Spoofing* consiste en falsificar la dirección IP o MAC de un dispositivo para obtener acceso no autorizado o interceptar tráfico.

En entornos segmentados por VLAN, esta técnica permite verificar el correcto funcionamiento de las políticas de control de acceso.

Con herramientas como Ettercap o Macchanger es posible realizar estos ataques en laboratorio. El IDS debe registrar paquetes con encabezados anómalos o inconsistentes y correlacionar comportamientos sospechosos con intentos de suplantación.

En la Tabla 15 se ofrece un resumen de las técnicas de ataque simuladas (tales como escaneo de puertos, DoS y *Spoofing*), incluyendo sus propósitos, las herramientas empleadas y la respuesta anticipada del sistema IDS. Este recurso es muy útil en entornos educativos, ya que

permite a los estudiantes relacionar cada técnica con una respuesta concreta del sistema de seguridad, lo que ayuda a visualizar cómo se comporta una red ante distintas amenazas y cómo debe reaccionar una solución de defensa bien configurada.

Tabla 15: Comparación de técnicas reproducibles

Técnicas reproducibles			
Técnica simulada	Objetivo del atacante	Herramienta usada	Respuesta esperada del IDS
Port Scanning	Identificar servicios activos en la red	Nmap	Alerta por escaneo de puertos, con detalle en IP de origen
DoS	Saturar un servicio para provocar una caída	hping3, LOIC	Alerta por tráfico excesivo, posible bloqueo temporal
Spoofing	Suplantar un usuario o dispositivo autorizado	Ettercap, macchanger	Alerta por paquete anómalo o duplicidad de identidad

2.8.2. Herramientas de ofensiva ética: Nmap, hping3 y Ettercap

Un estudio práctico de la seguridad no estaría completo sin la comprensión y el uso controlado de herramientas de ofensiva ética, es decir, aquellas que se usan para simular ataques con fines educativos, de auditoría o de validación de sistemas defensivos como un IDS. En este proyecto, que incorpora un entorno WISP segmentado por perfiles de usuario, se realizaron pruebas activas con tres herramientas ampliamente utilizadas: Nmap, hping3 y Ettercap.

Herramientas empleadas

- **Nmap (Network Mapper):** Es una herramienta para escanear redes y puertos que permite descubrir dispositivos, servicios y configuraciones activas en una red. En redes WISP segmentadas, Nmap puede utilizarse para comprobar qué VLAN responden a qué tipos de escaneo.

Funciones principales:

- ✓ Escaneo de puertos TCP y UDP
- ✓ Detección de sistema operativo
- ✓ Reconocimiento de servicios
- ✓ Detección de hosts activos

El IDS debe alertar ante escaneos intensivos desde clientes no autorizados.

- **hping3:** Es una herramienta de generación de paquetes que permite enviar tráfico personalizado (ICMP, TCP, UDP) a un objetivo, simulando condiciones de ataque como *floods* o escaneos avanzados.

Funciones clave:

- ✓ Simulación de DoS (*floods*)
- ✓ Envío de paquetes fragmentados
- ✓ Prueba de *firewalls* y reglas de red

Esta técnica permite simular una saturación de peticiones a un servidor HTTP. El IDS debe generar alertas por volumen inusual o ataque SYN *flood*.

- **Ettercap:** Es una herramienta orientada a ataques de red locales como *Spoofing*, *Sniffing* y manipulación de tráfico. En un entorno con VLAN, se puede comprobar si un atacante puede suplantar identidades o interceptar comunicaciones entre usuarios.

Funciones:

- ✓ ARP *Spoofing*
- ✓ *Sniffing* de contraseñas
- ✓ Suplantación de dispositivos (MITM)
- ✓ Inyección de paquetes en sesiones activas

El IDS debe detectar paquetes ARP anómalos y tráfico redirigido de forma ilegítima.

En la Tabla 16 se presentan las características comparativas de herramientas de ofensiva ética utilizadas en entornos de laboratorio, considerando el tipo de ataque simulado, su uso dentro de las pruebas y la respuesta esperada del IDS.

Tabla 16: Características comparativas de herramientas de ofensiva ética

Herramientas de ofensiva ética			
Herramienta	Tipo de ataque simulado	Usos en laboratorio	Respuesta esperada del IDS
Nmap	Reconocimiento y escaneo	Identificación de puertos y servicios expuestos	Alerta por escaneo de puertos
hping3	DoS / manipulación de paquetes	Simulación de tráfico excesivo o malformado	Alerta por tráfico anómalo o volumen elevado
Ettercap	<i>Spoofing</i> / MITM	Suplantación de identidad y redirección de tráfico	Alerta por ARP falsificado o comportamiento MITM

2.8.3. Modelos de ataque y análisis de respuesta del IDS

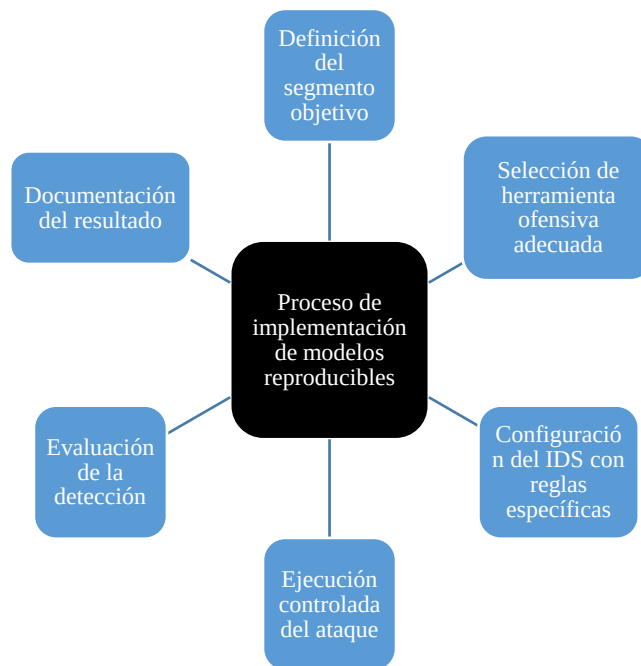
En la preparación de profesionales en telecomunicaciones y seguridad de redes, no es suficiente comprender los fundamentos teóricos de la ciberseguridad; también es indispensable experimentar en situaciones prácticas y medibles.

El diseño de modelos de ataque reproducibles permite la implementación de situaciones controladas donde alumnos y administradores pueden observar cómo diferentes amenazas se manifiestan en redes reales (como las WISP) y cómo un sistema IDS responde ante ellas. [12]

Un modelo de ataque reproducible es una secuencia planificada de acciones ofensivas ejecutadas con herramientas específicas en un entorno de laboratorio y bajo condiciones previamente definidas:

- ✓ Ser ejecutado múltiples veces, manteniendo sus parámetros.
- ✓ Generar los mismos efectos esperados.
- ✓ Ser medido y analizado en cuanto a impacto, detección y respuesta.

Figura 15: Proceso de implementación de modelos reproducibles



CAPÍTULO 3: PROPUESTA TECNOLÓGICA Y METODOLOGÍA DE IMPLEMENTACIÓN

3.1. Fase 1: Diagnóstico y planificación técnica

3.1.1. Análisis de requerimientos de red

El diseño de la infraestructura para el laboratorio WISP con sistema IDS requiere una planificación minuciosa de las capacidades de cada nodo de red. Para garantizar que los resultados de las métricas de desempeño sean válidos, se han identificado los siguientes requerimientos técnicos fundamentales:

3.1.1.1. Requerimientos de segmentación lógica y gestión

Para simular un entorno WISP real con perfiles diferenciados, la red debe soportar el estándar IEEE 802.1Q.

- **Aislamiento de tráfico:** Es crítico permitir la creación de VLAN independientes (ID 10, 20, 30 y 40) para los segmentos de administración, empresarial, VIP y residencial.
- **Identificación en el IDS:** Esta segmentación permite que el sistema IDS Suricata aplique reglas de detección diferenciadas por segmento, facilitando la identificación inmediata del origen de un ataque dentro de la subred específica.

3.1.1.2. Requerimientos de monitoreo y captura pasiva

El pilar de esta tesis es el análisis de tráfico sin afectar el rendimiento del usuario final.

- **Función de *Port Mirroring*:** Es un requisito indispensable que el *switch* de agregación (TL-SG3428) cuente con la función de espejo de puertos o SPAN.

- **Análisis pasivo:** Con esta técnica se consigue que el tráfico de las VLAN se duplique hacia una interfaz dedicada para el servidor IDS, sin introducir latencia adicional a la navegación real de los abonados y preservando la integridad de los datos originales.

3.1.1.3. Requerimientos de infraestructura inalámbrica

La distribución de señal debe ser estable para que las métricas de seguridad no se vean alteradas por interferencias externas.

- **Tecnología PtMP:** El sistema requiere una arquitectura punto a multipunto donde una antena sectorial (Ubiquiti LAP-120) actúe como transmisor central y tres antenas CPE (Loco5AC) funcionen como estaciones de destino.
- **Estabilidad del espectro:** Se determina el uso de la banda de 5 GHz y de la tecnología airMAX AC para asegurar enlaces robustos frente al ruido electromagnético, lo cual es vital durante las pruebas de ataques de denegación de servicio (DoS).

3.1.1.4. Requerimientos de rendimiento y conectividad física

Para evitar cuellos de botella durante la inspección profunda de paquetes (DPI) realizada por el IDS, la capacidad de conmutación debe ser superior a la tasa de tráfico simulada. [4]

- **Interfaces Gigabit:** Todos los puertos físicos del *router*, *switch* y antenas deben ser 10/100/1000 Mbps. Esto garantiza que el *throughput* medido en la fase de evaluación no se vea limitado por el *hardware* de red.
- **Protección ESD:** Debido a la naturaleza de los equipos inalámbricos, se requiere el uso de cableado FTP Cat6 y protectores pararrayos (Mimosa NID) para drenar descargas electrostáticas y proteger la vida útil de las interfaces Gigabit.

Tabla 17: Matriz de requerimientos frente a objetivos técnicos

Requerimiento técnico	Parámetro de diseño	Objetivo de seguridad en la tesis
Aislamiento de usuarios	VLAN 802.1Q (IDs 10, 20, 30, 40)	Aplicar políticas diferenciadas para los perfiles VIP, empresarial y residencial.
Captura de tráfico	<i>Port Mirroring</i> / <i>SPAN</i>	Permitir el análisis pasivo mediante Suricata sin afectar el tráfico real.
Integridad de datos	Interfaces Gigabit Ethernet	Evitar cuellos de botella durante la inspección profunda de paquetes (DPI).
Control de acceso	Funciones de <i>firewall</i> implementadas en el <i>router</i> MikroTik	Aplicar reglas de filtrado y mitigación de eventos asociados a patrones compatibles con actividades de interés.

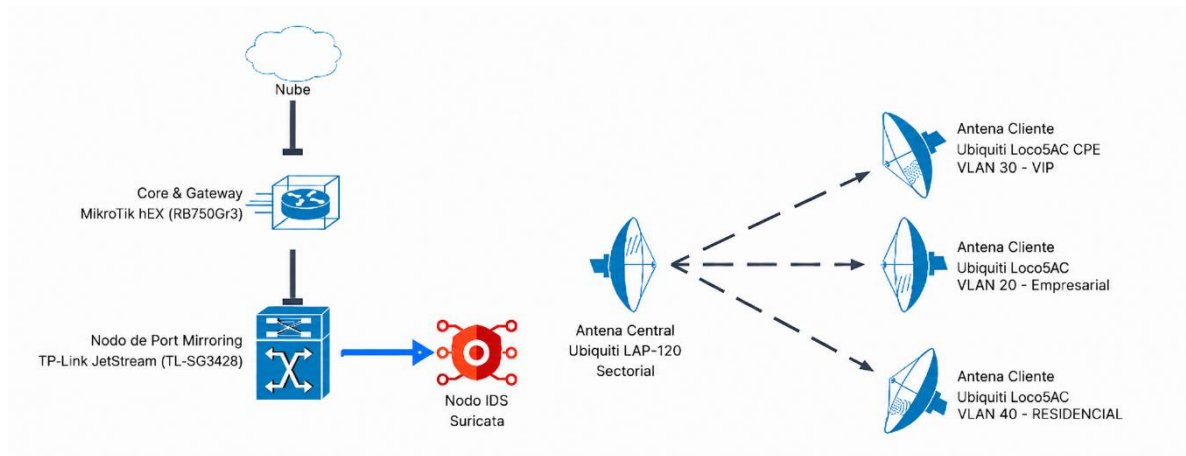
La Tabla 17 establece la relación directa entre los requerimientos técnicos del sistema y los objetivos de seguridad propuestos. Cada elemento ha sido seleccionado teniendo en cuenta principios fundamentales de diseño de redes seguras y eficientes.

El uso de VLAN bajo el estándar IEEE 802.1Q permite el aislamiento lógico del tráfico, lo cual es esencial para evitar accesos no autorizados entre segmentos de red. Esta segmentación no solo mejora la organización del tráfico, sino que también permite aplicar políticas diferenciadas de seguridad y calidad de servicio (QoS) según el tipo de usuario, alineándose con modelos de redes WISP reales.

3.1.2. Especificaciones técnicas y justificación del *hardware* seleccionado

La implementación del sistema de detección de intrusos en un entorno WISP demanda *hardware* con altas capacidades de procesamiento y conmutación. [14]

Figura 16: Arquitectura física de la red WISP con sistema IDS integrado para monitoreo del tráfico



Con base en la Figura 16, se presenta la arquitectura física general de la red WISP, incluyendo el núcleo de red, el *switch* de agregación y la distribución inalámbrica mediante antenas sectoriales hacia los clientes.

Se incluye un sistema IDS que permite monitorear el tráfico de red mediante técnicas de análisis pasivo, lo que ayuda a la detección de posibles amenazas y mejora la seguridad del sistema.

Con base en el análisis de requerimientos previo, se justifica la selección de los siguientes equipos detallados en la planificación técnica:

3.1.2.1. Nodo de enrutamiento y gestión: Mikrotik hEX (RB750Gr3)

Este dispositivo actúa como el núcleo de red (*core*), encargándose del enrutamiento inter-VLAN y la aplicación de políticas de *firewall* integradas en RouterOS.

- **Especificaciones críticas:** Cuenta con una CPU de doble núcleo a 880 MHz y 256 MB de memoria RAM.
- **Justificación técnica:** Esa potencia es necesaria para mantener el rendimiento cuando el motor de reglas de Mikrotik tenga que filtrar paquetes sospechosos

detectados por el IDS. Sus 5 puertos Gigabit aseguran que el tráfico de los tres perfiles de usuario (VIP, empresarial y residencial) llegue al *switch* sin cuellos de botella.

3.1.2.2.Nodo de conmutación y captura: TP-Link (TL-SG3428)

Es uno de los componentes más críticos para la seguridad del proyecto, ya que gestiona el flujo de datos hacia el sensor IDS.

- **Especificaciones críticas:** *Switch* administrable JetStream L2+ de 24 puertos Gigabit RJ45 con 4 ranuras SFP, compatible con segmentación VLAN, funciones de monitoreo y administración centralizada.
- **Justificación técnica:** Se elige este modelo por su capacidad para soportar segmentación lógica a través de VLAN y por disponer de funciones de replicación de tráfico, como *Port Mirroring*, necesarias para integrar el sistema IDS en modo pasivo. El servidor Suricata puede recibir una copia del tráfico sin intervenir en la ruta de transmisión principal, preservando la estabilidad de la red y evitando la introducción de latencia adicional en la operación normal del sistema.

3.1.2.3.Infraestructura de distribución inalámbrica: Ubiquiti airMAX AC

Para simular el entorno WISP, se implementa una arquitectura punto a multipunto (PtMP) en la banda de 5 GHz, utilizando una estación base inalámbrica y nodos cliente CPE compatibles con la tecnología airMAX AC.

- **Estación base (Ubiquiti LAP-120):** *Access point* airMAX AC de 5 GHz, con ganancia de 16 dBi, interfaz Gigabit Ethernet y alimentación mediante adaptador *Passive PoE* 24 V / 0,5 A incluido.

- **Nodos de abonado (Loco5AC):** Equipos CPE de la misma familia tecnológica, empleados para representar a los clientes de la red y validar el comportamiento del IDS ante tráfico inalámbrico segmentado.

3.1.2.4. Accesorios de protección y conectividad

La integridad física del laboratorio y la fidelidad de los datos dependen de la calidad del medio de transmisión.

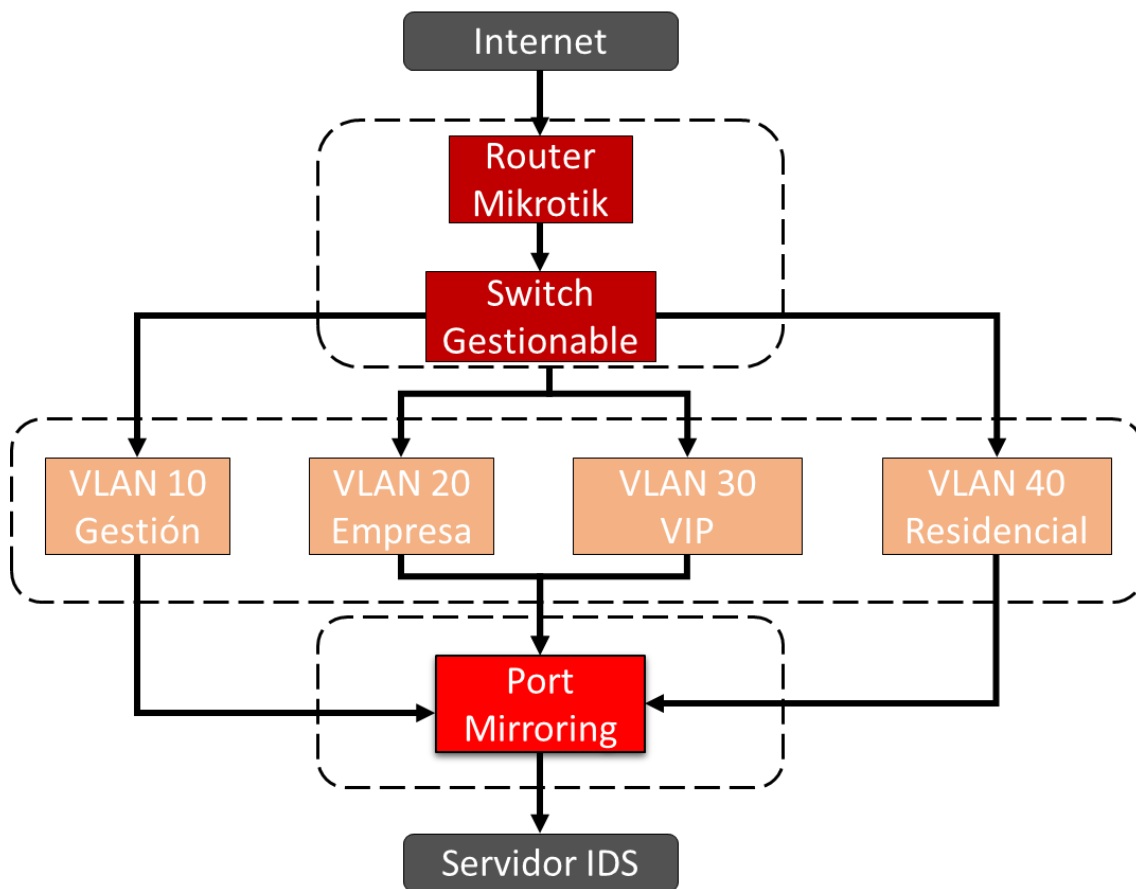
- **Protección contra descargas (Mimosa NID):** Se instalan protectores de sobretensiones ESD/EMD en cada enlace para proteger las interfaces Gigabit de los equipos ante voltajes transitorios.
- **Medio físico:** Se utiliza cable FTP Cat6 de cobre al 100 % blindado y con hilo de descarga a tierra. Esto es fundamental para reducir la interferencia electromagnética (EMI) que podría generar falsos positivos o errores en la tasa de transferencia (*Throughput*) medida durante las pruebas de seguridad.

3.2. Fase 2: Diseño lógico y físico del sistema

3.2.1. Plan de direccionamiento IP y segmentación VLAN

El diseño lógico del sistema se basa en la segregación de tráfico mediante el estándar IEEE 802.1Q. Esta técnica permite la división de la infraestructura física en múltiples dominios de difusión (VLAN), lo cual es un requisito indispensable para la administración de perfiles diferenciados en una red WISP y la correcta operación del sistema IDS. [10]

Figura 17: Arquitectura lógica de la red WISP con segmentación VLAN e implementación del IDS mediante *Port Mirroring*



La Figura 17 muestra la arquitectura lógica de la red WISP propuesta, basada en la segmentación VLAN para separar los perfiles de usuario y aislar la red de gestión. También se

muestra la integración del sistema IDS mediante *Port Mirroring*, permitiendo el monitoreo pasivo del tráfico y la identificación del segmento lógico de origen de los eventos de seguridad.

3.2.1.1. Definición de segmentos y roles de red

Para el entorno controlado, se definió un esquema de direccionamiento basado en el rango privado RFC 1918, lo que permite un aislamiento total entre la red de gestión y los abonados. A continuación, se muestra el plan de segmentación que se configuró en el *router* MikroTik (RB750Gr3), que actúa como núcleo de red, y en el *switch* TP-Link (TL-SG3428). [7]

Tabla 18: Matriz de segmentación lógica y direccionamiento

Perfil de Servicio	VLAN ID	Subred (CIDR)	Gateway	Rango DHCP	Prioridad (QoS)
Administración	10	192.168.99.0/24	192.168.99.1	.10 — .50	Crítica
Empresarial	20	172.17.10.0/24	172.17.10.1	.10 — .254	Alta
VIP	30	172.17.20.0/24	172.17.20.1	.10 — .254	Media-Alta
Residencial	40	172.17.30.0/24	172.17.30.1	.10 — .254	Normal

La Tabla 18 presenta el esquema de segmentación lógica y direccionamiento IP diseñado para el entorno WISP propuesto, el cual se basa en principios de aislamiento, escalabilidad y control de tráfico.

El empleo de direcciones privadas según el estándar RFC 1918 permite una estructuración de la red de forma segura y organizada, evitando conflictos con las direcciones públicas y facilitando la gestión interna del direccionamiento.

Se asignan VLAN diferenciadas para cada perfil de usuario (VIP, empresarial y residencial), con el fin de segmentar el tráfico de acuerdo con los niveles de prioridad y comportamiento esperado. Esta separación reduce la superficie de ataque, limita la propagación de las amenazas y permite una mejor administración del ancho de banda.

3.2.1.2. Justificación técnica de la segmentación

La estructuración de estas VLAN responde a tres objetivos estratégicos de seguridad y gestión definidos para el proyecto:

a) Aislamiento de la infraestructura crítica

La VLAN 10 (Administración) está aislada de los segmentos de abonados. Esto evita que un cliente malicioso en el segmento residencial pueda realizar ataques de reconocimiento o escaneo de puertos de las interfaces de gestión del *router*.

b) Optimización del análisis del IDS Suricata

Al dividir el tráfico, el sistema IDS puede implementar firmas de detección personalizadas en función del perfil de usuario. Por ejemplo, es posible establecer reglas de detección más estrictas de P2P en el segmento residencial (VLAN 40) sin limitar la libertad de puertos del segmento empresarial (VLAN 20).

c) Control de Calidad de Servicio (QoS)

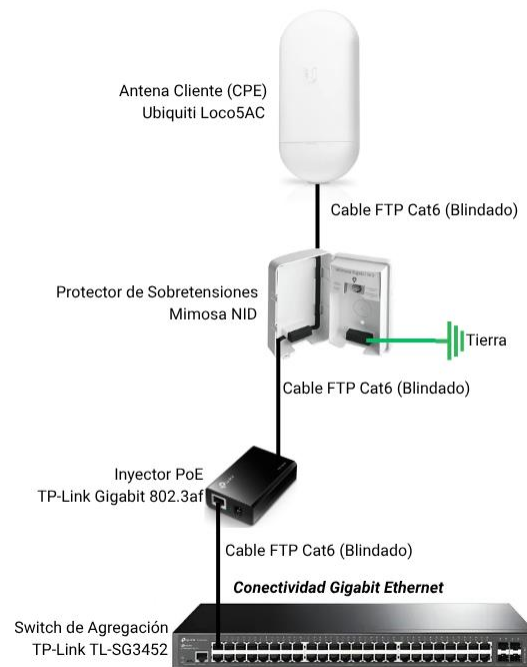
La identificación de paquetes por VLAN ID facilita la implementación de colas de tráfico (Simple Queues) en el entorno MikroTik. Esto asegura que, ante ataques de denegación de servicio (DoS) simulados, el sistema pueda priorizar el tráfico de la VLAN 30 (VIP) mientras el IDS procesa las alertas de seguridad.

3.2.1.3. Representación física de la infraestructura

Con el fin de complementar el diseño lógico presentado anteriormente, se muestra la representación física de la infraestructura de red WISP implementada. Esta incluye los dispositivos

de acceso, enlaces cableados, protección eléctrica y equipos de agregación que permiten la conectividad entre los clientes y el núcleo de red. [1]

Figura 18: Arquitectura física de conexión desde el cliente (CPE) hacia el *switch* de agregación en la red WISP



La Figura 18 representa la estructura física de conexión de un cliente dentro de la red WISP, incluyendo el equipo CPE, el sistema de protección contra sobretensiones, el inyector PoE y el *switch* de agregación.

Esta configuración permite verificar la correcta transmisión de datos, así como la protección de los equipos frente a descargas eléctricas, asegurando la estabilidad y continuidad del servicio.

3.2.1.4. Implementación física de la infraestructura de red

Una red WISP consta de infraestructura física, estructura lógica y procedimientos de operación. En el entorno implementado, los dispositivos se interconectan mediante cableado

estructurado que enlaza el enrutador con el conmutador de agregación y, desde este, con el sistema de protección eléctrica y el sistema IDS.

Figura 19: Conexión física de la infraestructura de red WISP



Adicionalmente, los equipos de protección como inyector PoE y supresores de sobretensión aseguran que los dispositivos permanezcan protegidos frente a las fluctuaciones eléctricas.

3.2.2. Alcance técnico de la propuesta

El desarrollo técnico presentado se enfoca en el diseño e integración de un sistema de detección de intrusos (IDS) dentro de una red WISP segmentada, implementada en un entorno de laboratorio controlado. Su alcance incluye la definición de requerimientos de implementación del

IDS, la segmentación lógica del tráfico por VLAN, el diseño del esquema de direccionamiento IP, la identificación de los puntos de captura y la integración del sensor mediante mecanismos de análisis pasivo como el *Port Mirroring*. Contempla también la elección del *hardware* y *software* necesarios para garantizar un funcionamiento estable del sistema, sin que se degrade significativamente el desempeño general de la red.

Quedan fuera del alcance de este proyecto las implementaciones directas de funciones asociadas a otros componentes del proyecto integrador, como el balanceo de carga, la optimización del rendimiento de los enlaces inalámbricos o el diseño del radioenlace de las antenas. Estos elementos son tomados como base de integración sobre los cuales se incorpora la capa de monitoreo y seguridad propuesta en esta tesis.

Por lo tanto, la contribución principal del trabajo es definir una arquitectura técnica que haga posible detectar eventos relevantes de seguridad dentro de la red WISP, mejorando la visibilidad del tráfico, la segmentación segura y la capacidad de análisis del entorno, sin interferir directamente en la operación de los demás subsistemas.

3.2.3. Enfoque de seguridad adoptado

La propuesta plantea un enfoque de seguridad de tipo defensivo, dirigido al monitoreo, al análisis y a la detección de eventos sospechosos dentro de la red WISP. Desde este punto de vista, el sistema de seguridad se basa en un IDS operando en modo pasivo, diseñado para monitorear el tráfico de red, detectar patrones inusuales y emitir alertas ante posibles amenazas, sin participar directamente en el manejo de los paquetes. Para ello, el IDS se integra mediante la técnica de *Port Mirroring*, por la cual el *switch* gestionable hace una copia del tráfico hacia el sensor de análisis, lo que permite inspeccionar en tiempo real sin introducir latencia adicional ni alterar la operación normal de la red.

No se trata de un enfoque basado en la detección activa o en el filtrado “en línea”, sino que el modelo que se adopta se centra en la visibilidad del tráfico y en la capacidad de respuesta analítica. En este sentido, el sistema no bloquea directamente el tráfico detectado como sospechoso, sino que registra eventos, clasifica alertas y genera evidencia técnica que facilita la interpretación del comportamiento de la red y el análisis posterior de incidentes.

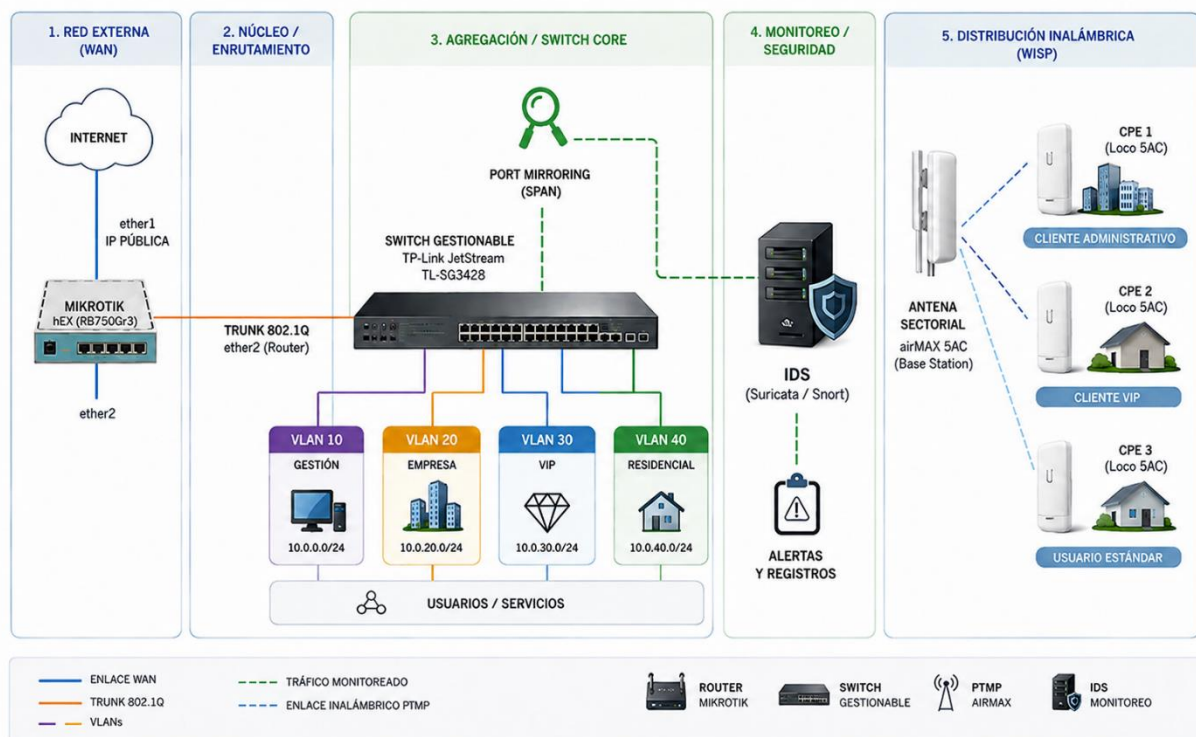
Esta visión se completa con la segmentación lógica mediante VLAN, lo que permite observar de forma diferenciada el tráfico asociado a cada perfil de usuario y mejorar la precisión de la detección según el contexto del segmento monitoreado. Con esta orientación, la validación del sistema se basa en eventos controlados y no disruptivos, como escaneos de puertos o tráfico de prueba con firmas identificables, y se centra en evaluar la capacidad de detección, monitoreo y generación de alertas del IDS.

3.3. Fase 3: Implementación del entorno de red y arquitectura general propuesta

3.3.1. Arquitectura general de la red WISP propuesta

La arquitectura general propuesta se basa en una red WISP segmentada desarrollada en laboratorio. Esta arquitectura integra un sistema de detección de intrusos (IDS) orientado al monitoreo y al análisis del tráfico. En la Figura 20 se muestra la organización funcional del sistema, con la interconexión entre la red externa, el *router* MikroTik, el *switch* gestionable, la distribución inalámbrica mediante una topología punto a multipunto (PtMP) y la integración del IDS por medio de *Port Mirroring*. Esta representación constituye la base para el desarrollo subsiguiente del diseño lógico, de la ubicación del IDS y del flujo del tráfico dentro de la propuesta.

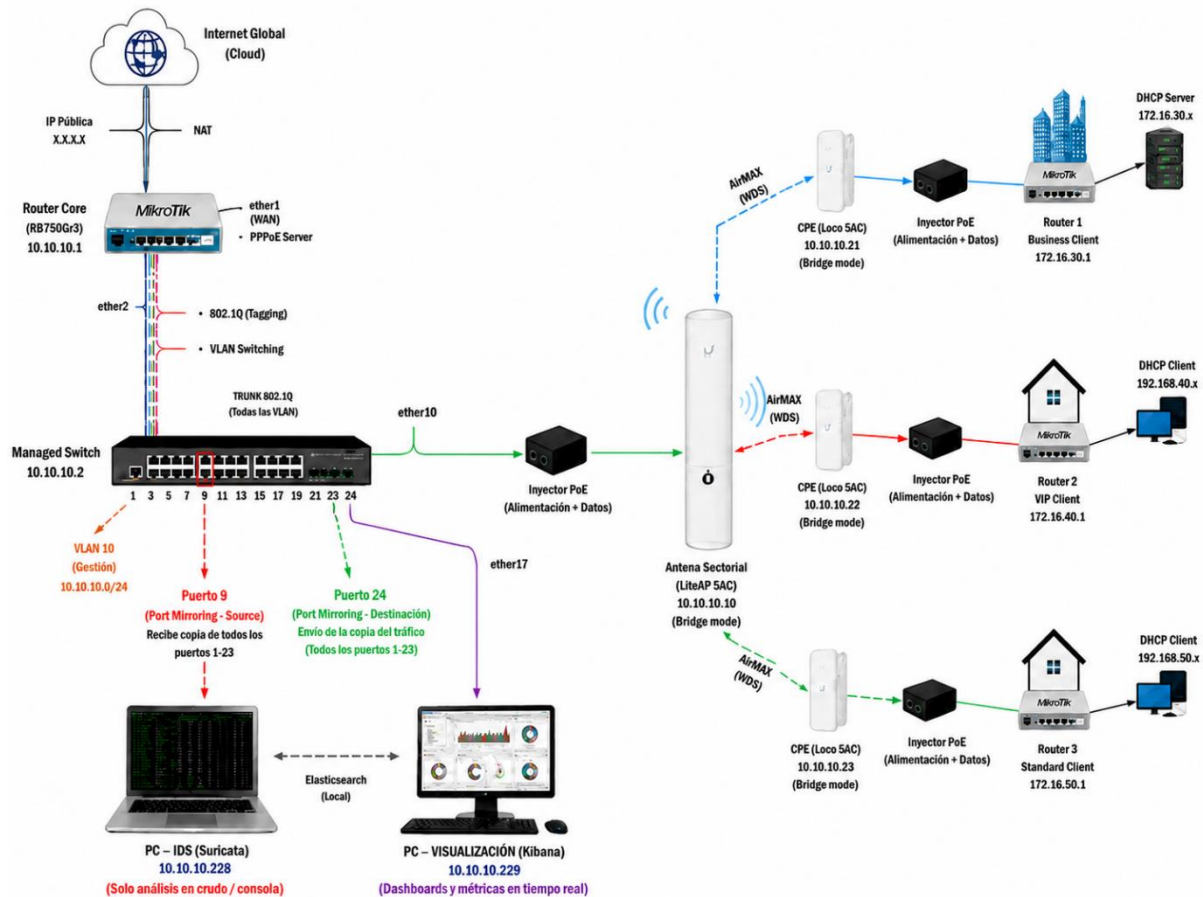
Figura 20: Arquitectura general de la red WISP propuesta con integración del sistema IDS



La Figura 20 presenta la arquitectura general del sistema propuesto, mostrando la interconexión entre la red externa, el *router* MikroTik, el *switch* gestionable, la distribución

inalámbrica mediante una topología punto a multipunto (PtMP) y la integración del sistema IDS a través de la técnica de *Port Mirroring*.

Figura 21: Arquitectura detallada con integración del sistema IDS

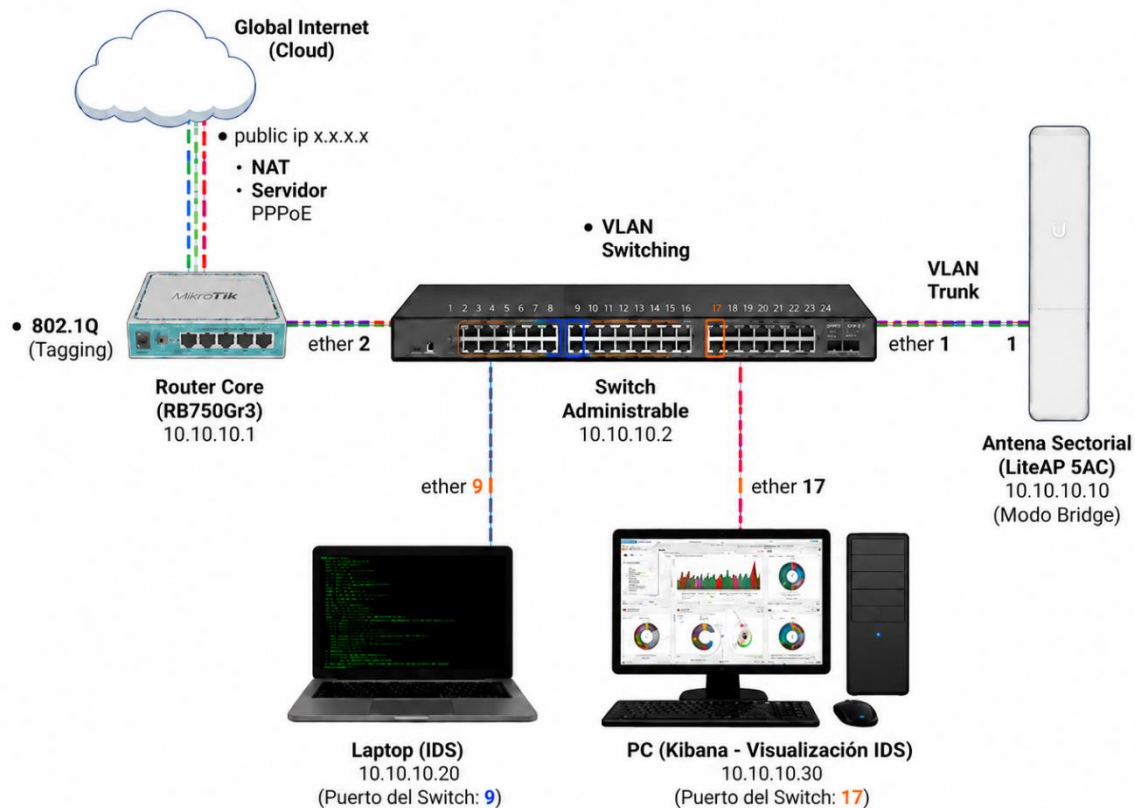


En esta ampliación de la arquitectura se incluye de manera explícita la integración del sistema IDS con el *switch* gestionable, estableciendo el puerto 9 como interfaz de captura mediante *Port Mirroring*, donde se recibe una copia del tráfico de red para ser analizado pasivamente mediante Suricata.

De igual forma, el puerto 17 se define como interfaz para el sistema de visualización Kibana, el cual permite la representación gráfica de los eventos, métricas y alertas generadas por

el IDS. Esta separación permite que el análisis del tráfico en bruto y la visualización de los datos procesados sean independientes entre sí.

Figura 22: Núcleo de red



La vista simplificada del *core* de red permite identificar el punto central de procesamiento del tráfico, desde el cual los datos se distribuyen hacia los diferentes segmentos de usuarios y hacia el sistema de monitoreo. Esta representación facilita la comprensión del papel que desempeña el núcleo de red dentro de la arquitectura general.

Desde el punto de vista estructural, la red parte de una conexión principal que representa el acceso a Internet o al proveedor externo. El tráfico llega al sistema por el *router* MikroTik, que cumple la función de núcleo de la red y asume las tareas de enrutamiento, administración del direccionamiento IP, aplicación de políticas de *firewall* y control general del tráfico.

Posteriormente, los datos son transferidos a un *switch* gestionable, el cual hace de punto de agregación y permite tanto la segmentación lógica mediante VLAN como la replicación del tráfico al IDS.

Se implementó la distribución inalámbrica del servicio mediante una topología PtMP, donde una antena sectorial actúa como estación base y los equipos CPE representan los nodos de cliente o abonado. La red contempla segmentos diferenciados para usuarios VIP, empresariales, residenciales y un segmento exclusivo de administración; esto permite una organización lógica del tráfico según perfiles de servicio, criterios de seguridad y prioridades de operación.

La propuesta tecnológica gira en torno a la integración del IDS. El sistema se incorpora de forma pasiva, obteniendo una copia del tráfico del *switch* gestionable por medio de *Port Mirroring*, sin que quede situado en la ruta principal de transmisión. Esta decisión permite monitorear el tráfico en tiempo real, generar alertas y reforzar la supervisión de la red sin interferir con el rendimiento ni con la operación de otros componentes.

La arquitectura propuesta puede entenderse como un conjunto modular que se compone de un núcleo de gestión, una capa de agregación, una capa de distribución inalámbrica y una capa de supervisión de seguridad. Esta organización aporta claridad técnica al diseño y sienta una base firme para las posteriores etapas de integración, validación y evaluación del sistema IDS en la red WISP propuesta.

Tabla 19: Componentes principales de la arquitectura general propuesta

Componente	Función dentro de la arquitectura
Conexión principal / Internet	Representa la entrada y salida del tráfico hacia la red externa o el proveedor de servicio.
Router MikroTik	Actúa como núcleo de la red, realizando funciones de enrutamiento, administración del tráfico, direccionamiento IP y aplicación de políticas de <i>firewall</i> .
Switch gestionable	Cumple la función de agregación de tráfico, segmentación mediante VLAN y replicación del flujo de datos hacia el sistema IDS mediante <i>Port Mirroring</i> .
Antena sectorial	Opera como estación base de distribución inalámbrica dentro de la topología punto a multipunto (PtMP).
Equipos CPE	Representan los nodos de cliente o abonado, encargados de recibir la señal inalámbrica y conectar a los usuarios finales con la red.
Sistema IDS	Monitorea el tráfico replicado desde el <i>switch</i> , analiza eventos de seguridad y genera alertas ante posibles amenazas o comportamientos anómalos.
Segmentos de usuario (VIP, empresarial y residencial)	Permiten la organización lógica del tráfico según perfiles diferenciados, facilitando la administración, el aislamiento y el monitoreo por tipo de servicio.
Segmento de administración	Aísla la infraestructura crítica de la red para proteger las interfaces de gestión y limitar el acceso a dispositivos sensibles.

La distribución funcional de estos componentes permite estructurar una red WISP organizada, segmentada y supervisada, en la que el sistema IDS se integra como una capa adicional de monitoreo sin interferir con el flujo normal del tráfico.

3.3.2. Ubicación del IDS dentro de la arquitectura

La ubicación del sistema de detección de intrusos dentro de la arquitectura propuesta responde a criterios de visibilidad, eficiencia operativa y no interferencia con el tráfico principal de la red. En esta propuesta, el IDS está situado en el punto de agregación del tráfico conectado al *switch* gestionable por medio de un puerto dedicado configurado mediante la función de *Port*

Mirroring. Esta posición permite al sensor recibir una copia del tráfico que circula por los diferentes segmentos de red sin estar situado directamente en la ruta principal de transmisión.

Figura 23: Criterios técnicos de la ubicación del IDS



Desde el punto de vista técnico, esta ubicación es adecuada porque el *switch* gestionable concentra el tráfico procedente del *router*, de las VLAN definidas y de los enlaces a usuarios finales. Por tanto, el IDS puede ver desde un único punto el comportamiento global de la red, facilitando la inspección del tráfico asociado a usuarios VIP, empresariales, residenciales y de administración. De esta forma, se logra una visión centralizada del sistema sin necesidad de múltiples sensores repartidos por cada tramo.

La decisión de ubicar el IDS en este punto también se justifica por el enfoque defensivo y pasivo que se adopta en la tesis. Al recibir solo una copia del tráfico, el sistema no altera el flujo normal de paquetes, no introduce latencia adicional y no interfiere con el funcionamiento de los demás componentes del proyecto. El IDS, por tanto, se inserta como capa extra de vigilancia, enfocada al análisis y la generación de alertas, sin incidir en la estabilidad operativa de la red.

Tabla 20: Justificación técnica de la ubicación del IDS

Criterio	Justificación técnica
Punto de conexión	El IDS se conecta al <i>switch</i> gestionable, que actúa como punto de agregación del tráfico de red.
Método de captura	Se utiliza <i>Port Mirroring</i> para replicar el tráfico hacia el sensor IDS sin afectar la ruta principal.
Modo de operación	El IDS trabaja en modo pasivo, limitado a observar, analizar y generar alertas.
Cobertura de monitoreo	Permite observar tráfico de múltiples VLAN desde un único punto de captura.
Impacto en la red	Minimiza el impacto sobre latencia, <i>jitter</i> y <i>throughput</i> al no operar de forma <i>inline</i> .

3.3.3. Flujo general del tráfico

El flujo global del tráfico dentro de la arquitectura propuesta ha sido concebido para posibilitar una correcta operación de la red WISP, permitiendo que el sistema IDS supervise el comportamiento del tráfico.

El tráfico parte desde la conexión principal al *router* MikroTik, continúa hasta el *switch* gestionable y luego se reparte hacia los diferentes segmentos de usuario que hay en la red. De forma paralela, se replica una copia del tráfico hacia el sensor IDS mediante la función de *Port Mirroring*, lo que permite su análisis sin interferir en la ruta principal de transmisión.

Desde el punto de vista funcional, el *router* MikroTik se constituye como el primer punto de control del tráfico, ya que recibe la conexión externa, administra el direccionamiento, aplica políticas de filtrado y enruta los paquetes hacia los distintos segmentos internos. Posteriormente, el *switch* gestionable recibe dicho tráfico y lo distribuye en función de la segmentación lógica establecida mediante VLAN. Esta organización permite que los distintos perfiles de usuario, como el perfil VIP, el empresarial o el residencial, operen de forma separada dentro de la misma infraestructura física.

Al mismo tiempo, el *switch* hace una copia del tráfico y lo envía al puerto donde está conectado el sistema IDS. El sensor analiza esta copia en tiempo real y detecta cualquier patrón de comportamiento sospechoso, intentos de acceso no autorizados o eventos anómalos que ocurran en la red.

Como consecuencia, el sistema es capaz de producir alertas sin que se produzca una intervención directa en el tráfico original, preservando un enfoque de vigilancia pasiva y no invasiva.

3.3.4. Escenario de validación controlada del IDS

Con el objetivo de complementar la arquitectura general y el flujo de tráfico descritos con anterioridad, se plantea un escenario de validación controlada del sistema IDS dentro de la red WISP propuesta. Este escenario permite ver de forma funcional cómo se genera un evento de prueba, cómo circula el tráfico por la infraestructura y cómo el sistema IDS realiza la detección, el registro y la presentación de evidencias sin interferir en la ruta principal de comunicación.

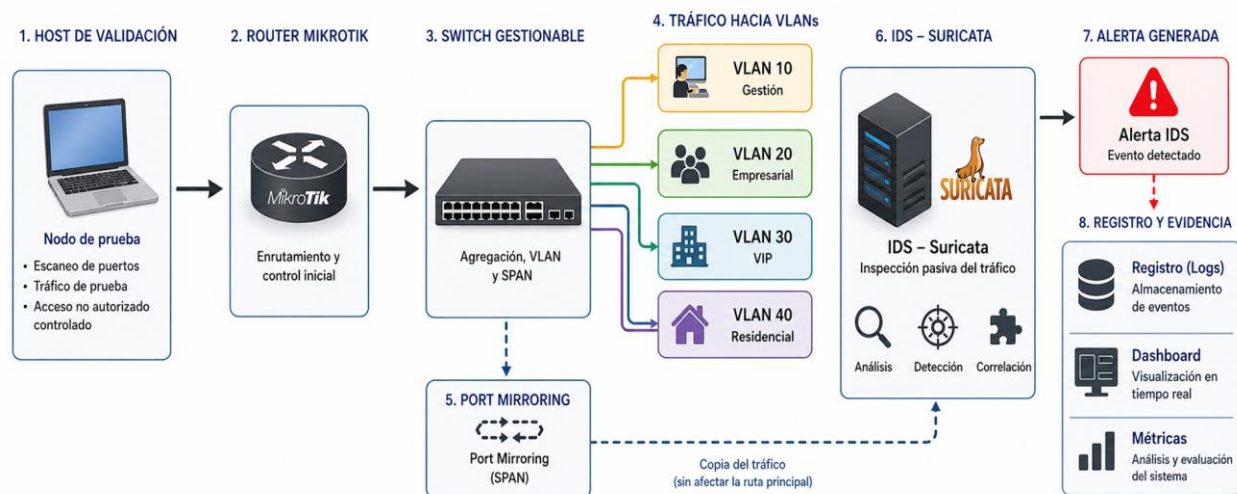
En este esquema, un nodo de validación genera tráfico de prueba controlado, que ingresa a la red por el *router* MikroTik y es posteriormente repartido por el *switch* gestionable a los

distintos segmentos VLAN definidos en la propuesta. El *switch*, paralelamente, envía una copia del tráfico mediante la función de *Port Mirroring* (SPAN) al sistema IDS basado en Suricata, lo cual permite la inspección pasiva de los paquetes y la identificación de eventos relevantes de seguridad.

A partir de este proceso, el IDS examina el tráfico recibido, aplica mecanismos de detección y correlación, y genera alertas al detectar comportamientos coincidentes con los eventos de validación configurados.

Por lo tanto, el sistema genera evidencia técnica mediante bitácoras, paneles de visualización y métricas de análisis, lo cual permite evaluar el funcionamiento del IDS en el entorno WISP propuesto.

Figura 24: Escenario de validación controlada del sistema IDS en la red WISP



La Figura 24 muestra la secuencia funcional de validación del sistema IDS, iniciando desde la generación del tráfico de prueba hasta la detección del evento y el almacenamiento de evidencias. Esta representación permite verificar que la propuesta no se limita a la integración del IDS dentro de la arquitectura, sino que también contempla un mecanismo de validación técnica

orientado a demostrar su capacidad de monitoreo, análisis y generación de alertas en un entorno controlado.

3.3.5. Modelo funcional de análisis, clasificación y generación de alertas del IDS

Con el fin de complementar la arquitectura general, la ubicación del IDS y el flujo del tráfico descritos en las subsecciones anteriores, se presenta el modelo funcional de operación del sistema IDS dentro de la red WISP propuesta. Este modelo representa la secuencia mediante la cual el tráfico replicado por *Port Mirroring* es inspeccionado por el sensor, procesado por el motor de tráfico y transformado en alertas, registros y evidencias útiles para la supervisión de la red.

Figura 25: Modelo funcional de análisis, clasificación y generación de alertas del IDS



La Figura 25 muestra el funcionamiento interno del IDS desde la recepción del tráfico replicado hasta la generación de alertas y el almacenamiento de evidencia. Esta representación permite entender que el sistema no solo observa el tráfico, sino que también lo procesa, clasifica y transforma en información útil para el monitoreo y la evaluación de la seguridad de la red WISP.

Tabla 21: Secuencia funcional del proceso

Etapa	Descripción breve
Captura del tráfico	El <i>switch</i> gestionable replica una copia del tráfico hacia el IDS mediante <i>Port Mirroring</i> , sin afectar la ruta principal de comunicación.
Análisis del tráfico	El IDS inspecciona los paquetes recibidos y aplica mecanismos de análisis, detección y correlación de eventos.
Clasificación del evento	El sistema determina el nivel de criticidad del evento detectado según reglas, patrones y comportamiento observado.
Generación de alertas	Una vez identificado el evento, el IDS produce alertas y notificaciones para su revisión técnica.
Registro y evidencia	El sistema almacena <i>logs</i> , genera visualizaciones en paneles y aporta métricas para el análisis del comportamiento de la red.

3.4. Fase 4: Aplicación de seguridad, monitoreo y criterios de evaluación del IDS

3.4.1. Indicadores técnicos de evaluación del IDS

Con el objetivo de evaluar el desempeño del sistema IDS en la red WISP propuesta, se establecen indicadores técnicos que permitan medir el comportamiento del tráfico y la capacidad de detección y respuesta del sistema. Estos indicadores se escogen de acuerdo con el marco teórico del trabajo, en donde se identifican métricas como la latencia, el *jitter*, el *throughput*, la pérdida de paquetes y la tasa de generación de alertas como fundamentales para evaluar redes segmentadas con mecanismos de seguridad. También se tienen en cuenta variables propias del funcionamiento del IDS, tales como el tiempo de detección, la precisión de las alertas y el consumo de recursos del sistema.

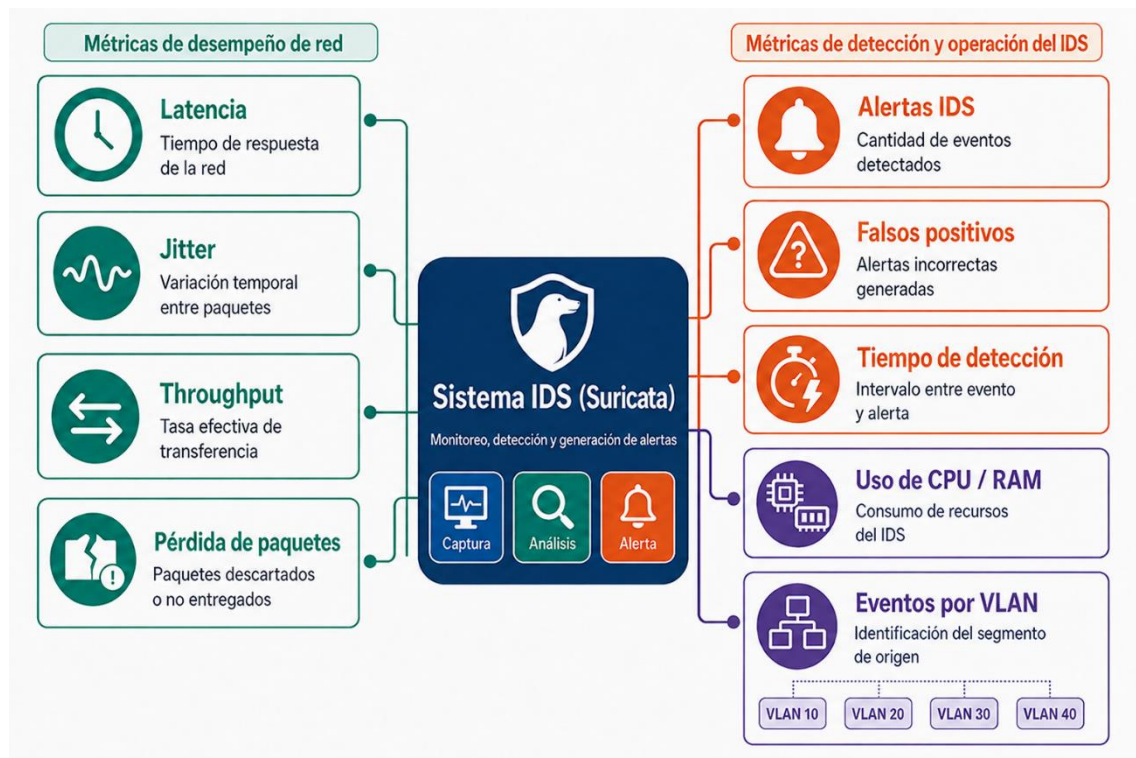
Estos indicadores no solo tienen como fin verificar que el sistema funciona correctamente, sino también determinar si su integración mediante *Port Mirroring* mantiene la estabilidad de la red, permite detectar eventos relevantes de seguridad y genera evidencia técnica útil para el análisis posterior. De esta forma, la evaluación no se limita al IDS como sensor, sino que también incluye su impacto en el entorno WISP y su contribución a la visibilidad, la trazabilidad y el soporte para el proceso de monitoreo.

Tabla 22: Indicadores técnicos de evaluación del sistema IDS

Indicador	Descripción	Unidad / criterio	Método de medición	Evidencia esperada
Latencia	Tiempo de respuesta de la red durante las pruebas con el IDS activo.	ms	iPerf / pruebas de conectividad	Variación controlada sin degradación crítica del servicio
Jitter	Variación temporal entre paquetes sucesivos.	ms	iPerf / monitoreo de tráfico	Estabilidad aceptable en tráfico segmentado
Throughput	Tasa efectiva de transferencia de datos con el IDS en operación.	Mbps	iPerf	Flujo sostenido sin cuellos de botella relevantes
Pérdida de paquetes	Porcentaje de paquetes descartados durante la circulación del tráfico.	%	iPerf / Wireshark	Nivel bajo de pérdida durante pruebas de validación
Tiempo de detección	Intervalo entre la generación del evento de prueba y la alerta del IDS.	s o ms	Logs del IDS / panel de monitoreo	Detección oportuna del evento controlado
Número total de alertas	Cantidad de alertas emitidas durante la prueba.	Conteo	Suricata / logs	Registro de eventos asociados al tráfico generado
Falsos positivos	Alertas generadas sin que exista un incidente real.	Conteo / %	Correlación entre evento y log	Nivel reducido de alertas incorrectas
Falsos negativos	Eventos de prueba que no son detectados por el sistema IDS.	Conteo / %	Comparación entre evento simulado y evidencia	Ausencia o mínima cantidad de eventos no detectados
Alertas por severidad	Clasificación de eventos según criticidad.	Bajo / medio / alto / crítico	Suricata / panel de alertas	Priorización correcta de los eventos detectados
Alertas por segmento VLAN	Relación entre evento detectado y segmento lógico de origen.	VLAN 10, 20, 30 y 40	IDS + segmentación lógica	Identificación del origen del evento por perfil
Uso de CPU del IDS	Carga de procesamiento del sistema durante la inspección del tráfico.	%	Monitor del sistema / Zabbix	Consumo estable y coherente con el tráfico analizado
Uso de memoria del IDS	Recursos de memoria empleados durante las pruebas.	MB o %	Monitor del sistema / Zabbix	Operación estable sin saturación del sistema

Los indicadores definidos en la Tabla 22 permiten estructurar una evaluación integral del sistema IDS, considerando tanto el rendimiento de la red como la precisión del proceso de detección. Su aplicación facilitará la comparación entre el comportamiento esperado y los resultados obtenidos durante las pruebas controladas, aportando criterios objetivos para determinar la efectividad del IDS dentro de la arquitectura WISP propuesta.

Figura 26: Panel conceptual de métricas de evaluación del IDS en la red WISP



La Figura 26 muestra de forma conceptual las métricas empleadas para la evaluación del sistema IDS dentro de la red WISP propuesta. Estos indicadores permiten valorar el desempeño de la red, la capacidad de detección del IDS, el uso de recursos del sistema y la identificación de eventos según el segmento lógico de origen.

3.4.2. Matriz de validación mediante eventos controlados

Con el fin de complementar los indicadores técnicos de evaluación del IDS, se incorpora una matriz de validación que permite relacionar los segmentos de red monitoreados con los eventos de seguridad evaluados, los mecanismos de detección aplicados por el IDS, las salidas generadas por el sistema y la evidencia técnica esperada. La estructura permite organizar el proceso de validación de forma metodológica, facilitando la trazabilidad entre la ocurrencia de un evento y la información obtenida como resultado del análisis.

La matriz propuesta se fundamenta en el enfoque seguido a lo largo del capítulo 3, donde la red WISP ha sido segmentada en perfiles diferenciados mediante VLAN, el IDS opera en modo pasivo mediante *Port Mirroring* y la validación se plantea mediante eventos controlados y no disruptivos. La matriz no muestra los resultados experimentales finales, sino una guía estructurada para comprobar el comportamiento esperado del sistema durante las pruebas de laboratorio.

Figura 27: Matriz visual de trazabilidad del sistema IDS en la red WISP

1. Segmento monitoreado	2. Evento de prueba o incidente	3. Mecanismo de detección del IDS	4. Salida generada por el IDS	5. Evidencia técnica esperada
 VLAN 10 Gestión	 Acceso no autorizado	 Regla Suricata (Acceso restringido)	 Alerta crítica generada	• IP origen / destino • Puerto / protocolo • Timestamp • VLAN de origen • Severidad • Tipo de alerta
 VLAN 20 Empresarial	 Escaneo de puertos	 Detección por firma (Reconocimiento)	 Alerta de alta prioridad	• IP origen / destino • Puertos escaneados • Protocolo detectado • Timestamp • Severidad
 VLAN 30 VIP	 Tráfico anómalo	 Correlación de eventos (Análisis de patrón)	 Registro en logs + Dashboard	• Protocolo / servicio • Volumen / frecuencia • IP origen / destino • VLAN de origen • Severidad
 VLAN 40 Residencial	 Flood controlado	 Detección por patrón + Volumen anormal	 Alerta + Log (Clasificación por criticidad)	• Tasa de paquetes • IP origen / destino • Timestamp • Severidad • Tipo de evento

La Figura 27 muestra la relación entre los segmentos lógicos de la red, los eventos de seguridad que se consideran en el proceso de validación, los mecanismos de detección que utiliza el IDS y la evidencia técnica que se espera obtener como resultado del análisis. Esta matriz permite verificar no solo la capacidad del sistema para identificar eventos, sino también su capacidad para asociarlos al segmento de origen, clasificarlos según su criticidad y generar información útil para su revisión técnica. En este sentido, la figura refuerza el enfoque metodológico adoptado en la propuesta, al aportar una visión estructurada de la trazabilidad del IDS dentro del entorno WISP segmentado.

3.5. Fase 5: Evaluación, pruebas y documentación del entorno IDS

Antes de conectar físicamente el servidor IDS al conmutador administrado de la red WISP, se realizó una prueba preliminar en un entorno controlado, empleando una computadora portátil configurada como servidor analítico. En esta etapa se buscó verificar que los servicios principales del sistema IDS funcionaran correctamente, que Suricata generara alertas ante tráfico de prueba y que estas alertas pudieran ser enviadas a Elasticsearch para su posterior visualización en Kibana.

La validación preliminar no representa todavía la prueba final de la red WISP segmentada por VLAN, ya que la integración de la infraestructura inalámbrica, el *switch* gestionable y los perfiles de usuario se realizó en una fase posterior. Sin embargo, esta prueba permite evidenciar el avance funcional del sistema IDS en lo que respecta a la captura de tráfico, la generación de eventos, el almacenamiento de registros y la visualización gráfica de alertas.

3.5.1. Entorno de prueba utilizado

En la fase inicial de validación del sistema IDS se utilizó una *laptop* con Ubuntu Server, la cual cumplió la función de servidor de monitoreo y análisis de tráfico. En este equipo se incorporaron herramientas de seguridad y de visualización, principalmente Suricata, Filebeat, Elasticsearch y Kibana. Se conectó la *laptop* a una red doméstica con acceso a Internet mediante un cable Ethernet, con el objetivo de verificar la conectividad del equipo, el funcionamiento de los servicios instalados y la generación de eventos de prueba, antes de integrar la *laptop* a la red WISP.

Se utilizó Suricata como motor IDS para inspeccionar el tráfico de red y generar alertas a partir de reglas locales configuradas. Filebeat permitió enviar los registros generados por Suricata hacia Elasticsearch, mientras que se utilizó Kibana como interfaz gráfica para visualizar las alertas mediante paneles, filtros KQL y gráficos estadísticos. Con este flujo se pudo comprobar que el

sistema era capaz de transformar eventos de red en información visual de utilidad para el análisis técnico.

Tabla 23: Componentes utilizados en la validación preliminar del entorno IDS

Componente	Función dentro de la validación preliminar	Evidencia o uso dentro de la prueba
Laptop IDS	Equipo físico utilizado como servidor de monitoreo y análisis.	Permitió alojar Ubuntu Server, Suricata, Filebeat, Elasticsearch y Kibana.
Ubuntu Server	Sistema operativo base del servidor IDS.	Proporcionó el entorno para instalar y ejecutar los servicios de seguridad y monitoreo.
Suricata	Motor IDS encargado de analizar el tráfico de red y generar alertas.	Registró eventos de prueba en archivos como <code>fast.log</code> y <code>eve.json</code> .
Reglas locales de Suricata	Reglas personalizadas para validar la detección de eventos controlados.	Permitieron generar alertas ante tráfico ICMP de prueba.
Filebeat	Agente encargado de enviar los registros de Suricata hacia Elasticsearch.	Permitió transportar los eventos desde el servidor IDS hacia el sistema de almacenamiento.
Elasticsearch	Motor de almacenamiento e indexación de eventos.	Recibió y organizó los registros generados por Suricata.
Kibana	Interfaz gráfica para visualizar los eventos del IDS.	Permitió crear gráficos, filtros KQL y <i>dashboards</i> de alertas.
Conexión Ethernet	Medio de conexión utilizado durante la prueba preliminar.	Permitió conectar la <i>laptop</i> IDS a la red doméstica con acceso a Internet.
Tráfico ICMP de prueba	Tráfico generado para comprobar la detección inicial del IDS.	Activó alertas visibles en Suricata y posteriormente en Kibana.

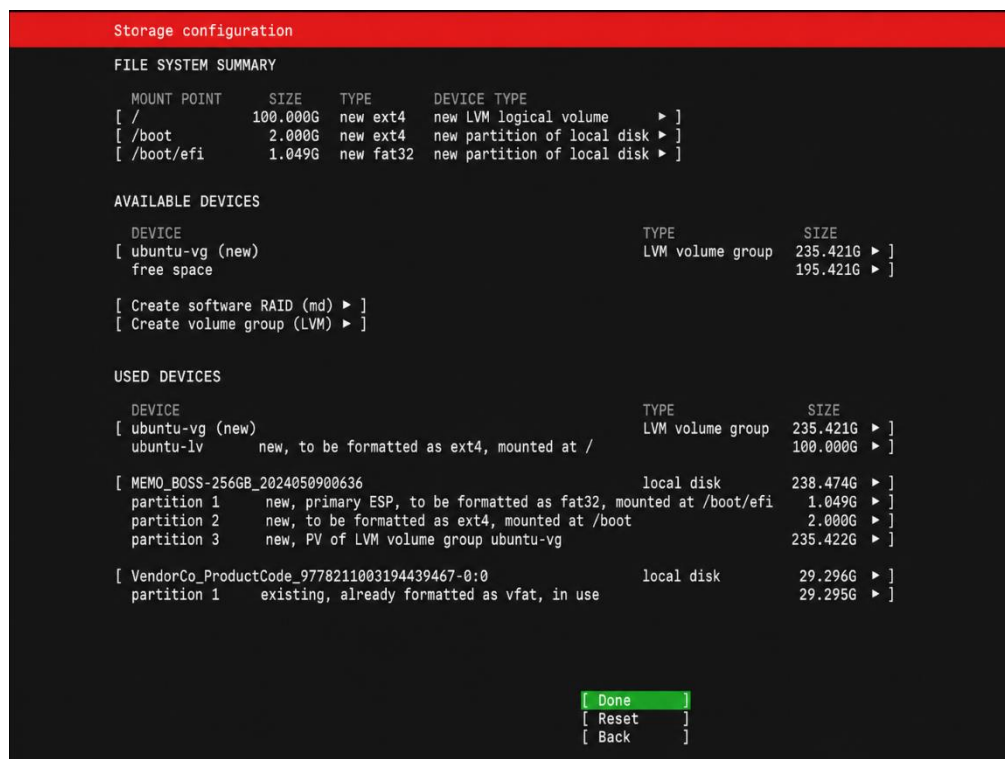
La validación se realizó en un entorno reducido, ya que el servidor IDS aún no estaba conectado al *switch* gestionable ni al esquema WISP con VLAN. Por eso, las pruebas se centraron principalmente en comprobar el funcionamiento interno del sistema IDS y la comunicación entre sus componentes. Se comprobó que la infraestructura lógica de monitoreo estuviera lista para recibir posteriormente el tráfico replicado mediante *Port Mirroring* desde la red WISP.

3.5.1.1. Preparación e instalación del sistema operativo base

Para preparar el servidor IDS, se instaló Ubuntu Server en una *laptop* destinada al monitoreo y análisis del tráfico de la red. La razón para elegir este sistema operativo fue su compatibilidad con herramientas de seguridad de código abierto, la estabilidad para ejecutar servicios en segundo plano y la facilidad de integración con Suricata, Filebeat, Elasticsearch y Kibana.

El proceso de instalación comenzó configurando el almacenamiento interno de la computadora portátil, estableciendo las particiones requeridas para el sistema operativo, el arranque y el área de trabajo principal. En esta fase se preparó el disco para que pudiera albergar el entorno base sobre el cual se instalarían más adelante los componentes del sistema IDS.

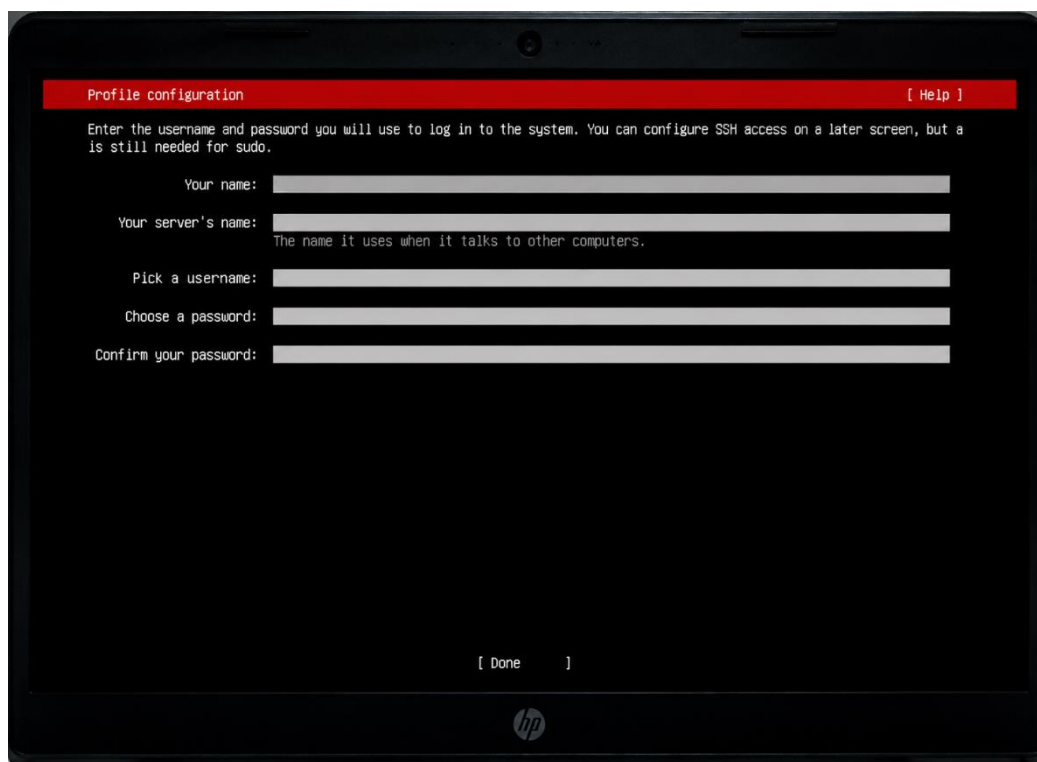
Figura 28: Configuración del almacenamiento durante la instalación de Ubuntu Server



La Figura 28 muestra la configuración de almacenamiento durante la instalación de Ubuntu Server en la *laptop* IDS. Esta fase permitió definir el espacio que ocuparía el sistema operativo, la partición de arranque y el volumen principal donde luego fueron ubicadas las herramientas de monitoreo y análisis de tráfico.

Después, se configuró el perfil del sistema: se dio un nombre al servidor y se creó un usuario administrador para la gestión local. Esta configuración permitió identificar el equipo dentro del entorno de laboratorio y facilitar la administración de los servicios instalados durante la implementación.

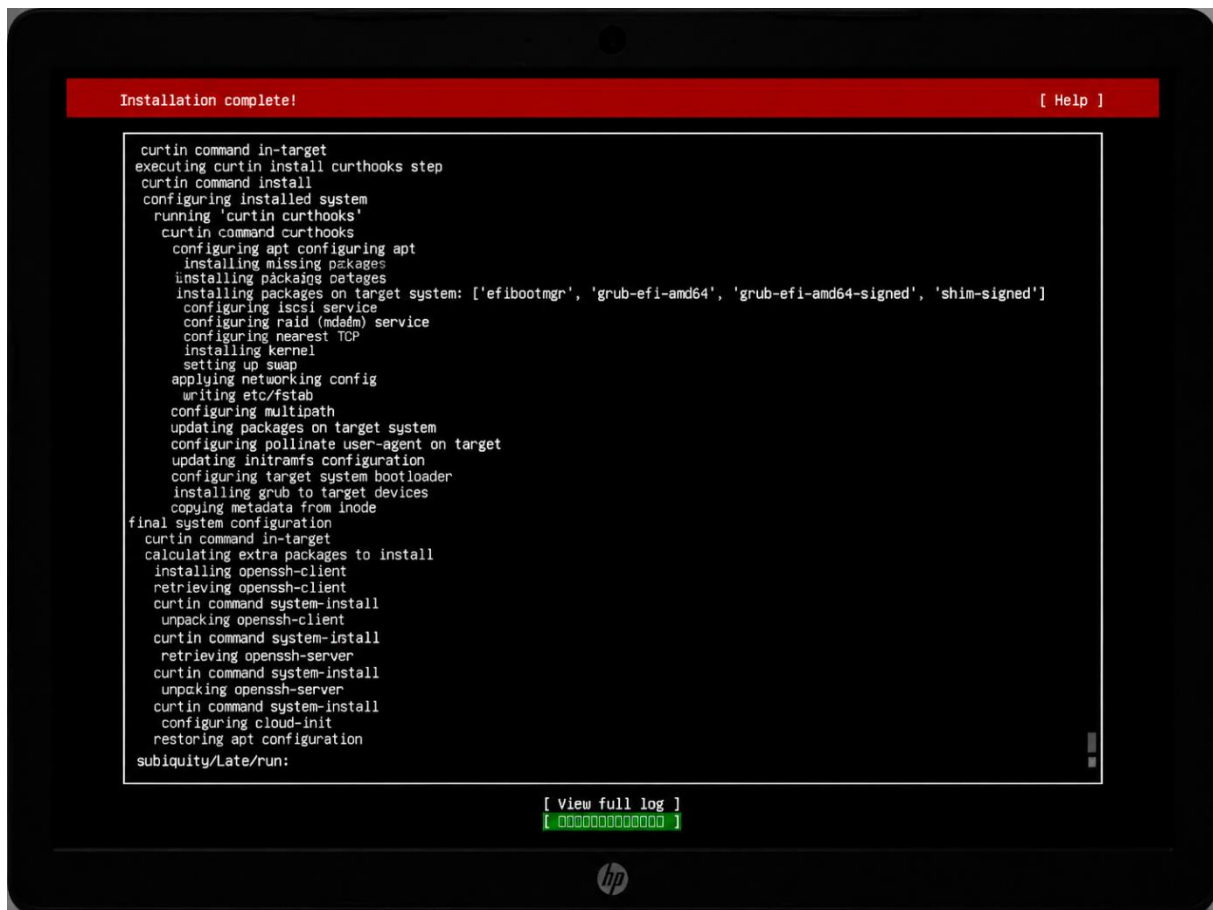
Figura 29: Configuración del perfil del servidor IDS durante la instalación



En la Figura 29 se observa la configuración del perfil del servidor durante la instalación de Ubuntu Server. En esta etapa se establecieron los datos básicos del equipo, por ejemplo, el nombre del servidor y las claves de acceso.

Terminado el proceso de instalación, el sistema operativo quedó listo para arrancar por primera vez desde el almacenamiento interno de la *laptop*. En esta etapa se comprobó que la instalación del sistema base se realizó correctamente, por lo que se pudo continuar con la configuración de los servicios IDS y de monitoreo.

Figura 30: Finalización de la instalación de Ubuntu Server en la *laptop* IDS

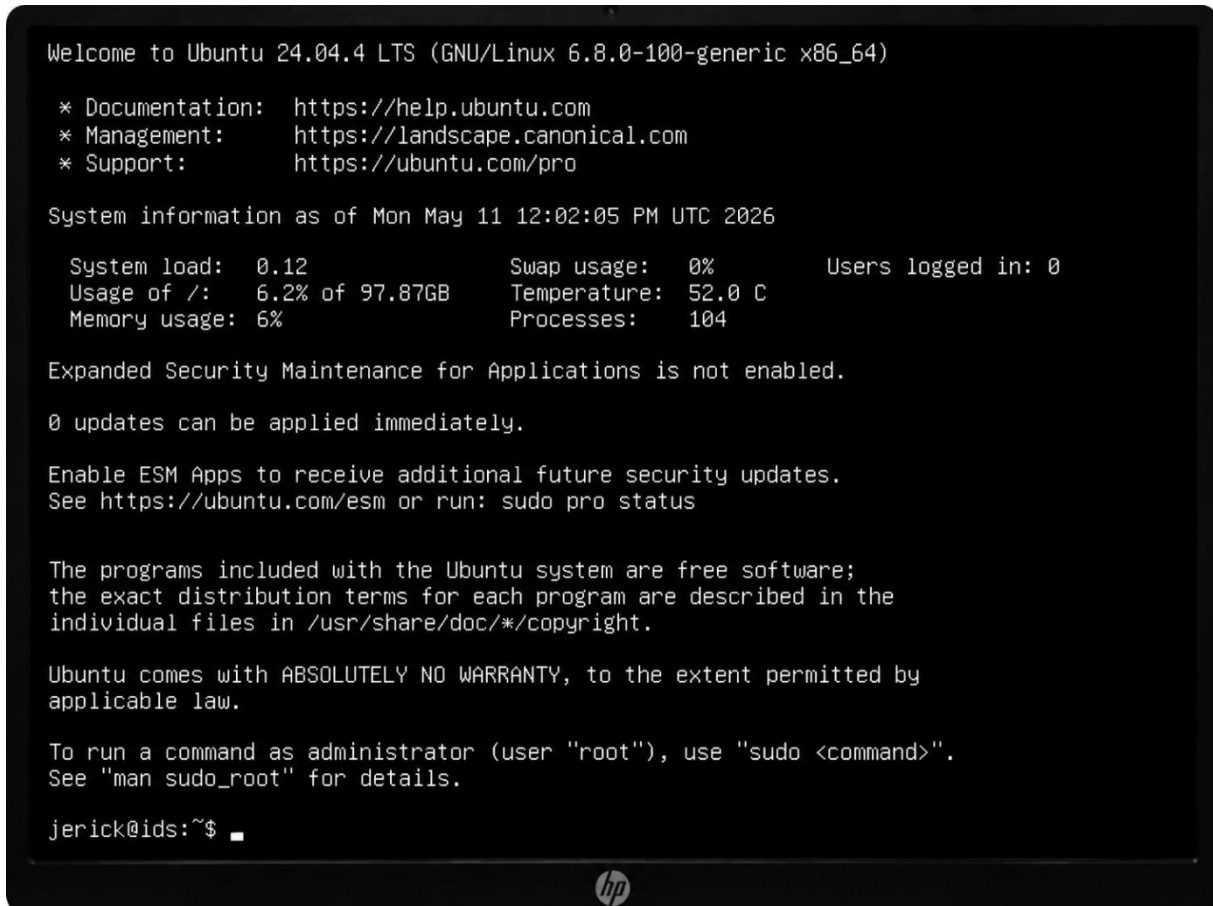


En la Figura 30 se visualiza cómo quedó Ubuntu Server tras finalizar el proceso de instalación. Esta evidencia confirma que el sistema operativo se instaló correctamente y quedó listo para su primer arranque en la *laptop* que serviría de servidor IDS.

Por último, se inició sesión por primera vez en Ubuntu Server y se comprobó la información básica del sistema como el nombre del equipo, la versión del sistema operativo, el uso

del almacenamiento y la memoria disponible. Esta prueba permitió confirmar que la *laptop* IDS estaba operativa y lista para instalar Suricata, Filebeat, Elasticsearch y Kibana.

Figura 31: Verificación inicial del sistema operativo Ubuntu Server instalado



```
Welcome to Ubuntu 24.04.4 LTS (GNU/Linux 6.8.0-100-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/pro

System information as of Mon May 11 12:02:05 PM UTC 2026

System load:  0.12           Swap usage:   0%           Users logged in: 0
Usage of /:   6.2% of 97.87GB Temperature: 52.0 C
Memory usage: 6%           Processes:   104

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

jerick@ids:~$
```

La Figura 31 muestra la verificación inicial del sistema operativo instalado en la *laptop* IDS. Se comprueba el nombre del equipo, la fecha del sistema, las interfaces de red, el uso del almacenamiento y la memoria disponible, confirmando que el entorno base se encontraba operativo para continuar con la implementación del sistema IDS.

Tabla 24: Etapas de preparación del sistema operativo base

Etapas	Descripción	Evidencia
Configuración de almacenamiento	Se definieron las particiones y el volumen principal para instalar Ubuntu Server.	Pantalla de configuración de disco
Configuración del perfil	Se asignó el nombre del servidor y el usuario administrador.	Pantalla de perfil del sistema
Instalación del sistema	Se completó la instalación del sistema operativo en la <i>laptop</i> IDS.	Pantalla de instalación finalizada
Primer inicio	Se accedió al sistema operativo instalado.	Pantalla de bienvenida de Ubuntu Server
Verificación básica	Se revisaron el nombre del equipo, las interfaces, el disco y la memoria.	Comandos <code>hostname</code> , <code>ip a</code> , <code>df -h</code> y <code>free -h</code>

Con la instalación y la prueba inicial de Ubuntu Server, la *laptop* quedó lista como plataforma base para alojar los servicios de seguridad y de monitoreo. Esta fase fue clave para que el sistema IDS dispusiera de un entorno operativo estable antes de instalar y configurar Suricata, Filebeat, Elasticsearch y Kibana.

3.5.2. Generación de eventos controlados

Con el fin de verificar el funcionamiento inicial del sistema IDS, se generaron eventos de red controlados dentro del entorno de prueba. Con esta actividad se pudo comprobar que Suricata era capaz de identificar tráfico específico, guardar alertas en sus archivos de eventos y enviar dicha información a la plataforma de visualización mediante Filebeat, Elasticsearch y Kibana.

En la primera prueba se generó tráfico ICMP mediante solicitudes de conectividad a direcciones externas y a la red local. Se seleccionó este tipo de tráfico por su facilidad de reproducción y por permitir una verificación directa del funcionamiento del motor IDS. A partir de esta prueba, Suricata generó alertas asociadas a la regla local configurada para tráfico ICMP, lo que permitió confirmar que el sistema estaba capturando paquetes y produciendo registros válidos para un análisis posterior.

De forma complementaria se realizaron pruebas de reconocimiento mediante escaneo controlado de puertos, con el objetivo de simular un comportamiento típico de identificación de servicios activos en una red. Esta prueba permitió verificar cómo el IDS registraba eventos relacionados con tráfico de exploración, lo cual resulta útil para validar la capacidad del sistema ante actividades que podrían representar una fase inicial de intrusión o análisis no autorizado de la infraestructura.

Tabla 25: Eventos controlados considerados en la validación preliminar del IDS

Evento de prueba	Herramienta o método utilizado	Propósito de la prueba	Evidencia esperada
Tráfico ICMP	Solicitudes de conectividad mediante ping	Verificar que Suricata detecte tráfico básico de red y genere alertas iniciales.	Registro de alertas ICMP en Suricata y visualización en Kibana.
Escaneo controlado de puertos	Prueba de reconocimiento con Nmap	Simular una actividad de exploración de servicios activos dentro del entorno de prueba.	Registro de eventos asociados a tráfico de reconocimiento o comportamiento sospechoso.
Visualización de eventos	<i>Dashboard</i> en Kibana	Comprobar que los eventos registrados por Suricata puedan ser enviados, indexados y representados gráficamente.	Gráficos de alertas por tiempo y por dirección IP de origen.
Tráfico TCP SYN	Prueba planificada para etapa posterior	Validar la detección de paquetes TCP SYN cuando el IDS sea integrado a la red WISP.	Alerta TCP SYN pendiente de validación con la red WISP conectada al <i>switch</i> .
Tráfico por VLAN	Prueba planificada para etapa posterior	Comprobar la detección diferenciada por segmentos de usuario: VIP, empresarial y residencial.	Alertas clasificadas según segmento lógico de origen.

Durante esta fase de validación preliminar, las pruebas se hicieron en un ambiente controlado y no sobre la red final WISP. Por ello, algunos eventos más puntuales, como pruebas

TCP SYN, tráfico por VLAN segmentado o la detección diferenciada por perfiles de usuario, quedaron pendientes hasta la etapa en la que se conectó el servidor IDS al *switch* gestionable mediante *Port Mirroring*. Sin embargo, los ensayos realizados permitieron comprobar el flujo básico de detección, registro y visualización de alertas.

3.5.3. Visualización de alertas en Kibana

Luego de la generación de eventos controlados, las alertas registradas por Suricata fueron enviadas hacia Elasticsearch mediante Filebeat, lo que permitió visualizarlas posteriormente en Kibana. Esta integración permitió convertir los registros producidos por el IDS en una presentación gráfica y organizada, facilitando el análisis de los sucesos detectados durante la fase preliminar de verificación.

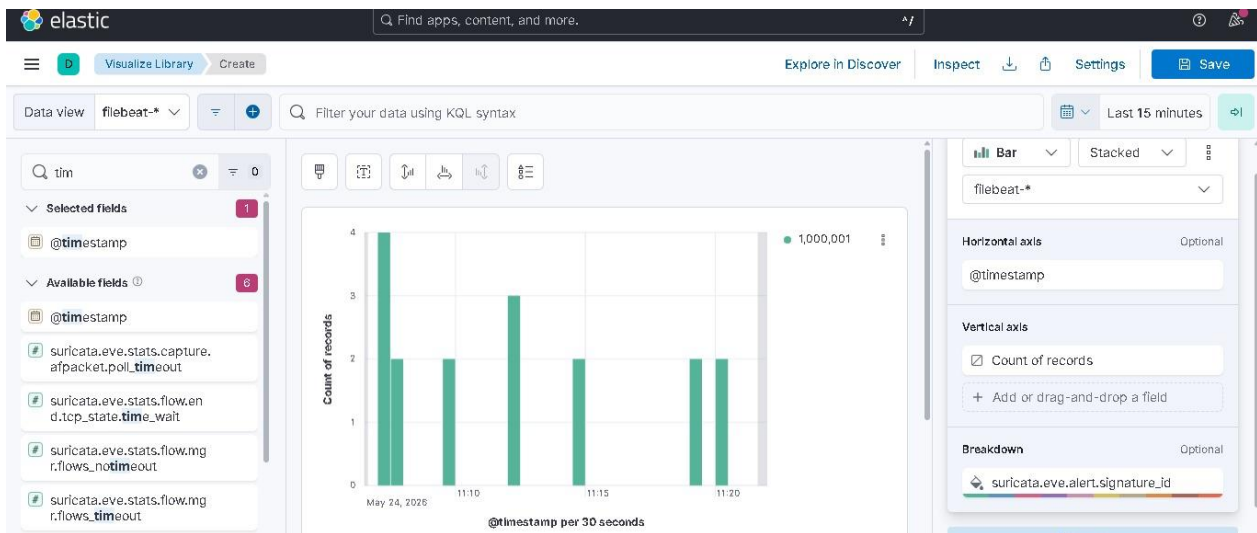
Tabla 26: Visualizaciones configuradas en Kibana para la validación preliminar del IDS

Visualización	Campo principal utilizado	Propósito de la visualización	Evidencia obtenida
Alertas ICMP por intervalo de tiempo	Fecha y hora del evento	Observar la cantidad de alertas ICMP generadas durante la prueba de conectividad.	Gráfico de barras con alertas distribuidas por intervalo temporal.
Alertas por dirección IP de origen	Dirección IP de origen	Identificar el host que generó la mayor cantidad de eventos durante la validación.	Gráfico de barras por origen del host.
Distribución por tipo de evento	Tipo de evento registrado	Diferenciar los eventos generados por el IDS según su clasificación.	Barras diferenciadas por tipo de evento.
Dashboard preliminar del IDS	Conjunto de visualizaciones	Integrar varias gráficas en una sola vista de monitoreo.	Panel gráfico con alertas detectadas por Suricata y visualizadas en Kibana.

En Kibana se empleó la sección de visualización para crear gráficos a partir de los campos que Suricata había registrado, como la fecha y hora del evento, la dirección IP de origen, el tipo

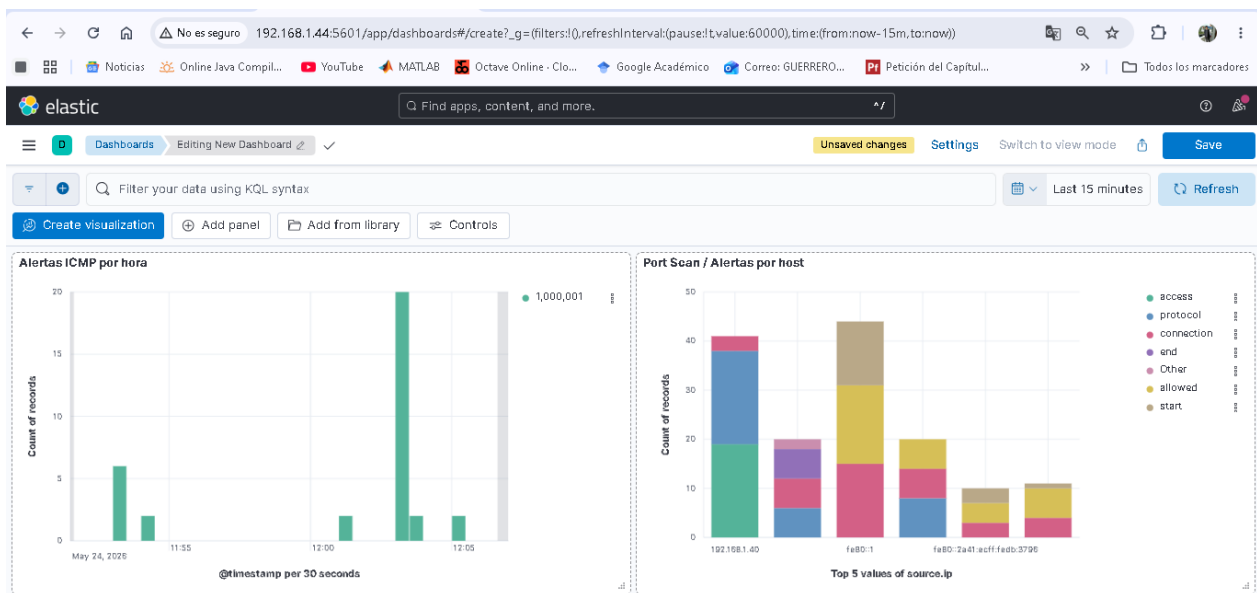
de evento, el identificador de regla y la firma de alerta. Con estos campos se configuraron visualizaciones que permitieron ver la cantidad de alertas detectadas por periodos de tiempo y la distribución de eventos por host de origen.

Figura 32: *Dashboard* preliminar de alertas IDS visualizadas en Kibana



La Figura 32 muestra el *dashboard* preliminar configurado en Kibana, donde se integran las visualizaciones generadas a partir de los eventos detectados por Suricata. Esta vista permite observar de manera conjunta la cantidad de alertas ICMP registradas por intervalo de tiempo y la distribución de eventos según la dirección IP de origen.

Figura 33: Distribución de alertas por dirección IP de origen



La Figura 33 muestra la cantidad de eventos registrados según la dirección IP de origen. Esta visualización facilita la identificación del equipo de origen del tráfico durante la prueba, aportando trazabilidad al proceso de monitoreo del IDS.

En primer lugar, se muestran las alertas ICMP que ha detectado Suricata. Se utilizó el campo temporal del evento como eje horizontal y el conteo de registros como eje vertical. Esta representación permitió observar la concentración de alertas generadas durante la prueba de conectividad, evidenciando que el IDS registró correctamente los paquetes ICMP generados en el entorno de prueba.

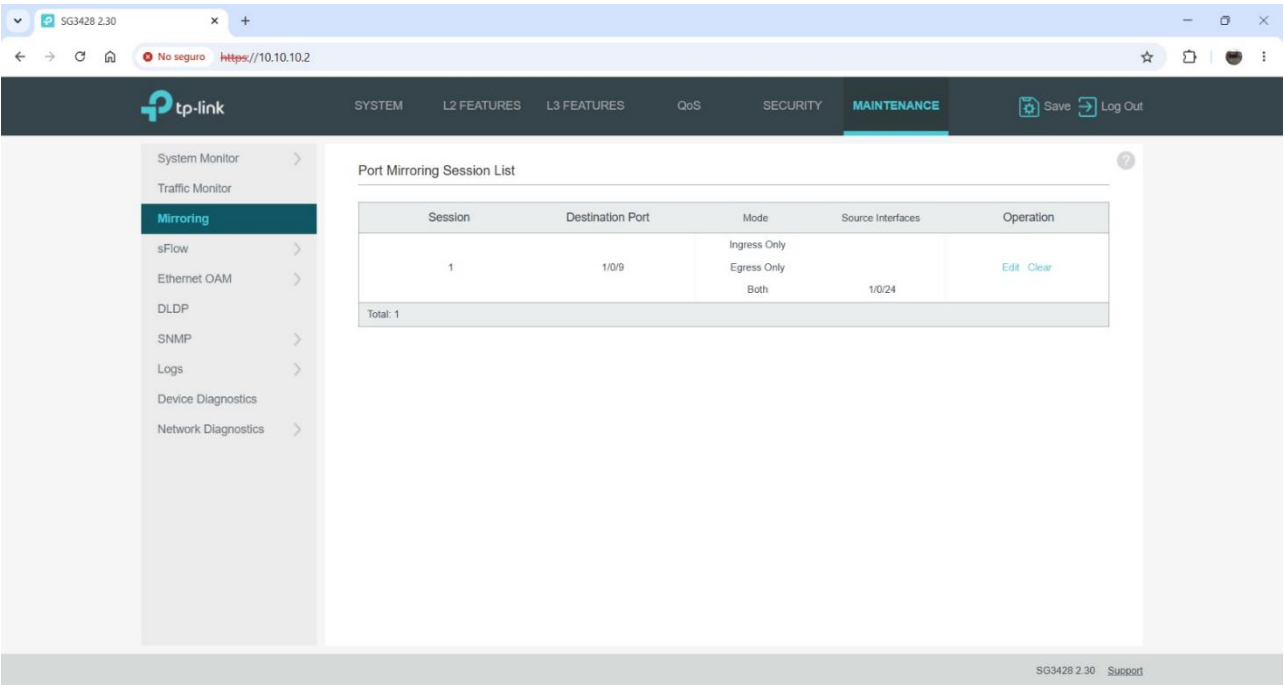
Asimismo, se armaron visualizaciones por dirección IP de origen, con el objetivo de ver qué host generó mayor cantidad de eventos en la validación. Esta gráfica ayuda a relacionar las alertas registradas con el origen del tráfico, lo cual es útil para el posterior análisis de eventos sospechosos o comportamientos anómalos dentro de una red monitoreada.

3.5.4. Integración del IDS con la infraestructura de red

En esta fase se realizó la integración física del sistema de detección de intrusos (IDS) dentro de la infraestructura de red WISP propuesta. El servidor configurado con Ubuntu Server y la herramienta Suricata se incorporó como nodo de análisis, estableciendo su conexión directa con el *switch* gestionable mediante un puerto configurado específicamente para la técnica de *Port Mirroring*.

En el *switch* gestionable se configuró la función de duplicación de puertos (*Port Mirroring*) para permitir la captura del tráfico de red sin interferir con el funcionamiento de la infraestructura. Este método permite copiar el tráfico de uno o más puertos a un puerto conectado al sistema IDS, habilitando la supervisión pasiva de la red.

Figura 34: Configuración del *Port Mirroring* en el *switch* TP-Link TL-SG3428



En la Figura 34, el *switch* permite seleccionar el puerto de origen del tráfico y el puerto de destino al que se envía la copia para su análisis por el sistema IDS. Este ajuste es necesario para

que Suricata opere en modo de monitorización pasiva y permita analizar el tráfico en tiempo real sin interferir con el funcionamiento de la red.

Para la correcta implementación del *Port Mirroring*, se establecen los puertos de origen y destino dentro del *switch* gestionable, de manera que el tráfico de la red sea replicado hacia el sistema IDS sin interferir con la operación normal del sistema.

Tabla 27: Configuración de puertos para *Port Mirroring* en el *switch*

Función	Puerto
Tráfico de origen	1/0/24
Puerto espejo del IDS	1/0/9

Esta configuración permite que el sistema IDS reciba una copia del tráfico generado en los distintos segmentos de la red (VLAN de administración, usuarios VIP, empresariales y residenciales), sin intervenir en la ruta principal de comunicación ni afectar el rendimiento de la red operativa.

El IDS opera en modo pasivo, analizando el tráfico en tiempo real y generando alertas ante eventos sospechosos o patrones anómalos detectados dentro de la red. Los eventos son posteriormente registrados para su procesamiento y visualización en la plataforma Kibana.

Configuración de la interfaz de captura en modo promiscuo

El sistema requiere habilitar la interfaz de red en modo promiscuo para permitir la captura de todos los paquetes que son enviados por el *switch* mediante *Port Mirroring*.

```
jerick@ids:~$ sudo ip link set enp4s0 promisc on
```

Este comando permite que la tarjeta de red del servidor IDS pueda analizar todo el tráfico que recibe, independientemente de la dirección MAC o IP de destino.

Verificación del modo promiscuo de la interfaz

Para validar que la interfaz de red se encuentra correctamente configurada en modo promiscuo, se ejecuta el siguiente comando:

```
jerick@ids:~$ ip link show enp4s0
```

Este comando permite comprobar que la interfaz está activa en modo PROMISC, lo cual es indispensable para el correcto funcionamiento del IDS.

Inicialización del sistema IDS Suricata

Una vez configurada la interfaz de captura, se procede a la ejecución del sistema IDS Suricata, el cual se encarga de analizar el tráfico de red en tiempo real.

```
jerick@ids:~$ sudo suricata -i enp4s0 -D
```

Este comando inicia Suricata en segundo plano, habilitando la inspección del tráfico replicado desde el *switch* gestionable.

Monitoreo de eventos generados por el IDS

Para verificar la generación de alertas en tiempo real, se realiza la visualización del archivo de *logs* del sistema IDS.

```
jerick@ids:~$ sudo tail -f /var/log/suricata/fast.log
```

Este comando permite observar las alertas generadas por Suricata, las cuales corresponden a eventos detectados durante el análisis del tráfico de red.

Flujo de procesamiento de la información

El sistema IDS implementado se integra con una arquitectura de análisis de datos basada en la pila ELK; con ello se logra el procesamiento y la visualización de los eventos generados.



Este flujo permite que los eventos detectados por el IDS sean enviados, almacenados y visualizados en *dashboards* interactivos, facilitando el análisis del comportamiento de la red.

Resultado de la integración

La integración del IDS con la infraestructura de red permite validar su funcionamiento como sistema de monitoreo pasivo, garantizando que el análisis del tráfico no interfiera con la operación normal de la red WISP.

Se confirma que el sistema es capaz de detectar eventos de seguridad, generar registros y visualizar la información mediante herramientas gráficas como Kibana, cumpliendo con los objetivos planteados en la propuesta de tesis.

3.5.5. Configuración del sistema de notificación por correo electrónico

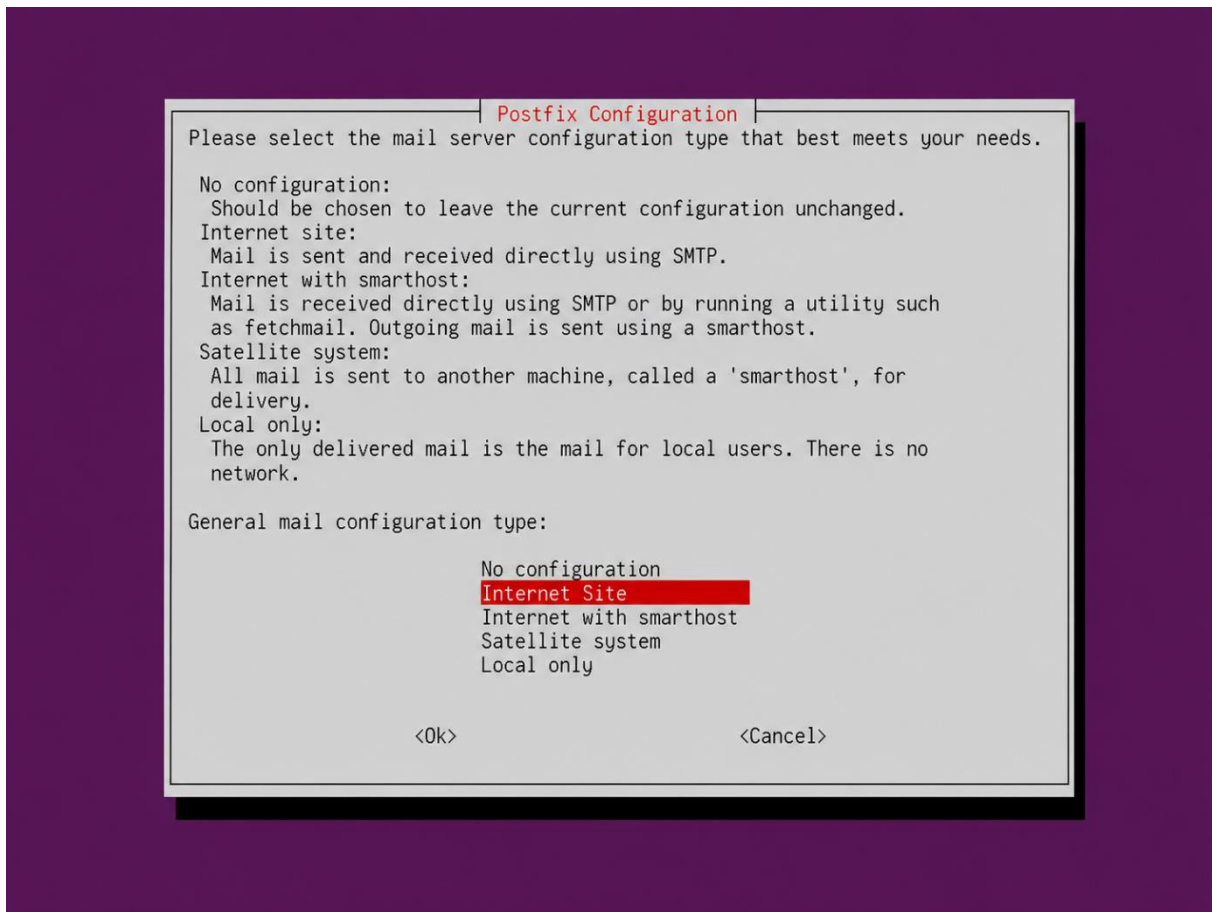
Como complemento al sistema IDS implementado, se configuró un mecanismo de notificación por correo electrónico con el objetivo de alertar al administrador cuando el sistema identifique eventos relevantes dentro del tráfico monitoreado. Esta funcionalidad permite ampliar la capacidad de respuesta del entorno IDS, ya que no se limita únicamente a la visualización de eventos en Kibana, sino que también permite remitir avisos hacia un dispositivo externo mediante correo electrónico.

La implementación de este mecanismo se realizó en la *laptop* IDS con Ubuntu Server, utilizando un cliente SMTP para el envío de mensajes. Este proceso se integró al análisis de los registros generados por Suricata, específicamente a partir del archivo `eve.json`, donde se almacenan los eventos capturados durante el monitoreo de la red. De esta manera, el sistema puede revisar continuamente los registros del IDS y enviar notificaciones cuando se detecten eventos como actividad DNS, tráfico HTTP o incremento anómalo del volumen de datos.

3.5.5.1. Configuración inicial del servicio de correo

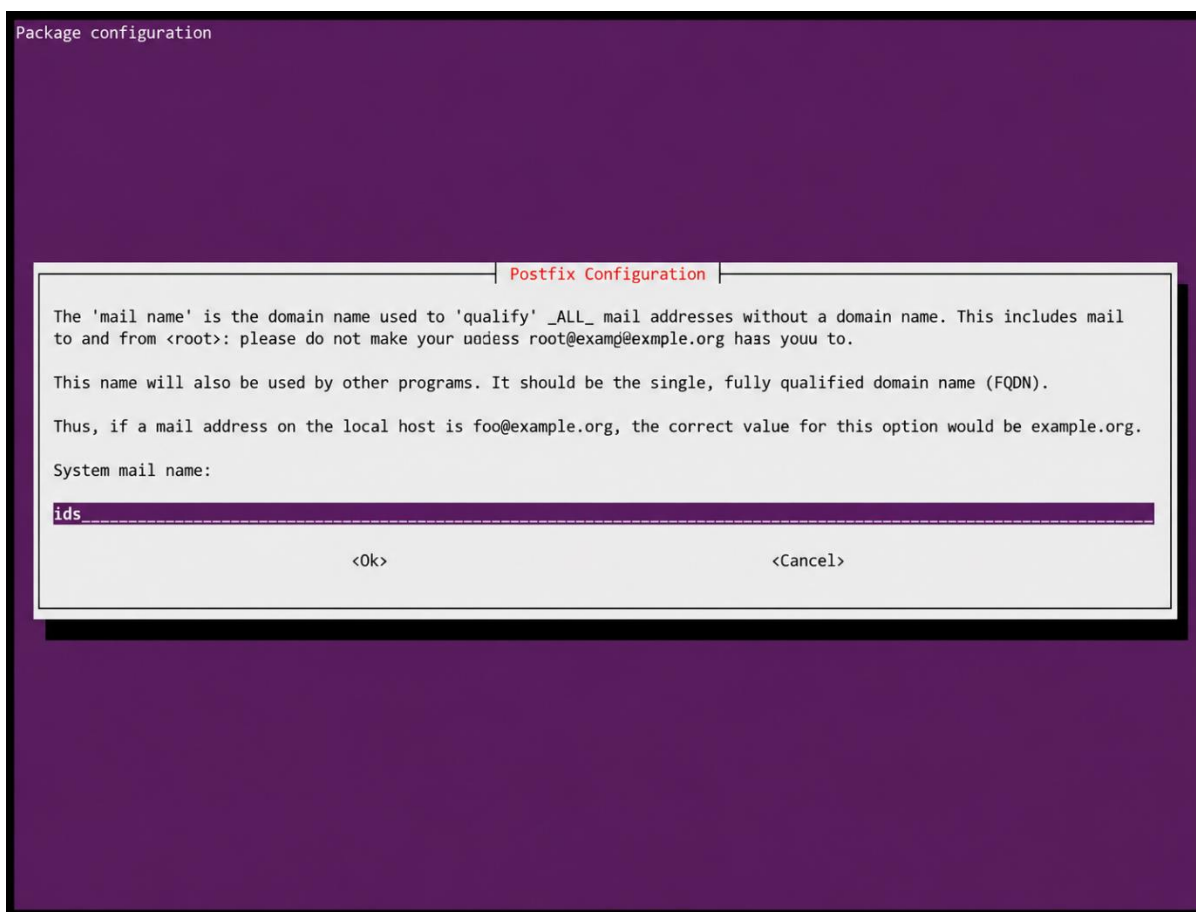
Para habilitar el envío de notificaciones desde el servidor IDS, se instalaron los paquetes necesarios para el manejo de correo electrónico desde la línea de comandos. Durante este proceso se configuró Postfix como servicio base de correo local, seleccionando la opción *Internet Site*, debido a que el servidor IDS requiere enviar mensajes hacia una cuenta externa.

Figura 35: Configuración inicial de Postfix para el envío de correo desde el servidor IDS



En la Figura 35 se muestra la configuración inicial del servicio Postfix, donde se seleccionó el tipo de configuración “*Internet Site*”. Esta opción permite al sistema operativo preparar el envío de mensajes mediante SMTP, sirviendo como base para la integración posterior con el cliente de correo utilizado por el IDS.

Figura 36: Definición del nombre del sistema de correo del servidor IDS

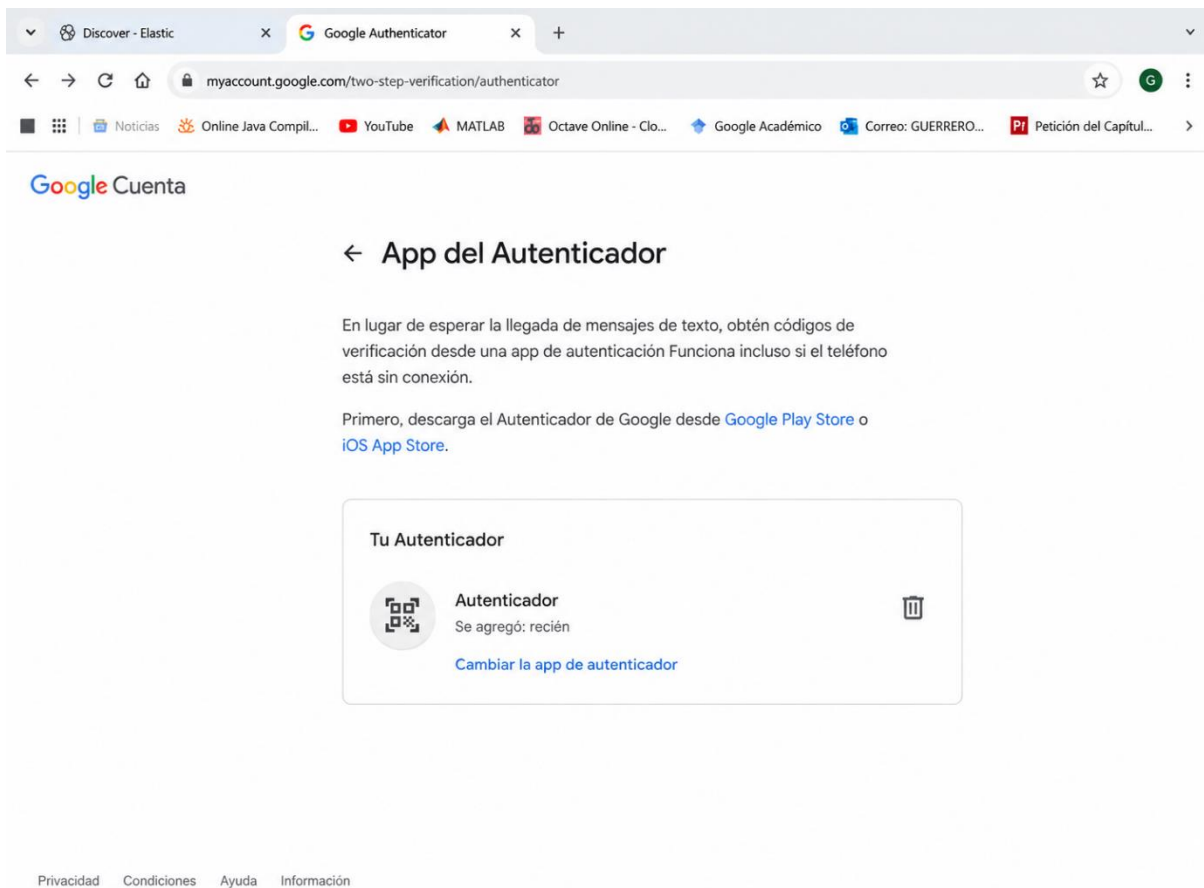


En la Figura 36 se observa la asignación del nombre del sistema de correo como ids, identificando al servidor de monitoreo dentro del proceso de envío de notificaciones. Esta configuración permite diferenciar los mensajes generados desde la *laptop* IDS dentro del entorno de prueba.

3.5.5.2. Configuración de autenticación segura en Gmail

Para permitir el envío de correos desde el servidor IDS hacia una cuenta externa, se habilitó la verificación en dos pasos en la cuenta de correo utilizada para las pruebas. Posteriormente, se generó una contraseña de aplicación asociada al nombre IDS_SURICATA, la cual fue empleada como credencial segura para la autenticación SMTP.

Figura 37: Configuración de autenticación segura para el envío de alertas IDS

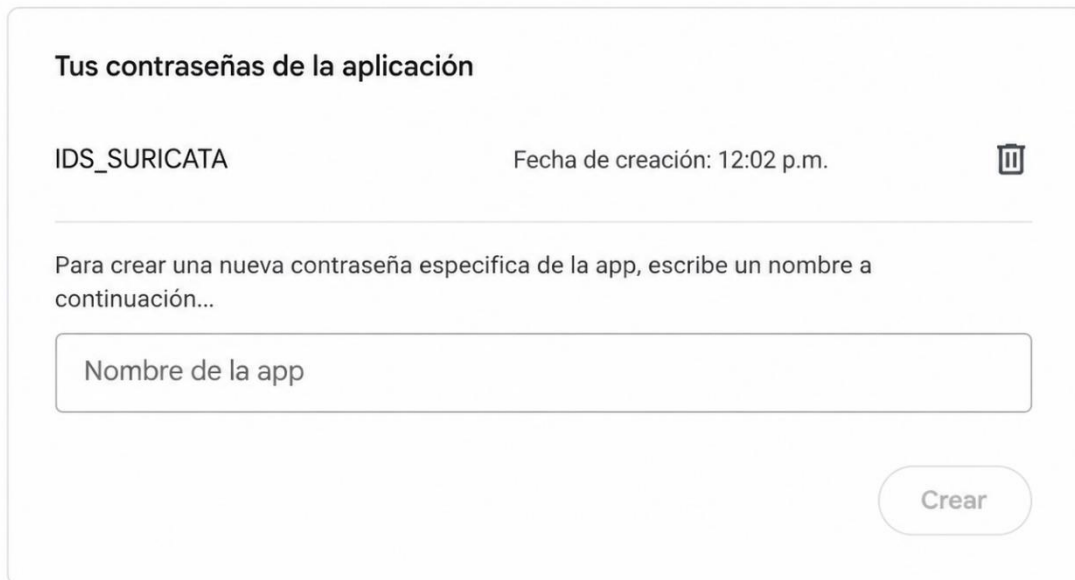


En la Figura 37 se muestra la configuración del mecanismo de autenticación en dos pasos, utilizado para reforzar la seguridad de la cuenta de correo empleada por el sistema IDS. Esta configuración fue necesaria para permitir el uso de una contraseña de aplicación en el envío automatizado de mensajes.

Figura 38: Creación de contraseña de aplicación para el sistema IDS

Las contraseñas de la aplicación son menos seguras que usar apps y servicios actualizados que cuentan con estándares de seguridad modernos. Antes de crear una contraseña de la aplicación, debes verificar si la app la necesita para acceder.

[Más información](#)



The screenshot shows a web interface titled "Tus contraseñas de la aplicación". It displays a list of application passwords. The first entry is "IDS_SURICATA" with a creation date of "Fecha de creación: 12:02 p.m." and a trash icon to its right. Below the list, there is a text prompt: "Para crear una nueva contraseña específica de la app, escribe un nombre a continuación...". Underneath this prompt is a text input field labeled "Nombre de la app". At the bottom right of the interface is a button labeled "Crear".

En la Figura 38 se evidencia la creación de una contraseña de aplicación identificada como IDS_SURICATA, empleada para autenticar el envío de correos desde el servidor IDS. Por motivos de seguridad, la credencial generada fue omitida en la documentación final.

3.5.5.3. Configuración del cliente de correo msmtplib

Se configuró el cliente **msmtplib**, el cual permite enviar correos electrónicos desde *scripts* ejecutados en Linux. Para ello, se editó el archivo de configuración ubicado en el directorio del usuario del sistema:

```
jerick@ids:~$ nano ~/.msmtplibrc
```

La configuración aplicada fue la siguiente:

```
defaults
auth on
tls on
tls_starttls on
tls_trust_file /etc/ssl/certs/ca-certificates.crt
logfile ~/.msmtp.log

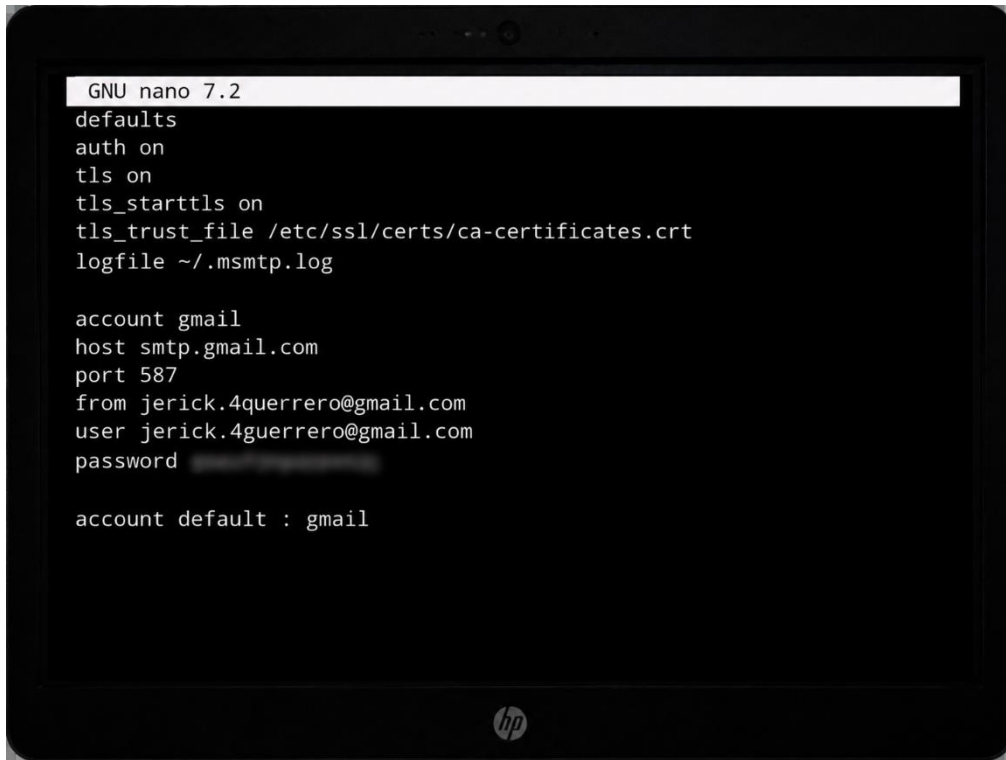
account gmail
host smtp.gmail.com
port 587
from correo_administrador@gmail.com
user correo_administrador@gmail.com
password CONTRASEÑA_DE_APLICACION_OCULTA

account default : gmail
```

Luego se asignaron permisos restrictivos al archivo de configuración, debido a que contiene información sensible de autenticación:

```
jerick@ids:~$ chmod 600 ~/.msmtprc █
```

Figura 39: Configuración del cliente msmtplib en el servidor IDS



```
GNU nano 7.2
defaults
auth on
tls on
tls_starttls on
tls_trust_file /etc/ssl/certs/ca-certificates.crt
logfile ~/.msmtplib.log

account gmail
host smtp.gmail.com
port 587
from jerick.4querrero@gmail.com
user jerick.4querrero@gmail.com
password *****

account default : gmail
```

En la Figura 39 se muestra la configuración del cliente msmtplib, utilizado para el envío de notificaciones desde el servidor IDS hacia una cuenta de correo externa. La configuración incluye el servidor SMTP, el puerto de comunicación, el uso de TLS y la autenticación mediante contraseña de aplicación. La contraseña fue ocultada por motivos de seguridad.

3.5.5.4. *Script de monitoreo y envío de notificaciones*

Para automatizar el envío de mensajes, se creó un *script* en Bash encargado de monitorear el archivo de eventos generado por Suricata. Este *script* revisa continuamente el archivo eve.json y envía una notificación cuando identifica eventos relevantes dentro del tráfico monitoreado.

El *script* fue creado mediante el siguiente comando:

```
jerick@ids:~$ nano ids_alert.sh
```

Luego se implementó la lógica de monitoreo de eventos:

Figura 40: Lógica de monitoreo de eventos

```
#!/bin/bash

LOG="/var/log/suricata/eve.json"
DESTINO="correo_administrador@gmail.com"

LAST_DNS_TIME=0
LAST_HTTP_TIME=0
LAST_TRAFFIC_TIME=0

COOLDOWN_DNS=300
COOLDOWN_HTTP=300
COOLDOWN_TRAFFIC=120
THRESHOLD_BYTES=5000000

tail -Fn0 "$LOG" | while read line ; do

    NOW=$(date +%s)

    if echo "$line" | grep -q "dns"; then
        if [ $((NOW - LAST_DNS_TIME)) -gt $COOLDOWN_DNS ]; then
            echo "ACTIVIDAD DNS DETECTADA EN RED WISP" | msmtp "$DESTINO"
            LAST_DNS_TIME=$NOW
        fi
    fi
    if echo "$line" | grep -q "http"; then
        if [ $((NOW - LAST_HTTP_TIME)) -gt $COOLDOWN_HTTP ]; then
            echo "TRÁFICO HTTP DETECTADO EN EL SISTEMA IDS" | msmtp "$DESTINO"
            LAST_HTTP_TIME=$NOW
        fi
    fi
    BYTES=$(echo "$line" | grep -o "bytes:[0-9]\+" | grep -o '[0-9]\+')
    if [ "$BYTES" == "[0-9]\+" ]; then
        if [ "$BYTES" -gt "$THRESHOLD_BYTES" ]; then
            if [ $((NOW - LAST_TRAFFIC_TIME)) -gt $COOLDOWN_TRAFFIC ]; then
                echo "ALTO TRÁFICO DETECTADO EN RED WISP: $BYTES bytes" | msmtp "$DESTINO"
                LAST_TRAFFIC_TIME=$NOW
            fi
        fi
    fi
done
```

Después, se otorgaron permisos de ejecución al *script*:

```
jerick@ids:~$ chmod +x ids_alert.sh
```

El *script* fue ejecutado mediante:

```
jerick@ids:~$ ./ids_alert.sh
```

Con esta configuración, el sistema IDS no solo registra y visualiza eventos mediante Kibana, sino que también incorpora un mecanismo de notificación externa mediante correo

electrónico. Esta funcionalidad mejora la capacidad de monitoreo del entorno WISP, ya que permite alertar al administrador ante eventos relevantes sin necesidad de revisar constantemente el *dashboard* del sistema.

CAPÍTULO 4: RESULTADOS Y ANÁLISIS DEL SISTEMA IDS IMPLEMENTADO

4.1. Resultados de la implementación del IDS

En esta sección se presentan los resultados obtenidos tras la implementación del sistema de detección de intrusos (IDS) basado en Suricata, integrado con la pila ELK (Elasticsearch, Logstash/Filebeat y Kibana), desplegado en un entorno de red WISP con *Port Mirroring* configurado en un *switch* administrable.

La arquitectura implementada permitió la captura pasiva del tráfico de red, el procesamiento de eventos de seguridad y su visualización en tiempo real mediante *dashboards* en Kibana.

4.1.1. Verificación del funcionamiento del IDS

La primera etapa de la validación consistió en verificar el funcionamiento de los servicios principales que constituyen la plataforma IDS desplegada en la red WISP. Esta comprobación permitió asegurar que los componentes involucrados en la detección de eventos, el almacenamiento y la visualización estuvieran en funcionamiento antes de ejecutar las pruebas de monitoreo y generar tráfico sintético.

En esta verificación se comprobó el estado de los servicios de Suricata, Elasticsearch y Kibana, que realizan funciones clave dentro de la arquitectura desplegada. En esta arquitectura, Suricata es el motor de detección de intrusiones, Elasticsearch se utiliza para almacenar e indexar los eventos creados por el propio Suricata y Kibana visualiza los datos capturados.

Figura 41: Verificación del funcionamiento del servicio Suricata del sistema IDS

```
jerick@ids:~$ sudo systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
   Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; preset: enabled)
   Active: active (running) since Sat 2026-06-27 08:36:57 -05; 8min ago
     Docs: man:suricata(8)
           man:suricatasc(8)
           https://suricata.io/documentation/
  Process: 922 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid
 Main PID: 966 (Suricata-Main)
    Tasks: 8 (limit: 4466)
  Memory: 510.0M (peak: 549.1M)
     CPU: 2min 21.518s
   CGroup: /system.slice/suricata.service
           └─966 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid

Jun 27 08:36:56 ids systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon...
Jun 27 08:36:57 ids suricata[922]: i: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
Jun 27 08:36:57 ids systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
jerick@ids:~$
```

Figura 42: Verificación del funcionamiento del servicio Elasticsearch del sistema IDS

```
jerick@ids:~$ sudo systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; preset: enabled)
   Active: active (running) since Sat 2026-06-27 08:39:39 -05; 6min ago
     Docs: https://www.elastic.co
 Main PID: 917 (java)
    Tasks: 94 (limit: 4466)
  Memory: 1.1G (peak: 1.1G)
     CPU: 6min 17.626s
   CGroup: /system.slice/elasticsearch.service
           └─ 917 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+UseSerialGC -Dcli.name=server -Dcli.script=/usr/share/...
             1020 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negative.ttl=...
             1196 /usr/share/elasticsearch/modules/x-pack-m1/platform/linux-x86_64/bin/controller

Jun 27 08:39:56 ids systemd[1]: Starting elasticsearch.service - Elasticsearch...
Jun 27 08:39:39 ids systemd[1]: Started elasticsearch.service - Elasticsearch.
lines 1-15/15 (END)
```

Figura 43: Verificación del funcionamiento del servicio Kibana del sistema IDS

```
jerick@ids:~$ sudo systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/usr/lib/systemd/system/kibana.service; enabled; preset: enabled)
   Active: active (running) since Sat 2026-06-27 08:36:56 -05; 9min ago
     Docs: https://www.elastic.co
   Main PID: 919 (node)
    Tasks: 11 (limit: 4466)
   Memory: 1.0G (peak: 1.3G)
      CPU: 2min 42.281s
   CGroup: /system.slice/kibana.service
           └─919 /usr/share/kibana/bin/./node/glibc-217/bin/node /usr/share/kibana/bin/./src/cli/kibana/l

Jun 27 08:41:56 ids kibana[919]: [2026-06-27T08:41:56.894-05:00] [INFO ] [plugins.securitySolution.telemetry_event]
Jun 27 08:41:56 ids kibana[919]: [2026-06-27T08:41:56.902-05:00] [INFO ] [plugins.securitySolution.telemetry_event]
Jun 27 08:41:56 ids kibana[919]: [2026-06-27T08:41:56.905-05:00] [INFO ] [plugins.securitySolution.telemetry_event]
Jun 27 08:41:57 ids kibana[919]: [2026-06-27T08:41:57.150-05:00] [INFO ] [plugins.fleet.fleet:upgrade-agentless-agent]
Jun 27 08:41:57 ids kibana[919]: [2026-06-27T08:41:57.166-05:00] [INFO ] [plugins.fleet.fleet:upgrade-agentless-agent]
Jun 27 08:41:58 ids kibana[919]: [2026-06-27T08:41:58.177-05:00] [INFO ] [plugins.fleet.fleet:upgrade-agentless-agent]
Jun 27 08:41:59 ids kibana[919]: [2026-06-27T08:41:59.133-05:00] [INFO ] [plugins.securitySolution.telemetry_event]
Jun 27 08:41:59 ids kibana[919]: [2026-06-27T08:41:59.623-05:00] [INFO ] [plugins.securitySolution.telemetry_event]
Jun 27 08:42:50 ids kibana[919]: [2026-06-27T08:41:59.623-05:00] [INFO ] [plugins.securitySolution.telemetry_event]
Jun 27 08:42:00 ids kibana[919]: [2026-06-27T08:42:00.250-05:00] [INFO ] [plugins.securitySolution.telemetry_event]
Jun 27 08:42:03 ids kibana[919]: [2026-06-27T08:42:03.542-05:00] [INFO ] [plugins.screenshots.chromium] Browser
lines 1-21/21 (END)
```

Figura 44: Verificación del funcionamiento del servicio puerto 5601 para el acceso web a Kibana del sistema IDS

```
jerick@ids:~$ ss -tulnp | grep 5601
tcp    LISTEN 0          511                0.0.0.0:5601        0.0.0.0:*
jerick@ids:~$ _
```

En las Figuras 41, 42, 43 y 44, como se aprecia, los servicios principales de este sistema están en funcionamiento. La ejecución de Suricata confirma que el IDS está en ejecución para analizar el tráfico de red; Elasticsearch está activo y listo para almacenar los eventos generados, y Kibana sigue disponible para la visualización mediante interfaz web usando el puerto 5601. Esta validación es una condición necesaria para registrar y analizar correctamente las pruebas posteriores.

Mediante esta verificación se confirma que la plataforma IDS está lista para recibir eventos de red y registros generados por Suricata, presentándolos bajo demanda en paneles de Kibana. Por

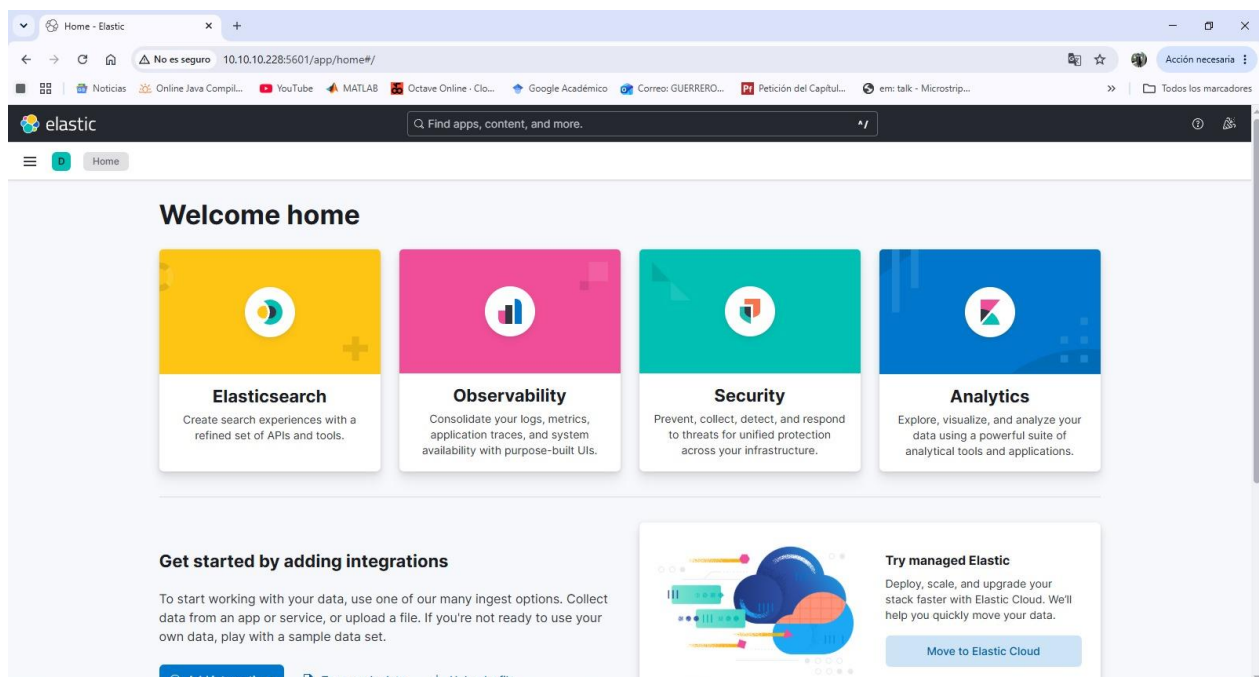
lo tanto, este paso valida el funcionamiento en tiempo real del sistema antes de iniciar la evaluación de alertas, tráfico y métricas provenientes del monitoreo.

4.1.2. Integración con ELK Stack

Después de verificar que todos los servicios IDS del sistema principal estaban en funcionamiento, se procedió a validar la conectividad con la plataforma de visualización de Kibana desde una máquina cliente ubicada en la misma red implementada. La validación confirmó que la interfaz web de este sistema de monitoreo estaba disponible de forma remota en una infraestructura física implementada.

Para la prueba, se utilizó la dirección IP asignada al servidor IDS y el puerto 5601 correspondiente al servicio de Kibana. El acceso desde una máquina cliente confirmó que la plataforma no está limitada únicamente al servidor local; se puede acceder a la plataforma desde cualquier dispositivo de la red WISP.

Figura 45: Acceso remoto a Kibana desde un equipo cliente



Por ejemplo, se verificó el acceso correcto a Kibana desde un navegador web en la máquina cliente de la red implementada como se muestra en la Figura 45. La prueba evidenció que el servicio era accesible mediante la dirección IP del servidor IDS y el puerto 5601, lo que permite el acceso remoto a los eventos y paneles generados por esta plataforma.

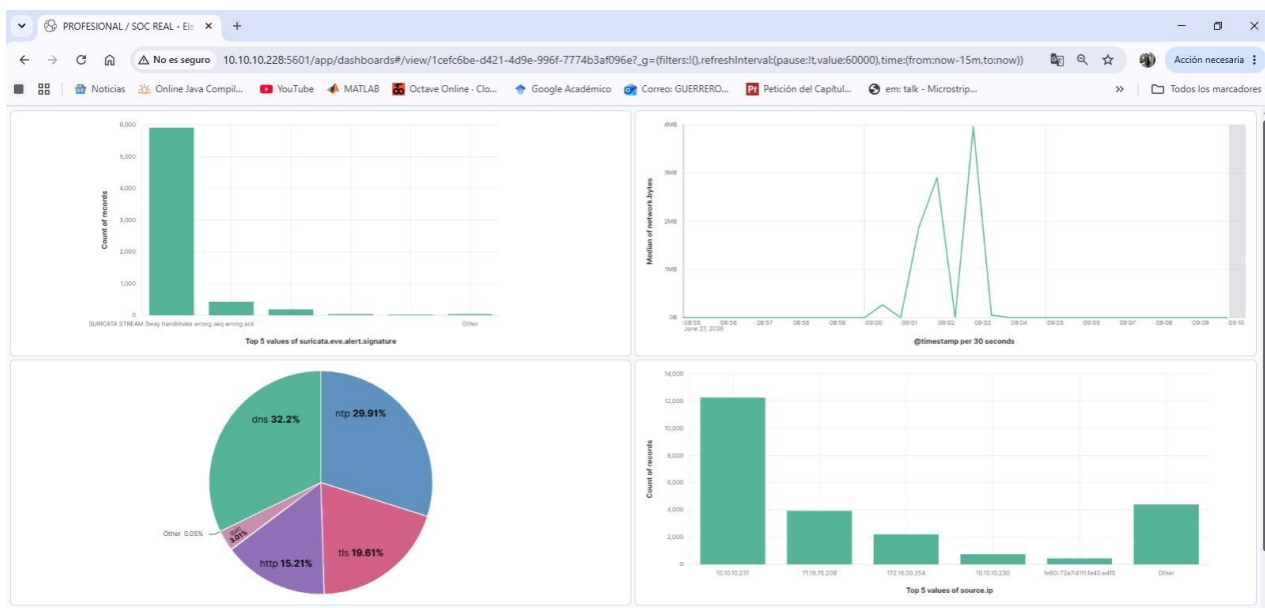
Un aspecto importante para la validación del acceso remoto es la capacidad de centralizar la monitorización desde una máquina externa hacia la interfaz del servidor de captura en cualquier red de área amplia (WAN). Se pueden gestionar y revisar los eventos sin acceder directamente a la *laptop* del IDS, permitiendo el análisis visual de los datos recopilados por Suricata y almacenados en Elasticsearch.

4.1.3. Visualización general del *dashboard* del IDS

Tras la confirmación de la conectividad entre la máquina cliente y Kibana, se evidenció el acceso de extremo a extremo a un panel que visualiza la ejecución general del sistema IDS implementado. Este panel permitió centralizar los eventos generados por Suricata y ofreció una representación gráfica del comportamiento del tráfico supervisado en la red WISP.

El panel en sí se creó para mostrar datos relevantes provenientes del sistema de detección, como eventos de alerta, firmas generadas por Suricata, evolución temporal del tráfico, protocolos detectados y direcciones IP de origen con mayor actividad. Esto permitió obtener una visión general del estado de la red y de los eventos registrados por el IDS.

Figura 46: *Dashboard* general del sistema IDS implementado en Kibana



La Figura 46 muestra el panel general construido en Kibana, que integra distintos paneles de análisis de los eventos producidos por el IDS Suricata. A través de la visualización es más fácil detectar las firmas que generan una alerta, ver si hay picos o caídas de tráfico en las redes,

identificar cuáles son los protocolos principales y saber qué direcciones IP de origen se registraron con mayor frecuencia.

Esta figura es importante porque muestra el aspecto y el funcionamiento de Suricata, Elasticsearch y Kibana operando en conjunto. Además, proporciona medios para validar si los eventos recopilados del IDS se almacenan, procesan y representan gráficamente con el fin de ayudar en la revisión de seguridad dentro de la estructura WISP.

Tabla 28: Paneles incluidos en el *dashboard* general del IDS

Panel del <i>Dashboard</i>	Campo o métrica utilizada	Descripción
Firmas de alerta	suricata.eve.alert.signature	Permite identificar los tipos de alertas generadas por Suricata IDS.
Tráfico de red	network.bytes	Muestra el comportamiento del tráfico monitoreado en función del tiempo.
Tipos de eventos	suricata.eve.event_type	Clasifica los eventos registrados, tales como alertas, DNS, HTTP, TLS o flujos de red.
Direcciones IP de origen	source.ip	Identifica los hosts que generan mayor cantidad de eventos dentro de la red monitoreada.

La Tabla 28 resume los paneles principales utilizados en el panel general de IDS. Estos elementos permiten que los datos recopilados por Suricata se interpreten de forma estructurada, de modo que sea más fácil identificar patrones de tráfico, informar sobre eventos de interés o posibles comportamientos anómalos en la red WISP.

4.2. Resultados de detección mediante escenarios controlados

Después de confirmar el funcionamiento de la plataforma IDS y visualizar los eventos a través de Kibana, se realizaron pruebas controladas con el fin de validar que el sistema era capaz de detectar eventos de seguridad. Estas pruebas permitieron generar tráfico controlado y analizar la respuesta del IDS Suricata mediante la plataforma Kibana.

La validación se llevó a cabo en la red WISP implementada, donde las pruebas antes mencionadas generaron eventos que pudieron detectarse, procesarse y visualizarse en la plataforma mediante herramientas de análisis de red. Así se confirmó que el sistema IDS era funcional y, además, permitía registrar actividades asociadas a eventos de seguridad.

4.2.1. Prueba de escaneo de puertos con Nmap

Se realizó una prueba de escaneo de puertos con Nmap para corroborar si se detectaba alguna actividad sospechosa. Esta prueba generó tráfico de reconocimiento hacia un host dentro de la red, con el objetivo de verificar que Suricata IDS registrara alertas del escaneo y generara eventos que luego pudieran visualizarse en Kibana.

Figura 47: Ejecución del escaneo de puertos mediante Nmap

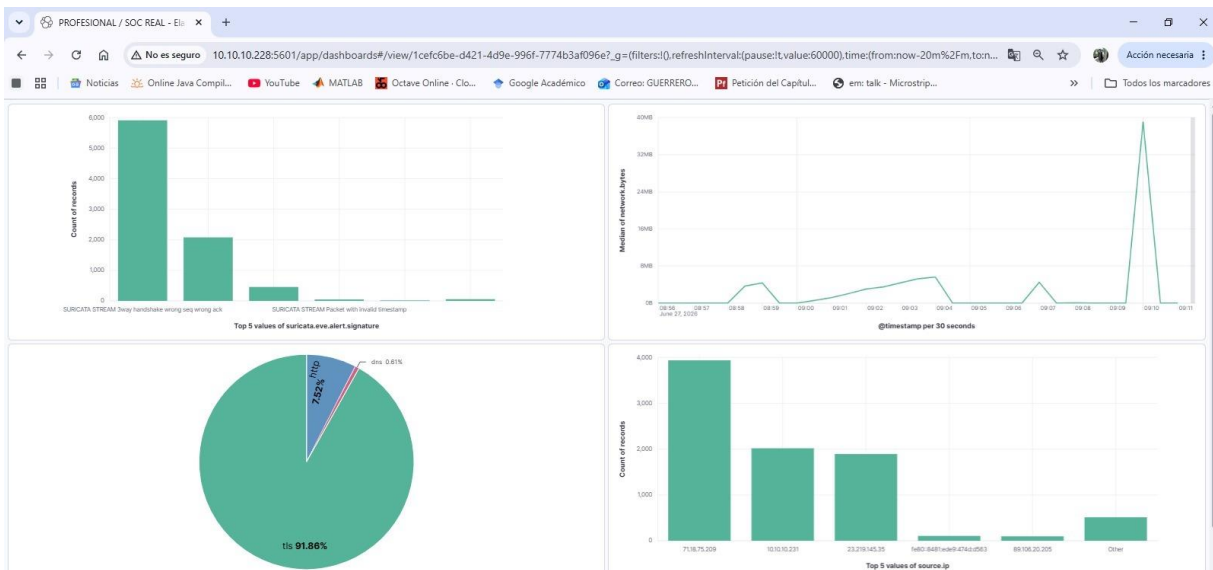
```
jerick@ids:~$ sudo nmap -sS 10.10.10.228
[sudo] password for jerick:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-06-27 09:14 -05
Nmap scan report for ids (10.10.10.228)
Host is up (0.000024s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
jerick@ids:~$
```

La Figura 47 muestra la ejecución del escaneo de puertos mediante Nmap desde la red hacia el host. Esta prueba permite determinar si el dispositivo objetivo está activo y qué servicios están expuestos, generando tráfico de escaneo SYN que puede ser interpretado por el IDS como actividad de reconocimiento dentro de la infraestructura de la organización.

Tras ejecutar la prueba, se confirmó en Kibana la existencia de eventos correspondientes al tráfico detectado por Suricata. Para ello se aplicó un filtro por eventos de tipo alerta, de modo que solo se mostraran los registros identificados como tales por el IDS.

Figura 48: Visualización de alertas generadas tras el escaneo con Nmap



En la Figura 48 se observan las alertas generadas por el IDS Suricata después del escaneo de puertos. El panel proporciona una visualización de los eventos relacionados con la actividad detectada, así como de los cambios en el tráfico observado durante el intervalo de tiempo utilizado para esta prueba. Esto aporta evidencia de que el sistema implementado es capaz de registrar y alertar sobre tráfico sospechoso dentro de una red inalámbrica.

Tabla 29: Resumen de la prueba de escaneo de puertos

Parámetro	Descripción
Herramienta utilizada	Nmap
Tipo de prueba	Escaneo SYN de puertos
Objetivo de la prueba	Generar tráfico de reconocimiento hacia un host de la red
Sistema de detección	Suricata IDS
Plataforma de visualización	Kibana
Resultado observado	Registro de eventos y alertas asociadas al tráfico generado
Evidencia obtenida	Visualización de alertas y variaciones de tráfico en el <i>dashboard</i>

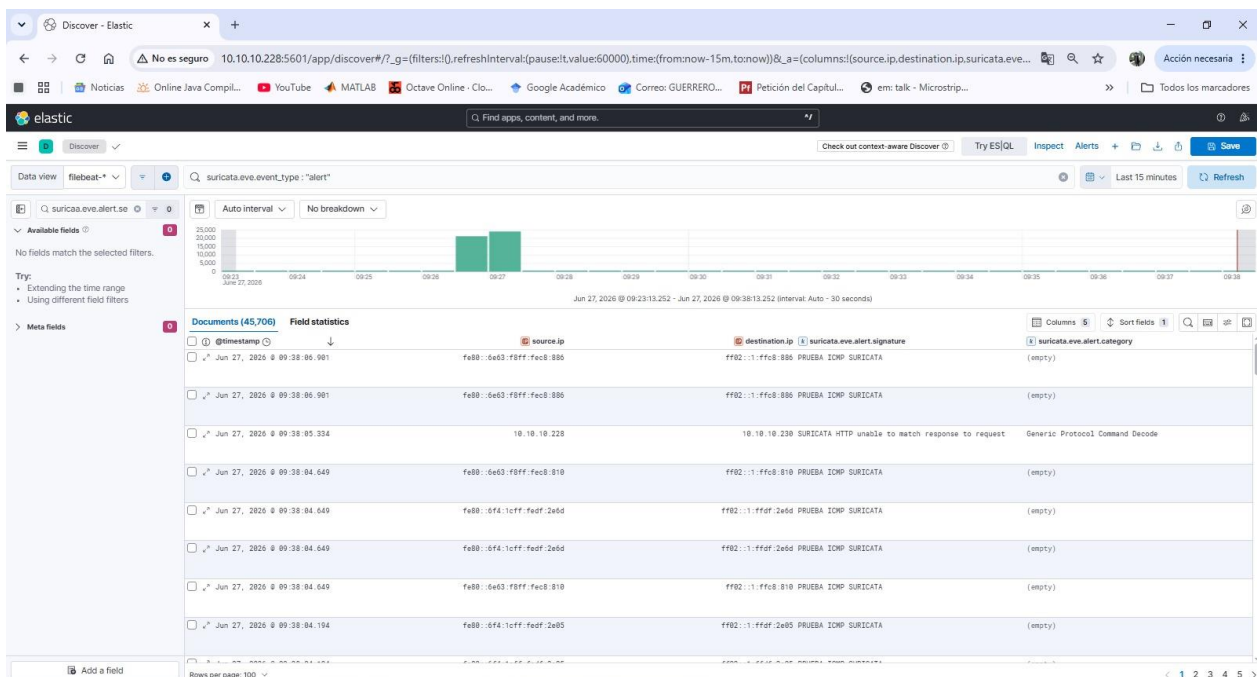
Los resultados obtenidos permiten comprobar que el IDS implementado respondió ante una prueba de reconocimiento de puertos, registrando eventos que posteriormente fueron visualizados en Kibana. Esta validación evidencia la integración funcional entre Suricata, Elasticsearch y Kibana para la detección y el análisis de tráfico potencialmente sospechoso.

4.2.2. Análisis técnico de las alertas registradas por Suricata IDS

Una vez ejecutada la prueba de escaneo de puertos y confirmados los eventos en el panel de Kibana, se analizaron en mayor profundidad las alertas generadas por Suricata IDS. Para ello se utilizó la herramienta Kibana Discover para inspeccionar los eventos almacenados en Elasticsearch y visualizar algunos de los campos técnicos que acompañan a cada evento.

Se utilizó un filtro de Suricata y el análisis se limitó a los eventos de tipo alerta: `eve.event_type : "alert"`. Con esta condición, se podían mostrar únicamente los registros generados por Suricata como alertas de seguridad, ignorando otros eventos (tráfico DNS, HTTP/TLS o flujos de red). De esta forma, se facilitó la revisión técnica de los eventos que resultaban realmente útiles para validar el IDS.

Figura 49: Detalle técnico de alertas registradas por Suricata IDS

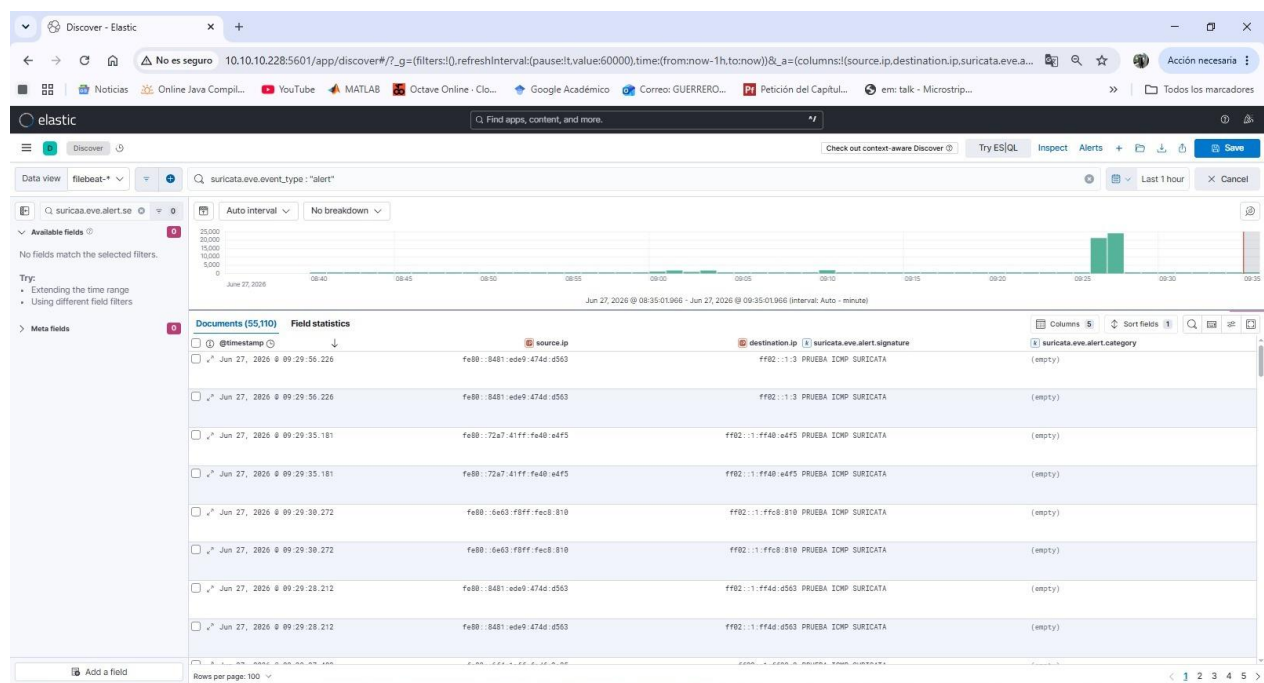


La Figura 49 muestra los detalles técnicos de las alertas generadas por Suricata IDS y visualizadas mediante Kibana Discover. Usando esa información, se identifican campos relevantes como la dirección IP de origen, la dirección IP de destino, la firma de la alerta, la marca de tiempo y el tipo de evento. Esta información se utiliza para analizar el origen y el destino del evento detectado, así como su tipo, dentro de una red supervisada.

Esta figura es importante porque permite comprobar que las alertas generadas por el IDS no solo aparecen en forma gráfica en el panel, sino que además se registran con mayor detalle técnico. Esto permite el análisis posterior de incidentes y proporciona la capacidad de relacionar eventos detectados con los equipos involucrados dentro de la infraestructura WISP.

Se revisaron las distribuciones basadas en el tiempo de las alertas registradas para observar la agrupación de eventos durante el periodo de prueba. Esta visualización permitió identificar momentos específicos con mayor actividad.

Figura 50: Línea de tiempo de alertas generadas por Suricata IDS



La Figura 50 presenta la cronología de alertas generadas por Suricata IDS. A través de los picos presentes en la gráfica, es posible identificar momentos de mayor actividad detectados por el IDS, lo cual resulta útil para correlacionar los eventos con las pruebas realizadas en la red.

Tabla 30: Herramienta utilizada para inspeccionar los eventos almacenados

Campo analizado	Descripción
suricata.eve.event_type	Identifica el tipo de evento registrado por Suricata IDS.
source.ip	Dirección IP del host que generó el tráfico detectado.
destination.ip	Dirección IP del host de destino involucrado en el evento.
suricata.eve.alert.signature	Firma o descripción de la alerta generada por Suricata.
@timestamp	Fecha y hora en la que se registró el evento.
Kibana Discover	Herramienta utilizada para inspeccionar los eventos almacenados.

Los principales campos técnicos observados durante el análisis de alertas en Kibana Discover se resumen en la Tabla 30. Estos campos permiten procesar de forma estructurada los eventos detectados por Suricata IDS y conocer con facilidad las características de cada detección:

el origen del tráfico, el destino involucrado, la firma que le corresponde y el momento exacto en que se activó la alerta.

De acuerdo con este análisis, se verificó que el sistema IDS implementado permite visualizar gráficamente las alertas y comprobar cada evento de forma individual. Esto mejora la capacidad de análisis del sistema, ya que proporciona valiosos detalles técnicos para la interpretación de incidentes en la red WISP.

4.2.3. Escenario de ataque controlado y análisis de tráfico en la infraestructura IDS WISP

Para ayudar a demostrar la capacidad de detección del sistema IDS desarrollado, se ejecutó un escenario de ataque controlado dentro del entorno del laboratorio WISP. Esta situación permite simular tráfico malicioso mediante herramientas de reconocimiento y generación de paquetes, además de comprobar cómo el sistema IDS Suricata responde a dicho tráfico y cómo se integra con la plataforma Kibana.

El escenario consistió en ejecutar un escaneo de red, generar tráfico anómalo y analizar los eventos obtenidos del monitoreo.

Figura 51: Ejecución de escaneo y generación de tráfico controlado mediante Nmap

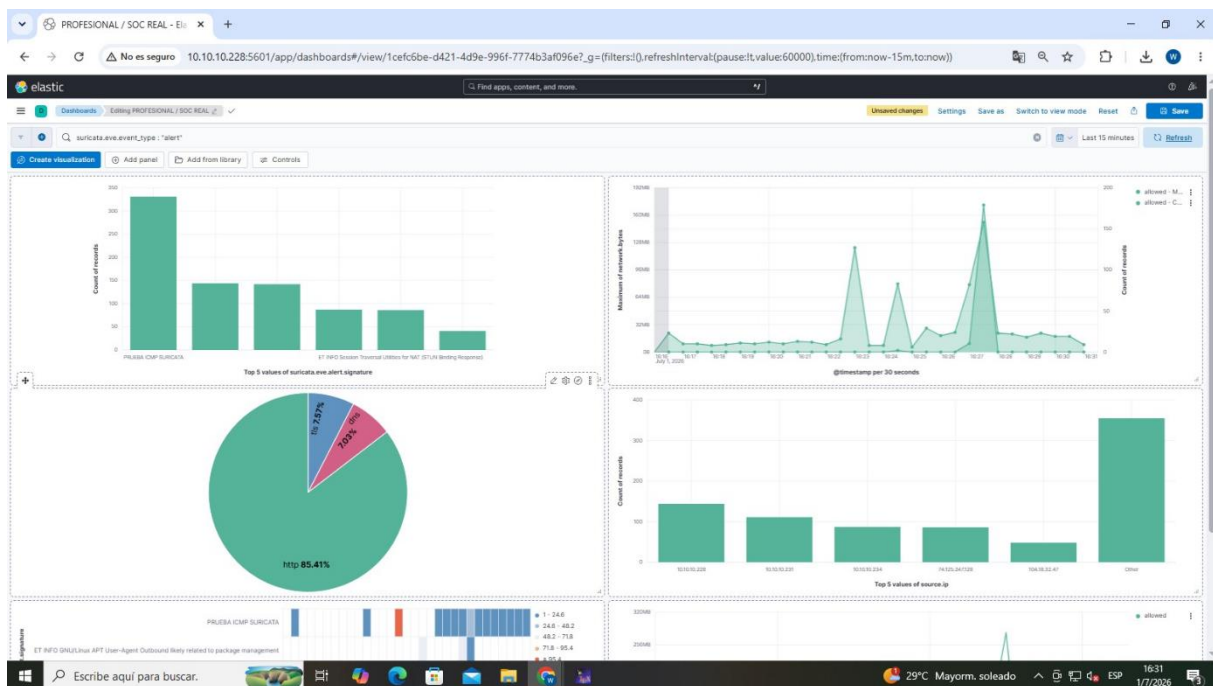
```
jerick@ids:~$ sudo nmap -A 10.10.10.228
[sudo] password for jerick:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-07-01 16:25 -05
Nmap scan report for ids (10.10.10.228)
Host is up (0.000073s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.16 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 ec:3e:ef:b9:34:14:e9:f7:dc:a0:2e:9e:41:e0:20:24 (ECDSA)
|_  256 a2:ef:44:03:1c:17:59:7e:ab:e1:7e:9d:17:0d:a1:0e (ED25519)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.89 seconds
jerick@ids:~$ sudo nmap -sS -Pn -p 1-1000 10.10.10.228
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-07-01 16:31 -05
Nmap scan report for ids (10.10.10.228)
Host is up (0.000024s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
jerick@ids:~$ sudo hping3 -S -p 80 --flood 10.10.10.228
HPING 10.10.10.228 (enp4s0 10.10.10.228): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Se realizó un escaneo de red utilizando Nmap con diferentes parámetros de reconocimiento, generando tráfico hacia el host objetivo dentro de la infraestructura WISP.

Figura 52: Visualización de eventos generados por Suricata IDS tras el ataque controlado



El sistema IDS registró eventos asociados al tráfico generado, lo que facilita la identificación de firmas de alerta y de comportamientos anómalos dentro de la red.

El filtrado de eventos permitió aislar únicamente las alertas de seguridad, reduciendo el ruido del tráfico general y facilitando el análisis de eventos relevantes para la evaluación del sistema IDS.

Tabla 31: Resumen del escenario de ataque controlado

Elemento	Descripción
Herramienta de ataque	Nmap / hping3
Tipo de ataque	Reconocimiento + <i>Flood</i>
IDS utilizado	Suricata
Plataforma	Kibana (ELK Stack)
Resultado	Detección exitosa de alertas

4.2.4. Escenario de saturación de tráfico y comportamiento anómalo en la red WISP

Luego, se ejecutó el segundo escenario de evaluación del desempeño para verificar cómo funcionaba el sistema IDS cuando hay una alta demanda de tráfico que ingresa a su interfaz de monitoreo. Este escenario permitió evaluar la detección del IDS frente a patrones de saturación y tráfico estable en la red WISP.

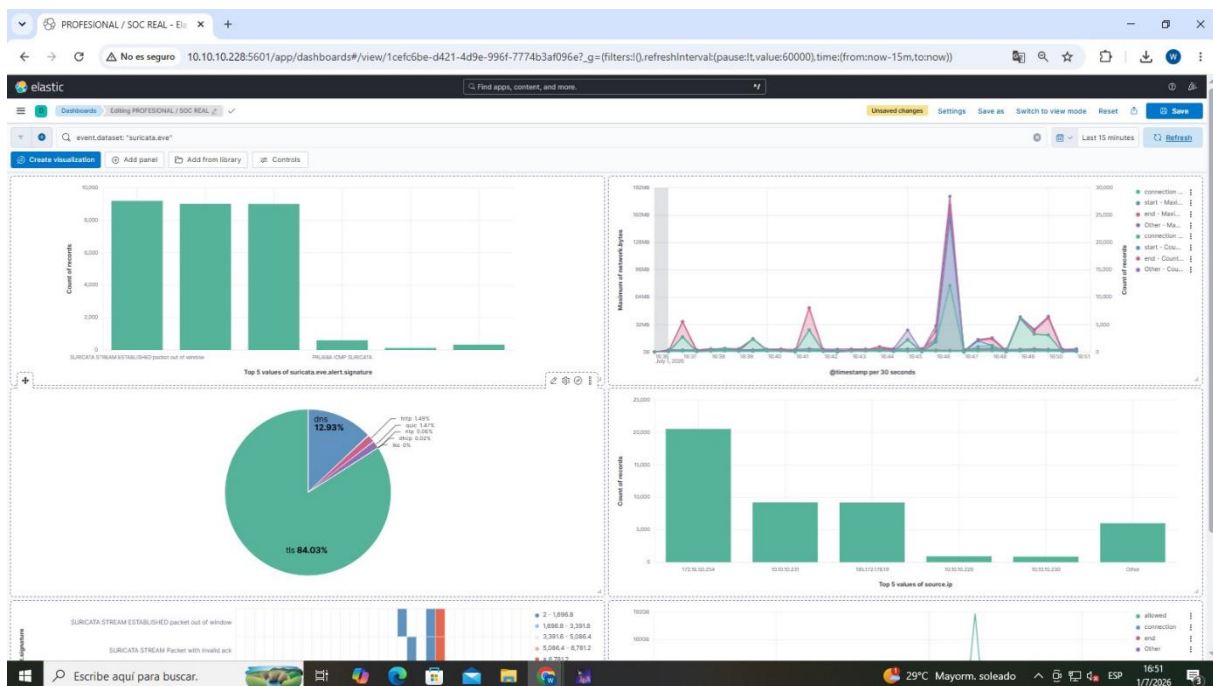
La prueba tuvo como objetivo crear condiciones de estrés controladas que permitan observar la reacción del sistema bajo una carga constante de solicitudes dirigidas a un servicio específico.

Figura 53: Generación de tráfico continuo hacia el servicio Kibana mediante saturación HTTP

```
jerick@ids:~$ while true; do curl http://10.10.10.228:5601; done
```

Se ejecutó un bucle continuo de solicitudes HTTP hacia la interfaz de Kibana, generando tráfico constante hacia el puerto 5601 del sistema IDS.

Figura 54: Comportamiento del tráfico y eventos generados durante el escenario de saturación



La visualización en Kibana permite observar un incremento sostenido en el volumen de tráfico, reflejado en picos de actividad y un aumento en la generación de eventos asociados a conexiones activas. Este comportamiento evidencia la capacidad del IDS para registrar condiciones de alta demanda dentro de la red.

4.3. Validación del sistema de notificación por correo electrónico

Como complemento al sistema de detección implementado con Suricata, se verificó el funcionamiento del mecanismo de notificación mediante correo electrónico, con el fin de comprobar que los eventos detectados dentro de la red WISP pudieran ser notificados automáticamente al administrador. Esta funcionalidad permite que el sistema no dependa solo de la visualización local de los eventos en Kibana, sino que envíe también alertas remotas en tiempo casi real.

El *script* de monitoreo se ejecutó con la finalidad de validar la lectura del archivo de eventos generado por Suricata (eve.json). El *script* mencionado monitoriza de forma continua los registros y, al detectar determinadas condiciones previamente definidas, crea un mensaje automático y lo envía al correo electrónico del administrador por medio del cliente de envío configurado en el servidor. Se comprobó que existe una integración funcional entre el IDS y el mecanismo de notificación externa.

Se comprobó la recepción de correos automáticos por actividad detectada en la red monitoreada. Entre los mensajes recibidos, se registró una notificación por actividad DNS y otra correspondiente a una alerta del IDS.

4.3.1. Notificación por actividad DNS detectada

Se utilizó la actividad DNS como primera evidencia para validar el sistema de notificación de un evento registrado dentro de la red monitoreada. Con este tipo de evento se verificó que el *script* de monitoreo fuera capaz de identificar los registros generados por Suricata relacionados con consultas de nombres de dominio y de activar el envío automático de una alerta al correo del administrador.

El monitoreo DNS es importante para el IDS, ya que permite identificar patrones de navegación, resolución de dominios y posibles comportamientos anómalos relacionados con consultas repetitivas o dominios inesperados dentro de la red WISP.

Figura 55: Notificación por actividad DNS detectada en la red WISP



En la Figura 55 se muestra el correo electrónico que el sistema envía automáticamente al administrador cuando se detecta actividad DNS en la red WISP. Esta evidencia comprueba el funcionamiento del mecanismo de notificación remota asociado al sistema IDS.

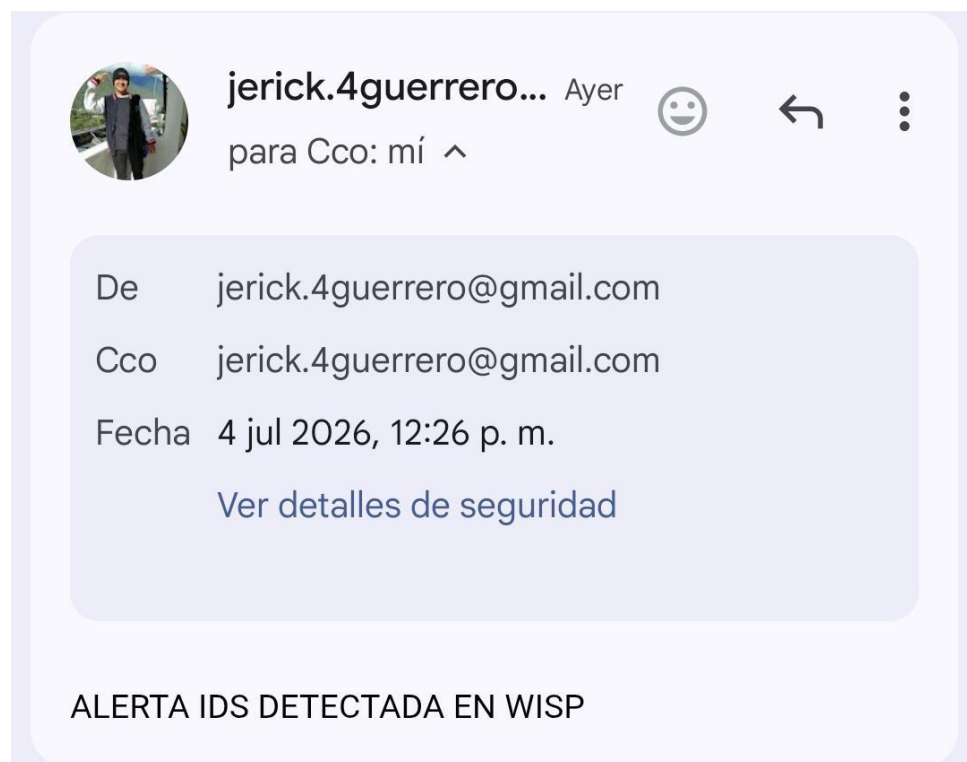
4.3.2. Notificación de alerta IDS detectada

Como segunda prueba de validación, se tomó una notificación producida a partir de una alerta registrada por el sistema IDS. Este tipo de evento, a diferencia de la actividad DNS, está directamente relacionado con una condición que Suricata detectó como alerta de seguridad. De

esta forma, es posible comprobar la capacidad del sistema para informar sobre eventos más relevantes dentro del tráfico que se monitorea.

La prueba permitió validar que el mecanismo de correo electrónico no solo responde ante eventos informativos, sino también ante alertas generadas por el IDS, reforzando la capacidad de supervisión del administrador ante posibles comportamientos sospechosos dentro de la infraestructura WISP.

Figura 56: Notificación de alerta IDS detectada en la red WISP



En la Figura 56 se observa el correo electrónico enviado automáticamente por el sistema ante una alerta detectada por el IDS.

La recepción de ambas notificaciones es evidencia de que el sistema implementado pudo completar satisfactoriamente el flujo de detección, registro y aviso. En primer lugar, Suricata identificó los eventos que estaban presentes en el tráfico de red; posteriormente, fue el *script* de

monitoreo el que procesó los registros generados y activó el envío automático de correos electrónicos. Esto refuerza la capacidad de respuesta del sistema propuesto, ya que permite alertar al administrador aun cuando este no se encuentre revisando la interfaz de monitoreo directamente.

4.3.3. Resumen de validación del sistema de notificación

El funcionamiento del mecanismo de notificación implementado se resume en la Tabla 32, donde se presentan los elementos evaluados durante la validación: la herramienta IDS utilizada, el archivo monitoreado, el canal de notificación, el cliente de envío y los resultados obtenidos.

La siguiente tabla recopila las evidencias recogidas y ayuda a comprender cómo funciona el sistema de notificaciones como un proceso complementario al monitoreo visual en Kibana.

Tabla 32: Resumen de la validación del sistema de notificación por correo electrónico

Elemento evaluado	Resultado observado
Herramienta IDS	Suricata
Archivo monitoreado	/var/log/suricata/eve.json
Medio de notificación	Correo electrónico
Cliente de envío	msmtp
Evento 1	Actividad DNS detectada en la red WISP
Evento 2	Alerta IDS detectada en la red WISP
Evidencia	Correos recibidos en la cuenta del administrador
Resultado final	Notificación automática validada correctamente

Los resultados obtenidos hacen posible afirmar que el mecanismo de notificación mediante correo electrónico funcionó correctamente dentro del entorno de prueba. Esta característica es un

valor agregado en la propuesta, ya que permite mejorar el monitoreo de la red WISP introduciendo una forma de aviso automático ante eventos detectados por el IDS, lo que fortalece la supervisión y la respuesta del administrador ante cualquier situación que se presente.

4.4. Análisis de métricas de red

Después de probar y validar la detección de eventos con Suricata IDS y examinar los registros técnicos en Kibana Discover, se procedió a analizar algunas de las métricas derivadas de los paneles creados. Estas métricas permiten determinar el estado de la red supervisada, identificar los hosts más activos y reconocer patrones en los eventos generados por el propio IDS.

Este análisis es relevante porque permite avanzar desde una visión general de los eventos hacia una comprensión más precisa de la evidencia recopilada. De este modo, el sistema no solo demuestra que existen alertas, sino que también identifica con claridad las tendencias, las direcciones IP más activas y los protocolos y firmas de alerta predominantes en la infraestructura WISP.

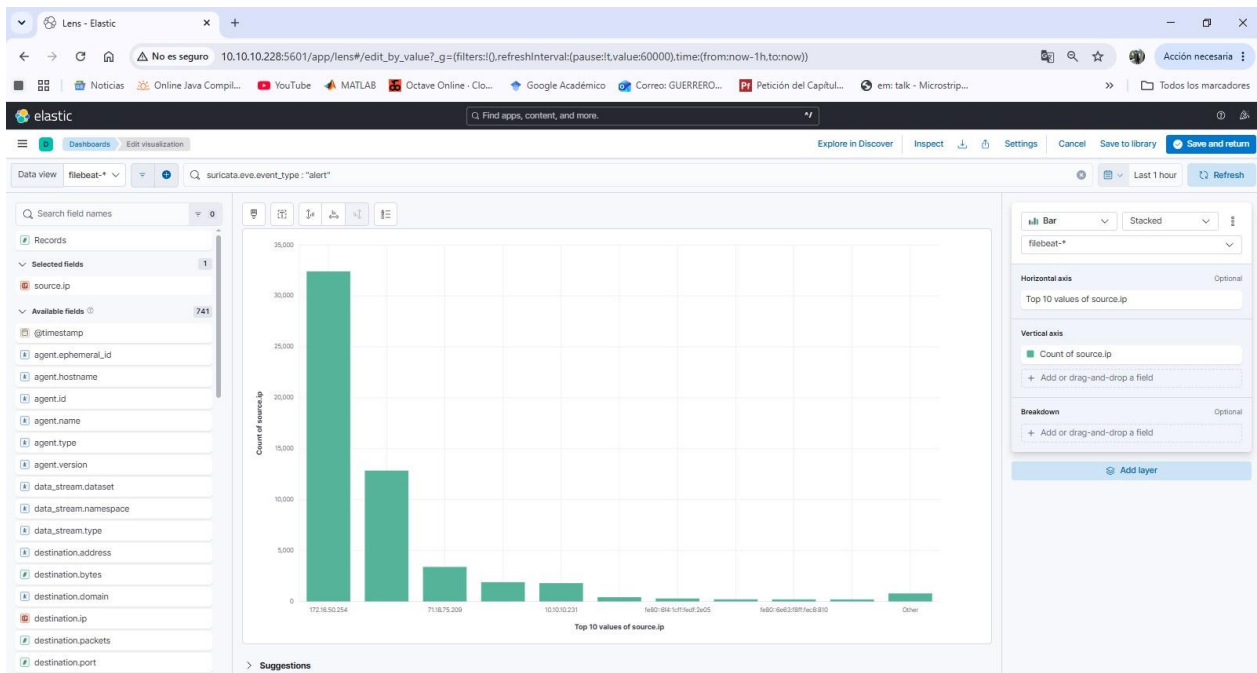
4.4.1. Distribución de alertas por dirección IP de origen

En esta sección se analiza la distribución de alertas generadas por el IDS según la dirección IP de origen, con el objetivo de identificar los hosts que presentan mayor actividad dentro de la red monitoreada.

Uno de los indicadores clave que se examina es cómo se distribuyen las alertas por dirección IP de origen. La visualización permite identificar con precisión qué hosts generan más eventos en la red supervisada, lo cual es útil para detectar posibles dispositivos anómalos o con una mayor participación en el tráfico que está siendo capturado por el IDS.

En este caso, se aplicó el filtro Suricata para visualizar los datos a través de Kibana Lens: `eve.event_type: "alert"`, agrupando por el campo `source.ip`. Se obtuvo un gráfico de las direcciones IP de origen con la mayor cantidad de alertas registradas durante el período considerado.

Figura 57: Distribución de alertas por dirección IP de origen



Estos datos se agregan posteriormente en función de la dirección IP de origen y se muestran en la Figura 57. Esto permite visualizar qué hosts generaron la mayor cantidad de eventos detectados por Suricata IDS. El valor de esta figura es que ayuda a identificar los dispositivos con mayor actividad en la red, que pueden estar asociados con tráfico legítimo frecuente, pruebas controladas o comportamientos potencialmente sospechosos.

La información adquirida a partir de esta métrica contribuye al análisis de alertas, en la medida en que identifica no solo la firma del evento, sino también el origen del tráfico que generó esos registros. Esto ayuda a comprender el comportamiento de la red WISP y mejora la capacidad de análisis en un sistema IDS.

Tabla 33: Interpretación de la métrica de alertas por IP de origen

Elemento analizado	Descripción
Campo utilizado	source.ip
Filtro aplicado	suricata.eve.event_type: "alert"
Métrica empleada	Conteo de registros
Objetivo del análisis	Identificar hosts con mayor generación de alertas
Herramienta utilizada	Kibana Lens
Utilidad del resultado	Reconocer equipos con mayor actividad o posible comportamiento anómalo

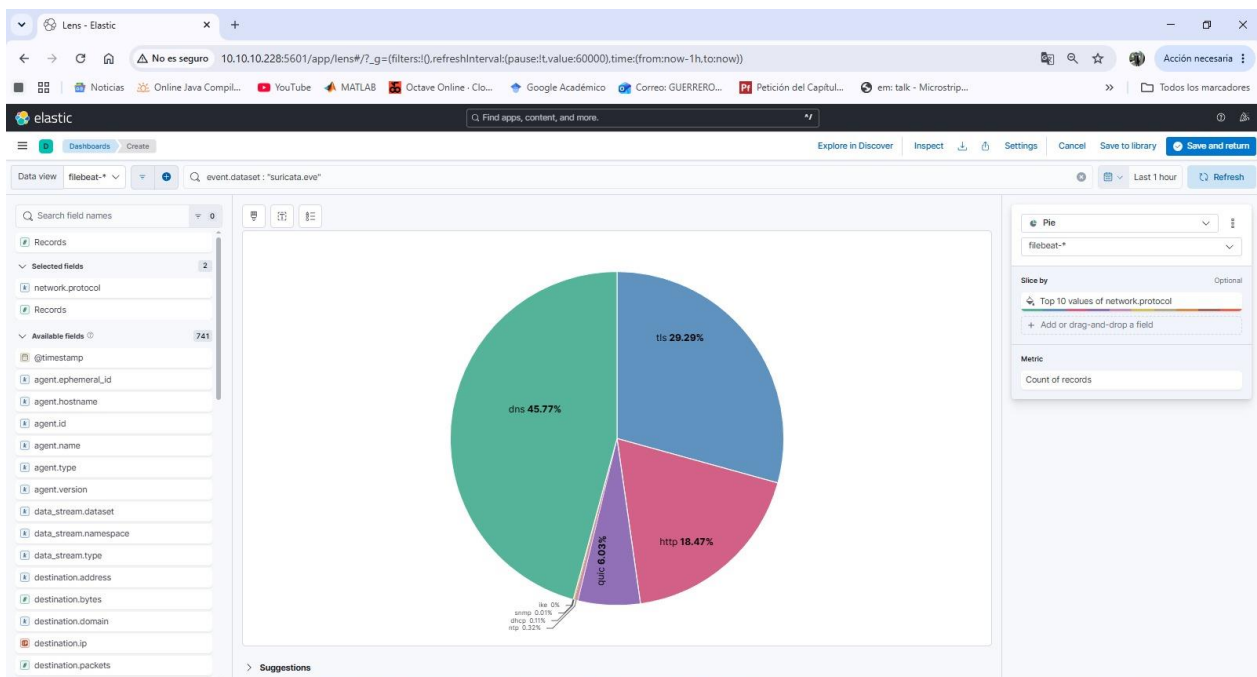
En la Tabla 33 se resumen los elementos utilizados para analizar la distribución de alertas por dirección IP de origen. Esta métrica permite correlacionar los eventos identificados por Suricata con los sistemas que generaron el tráfico y establecer qué hosts resultan relevantes dentro del monitoreo.

Mediante este análisis, se puede observar que Kibana organiza los eventos generados por el IDS de una manera más ordenada y permite identificar las IP con mayor participación en las alertas registradas. Esto ayuda a priorizar los sistemas específicos sobre los cuales se debe realizar el análisis.

4.4.2. Distribución de protocolos detectados por el IDS

La segunda métrica analizada en Kibana es la distribución de protocolos reconocidos por Suricata IDS durante el tiempo de monitoreo. Este análisis permitió identificar los tipos de tráfico que circulan en la red WISP, como DNS, HTTP, TLS, TCP u otros protocolos relacionados con el funcionamiento estándar de la infraestructura monitoreada.

Figura 58: Distribución de protocolos de red identificados por el IDS



En la Figura 58 se observa la distribución de los protocolos identificados por Suricata IDS en la red monitoreada. Esta visualización muestra distintos tipos de tráfico, lo que indica que el IDS no solo registra alertas, sino que también clasifica eventos relacionados con la actividad general en la red.

Esta métrica es importante porque proporciona información sobre el tráfico que circula por la infraestructura WISP. La clasificación de protocolos como DNS, HTTP o TLS permite distinguir la navegación web, la resolución de nombres y las conexiones seguras establecidas por los hosts conectados a la red.

Tabla 34: Parámetros utilizados para el análisis de protocolos

Elemento analizado	Descripción
Campo utilizado	network.protocol o suricata.eve.proto
Filtro aplicado	event.dataset: suricata.eve
Métrica empleada	Conteo de registros
Tipo de visualización	Gráfico circular o gráfico de barras
Objetivo del análisis	Identificar los protocolos predominantes dentro del tráfico monitoreado
Herramienta utilizada	Kibana Lens

Las dimensiones utilizadas para construir la visualización de los protocolos detectados por el IDS se resumen en la Tabla 34. Esta métrica permite comprender el tipo de tráfico que circula por la red WISP y ofrece una visión agregada del comportamiento de los servicios utilizados por los hosts monitoreados.

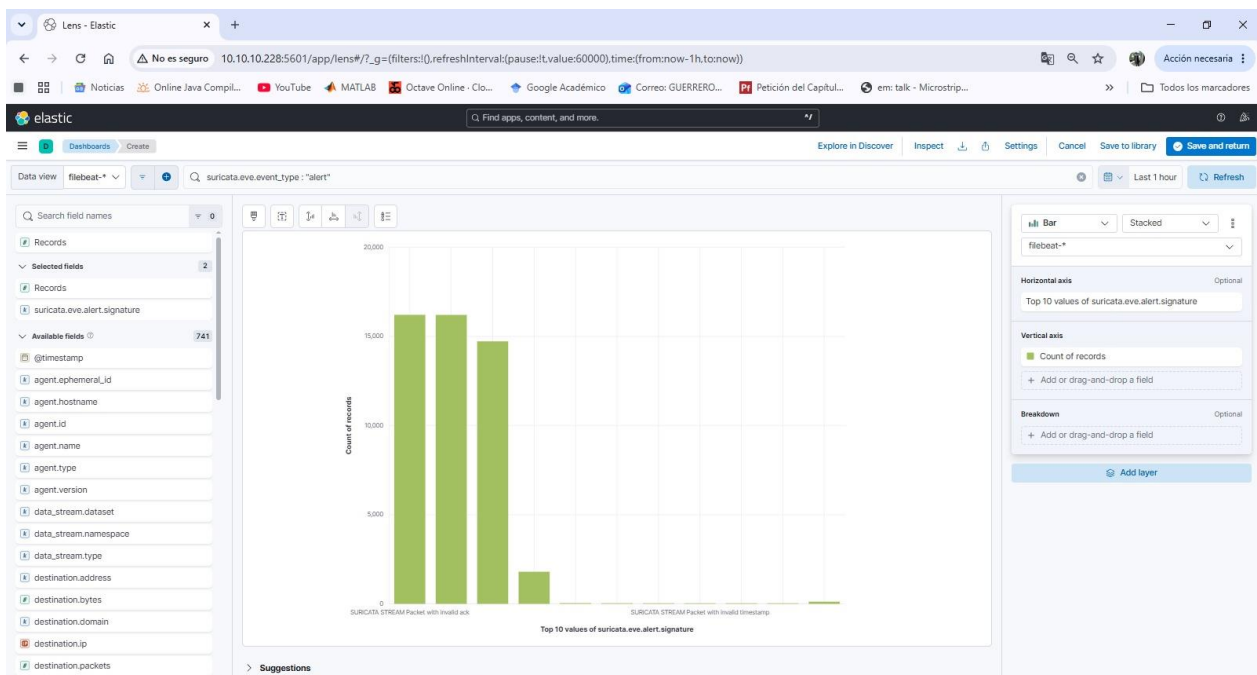
La plataforma IDS implementada no solo permite analizar eventos de seguridad, sino también caracterizar aspectos generales del tráfico de red. Esto hace que la monitorización sea más sólida al permitir caracterizar el comportamiento normal e identificar posibles anomalías.

4.4.3. Análisis de las principales firmas de alerta detectadas

La correlación cruzada de las firmas de alertas generadas por Suricata IDS permitió identificar qué eventos de seguridad estaban más presentes durante el período monitoreado. Esta sección se centra en el comportamiento relevante para la seguridad de la red WISP y no en las métricas generales del tráfico.

Se utilizó Kibana Lens para agrupar los registros por el campo `eve.alert.signature`, aplicando el filtro `suricata.eve.event_type: "alert"`. Esta configuración permitió generar visualizaciones con las firmas más frecuentes detectadas por el IDS y dar visibilidad a los patrones presentes en el tráfico ICMP, flujos TCP, eventos de conexión y posibles comportamientos atípicos.

Figura 59: Principales firmas de alerta detectadas por Suricata IDS



Las principales firmas de alerta que Suricata IDS señaló durante el período de análisis se ilustran en la Figura 59. Esta visualización muestra qué tipo de eventos se detectaron con mayor frecuencia, un aspecto clave para comprender el estado de seguridad de la red supervisada.

Esto indica que el IDS puede identificar múltiples clases de tráfico, etiquetar y registrar eventos para su posterior inspección, específicamente firmas relacionadas con pruebas de ICMP, eventos de flujo TCP o anomalías de conexión. Estos datos permiten distinguir entre el tráfico de diagnóstico, la actividad de conexión habitual y las señales de comportamiento potencialmente sospechoso.

Tabla 35: Interpretación de las principales firmas de alerta detectadas

Firma de alerta	Tipo de evento	Interpretación
ICMP TEST	Tráfico ICMP	Pruebas de conectividad detectadas correctamente
STREAM ESTABLISHED	Flujo TCP	Conexiones TCP normales monitoreadas
STREAM anomaly	Anomalía TCP	Posibles irregularidades en el flujo de datos
BAD WINDOW	TCP	Comportamiento anómalo en sesión TCP
UPDATE		
Otras firmas	General	Eventos adicionales del sistema IDS

La interpretación de las firmas de alerta, que asocia cada evento detectado con el tipo de tráfico que lo origina, se presenta en la Tabla 35. De este modo, la tabla traduce los registros detectados por el IDS en información que puede interpretarse para la evaluación de seguridad.

Esto constituye una ventaja clave, ya que el sistema no solo registra eventos de red, sino que también los categoriza según las firmas conocidas de Suricata. Esta capacidad fortalece el análisis del IDS, pues facilita la identificación de patrones de comportamiento y la priorización de los eventos que requieren una revisión adicional.

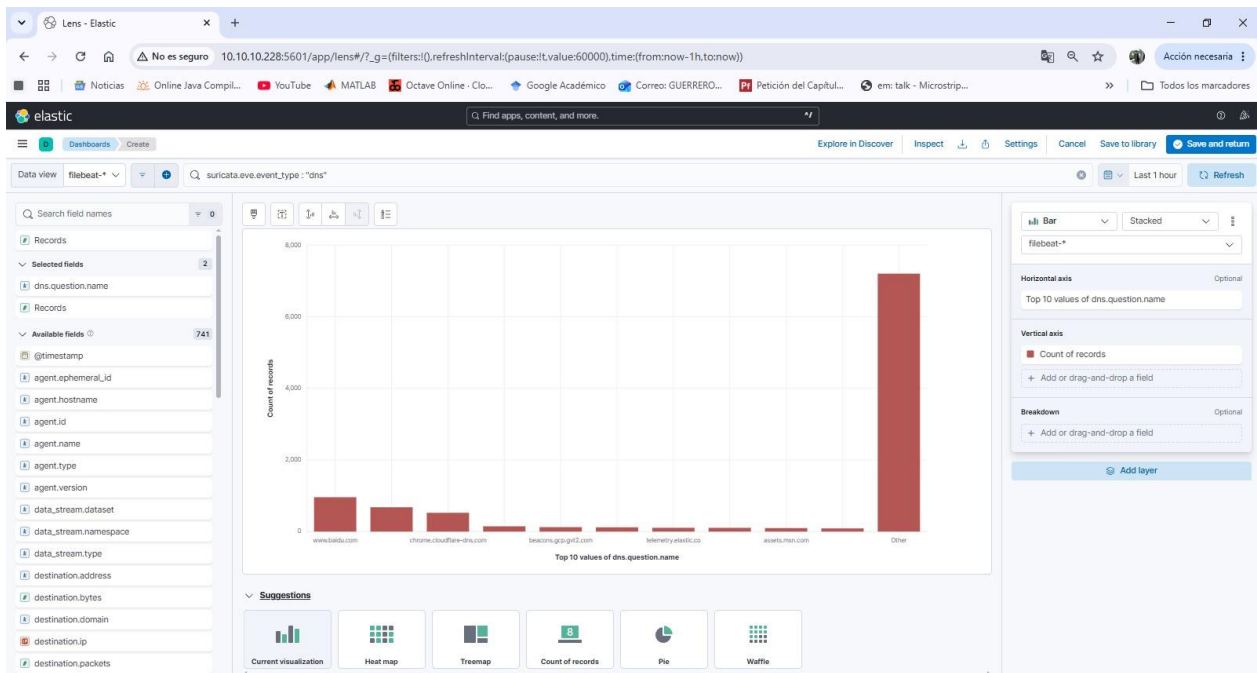
4.4.4. Análisis de consultas DNS registradas por el IDS

El análisis del tráfico DNS permitió identificar qué hosts, locales o externos, realizaron resoluciones de dominio en la red WISP durante el período de monitoreo. Esta información resulta relevante, ya que las consultas DNS permiten conocer los dominios a los que los hosts conectados realizaron solicitudes, así como parte de su comportamiento de navegación dentro de la infraestructura.

En este caso se utilizó Kibana Lens para agrupar los eventos DNS por el campo **dns.question.name**. Esta métrica permitió evaluar los dominios más consultados, una visión

general que complementa el análisis de alertas, ya que no se limita a los eventos de seguridad, sino que también permite observar los patrones normales de uso de la red.

Figura 60: Análisis de consultas DNS generadas en la red monitoreada



En la Figura 60 se muestran los nombres de dominio más consultados por los equipos monitoreados. La variedad de servicios asociados a los dominios indica que el IDS logró registrar el tráfico DNS real que atraviesa la red WISP. Esta información permite ver cómo los hosts resuelven nombres con el fin de utilizar recursos en Internet.

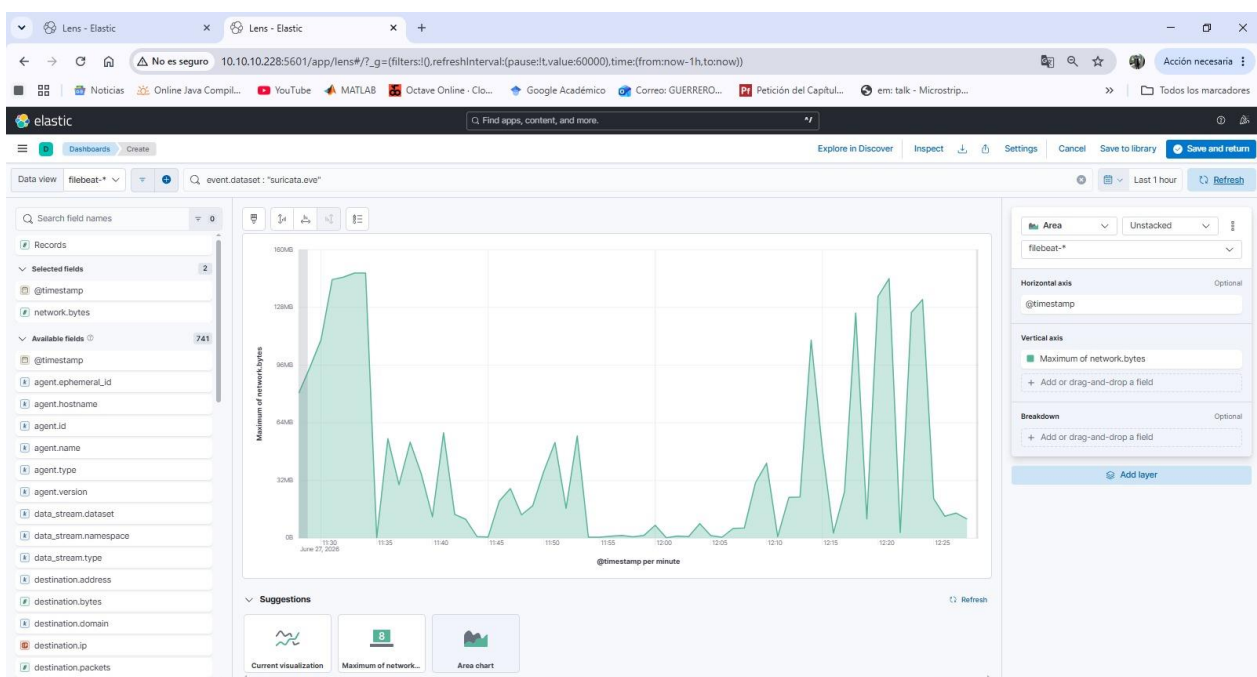
El análisis DNS es útil para el monitoreo porque permite comprender qué patrones de navegación predominan, qué dominios se resuelven con mayor frecuencia y qué comportamientos resultan inusuales. En el contexto de la red WISP, esta información ayuda a identificar actividades anómalas, consultas repetitivas o accesos a dominios inesperados.

4.4.5. Comportamiento del tráfico de red en la infraestructura WISP

El comportamiento del tráfico de red fue capturado y analizado para observar las variaciones del volumen de datos transferidos durante el período de monitoreo. Mediante esta métrica, se pudieron identificar los momentos de mayor actividad en la infraestructura WISP y caracterizar la carga de tráfico generada por los hosts conectados, en relación con los eventos registrados por el IDS.

Este análisis se centró en el comportamiento de toda la red (y no solo en visualizaciones centradas en alertas). Para ello, se observó el uso real de la infraestructura, lo que permitió identificar picos de tráfico y fluctuaciones mediante la métrica de bytes en función del tiempo.

Figura 61: Análisis del comportamiento del tráfico de red en la infraestructura WISP



Según las mediciones del IDS, el tráfico varió considerablemente durante el período analizado, tal como se aprecia en la Figura 61. Estos picos reflejan ráfagas de actividad en la red, que pueden referirse a actividades de navegación web, consultas DNS (sistema de nombres de

dominio), transferencia de datos (subida o descarga de archivos), conexiones seguras o pruebas controladas realizadas durante la validación del sistema.

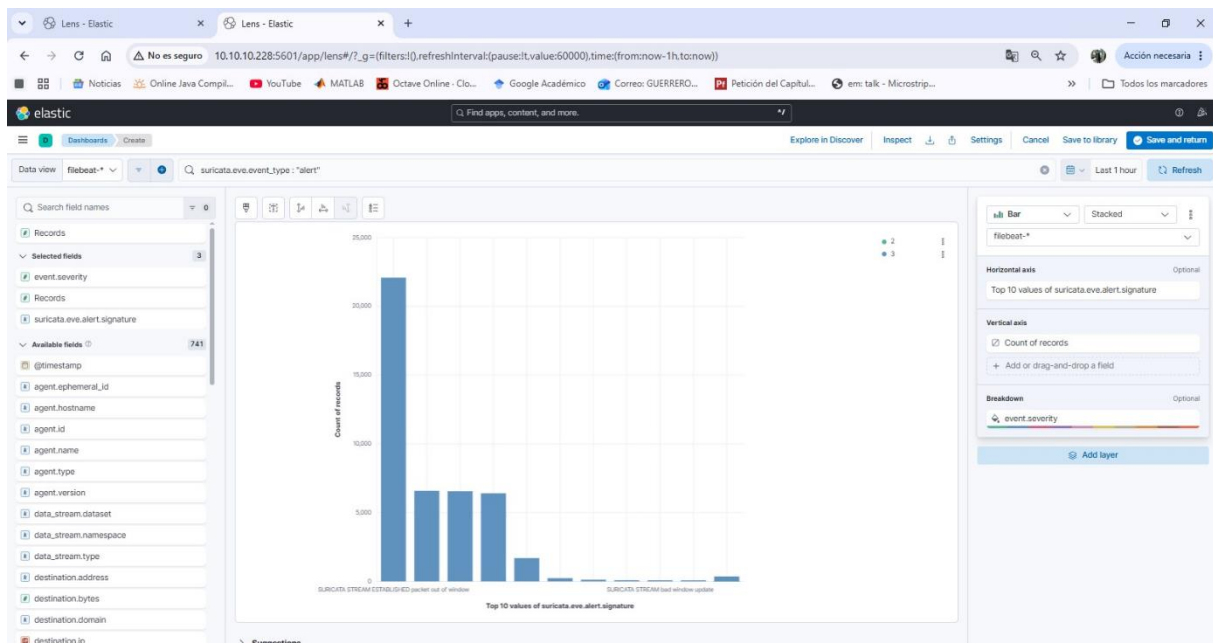
Esta información permite interpretar el comportamiento dinámico de la red WISP desde una perspectiva de monitoreo. Esto es útil para correlacionar la actividad de los usuarios con los eventos generados por Suricata (por ejemplo, alertas, comportamiento anómalo). Para ello se estableció la misma ventana de tiempo en ambos indicadores, lo que permitió observar el incremento del tráfico asociado a estos eventos.

4.4.6. Caracterización de eventos predominantes del IDS

Al examinar las firmas de alerta emitidas por Suricata IDS, es posible saber no solo cuántos eventos se registraron, sino también el tipo de tráfico predominante en la infraestructura monitoreada. Aquí se identificó la distribución de los eventos y, de forma paralela, se examinaron la firma de alerta y el nivel de severidad.

En contraste con las métricas anteriores basadas en direcciones IP o protocolos, este análisis se centra en los eventos registrados por el IDS interno sobre el tráfico entrante, con el fin de crear una base para reconocer patrones recurrentes de ocurrencias en la red WISP.

Figura 62: Correlación general del tráfico y eventos generados por el IDS en la infraestructura WISP



Hallazgos principales observados en la visualización:

- Se evidencia una alta concentración de eventos asociados a “SURICATA STREAM ESTABLISHED”, lo que indica predominancia de conexiones TCP establecidas.
- Eventos como “packet out of window” aparecen en menor proporción, asociados a comportamiento anómalo en flujos TCP.
- Las alertas de tipo “bad window update” presentan baja frecuencia, pero son relevantes desde el punto de vista de la integridad de la conexión.
- La severidad predominante corresponde a niveles intermedios (2 y 3), lo cual indica eventos de tipo informativo y de advertencia, más que críticos.

Tabla 36: Resumen cuantitativo de firmas detectadas

Firma de alerta	Frecuencia aproximada	Interpretación
SURICATA STREAM ESTABLISHED	Alta (~20k+)	Conexiones TCP normales establecidas
packet out of window	Media (~6k)	Posible desorden en flujo TCP
SURICATA STREAM bad window update	Baja (<1k)	Anomalía en actualización de ventana TCP
Otras firmas menores	Residual	Eventos no dominantes en el tráfico

Así, el comportamiento observado es tal que la red parece tener tráfico TCP legítimo, pero los eventos se generan a partir de la inspección profunda de flujos realizada por el IDS. Las alertas no representan ataques reales, sino variaciones de los eventos que cabe esperar en conexiones con estado y en el análisis de flujos.

Tabla 37: Distribución de severidad observada

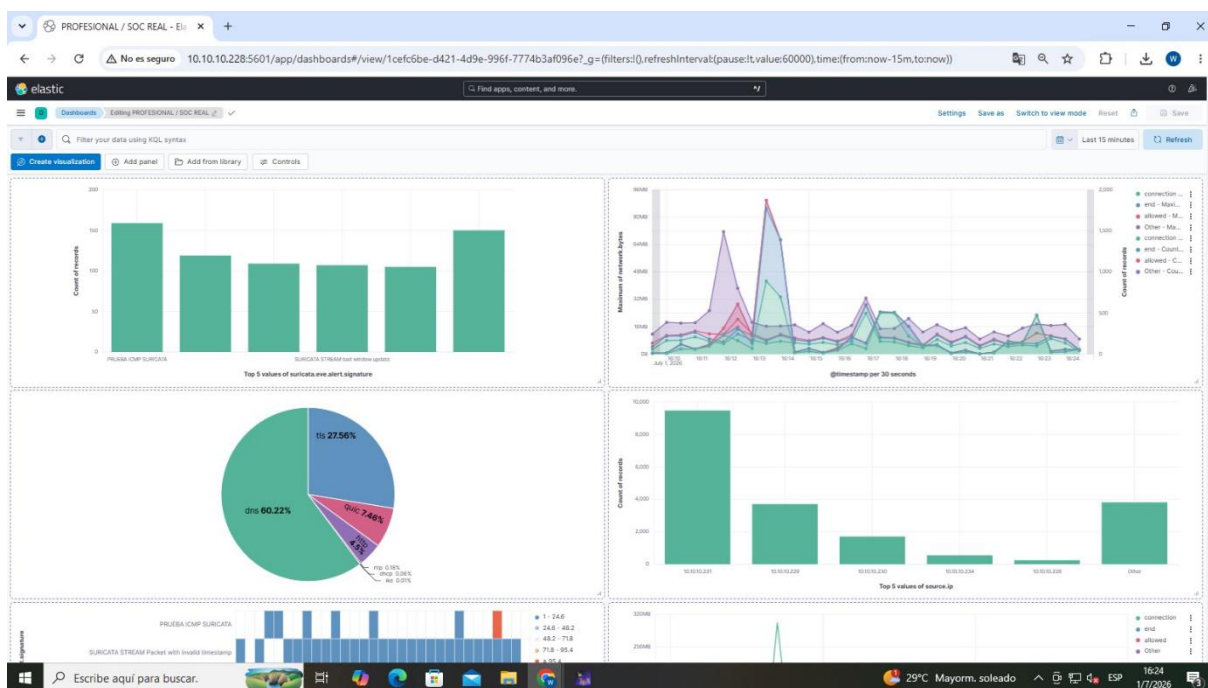
Nivel de severidad	Comportamiento asociado	Presencia
Nivel 2	Eventos informativos	Alta
Nivel 3	Eventos de advertencia	Media
Nivel 1	Eventos bajos o de diagnóstico	Baja

Este tipo de resultado ocurre en entornos de monitorización pasiva, donde el IDS no solo detecta ataques, sino que también registra lo que ocurre internamente con las condiciones del tráfico, permitiendo evaluar la estabilidad, el orden y la coherencia de las conexiones.

4.4.7. Comparación del comportamiento del tráfico en la vista general y con filtrado de alertas IDS

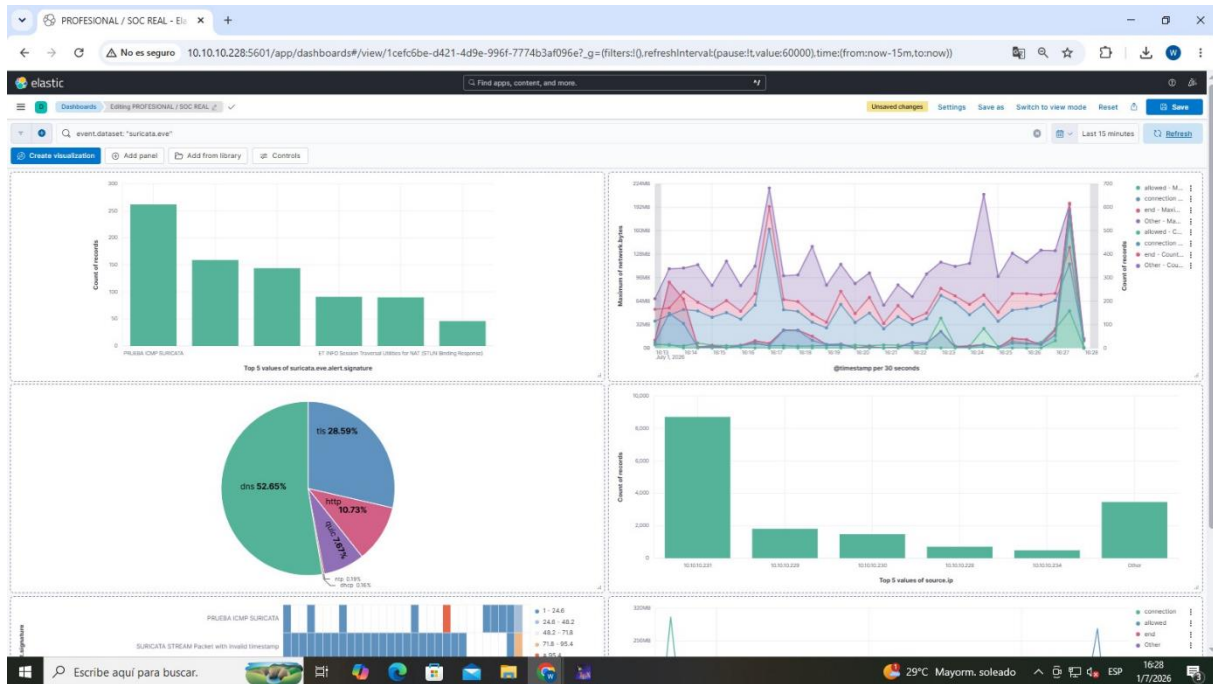
Para analizar con más detalle el comportamiento del IDS, se comparó el tráfico mostrado en Kibana bajo dos condiciones: una vista general de la red y una vista filtrada únicamente con los eventos de alerta generados por Suricata.

Figura 63: Visualización general del tráfico de red en Kibana



Esta vista muestra de forma explícita el comportamiento del tráfico de red, incluidos protocolos, conexiones, direcciones IP y volumen de datos a lo largo de todo el período analizado, sin aplicar ningún filtro de seguridad en particular.

Figura 64: Visualización filtrada de alertas generadas por Suricata IDS



Al aplicar el filtro de eventos de alerta se presenta únicamente el tráfico asociado a los eventos detectados por Suricata, de modo que el comportamiento de seguridad queda aislado dentro del conjunto total de datos.

Esto facilita la detección de patrones relevantes, ya que reduce el ruido del tráfico general y permite centrar el análisis en los eventos de seguridad.

Los resultados obtenidos permiten evidenciar que el sistema IDS implementado cumplió con las principales funciones planteadas en la propuesta, al permitir la captura pasiva de tráfico, el registro de eventos mediante Suricata, el almacenamiento de datos en Elasticsearch y la visualización de información en Kibana. También se agregó el sistema de notificación por correo electrónico, lo cual amplió la capacidad de respuesta del entorno, ya que los eventos relevantes se pudieron comunicar al administrador sin depender de la revisión manual del *dashboard*.

En líneas generales, se pudo comprobar que la arquitectura implementada permite observar el comportamiento del tráfico en la red WISP, identificar direcciones IP con mayor actividad, analizar protocolos predominantes, revisar firmas de alerta y validar escenarios controlados como escaneo de puertos, saturación de tráfico y generación de notificaciones automáticas. Los resultados obtenidos muestran que la propuesta no solo funciona como un sistema de monitoreo, sino que también sirve como herramienta de apoyo a la gestión y la seguridad de redes WISP en un entorno controlado.

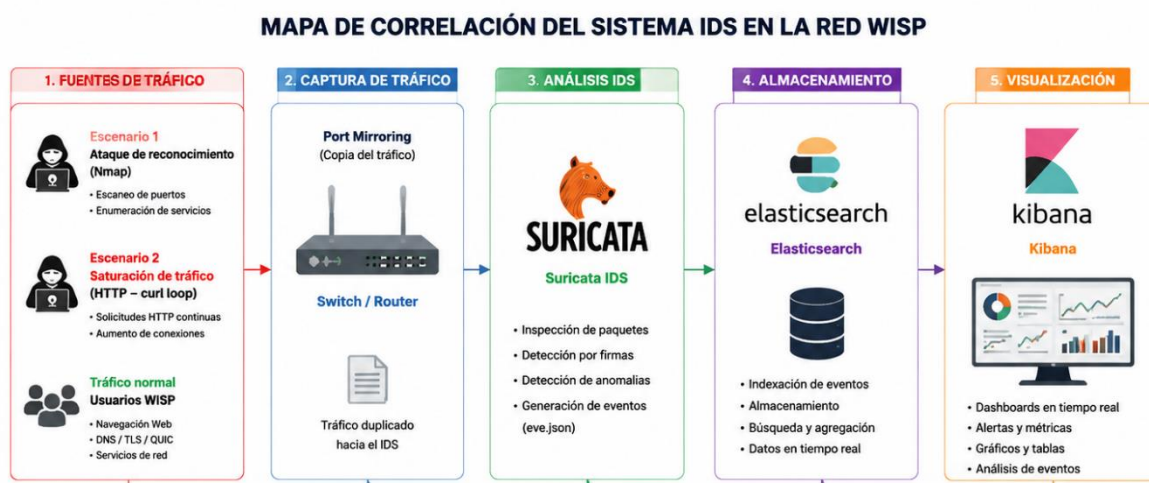
4.5. Correlación y validación integral del sistema IDS

4.5.1. Correlación global del comportamiento del sistema IDS en la red WISP

A partir de los resultados obtenidos en los escenarios de ataque controlado, en el análisis de tráfico y en las métricas de red generadas en Kibana, se realizó una correlación global del comportamiento del sistema de detección de intrusos (IDS) implementado en la infraestructura WISP.

Esta correlación busca integrar de forma estructurada los diferentes componentes del sistema, como la generación de tráfico, la captura por *Port Mirroring*, el análisis por Suricata IDS, el almacenamiento en Elasticsearch y la visualización en Kibana, para evidenciar la relación directa entre los eventos de red y su representación en la plataforma de monitoreo.

Figura 65: Mapa de correlación del sistema IDS en la red WISP



El mapa de correlación representa el flujo completo de operación del sistema IDS implementado, desde las fuentes de tráfico hasta la visualización de los resultados en tiempo real. Se identifican los siguientes componentes principales:

- **Fuentes de tráfico:** se contemplan escenarios de evento controlado como escaneo de puertos con Nmap, saturación de tráfico mediante peticiones HTTP continuas y tráfico normal generado por usuarios de la red WISP.
- **Captura de tráfico:** se logra con la técnica de *Port Mirroring* en el *switch* gestionable, lo que permite duplicar el tráfico hacia el sistema de análisis sin interferir con el funcionamiento de la red.
- **Análisis IDS:** Suricata se encarga de la detección de firmas, la inspección de paquetes y la generación de eventos de seguridad en un formato estructurado.
- **Almacenamiento:** se hace en Elasticsearch, donde los eventos son indexados para posteriores consultas y análisis.
- **Visualización:** se realiza mediante Kibana, donde se generan *dashboards* de tráfico, alertas, protocolos, IP y comportamiento de red en tiempo real.

La integración de los componentes anteriores permite establecer una relación directa entre la generación de tráfico en la red y la detección de eventos de seguridad. Los escenarios de ataque controlado permiten comprobar que el sistema IDS es capaz de identificar patrones de comportamiento anómalo, mientras que el tráfico normal de la red sirve como referencia.

También se comprueba que los eventos detectados por Suricata se guardan y muestran correctamente en Kibana, lo cual permite analizar de forma centralizada el comportamiento de la red WISP.

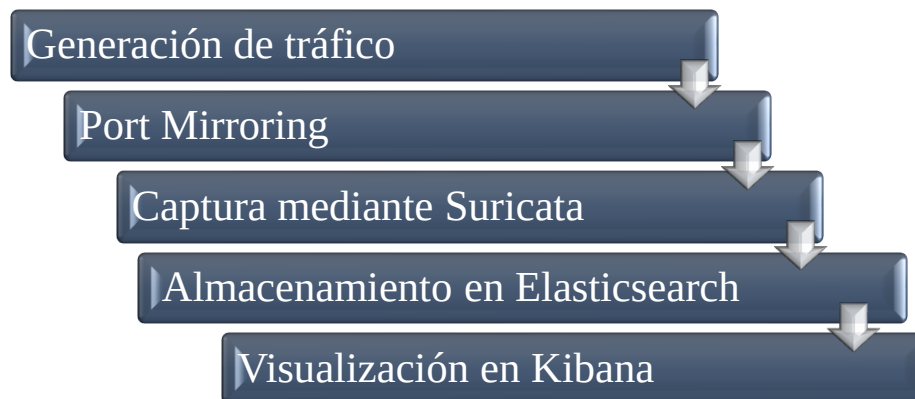
4.5.2. Validación funcional de la captura de tráfico

La validación funcional de la captura de tráfico consistió en verificar la capacidad del IDS en la infraestructura WISP para recuperar, analizar y presentar información a partir de paquetes de red.

Para esta prueba se validó el flujo completo de monitoreo definido en la arquitectura propuesta, junto con su configuración. Como parte de ella, el tráfico generado por los dispositivos de la red se replica mediante *Port Mirroring* en un *switch* administrado y se envía a un servidor IDS. Luego, Suricata inspecciona los paquetes, registra los eventos y los reenvía a Elasticsearch, donde se visualizan en Kibana.

Esta validación permite afirmar que el sistema funciona bajo un esquema de monitoreo pasivo, lo que significa que el IDS no interactúa directamente con ninguna comunicación de los usuarios, sino que analiza una réplica del tráfico sin afectar la operación normal de la red WISP.

El proceso evaluado se resume en la siguiente secuencia:



Para iniciar la validación funcional, se generó tráfico controlado mediante solicitudes ICMP desde un equipo cliente conectado a la infraestructura monitoreada. Esta prueba permitió

producir paquetes conocidos dentro de la red para verificar si los paquetes eran capturados, procesados y representados por el sistema IDS.

Figura 66: Generación de tráfico ICMP mediante prueba de conectividad

Los resultados obtenidos durante la prueba mostraron que el tráfico se generó correctamente y que se obtuvo una respuesta completa del destino evaluado. Esta prueba demostró que las comunicaciones estaban disponibles en el entorno de validación y proporcionó una entrada controlada de paquetes para su análisis por parte del sistema.

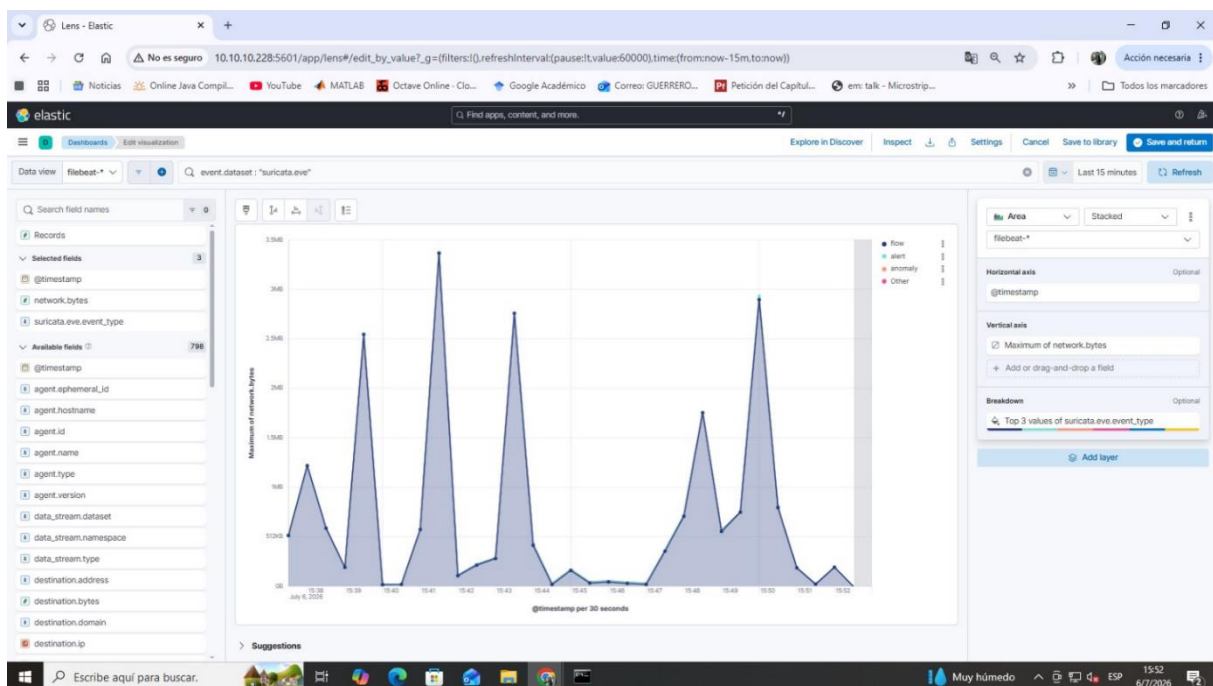
Parámetro	Resultado
Protocolo utilizado	ICMP
Cantidad de paquetes enviados	30

Cantidad de paquetes recibidos	30
Pérdida de paquetes	0 %
Tiempo promedio de respuesta	35 ms

La generación de este tráfico permitió continuar con la validación del proceso de captura realizado por Suricata mediante la interfaz conectada al puerto espejo del *switch*.

Después de generar el tráfico de prueba, se realizó una verificación para asegurar que los paquetes pudieran llegar al sistema IDS y ser analizados. Luego, se utilizó Kibana como capa de visualización de los datos almacenados por Elasticsearch a partir de los registros de Suricata. La visualización se construyó utilizando el campo **network.bytes** en función del tiempo mediante **@timestamp**, lo que permitió observar la variación del tráfico capturado durante el periodo evaluado.

Figura 67: Comportamiento del tráfico capturado por el sistema IDS mediante Kibana



Como se muestra en la Figura 67, el tráfico generado durante las pruebas puede rastrearse en los registros del sistema IDS. Los incrementos observados representan variaciones en el volumen de tráfico procesado por el IDS durante el periodo evaluado. Estos cambios evidencian que la captura mediante *Port Mirroring* permitió obtener visibilidad sobre la actividad generada dentro de la infraestructura WISP.

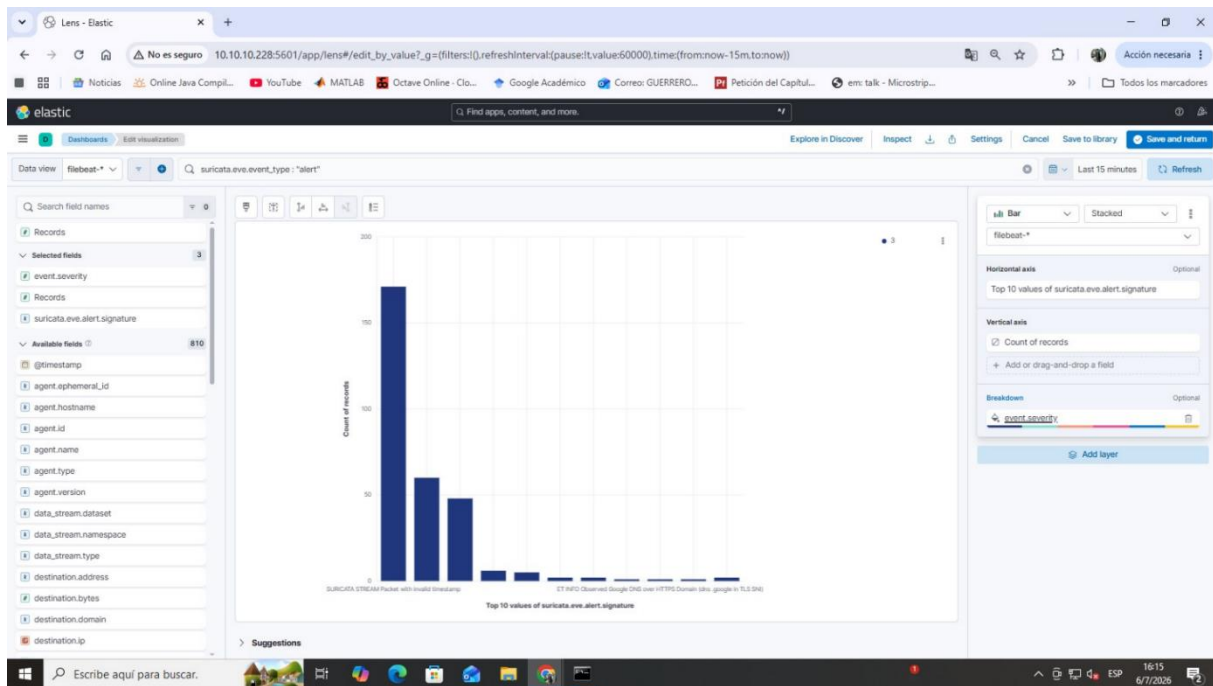
La existencia de registros asociados a distintos tipos de eventos evidencia que el sistema no solo recibe paquetes, sino que también realiza una clasificación inicial del tráfico capturado.

Después de comprobar la captura del tráfico, se evaluó la capacidad del sistema IDS para identificar eventos específicos mediante las firmas de detección configuradas en Suricata.

Para este análisis se aplicó el filtro **suricata.eve.event_type : "alert"**. Con ello se logró analizar únicamente los eventos clasificados como alertas de seguridad.

Posteriormente, se utilizó el campo **suricata.eve.alert.signature** para determinar las firmas con mayor frecuencia dentro del conjunto de eventos registrados.

Figura 68: Distribución de firmas de alerta detectadas por Suricata IDS



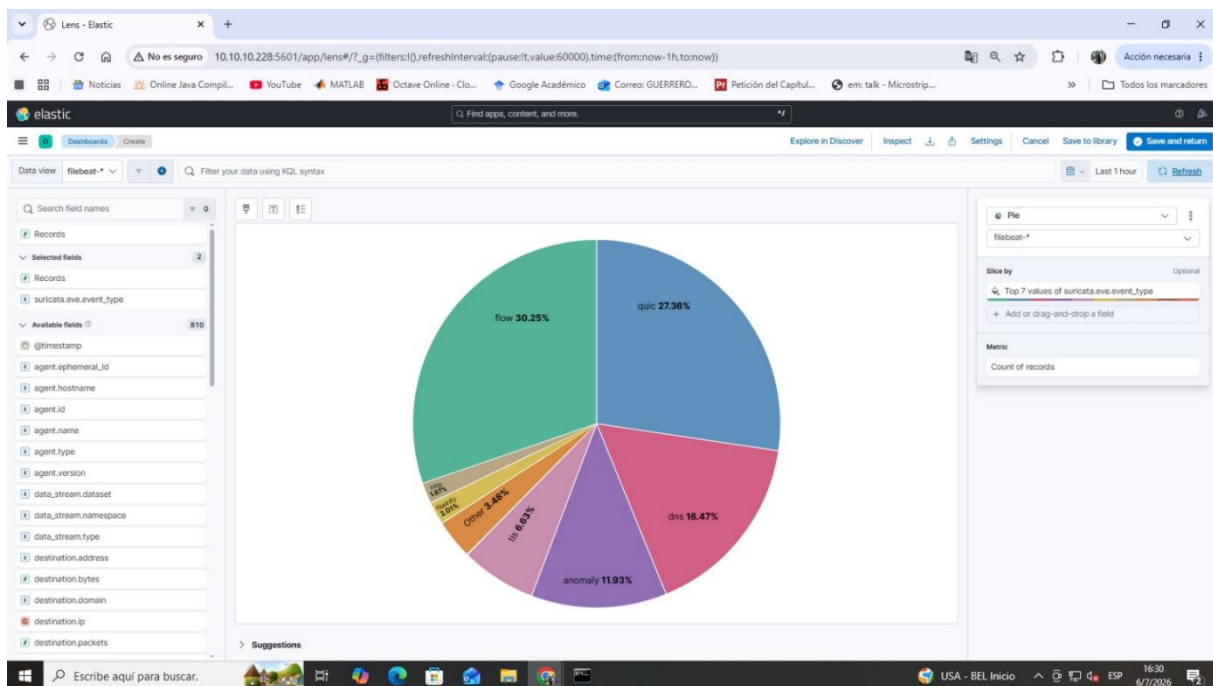
Los resultados muestran que Suricata clasificó el tráfico mediante las reglas de detección configuradas, permitiendo identificar eventos asociados tanto a comunicaciones normales como a comportamientos que requieren análisis adicional.

Estos datos indican al administrador qué eventos predominan en la red y ayudan a diferenciar el tráfico normal de los comportamientos anómalos que requieren una revisión más detallada.

Como complemento al análisis de firmas, se realizó una clasificación general de los eventos procesados por Suricata IDS, con el objetivo de identificar la distribución del tráfico registrado dentro de la infraestructura monitoreada.

Para ello, se utilizó el campo **suricata.eve.event_type**, lo que permitió clasificar los registros según su naturaleza, incluyendo eventos de flujo, DNS, TLS, QUIC, anomalías y alertas.

Figura 69: Distribución de eventos detectados por Suricata IDS



La distribución obtenida muestra que el IDS registra información sobre los distintos tipos de actividad presentes en la red. Los eventos relacionados con el flujo representan la mayor proporción debido al monitoreo continuo de las conexiones establecidas.

Los eventos DNS y TLS, junto con las anomalías registradas, permiten identificar los protocolos y patrones de comunicación detectados por Suricata.

Este resultado es esperado en un sistema IDS configurado en modo pasivo, debido a que la mayor parte del tráfico corresponde a comunicaciones establecidas que son registradas como flujos antes de generar una condición de alerta.

4.5.3. Resultado global de la validación del sistema IDS

La validación global del sistema IDS permitió integrar los resultados obtenidos durante los escenarios controlados, el análisis de métricas, las pruebas de captura de tráfico y la validación de

los mecanismos de visualización y notificación. A partir de estas evidencias se confirmó que la arquitectura implementada funciona de manera articulada, permitiendo capturar tráfico de red, procesarlo mediante Suricata, almacenar los eventos en Elasticsearch, visualizarlos en Kibana y generar notificaciones automáticas ante eventos relevantes.

El sistema desarrollado permitió establecer un flujo de monitoreo basado en captura pasiva mediante *Port Mirroring*, en el cual el tráfico generado dentro de la red es replicado hacia el servidor IDS sin alterar la comunicación principal de los usuarios. Posteriormente, Suricata procesó los paquetes capturados, generó eventos de seguridad y permitió su almacenamiento en Elasticsearch para su posterior visualización mediante Kibana.

Los resultados obtenidos permiten verificar cómo la solución presentada cumple funciones importantes de un IDS aplicado a una red WISP, las cuales son la visibilidad del tráfico, la detección de eventos relevantes y la generación de evidencia técnica necesaria para el monitoreo de la seguridad.

Tabla 39: Resumen de validación integral del sistema IDS implementado

Elemento evaluado	Método de validación	Evidencia obtenida	Resultado
Funcionamiento del motor IDS	Verificación del servicio Suricata	Servicio activo y procesamiento de eventos	Validado
Almacenamiento de eventos	Integración con Elasticsearch	Registros indexados correctamente	Validado
Visualización de información	<i>Dashboard</i> Kibana	Gráficos de tráfico, alertas y protocolos	Validado
Captura pasiva del tráfico	Configuración <i>Port Mirroring</i>	Recepción de copia del tráfico mediante puerto espejo	Validado
Detección de eventos controlados	Pruebas con Nmap y generación de tráfico	Alertas registradas por Suricata	Validado
Análisis de comportamiento de red	Métricas en Kibana	Distribución de IP, protocolos, firmas y eventos	Validado
Sistema de notificación	<i>Script</i> + cliente SMTP	Correos enviados ante eventos detectados	Validado

Correlación de información	Relación tráfico-alerta-visualización	Flujo completo del sistema IDS	Validado
-----------------------------------	---------------------------------------	--------------------------------	----------

La Tabla 39 resume la validación detallada del sistema IDS implementado y muestra que cada componente fue capaz de realizar la tarea prevista, tal como se especifica en el diseño propuesto.

La validación del motor Suricata aseguró que pudiera analizar el tráfico y generar registros vinculados a eventos de seguridad. Los datos recopilados durante el monitoreo también fueron almacenados, gracias a la integración con Elasticsearch, y posteriormente se visualizaron en Kibana mediante tableros que permitieron analizar el comportamiento de la red.

El esquema pasivo se verificó mediante la configuración de *Port Mirroring*, que proporcionó al IDS una copia del tráfico sin situarlo en la ruta principal de comunicación. En redes WISP, esta característica es clave, ya que añade una capa más de defensa sin cambiar los parámetros de latencia, disponibilidad o conectividad de los usuarios.

De acuerdo con las pruebas controladas realizadas mediante escaneo de puertos, generación de tráfico y análisis de eventos, Suricata pudo detectar patrones relacionados con el comportamiento generado durante esas pruebas y proporcionar información técnica como la dirección IP de origen, las firmas de alerta, los protocolos utilizados y las marcas de tiempo.

Los resultados obtenidos permitieron confirmar que el sistema IDS implementado cumplió con los objetivos planteados en la investigación, ya que fue capaz de integrar mecanismos de captura pasiva, análisis de tráfico, generación de alertas, almacenamiento de eventos y visualización gráfica.

La validación realizada demuestra que la arquitectura propuesta basada en Suricata, Elasticsearch y Kibana proporciona una solución funcional para mejorar la visibilidad y supervisión de una infraestructura WISP.

El mecanismo de notificación mediante correo electrónico amplía la capacidad de respuesta del sistema, permitiendo informar al administrador sobre eventos relevantes sin depender exclusivamente del monitoreo manual del *dashboard*.

La implementación del IDS dentro de la red WISP demuestra que una arquitectura basada en herramientas de código abierto puede proporcionar capacidades de monitoreo y análisis de seguridad adecuadas para entornos académicos y de laboratorio, permitiendo reproducir escenarios reales de detección y evaluación de amenazas.

Conclusiones

- ✓ La implementación del sistema IDS dentro de la infraestructura WISP permitió establecer una solución funcional para la captura, el análisis, la visualización y la notificación de eventos de red y seguridad. La arquitectura desarrollada integró Suricata, Filebeat, Elasticsearch y Kibana bajo un enfoque de monitoreo pasivo, demostrando que es posible fortalecer la supervisión de una red WISP sin alterar la operación normal del tráfico de los usuarios.
- ✓ El diseño lógico y físico de la red WISP permitió estructurar un entorno controlado con características similares a una infraestructura real de proveedor inalámbrico. La integración del *router* MikroTik, el *switch* gestionable TP-Link, los equipos inalámbricos Ubiquiti y el servidor IDS permitió organizar el flujo de tráfico, definir puntos de monitoreo y establecer una base técnica adecuada para evaluar eventos de seguridad dentro del laboratorio.
- ✓ La configuración del mecanismo de *Port Mirroring* en el *switch* gestionable permitió implementar una captura pasiva eficiente del tráfico. Esta técnica hizo posible replicar los paquetes hacia el servidor IDS sin ubicar el sistema de detección en la ruta principal de comunicación, evitando interrupciones, modificación de paquetes o degradación directa del servicio.
- ✓ La integración entre Suricata, Filebeat, Elasticsearch y Kibana permitió consolidar un flujo completo de tratamiento de eventos. Los registros generados por el IDS fueron recolectados, enviados, indexados y representados gráficamente, permitiendo transformar datos técnicos de bajo nivel en información visual útil para el análisis del comportamiento de la red.

- ✓ Las pruebas controladas mediante herramientas como Nmap, generación de tráfico controlado y pruebas ICMP permitieron evaluar la respuesta del sistema IDS ante escenarios reproducibles. El escaneo de puertos generó eventos asociados al reconocimiento de servicios, mientras que la saturación de tráfico y las pruebas de conectividad permitieron observar variaciones en el comportamiento de la red y validar la capacidad de registro del sistema.
- ✓ El análisis de las firmas detectadas por Suricata permitió diferenciar eventos asociados al tráfico normal, pruebas de conectividad y posibles condiciones anómalas. Esta clasificación resulta importante porque no toda alerta representa necesariamente un ataque crítico; algunas corresponden a comportamientos propios de conexiones TCP, pruebas ICMP o actividad esperada dentro de una red monitoreada.
- ✓ La comparación entre la visualización general del tráfico y el filtrado específico de alertas permitió evidenciar la importancia de separar el tráfico operativo de los eventos relevantes de seguridad. Esta diferenciación facilita reducir el ruido generado por la actividad normal de la red y enfocar el análisis en los eventos que requieren mayor revisión técnica.
- ✓ La prueba de tráfico ICMP permitió validar la existencia de comunicación efectiva dentro del entorno de evaluación. La ausencia de pérdida de paquetes y el tiempo promedio de respuesta obtenido demostraron que la red se encontraba operativa durante la validación, permitiendo utilizar dicho tráfico como base para verificar la captura y representación posterior en el sistema IDS.
- ✓ La distribución de eventos detectados por Suricata evidenció que el sistema no se limita únicamente a generar alertas de seguridad, sino que también permite caracterizar el tráfico

general de la red. La presencia de eventos de tipo flow, DNS, TLS, QUIC, alert y anomaly demuestra que el IDS proporciona visibilidad sobre diferentes capas del comportamiento de la infraestructura.

Recomendaciones

- ✓ Mantener el sistema IDS bajo un enfoque de monitoreo pasivo mediante *Port Mirroring*, debido a que esta configuración permite analizar el tráfico de la red WISP sin intervenir directamente en la ruta principal de comunicación. Esta práctica contribuye a preservar la estabilidad del servicio y evita que el IDS se convierta en un punto crítico de falla.
- ✓ Es conveniente utilizar una interfaz de red dedicada exclusivamente para la captura de tráfico y otra interfaz separada para la administración del servidor IDS. Esta separación permitiría diferenciar el tráfico monitoreado del tráfico de gestión, mejorando la organización operativa y reduciendo posibles interferencias durante el análisis.
- ✓ Resulta necesario actualizar periódicamente las reglas de detección de Suricata, incorporando firmas provenientes de fuentes confiables y reglas personalizadas de acuerdo con el comportamiento observado en la red. Esto facilita mejorar la detección de nuevas amenazas y reducir la presencia de alertas irrelevantes.
- ✓ Establecer una línea base del tráfico normal de la red antes de ejecutar nuevas pruebas de seguridad. Esta referencia permitiría identificar patrones habituales de comunicación, protocolos frecuentes, horarios de mayor actividad y posibles desviaciones asociadas a comportamientos anómalos.
- ✓ Optimizar los *dashboards* de Kibana con paneles específicos orientados a la seguridad, tales como alertas por severidad, eventos por tipo, firmas más frecuentes, direcciones IP de origen y destino, tráfico por protocolo y evolución temporal de eventos. Esta organización facilitaría la revisión técnica y la priorización de incidentes.

- ✓ Mejorar el mecanismo de notificación por correo electrónico mediante criterios de priorización por severidad, tipo de evento o firma detectada. El administrador recibiría alertas más relevantes y se evitaría la saturación de mensajes por eventos informativos o de baja criticidad.
- ✓ Monitorear de forma continua los recursos del servidor IDS, especialmente CPU, memoria, almacenamiento y carga de red. Este seguimiento contribuiría a determinar si el *hardware* utilizado es suficiente para el volumen de tráfico analizado y serviría como base para futuras ampliaciones.
- ✓ Documentar detalladamente las configuraciones aplicadas en el *router*, *switch* gestionable, servidor IDS, Suricata, Filebeat, Elasticsearch, Kibana y sistema de notificación. Esta documentación facilitaría la reproducción del laboratorio, la corrección de errores y la continuidad del proyecto en futuras prácticas académicas.
- ✓ Utilizar el entorno implementado como plataforma de prácticas académicas en asignaturas relacionadas con redes inalámbricas, seguridad de redes, monitoreo de tráfico y administración de telecomunicaciones. La infraestructura desarrollada permite reproducir escenarios reales, analizar eventos en tiempo real y fortalecer competencias técnicas en ciberseguridad aplicada a redes WISP.

Anexos

Anexo 1: Montaje y ajuste de la antena sectorial Ubiquiti en la infraestructura WISP



Anexo 2: Conexión del inyector o *switch* PoE para la alimentación del equipo inalámbrico



Anexo 3: Conexión del cableado Ethernet/PoE hacia el equipo inalámbrico de la red WISP



Anexo 4: Conexión física del puerto 9 destinado al IDS en el *switch* TP-Link Omada, identificada mediante un recubrimiento negro en el cable Ethernet.



Anexo 5: Generación adicional de tráfico para visualización del IDS en fase preliminar

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Versión 10.0.19045.4291]
(c) Microsoft Corporation. Todos los derechos reservados.

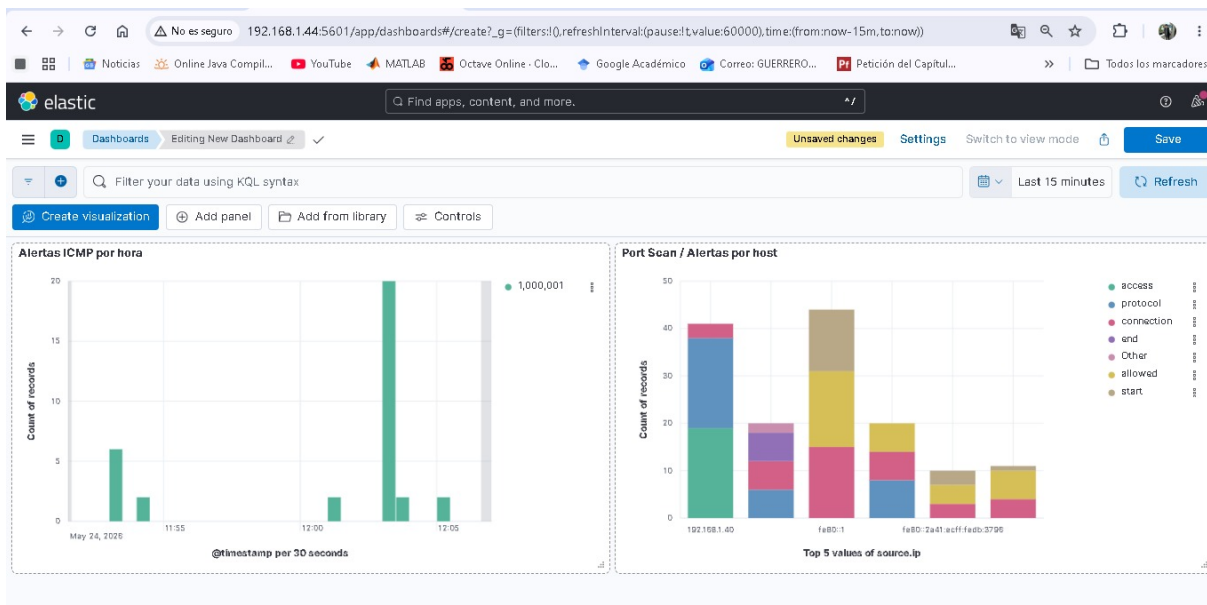
C:\Users\WISP>ping 8.8.8.8 -n 30

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 8.8.8.8: bytes=32 tiempo=35ms TTL=112
Respuesta desde 8.8.8.8: bytes=32 tiempo=35ms TTL=112
Respuesta desde 8.8.8.8: bytes=32 tiempo=35ms TTL=112
Respuesta desde 8.8.8.8: bytes=32 tiempo=35ms TTL=112
Respuesta desde 8.8.8.8: bytes=32 tiempo=35ms TTL=112
Respuesta desde 8.8.8.8: bytes=32 tiempo=35ms TTL=112
Respuesta desde 8.8.8.8: bytes=32 tiempo=35ms TTL=112
Respuesta desde 8.8.8.8: bytes=32 tiempo=35ms TTL=112
Respuesta desde 8.8.8.8: bytes=32 tiempo=35ms TTL=112
Respuesta desde 8.8.8.8: bytes=32 tiempo=35ms TTL=112
Respuesta desde 8.8.8.8: bytes=32 tiempo=35ms TTL=112
Respuesta desde 8.8.8.8: bytes=32 tiempo=35ms TTL=112
Respuesta desde 8.8.8.8: bytes=32 tiempo=35ms TTL=112
Respuesta desde 8.8.8.8: bytes=32 tiempo=35ms TTL=112
Respuesta desde 8.8.8.8: bytes=32 tiempo=36ms TTL=112
Respuesta desde 8.8.8.8: bytes=32 tiempo=35ms TTL=112
Respuesta desde 8.8.8.8: bytes=32 tiempo=36ms TTL=112
Respuesta desde 8.8.8.8: bytes=32 tiempo=35ms TTL=112
Respuesta desde 8.8.8.8: bytes=32 tiempo=30ms TTL=112
Respuesta desde 8.8.8.8: bytes=32 tiempo=30ms TTL=112
Respuesta desde 8.8.8.8: bytes=32 tiempo=30ms TTL=112

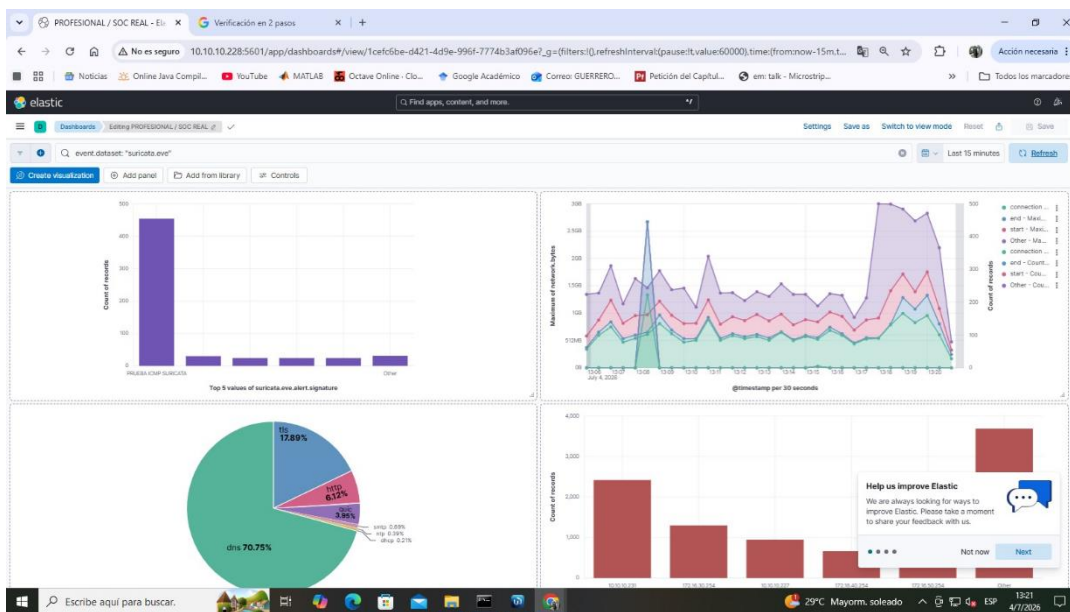
Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 30, recibidos = 30, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 30ms, Máximo = 36ms, Media = 35ms

C:\Users\WISP>
```

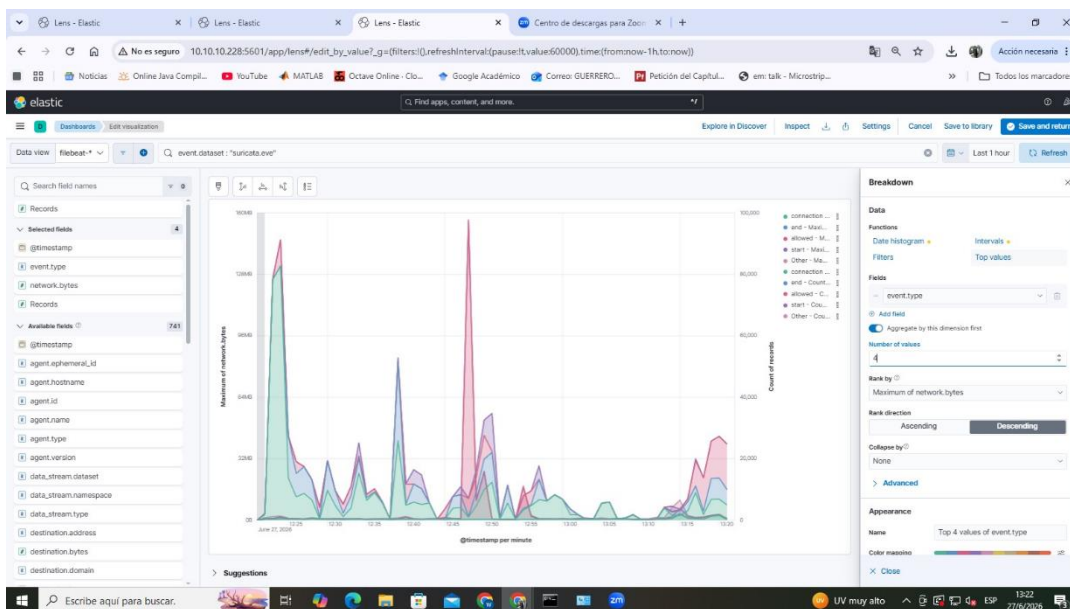
Anexo 6: Validación visual del sistema



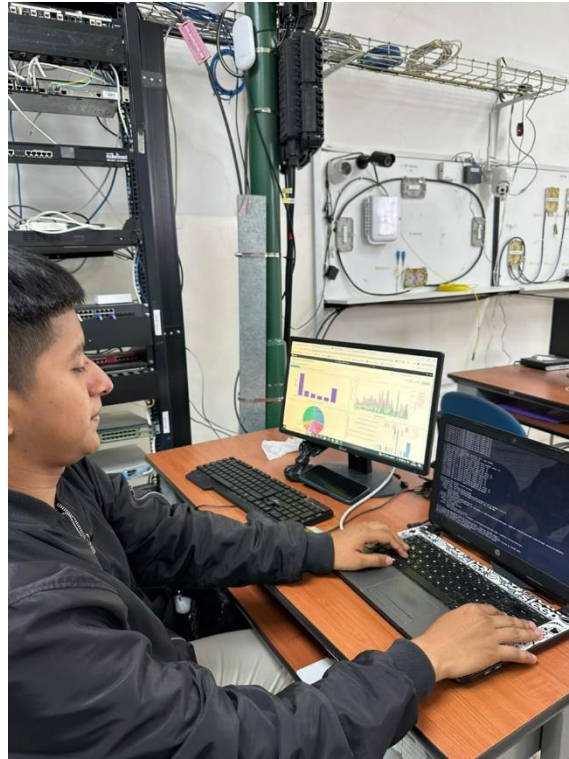
Anexo 7: Validación de Kibana en conjunto con toda la infraestructura WISP



Anexo 8: Validación del ancho de banda en la infraestructura WISP en tiempo real con varios usuarios usando los servicios de la red



Anexo 9: Verificación del servidor IDS y visualización de eventos en Kibana



Bibliografía

- [1] A. W. Párraga Lara y J. C. Aspiazu Rovira, «Análisis, diseño e implementación de módulo WISP como herramienta práctica y demostrativa del manejo de redes inalámbricas para uso en el laboratorio de telecomunicaciones de la Universidad Politécnica Salesiana,» p. 123, junio 2021.
- [2] A. A. Andrade Mafla, «Diseño e implementación de un sistema de gestión basado en políticas para el WISP (Wireless Internet Service Provider) TELYDATA CÍA. LTDA.,» p. 252, 11 abril 2013.
- [3] M. R. Velasco Rivera, «Diseño de un WISP (Wireless Internet Service Provider) en el campus de la Universidad Técnica del Norte para proveer servicios de internet inalámbrico utilizando un esquema Wireless Mesh con tecnología Wi-Fi,» p. 271, 27 noviembre 2009.
- [4] E. A. Arias, «Infraestructura de red de datos para WISP: Soluciones de conectividad y acceso a internet,» p. 105, 16 septiembre 2016.
- [5] J. E. Arteaga Pucha, «Evaluación de las funcionalidades de los sistemas de detección de intrusos basados en la red de plataformas Open Source utilizando la técnica de detección de anomalías,» p. 162, julio 2018.
- [6] H. A. Guerrero Erazo, L. A. Lasso Garces y P. A. Legarda Muñoz, «Identificación de vulnerabilidades de seguridad en el control de acceso al sistema de gestión documental, mediante pruebas de testeo de red en la empresa ingelec S.A.S,» p. 92, 18 abril 2015.
- [7] O. E. Cárdenas Villavicencio, J. P. Orellana Preciado, Á. M. Ramón Noblecilla y F. E. Montoya Naguas, «Análisis de seguridad y contramedidas frente al VLAN Hopping Attack: evaluación y simulación en entornos de red,» *Pro Sciences: Revista De Producción, Ciencias E Investigación*, vol. 8, nº 55, pp. 81-92, diciembre 2024.
- [8] Karen Scarfone y Peter Mell, «Guide to Intrusion Detection and Prevention Systems (IDPS),» *National Institute of Standards and Technology*, p. 127, febrero 2007.
- [9] C. M. Landacay Jaramillo, P. A. Quijije Mejía y C. D. Yopez, «Análisis técnico económico y regulatorio para la implementación del servicio de audio y video por suscripción usando tecnología iptv para un wisp del cantón general Villamil playas,» p. 115, 2018.
- [10] J. L. Oña Riera y M. A. Álvarez, «Diseño e implementación de una red WISP para interconectar tres sectores rurales en la Provincia de Bolívar, Cantón Guaranda, parroquia Simiatug,» 11 abril 2025.
- [11] C. Sanders, «Practical packet analysis: Using Wireshark to solve real-world network problems,» 2017.

- [12] C. F. Miño Verdezoto, «Diseño e implementación de un sistema de seguridad de detección de intrusos (IDS) para la plataforma Openstack utilizando código abierto,» p. 118, 12 julio 2020.
- [13] E. Y. Lozano, «SnorUNI: Aplicación móvil para Sistemas de Detección y Prevención de Intrusiones basados en Snort,» UNIVERSIDAD NACIONAL DE INGENIERÍA, Lima, Perú, 2017.
- [14] M. Barrios y D. Castillo, «Riesgos de ciberseguridad en redes WISP emergentes,» *Revista Digital de Ingeniería en Telecomunicaciones*, 2022.
- [15] A. Santiago Quintero y J. Reyes Guerrero, «Diseño de un proveedor de servicio de internet inalámbrico "WISP" en Ocaña, Norte de Santander,» p. 73, 17 julio 2014.
- [16] J. C. C. TANDAYAMO, «DISEÑO DE UNA RED WIFI PARA PROVEER SERVICIO DE INTERNET INALÁMBRICO EN LA ZONA URBANA NORTE DEL CANTÓN CAYAMBE,» vol. 100219843, n° 8, 2016.
- [17] W. S. Sarango Espinosa, «Implementación de enlaces backhaul para backbone de un wisp (wireless internet service provider), usando sistemas de radiocomunicaciones que utilicen técnicas de modulación digital de banda ancha en frecuencias no licenciadas, mediante el uso del sistema,» 1 julio 2011.
- [18] A. Espinoza, M. Gonzalez, C. Vera y N. Arreaga, «Análisis y diseño para la creación de un proveedor de servicios de internet inalámbrico (WISP),» p. 10, 25 febrero 2009.
- [19] O. A. P. Ruiz, «Migración Red GPON para proveedores de servicio inalámbrico (WISP),» 2023.