

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Tema:

CALIDAD DE SERVICIO (QOS) PARA LA OPTIMIZACIÓN DEL TRÁFICO EN LA RED LAN DEL CENTRO DE INVESTIGACIÓN Y DESARROLLO DE LA FUERZA AÉREA ECUATORIANA

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

ÁREA: Seguridad y redes.

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

AUTOR: Aida Esthela Cocha Muquinche

TUTOR: Ing. David Omar Guevara Aulestia, Mg.

Ambato - Ecuador

febrero – 2025

APROBACIÓN DEL TUTOR

En calidad de tutor del trabajo de titulación con el tema: CALIDAD DE SERVICIO (QOS) PARA LA OPTIMIZACIÓN DEL TRÁFICO EN LA RED LAN DEL CENTRO DE INVESTIGACIÓN Y DESARROLLO DE LA FUERZA AÉREA ECUATORIANA, desarrollado bajo la modalidad Proyecto de Investigación por la señorita Aida Esthela Cocha Muquinche, estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 17 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.3 del instructivo del reglamento referido.

Ambato, febrero 2025.



Ing. David Omar Guevara Aulestia, Mg.

TUTOR

AUTORÍA

El presente trabajo de titulación con el tema: CALIDAD DE SERVICIO (QOS) PARA LA OPTIMIZACIÓN DEL TRÁFICO EN LA RED LAN DEL CENTRO DE INVESTIGACIÓN Y DESARROLLO DE LA FUERZA AÉREA ECUATORIANA es absolutamente original, auténtico y personal y ha observado los preceptos establecidos en la Disposición General Quinta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, febrero 2025.



Aida Esthela Cocha Muquinche

C.C. 1804106068

AUTOR

DERECHOS DE AUTOR

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

Ambato, febrero 2025.

Firmado electrónicamente por:
AIDA ESTHELA
COCHA MUQUINCHE

Aida Esthela Cocha Muquinche

C.C. 1804106068

AUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del informe final del trabajo de titulación presentado por la señorita Aida Esthela Cocha Muquinche, estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado CALIDAD DE SERVICIO (QOS) PARA LA OPTIMIZACIÓN DEL TRÁFICO EN LA RED LAN DEL CENTRO DE INVESTIGACIÓN Y DESARROLLO DE LA FUERZA AÉREA ECUATORIANA, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 19 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.4 del instructivo del reglamento referido. Para cuya constancia suscribimos, conjuntamente con el señor Presidente del Tribunal.

Ambato, febrero 2025.

Firmado electrónicamente por:
FRANKLIN OSWALDO
MAYORGA MAYORGA

Ing. Franklin Oswaldo Mayorga Mayorga, Mg.
PRESIDENTE DEL TRIBUNAL

Firmado electrónicamente por:
EDISON HOMERO
ALVAREZ MAYORGA

Ing. Edison Álvarez Mayorga, Mg
PROFESOR CALIFICADOR

Firmado electrónicamente por:
ANDREA PATRICIA
SANCHEZ ZUMBA

Ing. Andrea Sánchez Zumba, Mg
PROFESOR CALIFICADOR

DEDICATORIA

A mi padre, Rogelio Cocha, quien desde el cielo guía mis pasos con su amor eterno y sus enseñanzas, siendo una luz que me inspira a no rendirme, este logro es un homenaje a tu memoria. A mi madre, Virginia Muquinche, por ser mi mayor apoyo en cada momento de esta travesía. Gracias por tu amor incondicional, tu fortaleza y tus palabras de aliento.

A mis hermanos, Patricio, Tania, Alex, Ángel, compañeros de vida y cómplices en este camino, y a mis sobrinos, pequeñas luces que iluminan mi vida con su alegría y amor. Su cariño, apoyo y confianza han sido una fuerza invaluable para alcanzar esta meta.

A todos ustedes, mi familia, dedico este trabajo con todo mi amor y gratitud, este logro es tanto suyo como mío.

Esthela.

AGRADECIMIENTO

Primeramente, quiero agradecer a Dios por darme la sabiduría, la fortaleza y el ánimo necesario para levantarme cada día y enfrentar los desafíos que se presentan en el camino.

A mi tutor, Ing. David Guevara, por su guía, paciencia y compromiso durante el desarrollo de este proyecto. Sus valiosas sugerencias y conocimientos enriquecieron significativamente este trabajo. Ing. Andrea Sánchez, Ing. Franklin Mayorga y Ing. Édison Álvarez sus valiosos consejos y liderazgos han sido fundamentales para el éxito de este proyecto.

A Vicky, Danix, Mateo, David, Paúl y Kevin amigos que han estado presente en este viaje, quienes con su apoyo, comprensión y palabras de aliento han estado a mi lado. Gracias por ser esa red de apoyo que me impulsó a seguir adelante incluso en los momentos más desafiantes.

Aquellos que fueron parte de mi proceso estudiantil y a cada una de las personas que me brindo una mano en cualquier momento difícil, quiero expresar mi más profundo agradecimiento. Cada gesto, palabra y ayuda recibida fue una luz en el camino, y por ello les digo gracias, deseando que Dios los bendiga siempre.

Esthela

ÍNDICE GENERAL DE CONTENIDOS

PORTADA ..... **i**

APROBACIÓN DEL TUTOR ..... **ii**

AUTORÍA ..... **iii**

DERECHOS DE AUTOR ..... **iv**

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

DEDICATORIA ..... **vi**

AGRADECIMIENTO ..... **vii**

ÍNDICE GENERAL DE CONTENIDOS ..... **viii**

ÍNDICE DE TABLAS ..... **xi**

ÍNDICE DE FIGURAS ..... **xiv**

ÍNDICE DE ANEXOS ..... **xvii**

RESUMEN EJECUTIVO ..... **xvii**

ABSTRACT ..... **xix**

CAPÍTULO I. MARCO TEÓRICO **1**

1.1 Tema de investigación 1

1.1.1 Planteamiento del problema 1

1.2 Antecedentes investigativos 2

1.3 Fundamentación teórica 7

1.3.1 Tecnologías de la Información 7

1.3.2 Seguridad de la información en redes y comunicación 7

1.3.3 Gestión de redes 8

1.3.4 Calidad de Servicio 9

1.3.5 Administración de congestión 9

1.3.6 Infraestructura de redes 9

1.3.7 Conmutación y enrutamiento 10

1.3.8 Monitorización de la red 11

1.3.9 Red de Area Local (LAN) 12

1.3.10 VLAN 12

1.4 Objetivos 12

1.4.1 Objetivo general 12

1.4.2 Objetivos específicos 12

CAPÍTULO II. METODOLOGÍA 13

2.1 Materiales 13

2.2 Métodos 17

2.2.1 Modalidad de la investigación 17

2.2.2 Población y muestra 18

2.2.3 Recolección de información 19

2.2.4 Procesamiento y análisis de datos 36

CAPÍTULO III. RESULTADOS Y DISCUSIÓN 40

3.1 Análisis y discusión de resultados 40

3.1.1 Análisis de los problemas y alternativas de solución 40

3.1.2 Análisis de equipos de la red que soportan QoS 40

3.1.3 Parámetros de QoS 43

3.1.4 Modelos para la obtención de QoS 43

3.1.5 Tipos de encolamiento para gestión de congestión en la red 44

3.1.6 Mecanismo de regulación de tráfico 46

3.1.7 Metodología de desarrollo 46

3.2 Desarrollo de la propuesta 48

3.3 Aplicación de la metodología de trabajo 48

3.3.1 Fase I: Preparar 49

3.3.2 Fase II: Planear 49

3.3.3 Fase III: Diseñar 64

3.3.4 Fase IV: Implementar 71

3.3.5 Fase V: Operar 80

3.3.6 Fase VI: Optimizar 87

CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES 90

4.1 Conclusiones 90

4.2 Recomendaciones 91

REFERENCIAS BIBLIOGRÁFICAS 92

ANEXOS 99

ÍNDICE DE TABLAS

Tabla 1. Cadenas de búsqueda 2

Tabla 2. Búsqueda aplicada en repositorio de universidades del Ecuador 3

Tabla 3. Criterios de inclusión y exclusión 4

Tabla 4. Guía de entrevista que consta de 10 preguntas 16

Tabla 5. Guía de ficha de observación 17

Tabla 6. Población de estudio 18

Tabla 7. Coeficiente de Alfa de Cronbach 19

Tabla 8. Niveles de confiabilidad – Alfa de Cronbach 19

Tabla 9. Entrevista aplicada al jefe del DTIC 30

Tabla 10. Resultados obtenidos de la ficha de observación del SW_PROYECTOS. 32

Tabla 11. Resultados obtenidos de la ficha de observación del SW_HANGAR..... 32

Tabla 12. Resultados obtenidos de la ficha de observación del SW_GOMAI 33

Tabla 13. Resultados obtenidos de la ficha de observación del TPLINK_COMANDO 33

Tabla 14. Resultados obtenidos de la ficha de observación del CORESWITCH..... 34

Tabla 15. Resultados obtenidos de la ficha de observación del FortiGate..... 34

Tabla 16. Resultados obtenidos de la ficha de observación MIKROBOARD 35

Tabla 17. Resultados obtenidos de la ficha de observación de la ONT..... 36

Tabla 18. Preguntas para el análisis de la encuesta..... 37

Tabla 19. Diagnóstico y Plan de Acción para la Red..... 40

Tabla 20. Parámetros de QoS 43

Tabla 21. Servicios de comportamiento por salto 44

Tabla 22. Comparación de tipos de encolamiento 45

Tabla 23. Comparativa entre Traffic Shapping y Policing 46

Tabla 24. Comparativas de metodologías 47

Tabla 25. Fases del proyecto 48

Tabla 26. Características herramientas de monitoreo 50

Tabla 27. Monitoreo mediante Pingplotter 55

Tabla 28. Análisis de latencia y pérdida de paquetes según la jornada 56

Tabla 29. Capturas del tráfico utilizando Wireshark 58

Tabla 30. Comportamiento de la red 60

Tabla 31. Requerimiento de ancho de banda 60

Tabla 32. Cálculo de ancho de banda 62

Tabla 33. Parámetros de QoS 62

Tabla 34. Valores DSCP 62

Tabla 35. Aplicaciones, valores de DSCP y ancho de banda para configuración de QoS 63

Tabla 36. Segmentación en subredes 67

Tabla 37. Ip´s de administración de los equipos 68

Tabla 38. Conexión enlaces 68

Tabla 39. Direccionamiento Ip en las VLANs 68

Tabla 40. Modelado de tráfico 76

Tabla 41. Métodos de Traffic Shaping..... 78

Tabla 42. Resultado de la videoconferencia 84

Tabla 43. Pérdida de paquetes – Mañana (antes)..... 85

Tabla 44. Pérdida de paquetes – Medio día (antes) 85

Tabla 45. Pérdida de paquetes – Tarde (antes) 85

Tabla 46. Pérdida de paquetes – Mañana (después) 86

Tabla 47. Pérdida de paquetes – Medio día (después)..... 86

Tabla 48. Pérdida de paquetes – Tarde (después)..... 86

Tabla 49. Análisis de un antes y después..... 86

Tabla 50. Corrección de errores..... 87

ÍNDICE DE FIGURAS

Figura 1. Resultados de la encuesta Pregunta 1 20

Figura 2. Resultados de la encuesta Pregunta 2 21

Figura 3. Resultados de la encuesta Pregunta 3 22

Figura 4. Resultados de la encuesta Pregunta 4 23

Figura 5. Resultados de la encuesta Pregunta 5 24

Figura 6. Resultados de la encuesta Pregunta 6 25

Figura 7. Respuestas de la encuesta Pregunta 7 26

Figura 8. Resultados de la encuesta Pregunta 8 27

Figura 9. Respuestas de la encuesta Pregunta 9 28

Figura 10. Resultados de la encuesta Pregunta 10 29

Figura 11. Estadísticas respuesta encuesta 38

Figura 12. Monitoreo y patrones de uso Fortigate 7 días (Parte 1) 51

Figura 13. Monitoreo y patrones de uso Fortigate 7 días (Parte 2) 52

Figura 14. Monitoreo y patrones de uso Fortigate 7 días 52

Figura 15. Monitoreo y patrones de uso Fortigate 24 horas 53

Figura 16. Monitoreo y patrones de uso Fortigate 24 horas 53

Figura 17. Monitoreo de tráfico de red en el firewall Palo Alto. 55

Figura 18. Monitoreo realizado en la mañana 55

Figura 19. Monitoreo realizado al medio día 55

Figura 20. Monitoreo realizado en la tarde 56

Figura 21. Captura en Wireshark - Tarde en el área PROYECTOS 58

Figura 22. Captura en Wireshark - Mañana en el área HANGAR 58

Figura 23. Captura en Wireshark - Mañana en el área COMANDO 58

Figura 24. Captura en Wireshark - Tarde en el área GOMAI 58

Figura 25. Diseño de planificación 64

Figura 26. Diagrama de la red CIDFAE 65

Figura 27. Diseño de la red CIDFAE 70

Figura 28. Logo de GNS3 71

Figura 29. Red LAN CIDFAE en GNS3 72

Figura 30. Configuración SW_CORE 73

Figura 31. Configuración SW_COMANDO 73

Figura 32. Creación de VLANs en FortiGate 74

Figura 33. Verificación de conectividad 74

Figura 34. Sección de modelado de trafico 75

Figura 35. Configuración del perfil de tráfico 12 Mbps 76

Figura 36. Visualización de los perfiles de tráfico 76

Figura 37. Creación de la política para videoconferencia 79

Figura 38. Configuración de puertos 79

Figura 39. Horario para manejar las políticas 79

Figura 40. Políticas de tráfico 80

Figura 41. Adición de widget 80

Figura 42. Interfaz para gráfica de ancho de banda 81

Figura 43. Dashboard FortiGate 81

Figura 44. Consumo de ancho de banda 82

Figura 45. Logs del tráfico 82

Figura 46. Videoconferencia sin QoS 84

Figura 47. Videoconferencia con QoS 84

Figura 48. Capturas sin QoS -Mañana 84

Figura 49. Capturas con QoS -Mañana 84

Figura 50. Capturas sin QoS – Medio día 85

Figura 51. Capturas con QoS -Medio día 85

Figura 52. Capturas sin QoS -Tarde 85

Figura 53. Capturas con QoS -Tarde 85

Figura 54. Prueba nPerf antes de las implementaciones 88

Figura 55. Pruebas realizadas 88

Figura 56. Prueba nPerf después de las implementaciones 89

Figura 57. Pruebas realizadas 89

ÍNDICE DE ANEXOS

Anexo A. Validación de encuesta 99

Anexo B. Configuración de SW_PROYECTOS, SW_HANGAR y SW_GOMAI 101

Anexo C. Configuraciones de perfiles de tráfico 102

Anexo D. Configuración de puertos 103

Anexo E. Configuración del generador de tráfico 105

Anexo F. Manual de usuario 108

RESUMEN EJECUTIVO

El presente proyecto detalla la implementación de políticas de Calidad de Servicio (QoS) para la red del Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana, con el objetivo de gestionar y priorizar eficientemente el tráfico de la red mejorando el rendimiento de la infraestructura proporcionando estabilidad, escalabilidad y soporte adecuado a las aplicaciones importantes de la institución.

La investigación se desarrolló bajo la metodología PPDIOO de Cisco, permitiendo estructurar el trabajo en varias fases. Se aborda el análisis del estado actual de la red, identificación de áreas de mejora y diseño de soluciones enfocándose en optimizar el uso del ancho de banda mediante la identificación de los puertos y protocolos utilizados por aplicaciones.

El proceso experimental se centró en establecer un esquema QoS funcional en un entorno simulado de red, priorizando las aplicaciones según su importancia y requerimientos. Este proceso incluyó la segmentación de la red utilizando VLANs, la implementación de traffic shaping mediante la asignación de políticas de ancho de banda para los distintos tipos de tráfico y el marcado de paquetes con valores DSCP. Además, se definió el tipo de encolado en el dispositivo Fortigate de la institución asegurando una gestión óptima del tráfico según las prioridades establecidas.

Finalmente, los resultados obtenidos permitieron evaluar las ventajas que trae consigo el uso de QoS y determinar la optimización del tráfico que puede tomar la red del sitio promoviendo una red más robusta y preparada para el crecimiento y la adopción de nuevas tecnologías.

Palabras clave: Calidad de Servicio, optimización de la red LAN, segmentación de la red, traffic shapping, encolamiento.

ABSTRACT

This project details the implementation of Quality of Service (QoS) policies for the Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana network, with the objective of efficiently managing and prioritizing network traffic, improving the performance of the infrastructure for providing stability, scalability and adequate support to the institution's important applications.

The research was developed using the Cisco's PPDIOO methodology, allowing the work to be structured in several phases. The analysis of the current state of the network, identification of areas for improvement and design of solutions focused| on optimizing the use of bandwidth by identifying the ports and protocols used by applications.

The experimental process focused on establishing a functional QoS scheme in a simulated network environment, prioritizing applications based to their importance and requirements. This process included the segmentation of the network using VLANs, the implementation of traffic shaping by assigning bandwidth policies for the different types of traffic and marking packets with DSCP values. Additionally, the queuing type on the institution's FortiGate device was configured to ensure optimal traffic management based on established priorities.

Finally, the results obtained allowed to evaluate the advantages of using QoS and to determine the optimization of the traffic that the CIDFAE network can take, promoting a more robust network prepared for growth and the adoption of new technologies.

Keywords: Quality of Service, LAN optimization, network segmentation, traffic shapping, queuing.

CAPÍTULO I. MARCO TEÓRICO

1.1 Tema de investigación

CALIDAD DE SERVICIO (QOS) PARA LA OPTIMIZACIÓN DEL TRÁFICO EN LA RED LAN DEL CENTRO DE INVESTIGACIÓN Y DESARROLLO DE LA FUERZA AÉREA ECUATORIANA

1.1.1 Planteamiento del problema

El crecimiento tecnológico a nivel mundial ha impulsado la interconexión, digitalización y distribución de manera exponencial con cada dispositivo capaz de procesar datos, las redes informáticas se vuelven más distribuidas y conectadas [1]. A medida que Internet evoluciona con la llegada de 5G y más allá, mantener un equilibrio entre las conexiones básicas y los servicios avanzados se vuelve fundamental para la Industria 4.0 y la evolución de redes [2].

El aumento de usuarios de Internet en América Latina y el Caribe supera el promedio mundial con una penetración que ha pasado del 50% al 70% en los últimos cinco años, equivalente a unos 130 millones de nuevos usuarios, lo que implica que la infraestructura de redes debe garantizar la conectividad a nuevos usuarios con condiciones competitivas para economías de escala a costos razonables [3]. Asimismo, se hace evidente la necesidad de abordar eficientemente aspectos críticos como la confiabilidad en la latencia, el ancho de banda y la gestión del tráfico para optimizar el rendimiento y la experiencia de los usuarios [4].

Ecuador experimenta desafíos y oportunidades en el ámbito de las Tecnologías de la Información y la Comunicación (TIC), evidenciando un notable incremento en el acceso a redes e internet entre 2015 y 2018. A pesar de la alta cobertura de servicios, la adopción y uso efectivo de estas tecnologías aún requieren mejora [5]. Las instituciones se han enfocado en mejorar sus redes para satisfacer la demanda de tráfico de aplicaciones confidenciales como voz y video en tiempo real, evitando la degradación debido a factores como pérdida de paquetes, ancho de banda, retardo y jitter [6].

El Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana se enfrenta a desafíos significativos en la gestión del tráfico de su Local Area Network (LAN). La creciente demanda de servicios y aplicaciones especializadas ha puesto a prueba la capacidad de la red para manejar el tráfico de manera eficiente. Actualmente, la falta de una implementación adecuada y la ausencia de segmentación en la red LAN ha resultado en problemas de latencia, pérdida de paquetes y una experiencia de usuario subóptima. Estos problemas no solo afectan la productividad del personal, sino que también pueden comprometer la eficacia de las actividades de comunicación y transmisión de datos.

1.2 Antecedentes investigativos

Se realizó una revisión de la literatura examinando los artículos publicados en diversas bases de datos científicas que incluyen Scopus, IEEE Xplore y ACM Digital Library. Las cadenas de búsqueda se configuraron utilizando palabras clave relevantes como son: quality of service, network optimization, traffic management, local area network en un período que abarca desde el 2020 hasta 2024. Como resultado la Tabla 1 presenta las cadenas de búsqueda empleadas y la cantidad de artículos encontrados.

Tabla 1. Cadenas de búsqueda

	Revista	**Cadena**	**Núm. De Artículos**
Cadena 1	Scopus	(TITLE-ABS-KEY ("quality of service" OR "QoS") AND TITLE-ABS-KEY ("network optimization")) AND PUBYEAR > 2019 AND PUBYEAR < 2025	147
	IEEE Xplore	("All Metadata":"quality of service " OR "All Metadata":"QoS") AND ("All Metadata":"network optimization”) Filters Applied: 2020 - 2024	157
	ACM Digital Library	[[All: "quality of service"] OR [All: "qos"]] AND [All: "network optimization"] AND [E-Publication Date: (01/01/2020 TO 12/31/2024)]	185
Cadena 2	Scopus	(TITLE-ABS-KEY ("traffic management" OR "resource allocation") AND TITLE-ABS-KEY ("network management" OR "performance enhancement") AND TITLE-ABS-KEY ("local area network")) AND PUBYEAR > 2019 AND PUBYEAR < 2025	10
	IEEE Xplore	("All Metadata":"traffic management" OR "All Metadata":"resource allocation") AND ("All Metadata":"network management" OR "All Metadata":"performance enhancement") AND ("All Metadata":"local area network”)	8

		Filters Applied: 2020 - 2024	
	ACM Digital Library	[[All: "traffic management"] OR [All: "resource allocation"]] AND [[All: "network management"] OR [All: "performance enhancement"]] AND [All: "local area network"] AND [E-Publication Date: (01/01/2020 TO 12/31/2024)]	68
Cadena 3	Scopus	(TITLE-ABS-KEY ("QoS metrics" OR " QoS parameters ")) AND TITLE-ABS-KEY ("network management " OR " resource allocation") AND PUBYEAR > 2020 AND PUBYEAR > 2020 AND PUBYEAR < 2025	115
	IEEE Xplore	("All Metadata":"QoS metrics" OR "All Metadata":"QoS parameters") AND ("All Metadata":"network management" OR "All Metadata":"resource allocation") Filters Applied: 2020 - 2024	74
	ACM Digital Library	[[All: "qos metrics"] OR [All: " qos parameters "]] AND [[All: "network management "] OR [All: " resource allocation"]] AND [E-Publication Date: (01/01/2020 TO 12/31/2024)]	145
		Total	**909**

En este estudio, se tomaron en consideración proyectos de investigación disponibles en el repositorio institucional de la Universidad Técnica de Ambato (UTA) y Escuela Politécnica Nacional (EPN). Se seleccionaron títulos relevantes, en el periodo comprendido desde el año 2020 al 2024. Los criterios de búsqueda utilizados para este repositorio se presentan en la Tabla 2.

Tabla 2. Búsqueda aplicada en repositorio de universidades del Ecuador

Universidad	**Filtro de búsqueda**	**Término de búsqueda**	**N. De Artículos**
Universidad Técnica de Ambato	Facultad de Ingeniería en Sistemas, Electrónica e Industrial	Calidad de Servicio (QoS)	3
		Optimización de una red	10
		Redes LAN	1
Escuela Politécnica Nacional	Facultad de Ingeniería Eléctrica y Electrónica	Calidad de Servicio (QoS)	986
		Optimización de una red	990
		Redes LAN	250
		Total	**2240**

El principal objetivo de esta revisión bibliográfica es recopilar información de investigaciones anteriores relacionadas con de Calidad de Servicio (QoS) específicas para redes LAN, con el fin de optimizar el tráfico dentro de la red. Para realizar esta revisión, se llevaron a cabo búsquedas en el repositorio de la UTA y EPN, lo que resultó en la identificación de un total de 2240 trabajos de titulación. Sin embargo,

siguiendo criterios de inclusión y exclusión detallados en la Tabla 3, se procedió a descartar 2235 de estos artículos, dejando solamente 5 para un análisis más detallado.

Además de buscar en el repositorio de la UTA y EPN, se llevó a cabo investigaciones en bases de datos externas las cadenas de búsqueda utilizadas se detallan en la Tabla 1, a través de las búsquedas en Scopus, IEEE Xplore y ACM Digital Library se obtuvo un total de 909 artículos. Sin embargo, tras aplicar los criterios de selección como se describe en la Tabla 3, se eliminaron 906 artículos dejando solamente 3 artículos para un análisis más detallado. Resultando en el primer caso 5 y 3 en el segundo dejando un total de 8 artículos para su análisis.

Tabla 3. Criterios de inclusión y exclusión

Inclusión	Artículos que abordan la implementación de QoS en redes LAN.
	Relevancia a la optimización del tráfico en redes LAN.
	Investigaciones centradas en la implementación de soluciones tecnológicas en empresas, abarcando estudios de casos y prácticas destacadas
Exclusión	Artículos que no estén relacionados con la optimización de tráfico en la red.
	Artículos que solicitan remuneración económica.
	Estudios realizados antes del 2020.

En su proyecto de investigación, Robalino Mateo [7] propuso optimizar la infraestructura de red LAN para maximizar el rendimiento y brindar funcionalidades como la disponibilidad, resistencia a fallos, escalabilidad y calidad de servicio en la Unidad Educativa Bolívar. Se basó en diversas metodologías de Diseño de Redes como PPDIOO de Cisco, McCabe James, Long Cormac, Untiveros Sergio, Instituto Nacional de Estadística e Informática, Jerry Fitzgerald, Davis Etheridge y Errol Simón, así como Top-Down Network Design entre las cuales se destacó la Metodología PPDIOO de Cisco, que garantiza un enfoque integral y efectivo en la gestión y monitoreo. Los resultados obtenidos mostraron una mejora significativa en la escalabilidad gracias a la adecuada subdivisión de cada subred, lo que contribuye a una gestión y monitoreo más efectivos. En conclusión, la optimización y segmentación de las subredes evidenciaron una mejora en el rendimiento y la eficiencia de la red.

Zapata Nancy [8] en su proyecto de investigación detalla la implementación de un nodo de monitoreo de Calidad de Servicio (QoS), para mejora de la eficiencia del

tráfico y servicio óptimo para los usuarios de la empresa Ajnet incluye como metodología la investigación aplicada, documental y de campo, que implicaron un análisis de la situación actual de la empresa y la configuración de un servidor con routers Mikrotik para facilitar el enrutamiento de datos. Los resultados obtenidos revelaron que la implementación de este sistema, basado en QoS, ha tenido un impacto positivo en la optimización de los procesos logísticos y en la gestión de la calidad de servicio en la empresa. En conclusión, la introducción de este nodo de monitoreo ha demostrado ser una solución para mejorar la eficiencia del tráfico y garantizar un servicio óptimo para los usuarios.

En su trabajo de titulación, Mantilla Cristian [9] examinó el efecto de la QoS en los sistemas de transmisión multimedia en Software Defined Networking (SDN) centrándose específicamente en la influencia de los ataques de Denial of Service (DoS). Se enfoco en brindar una perspectiva sobre la seguridad de las redes en la transmisión de contenido multimedia. La metodología empleada fue experimental, realizando pruebas y comparaciones directas entre un escenario normal y uno bajo ataque de (DoS). Los resultados obtenidos muestran que el ataque al cliente multimedia tuvo un impacto significativo. El estudio concluye la importancia de implementar estrategias efectivas de mitigación y detección de ataques para garantizar la fiabilidad de los servicios.

En su proyecto de integración curricular, Silva Alejandra [10] propone calidad de servicio de la infraestructura de voz sobre IP mediante prácticas de laboratorio para capacitar a estudiantes en la configuración de Issabel y GNS3, con énfasis en la calidad del servicio (QoS) y seguridad. La metodología incluye cinco prácticas guiadas en Notion, desde conceptos básicos hasta avanzados, simulando entornos reales. Los resultados muestran mejoras en la comprensión de QoS, concluyendo que estas prácticas fortalecen habilidades para el entorno laboral.

Según Miranda Jesica [11], en su proyecto de investigación planteó la implementación de QoS para mejorar la calidad de la atención médica en la provincia de Pastaza. El objetivo fue establecer una red troncal con tecnología VoIP para la comunicación en tiempo real entre las unidades de salud, esto se respaldó con un sistema de gestión QoS para garantizar la calidad del servicio. Además, se integró el sistema con los existentes

sistemas de información para facilitar el intercambio de historias clínicas. Se implementaron medidas de seguridad para proteger la información de los pacientes. Se concluye que esta implementación es necesaria para optimizar los procesos médicos y mejorar la atención al paciente, subrayando la importancia de mantener altos estándares de calidad y seguridad en la infraestructura de red.

En su artículo, Huihui Wang et al. [12], presentan un algoritmo de optimización del retardo de end-to-end basado en el algoritmo BEB para redes distribuidas. Su investigación se enfocó en satisfacer los requisitos del control cooperativo distribuido de dos niveles sobre la calidad de la comunicación y el período de muestreo de las redes de sensores inalámbricos para maximizar la tasa de llegada de paquetes y obtener el período de muestreo mínimo del sistema de control, garantizando una comunicación inalámbrica ideal con una QoS suave. Los resultados de la simulación resaltan la influencia de varios parámetros de la red como la tasa de llegada de paquetes, el tamaño máximo de la ventana de retroceso, el número de saltos múltiples y el tamaño del paquete. Es importante mantener estándares de calidad en la comunicación inalámbrica, lo que contribuye significativamente a la fiabilidad y eficacia de los sistemas de redes distribuidas.

En su artículo, Badarla y Harigovidan [13], proponen un novedoso esquema de asignación de recursos basado en el mecanismo de Restricted Access Window (RAW), para abordar los desafíos de rendimiento en la red IoT multi-tasa IEEE 802.11ah. El esquema, denominado RAW-RA, se centró en la optimización de la red al agrupar las estaciones (STAs) en función de sus tasas de datos y asignar los intervalos RAW de manera proporcional. Mediante un modelo analítico preciso, se evalúo el rendimiento y la eficiencia energética de esta propuesta destacando una mejora significativa en comparación con el esquema de agrupamiento uniforme. Los resultados analíticos se respaldan con estudios de simulación extensos, validando la eficacia del enfoque propuesto para resolver la anomalía de rendimiento en las redes IoT.

Sebier Cristian et al. [14] en su artículo, abordan desafíos relacionados con la asignación de recursos en redes empresariales para aplicaciones heterogéneas, destacando el papel de la infraestructura de red. Se propone un diseño de sistema que utiliza principios de redes definidas por software para lograr un enrutamiento con

retraso limitado en la red y un ritmo de aplicación en los hosts finales. Se centró en la optimización del rendimiento de la red y en la garantía de una conectividad eficiente para una variedad de aplicaciones. Los resultados de la evaluación muestran mejoras significativas en el uso del enlace, la equidad en la distribución de recursos y la consistencia en el desempeño de la aplicación, lo que resalta la importancia de una infraestructura de red eficaz en entornos empresariales heterogéneos.

1.3 Fundamentación teórica

1.3.1 Tecnologías de la Información

Las Tecnologías de la Información y Comunicación (TIC) son un conjunto de herramientas, equipos y sistemas que permiten la captura, almacenamiento, procesamiento, transmisión y visualización de la información de manera digital. Esto incluye el uso de computadoras, Internet, software, dispositivos móviles, redes de comunicación y cualquier otra tecnología relacionada que facilite la creación, el intercambio y el acceso a la información [15].

1.3.2 Seguridad de la información en redes y comunicación

La seguridad en redes abarca un conjunto de medidas y estrategias destinadas a salvaguardar la integridad, confidencialidad y accesibilidad de la información transmitida a través de sistemas interconectados. Este enfoque comprende la implementación de mecanismos defensivos y ofensivos para prevenir, detectar y responder a posibles amenazas que puedan comprometer la infraestructura de comunicaciones y los datos que transitan por ella. Además, se considera la gestión de riesgos, la gobernanza y la adopción de buenas prácticas para garantizar la seguridad de los activos digitales y físicos involucrados en la interconexión de sistemas y dispositivos [16].

Las vulnerabilidades de los sistemas informáticos pueden clasificarse en tres categorías principales [17]:

a. Diseño

Se refieren a debilidades en los protocolos de red y políticas de seguridad deficientes o ausentes. Tales deficiencias pueden dejar a los sistemas más susceptibles a diversos tipos de ataques debido a fallas en su arquitectura.

b. Implementación

Incluyen errores de programación y la presencia de "puertas traseras" en los sistemas informáticos, estos errores de codificación pueden generar brechas de seguridad que los atacantes pueden explotar, mientras que las puertas traseras deliberadas introducidas por fabricantes o desarrolladores pueden permitir un acceso no autorizado al sistema.

c. Uso

Se encuentran la mala configuración de los sistemas informáticos, así como la falta de conocimiento y sensibilización por parte de los usuarios y responsables de informática. Además, la disponibilidad de herramientas que facilitan los ataques puede aumentar la vulnerabilidad de un sistema.

1.3.3 Gestión de redes

La gestión de redes es un conjunto de actividades y procesos diseñados para garantizar el funcionamiento óptimo, la disponibilidad y la calidad de los servicios ofrecidos por una red de comunicaciones. Este enfoque incluye la supervisión, control y mantenimiento de los dispositivos, recursos y aplicaciones que componen la infraestructura de red. Además, implica la implementación de estándares, protocolos y herramientas de gestión que faciliten la administración eficiente de los sistemas, así como la detección y resolución proactiva de posibles problemas [18].

1.3.4 Calidad de Servicio

Quality of Service (QoS), o Calidad de Servicio, es un conjunto de tecnologías y técnicas utilizadas en redes de comunicaciones para gestionar y priorizar el tráfico de datos según su importancia y requisitos de rendimiento. Su objetivo principal es garantizar una experiencia de usuario óptima al asignar recursos de red de manera eficiente y equitativa, especialmente en situaciones de congestión o limitaciones de ancho de banda. QoS permite identificar y priorizar ciertos tipos de tráfico, como voz o video, sobre otros menos críticos, asegurando así una entrega confiable y oportuna de los datos [19].

1.3.5 Administración de congestión

Una gestión eficiente de la congestión en QoS se basa en gran medida en la estrategia de encolado de paquetes que se implementa, el desafío surge cuando la demanda de ancho de banda supera el límite disponible en la red. Para prevenir esta sobrecarga es necesario asignar prioridad a determinados paquetes, lo que permite optimizar el flujo y regular el tráfico entrante [20].

1.3.6 Infraestructura de redes

La infraestructura de red se refiere al conjunto integral de hardware, software, sistemas y dispositivos que facilitan el flujo de datos dentro de una empresa, conectando a los usuarios, dispositivos, aplicaciones e Internet. Esta infraestructura es necesaria para garantizar la comunicación efectiva y el intercambio de información en toda la organización incluye componentes como routers, switches, servidores, cables de red, protocolos de comunicación y sistemas de gestión. Dada su importancia para el funcionamiento de la empresa y su conexión con el mundo exterior, la infraestructura de red debe ser segura y confiable para proteger los datos y asegurar un desempeño eficiente del sistema [21].

La infraestructura de red comprende diversos elementos interconectados que colaboran para asegurar un funcionamiento eficiente y fiable. Entre los componentes clave se encuentran [22]:

a. Servidores

Potentes computadoras que almacenan procesan y distribuyen información a otros dispositivos en la red, actuando como centros de datos y recursos para acceder a servicios en línea y aplicaciones.

b. Dispositivos de red

Tales como enrutadores y conmutadores, facilitan la transferencia de datos entre diferentes nodos de la red. Los enrutadores direccionan el tráfico en la dirección adecuada, mientras que los conmutadores permiten la comunicación entre dispositivos dentro de una red local.

c. Cableado y conexiones

Constituyen la base física de la infraestructura de red. Los cables de red transmiten datos entre ubicaciones, y las conexiones sólidamente establecidas garantizan una transferencia de datos rápida y fiable.

d. Protocolos de comunicación

Regulan cómo los dispositivos se comunican en una red. Por ejemplo, el Protocolo de Control de transmisión/Protocolo de Internet (TCP/IP) establece normas sobre cómo los datos deben ser fragmentados, transmitidos y reensamblados.

1.3.7 Conmutación y enrutamiento

La conmutación en TI y redes informáticas implica la transferencia de paquetes o bloques de datos a través de un dispositivo de conmutación de red, estos dispositivos llamados conmutadores, dirigen los datos desde los puertos de origen, como computadoras, hacia los puertos de destino, como enrutadores [23]. El enrutamiento consiste en elegir y establecer caminos para guiar el tráfico de paquetes IP dentro de una red o entre distintas redes, además de administrar el flujo general de datos en una red [24].

1.3.8 Monitorización de la red

El monitoreo de una red se refiere al proceso de supervisar activamente los elementos y el tráfico de una red de computadoras para detectar de manera oportuna posibles fallas, anomalías o problemas de rendimiento. Esta actividad es para garantizar un servicio óptimo a los usuarios, ya que permite identificar y solucionar problemas antes que impacten de manera considerable el funcionamiento de la red. A través del monitoreo, se recolecta y analiza información sobre el tráfico, el estado de los dispositivos y servicios, así como el uso de recursos como ancho de banda, Unidad Central de Procesamiento (CPU) y memoria [25].

Dentro de los diferentes tipos de protocolos de monitoreo de red se encuentran [26]:

a. Protocolo Simple de Administración de Redes (SNMP)

Es un protocolo de capa de aplicación que emplea un sistema de solicitud y respuesta para supervisar los estados de diversos dispositivos, desde switches hasta impresoras. SNMP se usa para revisar y gestionar tanto el estado como la configuración de los sistemas.

b. Protocolo de Mensajes de Control de Internet (ICMP)

Los dispositivos de red, como routers y servidores, hacen uso de ICMP para enviar información sobre operaciones por el Protocolo de Internet (IP) y para generar mensajes de error en caso de fallos en los dispositivos.

c. Protocolo de detección de Cisco

El Protocolo de descubrimiento de Cisco simplifica la gestión de dispositivos Cisco al detectarlos, determinar su configuración y permitir que los sistemas utilicen diversos protocolos de capa de red para obtener información mutua.

1.3.9 Red de Area Local (LAN)

Estas redes están diseñadas para establecer comunicación entre computadoras permitiendo el intercambio de información, aunque requieren que los dispositivos estén a corta distancia. Son comúnmente empleadas para interconectar computadoras personales en espacios laborales reducidos debido a su limitado alcance. Las redes de acceso suelen ser privadas y abarcan áreas como un edificio o un campus con una extensión de pocos metros. Su principal finalidad es conectar equipos para compartir recursos e intercambiar datos [27] .

1.3.10 VLAN

Una VLAN por sus siglas en inglés de Virtual Local Area Network o red de área local virtual, es una tecnología que permite crear redes lógicas independientes dentro de una misma red física. Esto ofrece ventajas como facilitar la segmentación, mejorar la seguridad, proporcionar flexibilidad y optimizar el rendimiento general de la red [28].

1.4 Objetivos

1.4.1 Objetivo general

Implementar Calidad de Servicio (QoS) para la optimización del tráfico en la red LAN del Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana.

1.4.2 Objetivos específicos

- Realizar un análisis del tráfico en la red para la identificación de áreas que requieran mejora.
- Investigar los tipos de encolamiento de QoS disponibles para una gestión eficiente de los recursos de las redes LAN.
- Establecer QoS para la optimización del tráfico en la red LAN del Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana.

CAPÍTULO II. METODOLOGÍA

2.1 Materiales

La recolección de información para este proyecto empleó un cuestionario que consta de 10 preguntas, dirigidas al personal del Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana, una entrevista dirigida al jefe del Departamento de Tecnologías de la Información y Comunicación (DTIC) y una ficha de observación hacia los equipos con el fin de obtener mayor conocimiento sobre el funcionamiento de la red LAN.

Encuesta dirigida al personal del Centro de investigación y Desarrollo de la Fuerza Aérea Ecuatoriana.

Objetivo: Evaluar la satisfacción de los usuarios con la Calidad de Servicio (QoS) de la red LAN del Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana, para identificar áreas de mejora en el rendimiento del tráfico.

Indicaciones: Estimado/a encuestado/a**,** se agradece su participación en esta encuesta. Las respuestas son importantes para comprender el estado de la red LAN. Por favor, marque la opción que mejor represente su punto de vista. Gracias por su colaboración.

Preguntas:

1. **¿ Alguna vez usted ha experimentado interrupciones en la conexión de Internet?**

- Siempre
- Casi siempre
- Casi nunca
- Nunca

2. **¿Considera que la red actual maneja eficientemente múltiples tareas simultáneamente sin degradar el rendimiento?**

- Si
- No

3. **¿Qué aspecto cree que podría mejorar en la red del CIDFAE?**

- Velocidad de conexión
- Estabilidad de la conexión
- Seguridad

4. **¿Usted considera que la red asegura suficiente ancho de banda para las aplicaciones esenciales de su trabajo?**

- Siempre
- Casi siempre
- Casi nunca
- Nunca

5. **¿Alguna vez los problemas de conectividad han afectado la realización de tareas en su puesto de trabajo?**

- Siempre
- Casi siempre
- Casi nunca
- Nunca

6. **¿Considera que la conexión de Internet es estable durante todo el día?**

- Siempre

- Casi siempre
- Casi nunca
- Nunca

7. ¿En qué momentos del día suelen notar más problemas de conexión?

- Mañana (de 8:00 a 12:00)
- Mediodía (de 12:00 a 14:00)
- Tarde (de 14:00 a 16:30)
- En ningún momento

8. ¿Con que frecuencia la velocidad de carga de las páginas web es satisfactoria?

- Siempre
- Casi siempre
- Casi nunca
- Nunca

9. ¿Qué tan a menudo puede realizar videoconferencias sin interrupciones?

- Siempre
- Casi siempre
- Casi nunca
- Nunca

10. ¿Qué beneficios cree que se obtendrá al implementar nuevas configuraciones para mejorar el rendimiento de la red?

- Mejora del rendimiento de la red

- Mayor confiabilidad en la red
- Aumento en la seguridad de la información

Entrevista dirigida al jefe del Departamento de Tecnologías de la Información y Comunicación (DTIC) del Centro de Investigación de la Fuerza Aérea Ecuatoriana

Tabla 4. Guía de entrevista que consta de 10 preguntas

Guía de Entrevista			
Nombre del entrevistado: Teniente Marco Garcés **Empresa:** Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana **Cargo:** Jefe del DTIC **Entrevistador:** Aída Cocha			
Objetivo: Conocer los principales problemas de rendimiento, herramientas de monitoreo, y políticas actuales de gestión de tráfico en la red LAN del CIDFAE, para identificar áreas de mejora.			
N°	**Pregunta**	**Respuesta**	**Observación**
1	¿Cuáles son los principales problemas de rendimiento que ha identificado en la red LAN del CIDFAE?		
2	¿Se ha realizado algún análisis reciente del tráfico en la red?		
3	¿Qué herramientas utiliza el DTIC para monitorear y analizar el tráfico de la red?		
4	¿Cuáles son las aplicaciones o servicios que requieren mayor consumo de ancho de banda en la red?		
5	¿Cómo se gestionan las solicitudes de usuarios para mejorar el rendimiento de la red?		
6	¿Qué cambios en la infraestructura de red se han realizado recientemente?		
7	¿Existen políticas de gestión de tráfico actuales?		
8	¿Hay algún plan de contingencia en caso de que alguna implementación cause algún problema imprevisto en la red?		
9	¿Cuál de las siguientes actividades considera que debería recibir la mayor prioridad en la red para asegurar un rendimiento óptimo en su trabajo (videoconferencias, transferencias de archivos grandes, Navegación web y correos electrónicos)?		
10	¿Cuál es la causa más común de los problemas de conectividad que experimenta con la red el CIDFAE (Problemas de configuración de red, problemas con el cableado, fallos en los equipos)?		
Conclusión:			

Matriz de observación

Tabla 5. Guía de ficha de observación

Ficha de observación	
Tipo de Observación: **Fecha:** **Observador:** **Objetivo:** Evaluar la capacidad y configuración de los equipos de red del Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana para garantizar la Calidad de Servicio (QoS)	
Detalles del Equipo	
Nombre de equipo	
Tipo de equipo	
Marca	
Modelo	
Sistema Operativo	
Ubicación	
Capacidad de hardware	
RAM	
Memoria FLASH	
Procesador	
Número de puertos	
Tipo de puerto	
Capacidad de QoS	
Soporta QoS	
Protocolos	
Observaciones Generales:	
Conclusión:	

2.2 **Métodos**

2.2.1 Modalidad de la investigación

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

a. Investigación de campo

La investigación de campo será esencial, dado que permitió al investigador obtener datos directos del centro de investigación a través de encuestas y evaluaciones de la infraestructura de red existente. Esta recopilación de datos proporcionó soluciones al problema estudiado, contribuyendo así a la optimización del tráfico en la red LAN.

b. Investigación bibliográfica – documental

Esta investigación empleó un enfoque bibliográfico-documental para examinar críticamente la literatura y los documentos relevantes en los campos de la gestión de redes, QoS. La revisión de fuentes bibliográficas como artículos científicos, libros y casos de estudio, permitió contextualizar y fundamentar el tema de la presente investigación

2.2.2 Población y muestra

La población con la cual se trabajó en el proyecto corresponde a los diferentes departamentos del CIDFAE. La Tabla 6, detalla los departamentos y el número de personal en cada uno, proporcionando una guía para el análisis de datos.

Tabla 6. Población de estudio

Población	**N° de Personas**	**Porcentaje %**
Centro de Investigación y Desarrollo FAE	1	1,59 %
Ingenieros y Técnicos en Mecánica Aeronáutica	14	22,22 %
Ingenieros y Técnicos en Telecomunicaciones, Sistemas y Sensores	4	6,35 %
Gestión de Proyectos	10	15,87 %
Apoyo Administrativo	2	3,17 %
Administración Central	2	3,17 %
Compras Públicas	2	3,17 %
Finanzas	2	3,17 %
Talento Humano	2	3,17 %
Seguridad y Defensa	12	19,05 %
Logística	2	3,17 %
Servicios Portuarios	5	7,94 %
Difusión	2	3,17 %
Puesto de Salud	3	4,76 %
Total	63	100,00 %

Este estudio se enfocó en una población de menos de cien individuos, por lo que no será necesario realizar una selección de muestras representativas. En lugar de ello, se trabajará de manera integral con la totalidad de la población.

2.2.3 Recolección de información

La recolección de información se realizó a través de los siguientes instrumentos: una encuesta dirigida al personal del CIDFAE, una entrevista aplicada al jefe del departamento del DTIC y una ficha de observación enfocada en los equipos de red.

a. Validación del instrumento

Al presentar un instrumento como un cuestionario, es importante conocer su validez y el nivel de confiabilidad de los datos recopilados. Para ello, se empleó el coeficiente Alfa de Cronbach en la mayoría de las preguntas que fueron elaboradas en formato de escala de Likert, con excepción de cuatro preguntas que no son adecuadas para este tipo de validación.

Para el cálculo de la confiabilidad del alfa de Cronbach se aplicó la siguiente ecuación:

$$\boldsymbol{\alpha = \left(\frac{k}{k-1}\right)\left(1 - \frac{\Sigma v_i}{v_t}\right)} \qquad (1)$$

Los cálculos fueron realizados en Excel como se muestra en el Anexo A, para mayor facilidad al aplicar la ecuación. La Tabla 7, muestra nivel de confiabilidad en el cual se obtuvo un valor de 0,705 lo que indica que el conjunto de ítems es aceptable como se muestra en la Tabla 8.

Tabla 7. Coeficiente de Alfa de Cronbach

Símbolo	**Significado**	**Valor**
α	Coeficiente de confiabilidad del cuestionario	0,705
k	Número de ítems	6
Σv_i	Sumatoria de las varianzas de los ítems.	2,593
vt	Varianza total	6,286

Tabla 8. Niveles de confiabilidad – Alfa de Cronbach

Rango	**Confiabilidad**
0,9 - 1	Excelente
0,8 - 0,9	Buena
0,7 - 0,8	Aceptable
0,6 - 0,7	Débil
0,5 - 0,6	Pobre
< 0,5	Inaceptable

b. Resultados de la encuesta

Pregunta 1.- ¿Alguna vez usted ha experimentado interrupciones en la conexión de Internet?

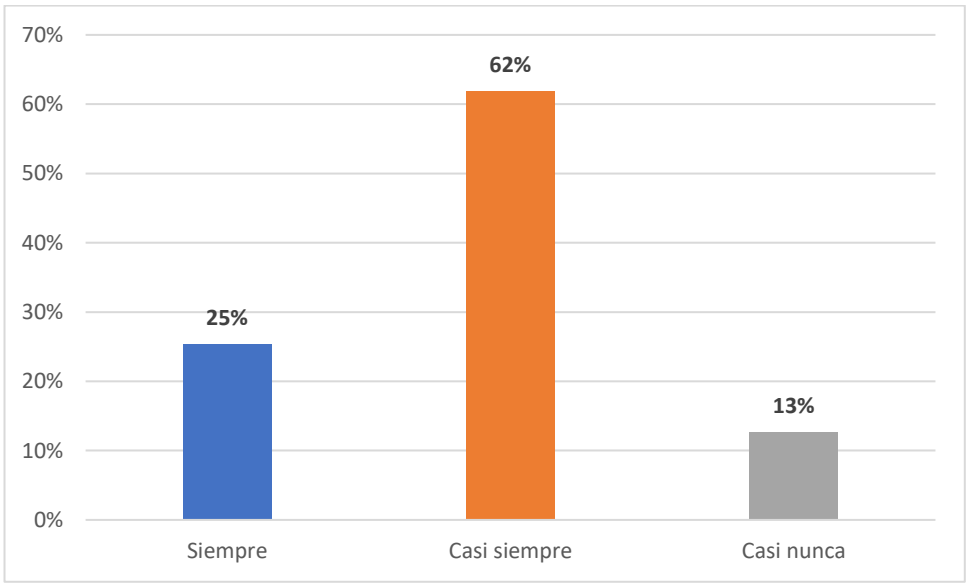


Figura 1. Resultados de la encuesta Pregunta 1

Análisis e interpretación

Los datos reflejados en el gráfico de barras de la Figura 1 es el siguiente: el 62% del personal indica que casi siempre experimenta interrupciones, el 25% afirma que siempre las experimenta, mientras que el 13% indica que nunca los ha experimentado. Esto significa que la mayoría con el 87% enfrenta interrupciones en su conexión a Internet, lo que resalta un problema significativo que puede afectar la productividad y la satisfacción laboral.

Pregunta 2.- ¿Considera usted que una conexión a Internet tiende a volverse lenta cuando se realizan múltiples tareas al mismo tiempo?

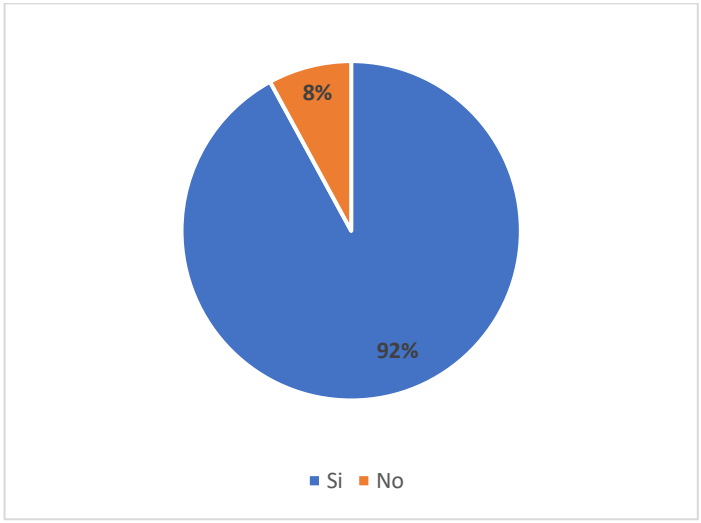


Figura 2. Resultados de la encuesta Pregunta 2

Análisis e interpretación

El gráfico tipo pastel presentado en la Figura 2, indica que el 92% del personal es consciente que, al realizar múltiples tareas, la velocidad de la conexión a Internet tiende a disminuir, mientras que el 8% opina que no es así. El alto porcentaje de personas que reconocen la disminución de la velocidad al realizar múltiples tareas indica un nivel de conciencia generalizado sobre este fenómeno. Esto sugiere que los usuarios han experimentado las limitaciones de sus conexiones cuando intentan llevar a cabo diversas actividades en línea de forma simultánea, lo que resalta la necesidad de estrategias para optimizar el uso de Internet en entornos de trabajo.

Pregunta 3.- ¿Qué aspecto cree que podría mejorar en la red del CIDFAE?

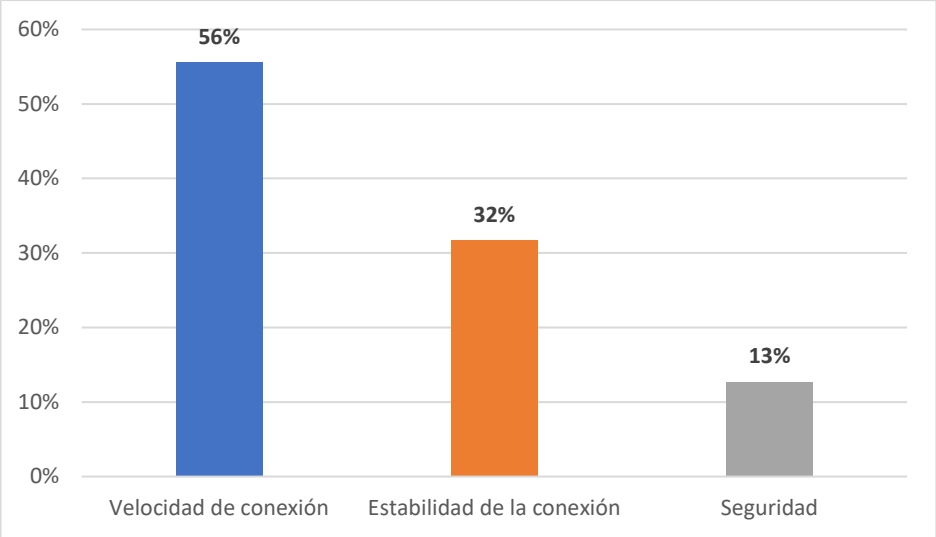


Figura 3. Resultados de la encuesta Pregunta 3

Análisis e interpretación

De acuerdo con los resultados de la Figura 3, el 56% del personal señala que la velocidad de conexión es un aspecto importante que mejorar, seguido por el 32% que menciona la estabilidad de la conexión y el 13% que se preocupa por la seguridad. Esta tendencia indica que la velocidad de conexión es la principal preocupación del personal, lo que indica que la red actual no cumple con las expectativas de conectividad necesarias.

Pregunta 4.- ¿Usted considera que la red asegura suficiente ancho de banda para las aplicaciones esenciales de su trabajo?

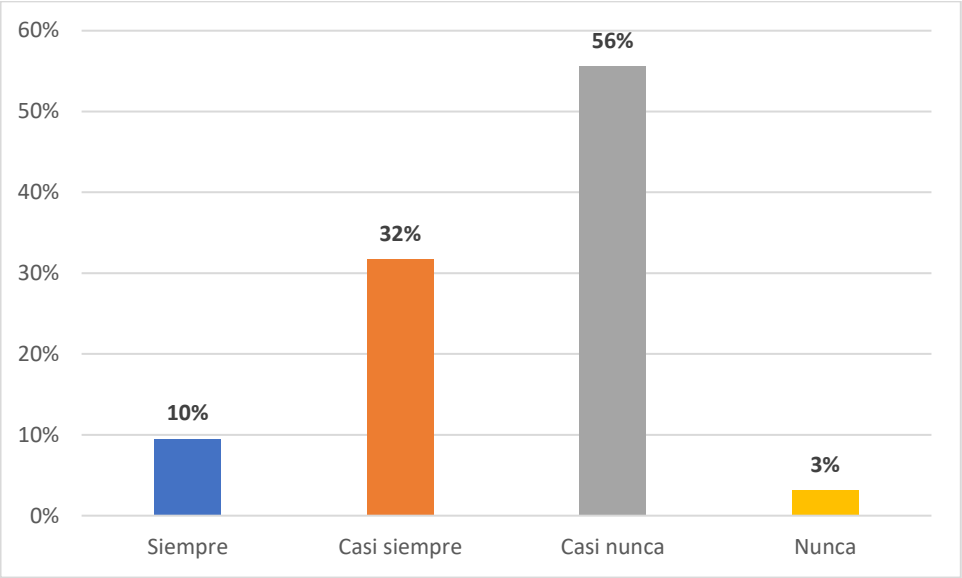


Figura 4. Resultados de la encuesta Pregunta 4

Análisis e interpretación

Los resultados de la Figura 4 muestran que el 56% del personal indica que casi nunca tiene suficiente ancho de banda para llevar a cabo sus tareas esenciales, seguido por el 32% que casi siempre lo tiene, el 10% que siempre dispone de suficiente ancho de banda y el 3% que nunca lo tiene. Esto demuestra que una gran parte del personal enfrenta dificultades en el acceso a la red, lo que podría obstaculizar el rendimiento y la eficiencia en sus funciones diarias.

Pregunta 5.- ¿Alguna vez los problemas de conectividad han afectado la realización de tareas en su puesto de trabajo?

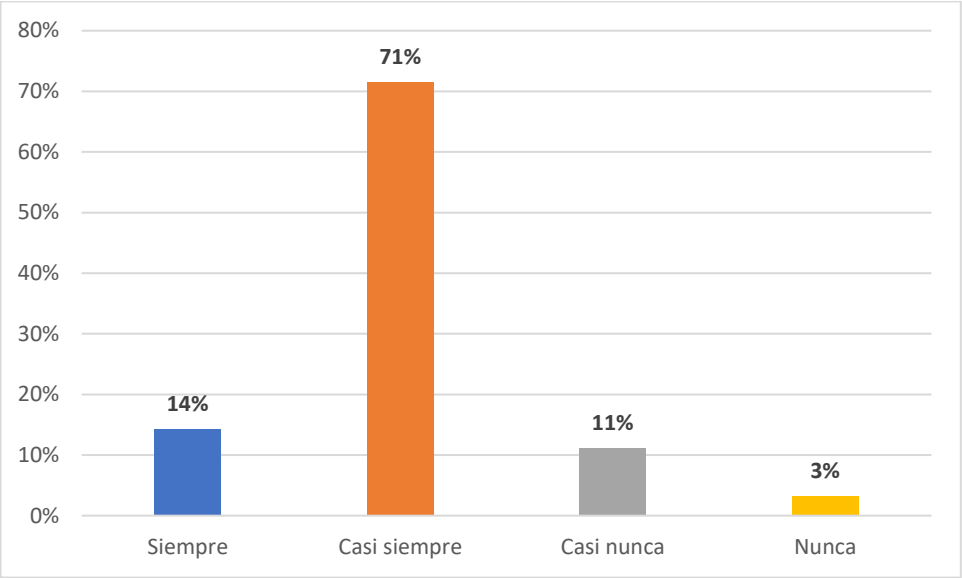


Figura 5. Resultados de la encuesta Pregunta 5

Análisis e interpretación

En cuanto a los resultados de la Figura 5 muestra que el 71% del personal indica que casi siempre su realización de tareas se ha visto afectada por problemas de conectividad a Internet, el 14% afirma que siempre se ha visto afectado, mientras que el 11% manifiesta que casi nunca ha experimentado esta situación y el 3% señala que nunca. Estos resultados confirman que la mayoría del personal está siendo afectado por problemas de conectividad, lo que puede impactar negativamente su desempeño laboral y la eficiencia general en el centro de investigación.

Pregunta 6.- ¿Considera que la conexión de Internet es estable durante todo el día?

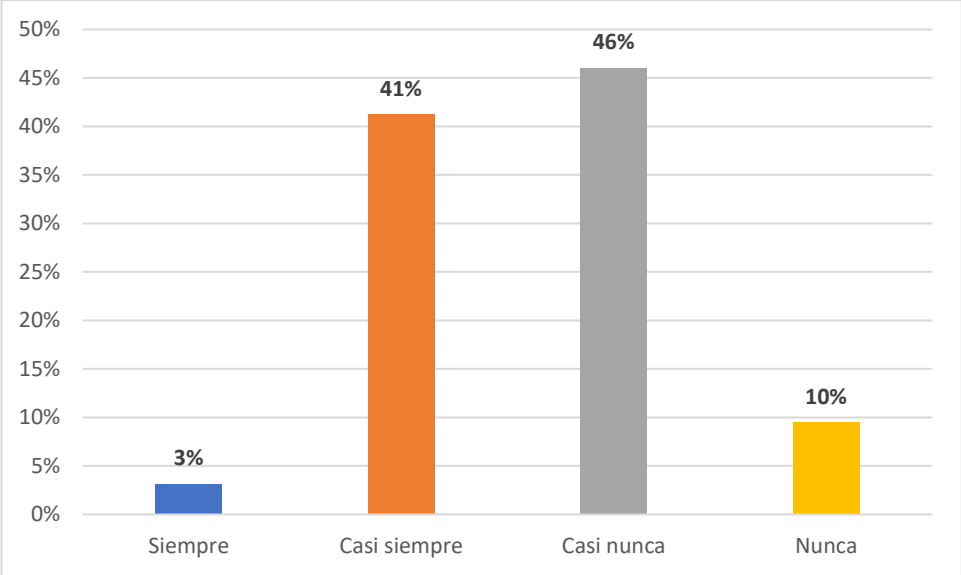


Figura 6. Resultados de la encuesta Pregunta 6

Análisis e interpretación

La Figura 6 representa que, el 46% del personal opina que la conexión a Internet casi nunca es estable, mientras que el 41% considera que casi siempre lo es. El 10% señala que nunca experimenta estabilidad en la conexión y el 3% afirma que sí lo es. Esta disparidad en las percepciones puede ser atribuida a diversos factores, como la ubicación, el dispositivo utilizado o la hora del día. Esto sugiere que la red se consideraría como inestable, lo que puede afectar tanto la productividad del personal. Implementar medidas que permitan mejorar la estabilidad de la red podría resultar en un entorno más eficiente y satisfactorio.

Pregunta 7.- ¿En qué momentos del día suelen notar más problemas de conexión?

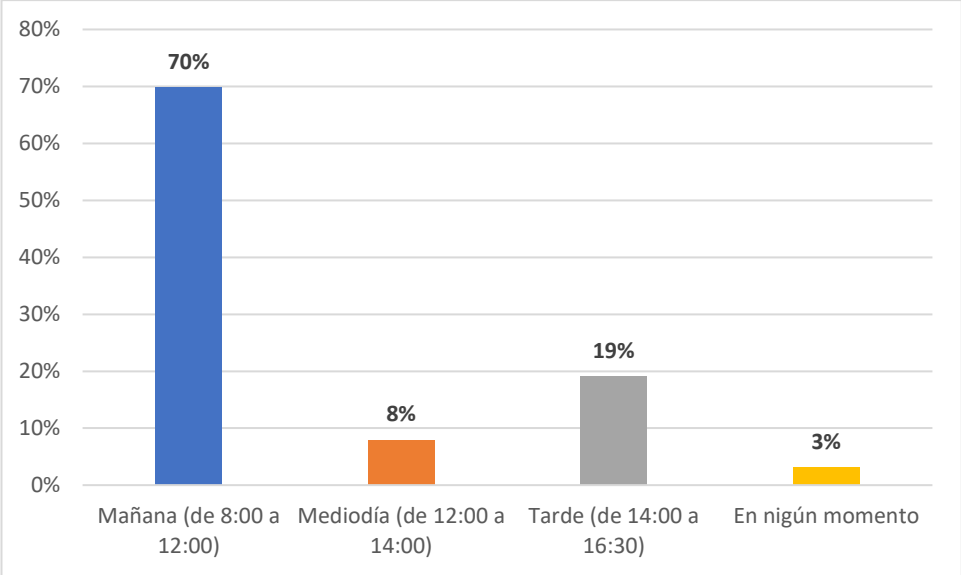


Figura 7. Respuestas de la encuesta Pregunta 7

Análisis e interpretación

Según los resultados presentados en la Figura 7, el 70% del personal indica que experimenta más problemas de conexión por la mañana (de 8:00 a 12:00). Un 19% señala que los inconvenientes ocurren principalmente por la tarde (de 14:00 a 16:30), mientras que el 8% menciona que los problemas se presentan al mediodía (de 12:00 a 14:00). Solo el 3% afirma que no enfrenta dificultades en ningún momento del día. Estos datos sugieren que las mañanas son especialmente críticas en términos de conectividad, lo que puede afectar la capacidad del personal para iniciar sus tareas de manera efectiva. La congestión de la red en este período podría estar relacionada con un mayor número de usuarios conectados. Por lo tanto, es importante evaluar y optimizar la infraestructura de Internet durante las horas pico.

Pregunta 8.- ¿Con que frecuencia la velocidad de carga de las páginas web es satisfactoria?

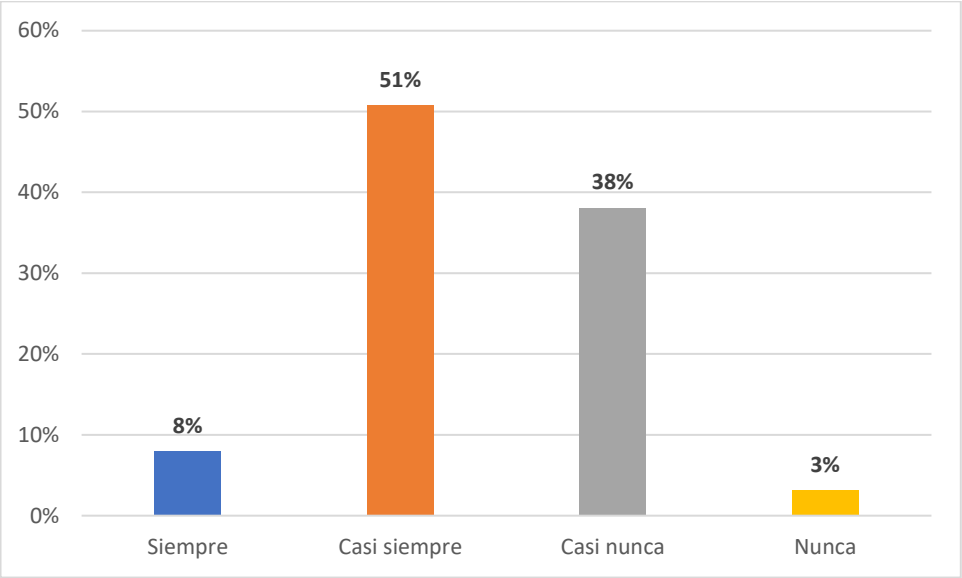


Figura 8. Resultados de la encuesta Pregunta 8

Análisis e interpretación

En la Figura 8, se evidencia que la velocidad de carga de las páginas web casi siempre es satisfactoria para el 51%, casi nunca para el 38%. Además, el 8% afirma que siempre es satisfactoria y el 3% indica que nunca lo es. Este resultado muestra que la mayoría del personal se encuentra en un punto intermedio entre la satisfacción y la insatisfacción. Esta tendencia sugiere que, aunque una parte significativa del personal percibe una carga aceptable, una porción considerable enfrenta problemas de velocidad. Esto destaca la necesidad de realizar configuraciones adecuadas para mejorar el tráfico en la red.

Pregunta 9.- ¿Qué tan a menudo puede realizar videoconferencias sin interrupciones?

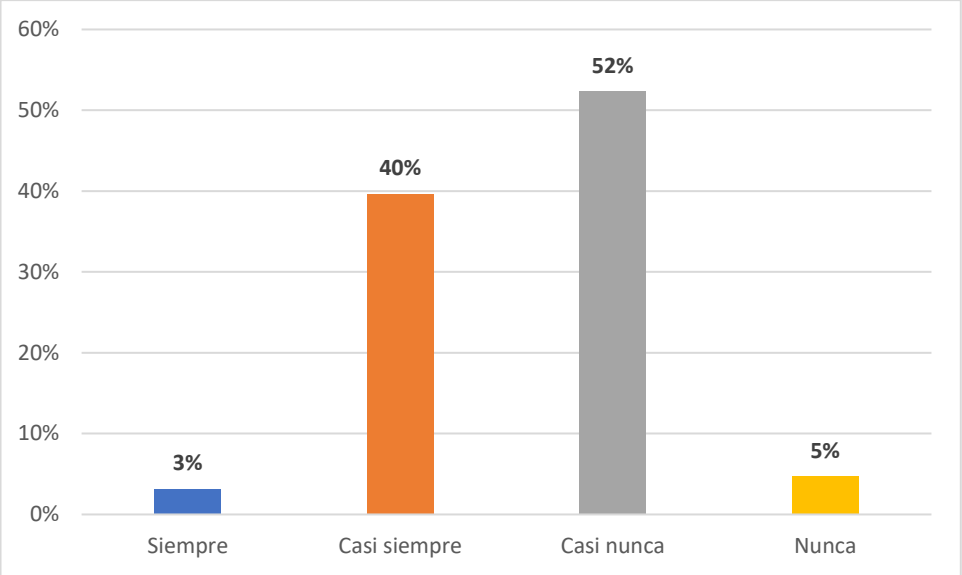


Figura 9. Respuestas de la encuesta Pregunta 9

Análisis e interpretación

Los resultados obtenidos en la Figura 9, el 52% del personal indica que casi nunca puede llevar a cabo videoconferencias sin interrupciones debido a problemas de conexión a Internet. En contraste, el 40% menciona que casi siempre logra realizar videoconferencias sin inconvenientes, el 5% afirma que nunca las realizar sin interferencias, y el 3% siempre lo hace sin interrupciones. Estos resultados evidencian que la mayor parte del personal enfrenta dificultades durante las videoconferencias, dado que el centro de investigación depende en gran medida de las videoconferencias para coordinar actividades, realizar capacitaciones y mantener una comunicación fluida con colegas.

Pregunta 10.- ¿Qué beneficios cree que se obtendrá al implementar nuevas configuraciones para mejorar el rendimiento de la red?

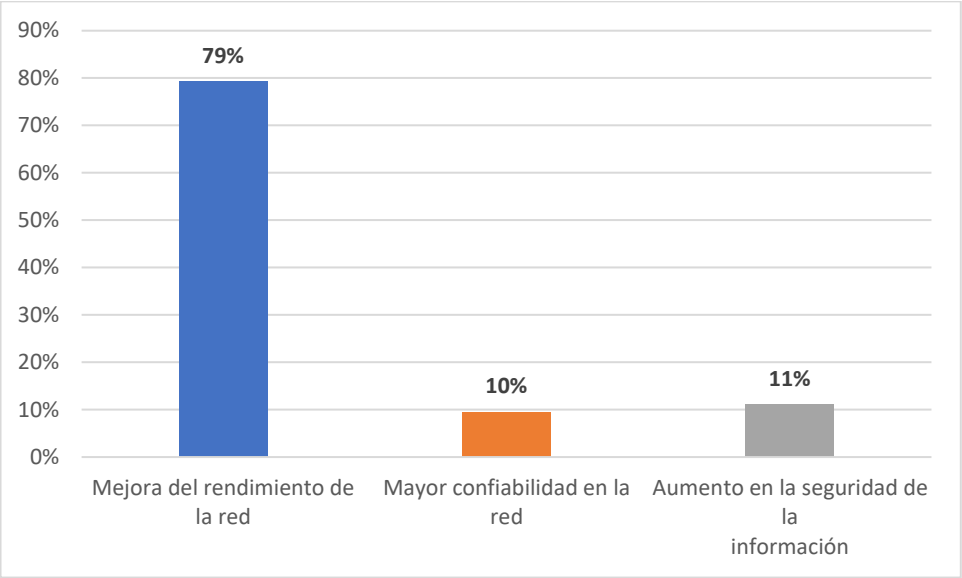


Figura 10. Resultados de la encuesta Pregunta 10

Análisis e interpretación

Según los resultados presentados en la Figura 10, muestra que el 79% del personal espera que estas nuevas configuraciones mejoren el rendimiento general de la red, en segundo lugar el 11% espera un aumento en la seguridad de la información y el 10% busca mayor confiabilidad en la conexión. Esto demuestra que la mejora del rendimiento es una prioridad para el personal, ya que una red más eficiente facilitaría el cumplimiento de tareas diarias.

A través de la guía de entrevista se obtuvo la siguiente información, que proporciona una visión integral sobre el estado actual de la red LAN del CIDFAE.

GUÍA DE ENTREVISTA

Tabla 9. Entrevista aplicada al jefe del DTIC

Entrevista dirigida al jefe del Departamento de Tecnologías de la Información y Comunicación (DTIC) del Centro de Investigación de la Fuerza Aérea Ecuatoriana			
Nombre del entrevistado: Teniente Marco Garcés **Empresa:** Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana **Cargo:** Jefe del DTIC **Entrevistador:** Aída Cocha			
Objetivo: Conocer los principales problemas de rendimiento, herramientas de monitoreo, y políticas actuales de gestión de tráfico en la red LAN del CIDFAE, para identificar áreas de mejora.			
N°	**Pregunta**	**Respuesta**	**Observación**
1	¿Cuáles son los principales problemas de rendimiento que ha identificado en la red LAN del CIDFAE?	Existe lentitud en ciertos momentos debido a que no se cuenta con cableado estructurado en todas las dependencias.	Existe interrupciones en la conexión a Internet.
2	¿Se ha realizado algún análisis reciente del tráfico en la red?	Sí, se llevó a cabo un análisis con la empresa TELCONET, el cual reveló que el ancho de banda disponible no es suficiente para cubrir las necesidades de todos los usuarios.	Se está considerando el cambio de empresa proveedora de Internet.
3	¿Qué herramientas utiliza el DTIC para monitorear y analizar el tráfico de la red?	El DTIC utiliza Palo Alto para el monitoreo y las restricciones en la red de la Fuerza Aérea.	Solo existe una herramienta de monitoreo.
4	¿Cuáles son las aplicaciones o servicios que requieren mayor consumo de ancho de banda en la red?	Actualmente, el mayor uso de ancho de banda proviene de plataformas que permiten difundir información rápidamente, manteniendo a la población informada sobre la situación del país y las actividades de las Fuerzas Armadas.	Las plataformas más utilizadas son Teams y Zoom, Google Meets, Jitsi para videoconferencias.
5	¿Cómo se gestionan las solicitudes de usuarios para mejorar el rendimiento de la red?	Se gestiona a través de órdenes de trabajo, para que los técnicos del DTIC acudan a las dependencias y solucionen los problemas.	
6	¿Qué cambios en la infraestructura de red se han realizado recientemente?	Se realizó el cableado estructurado en algunas dependencias y pronto se tiene la intención de cambiar el cable UTP por fibra óptica.	No todas las áreas cuentan con cableado estructurado.
7	¿Existen políticas de gestión de tráfico actuales?	Existen políticas que bloquean el acceso a ciertos sitios.	Las políticas de gestión específicas para el tráfico no están implementadas, lo que significa que no existe un control sobre cómo se distribuye el ancho de banda y cómo se priorizan las aplicaciones y servicios.
8	¿Hay algún plan de contingencia en caso de que alguna implementación cause algún problema imprevisto en la red?	No hay	No existe un plan de contingencia ante situaciones imprevistas

9	¿Cuál de las siguientes actividades considera que debería recibir la mayor prioridad en la red para asegurar un rendimiento óptimo en su trabajo (videoconferencias, transferencias de archivos grandes, Navegación web y correos electrónicos)?	Lo que tendría que optimizarse son las videoconferencias, son importantes para las reuniones que se dan entre el comando conjunto y los diferentes comandantes. También es importante asegurar un buen rendimiento en las páginas web, ya que esto apoya la investigación y el desarrollo de proyectos en las operaciones aéreas.	Las actividades principales no reciben un ancho de banda adecuado.
10	¿Cuál es la causa más común de los problemas de conectividad que experimenta con la red el CIDFAE (Problemas de configuración de red, problemas con el cableado, fallos en los equipos)?	Actualmente, la red enfrenta problemas tanto con el proveedor de internet como con el cableado. Se está en proceso de renovación de dispositivos.	No todos los dispositivos cuentan con una configuración previa, ni una segmentación de la red.
Conclusión: La entrevista con el Teniente Marco Garcés destacó problemas en la red LAN del CIDFAE, como la falta de cableado estructurado y ancho de banda insuficiente además, los switches no tienen configuración previa y la red no está segmentada, lo que afecta el rendimiento. Es importante priorizar las videoconferencias y mejorar las políticas de tráfico para optimizar la red.			

FICHA DE OBSERVACIÓN

A través de la ficha de observación se recopiló información clave sobre el acceso a los equipos de red. Para ingresar a los switches Cisco, fue necesario utilizar un cable de consola, ya que estos dispositivos no contaban con IPs de administración, permitiendo el acceso únicamente a través del puerto de consola. En el caso del switch TP-Link, se accedió mediante su IP de administración predeterminada. Para el FortiGate, se utilizó su IP de administración para la conexión. Sin embargo, no fue posible acceder directamente al MikroTik ni a la ONT, ya que eran equipos pertenecientes al proveedor de servicio y no se contaba con los permisos necesarios. No obstante, la ficha fue completada a partir de una investigación previa, ya que se conocían tanto la marca como el modelo de los dispositivos.

Tabla 10. Resultados obtenidos de la ficha de observación del SW_PROYECTOS

Ficha de observación	
Tipo de Observación: Semiestructurada **Fecha:** 19/09/2024 **Observador:** Aida Cocha **Objetivo:** Evaluar la capacidad y configuración de los equipos de red del Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana para garantizar la Calidad de Servicio (QoS).	
Detalles del Equipo	
Nombre de equipo	SW_PROYECTOS
Tipo de equipo	Switch
Marca	Cisco
Modelo	WS-C2960-24LT-L
Sistema Operativo	Cisco IOS Software
Ubicación	CIDFAE-Proyectos
Configuración previa	No
Capacidad de hardware	
RAM	64 MB
Memoria FLASH	32 MB
Procesador	PowerPC405
Número de puertos	26 puertos
Tipo de cable en los puertos	UTP
Capacidad de QoS	
Soporta QoS	Si
Protocolos	ACL, ARP, DiffServ, IGMP, IP, RADIUS, SSH, TCP, UDP, DHCP, TFTP
Observaciones Generales: El switch se presenta en un estado bueno, con casi todos los puertos en condiciones adecuadas salvo el puerto 20. No se han realizado configuraciones previas, lo que sugiere una buena oportunidad para implementar ajustes específicos que optimicen la red.	
Conclusión: El equipo, se encuentra en buenas condiciones para llevar a cabo configuraciones que aseguren una calidad de servicio. La posibilidad de implementar QoS y la creación de VLANs brindan una excelente plataforma para la segmentación y gestión eficiente de la red.	

Tabla 11. Resultados obtenidos de la ficha de observación del SW_HANGAR

Ficha de observación	
Tipo de Observación: Semiestructurada **Fecha:** 19/09/2024 **Observador:** Aida Cocha **Objetivo:** Evaluar la capacidad y configuración de los equipos de red del Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana para garantizar la Calidad de Servicio (QoS).	
Detalles del Equipo	
Nombre de equipo	SW_HANGAR
Tipo de equipo	Switch
Marca	Cisco
Modelo	WS-C2960-24LT-L
Sistema Operativo	Cisco IOS Software
Ubicación	CIDFAE-HANGAR
Configuración previa	No
Capacidad de hardware	
RAM	64 MB
Memoria FLASH	32 MB
Procesador	PowerPC405
Número de puertos	26 puertos
Tipo de cable en los puertos	UTP

Capacidad de QoS	
Soporta QoS	Si
Protocolos	ACL, ARP, DiffServ, IGMP, IP, RADIUS, SSH, TCP, UDP, DHCP, TFTP
Observaciones Generales: El switch se presenta en un estado óptimo, todos los puertos en condiciones adecuadas. No se han realizado configuraciones previas, lo que sugiere una buena oportunidad para implementar ajustes específicos que optimicen la red	
Conclusión: El equipo, se encuentra en buenas condiciones para llevar a cabo configuraciones que aseguren una calidad de servicio. La posibilidad de implementar QoS y la creación de VLANs brindan una excelente plataforma para la segmentación y gestión eficiente de la red.	

Tabla 12. Resultados obtenidos de la ficha de observación del SW_GOMAI

Ficha de observación	
Tipo de Observación: Semiestructurada **Fecha:** 19/09/2024 **Observador:** Aida Cocha **Objetivo:** Evaluar la capacidad y configuración de los equipos de red del Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana para garantizar la Calidad de Servicio (QoS).	
Detalles del Equipo	
Nombre de equipo	SW_GOMAI
Tipo de equipo	Switch
Marca	Cisco
Modelo	WS-C2960-24LT-L
Sistema Operativo	Cisco IOS Software
Ubicación	CIDFAE-GOMAI
Configuración previa	Si
Capacidad de hardware	
RAM	64 MB
Memoria FLASH	32 MB
Procesador	PowerPC405
Número de puertos	26 puertos
Tipo de cable en los puertos	UTP
Capacidad de QoS	
Soporta QoS	Si
Protocolos	ACL, ARP, DiffServ, IGMP, IP, RADIUS, SSH, TCP, UDP, DHCP, TFTP
Observaciones Generales: El switch tiene 10 puertos dañados. Consta de una clave la cual no se encontraba documentada.	
Conclusión: A pesar de los puertos dañados, el switch SW_GOMAI se encuentra en buen estado y sin configuraciones previas más que la clave, lo que ofrece una gran oportunidad para implementar configuraciones de VLANs lo que permitirá optimizar el rendimiento de la red.	

Tabla 13. Resultados obtenidos de la ficha de observación del TPLINK_COMANDO

Ficha de observación	
Tipo de Observación: Semiestructurada **Fecha:** 20/08/2024 **Observador:** Aida Cocha **Objetivo:** Evaluar la capacidad y configuración de los equipos de red del Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana para garantizar la Calidad de Servicio (QoS)	
Detalles del Equipo	
Nombre de equipo	TPLINK_COMANDO
Tipo de equipo	Switch
Marca	TP-Link

Modelo	TL-SG1024DE
Sistema Operativo	N/A- Tiene un firmware específico de TP-Link
Configuración previa	No
Ubicación	CIDFAE-Comando
Capacidad de hardware	
RAM	16 MB
Memoria FLASH	4 MB
Procesador	Realtek
Número de puertos	24
Tipo de puerto	UTP
Capacidad de QoS	
Soporta QoS	Si (Soporta QoS básico)
Protocolos	802.1p, 802.1Q
Observaciones Generales: El switch se encuentra en buenas condiciones físicas y operativas, pero sus funcionalidades de QoS son limitadas en comparación con modelos más avanzados.	
Conclusión: El equipo cumple con los requisitos básicos para la gestión de tráfico en la red, pero se sugiere considerar la actualización a un modelo que ofrezca capacidades de QoS más avanzadas y soporte para más protocolos.	

Tabla 14. Resultados obtenidos de la ficha de observación del CORESWITCH

Ficha de observación	
Tipo de Observación: Semiestructurada **Fecha:** 20/09/2024 **Observador:** **Objetivo:** Evaluar la capacidad y configuración de los equipos de red del Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana para garantizar la Calidad de Servicio (QoS)	
Detalles del Equipo	
Nombre de equipo	CORESWITCH
Tipo de equipo	Switch
Marca	Cisco
Modelo	WS-C3750G-24PS-S
Sistema Operativo	Cisco IOS Software
Ubicación	CIDFAE-Comando
Configuración previa	No
Capacidad de hardware	
RAM	128 MB
Memoria FLASH	16 MB
Procesador	266 MHz
Número de puertos	24
Tipo de puerto	UTP
Capacidad de QoS	
Soporta QoS	Si
Protocolos	STP, RSTP, LACP, VTP, DTP, OSPF, EIGRP, HSRP, IGMP
Observaciones Generales: El switch se presenta en un estado óptimo, con todos los puertos en condiciones adecuadas. No se han realizado configuraciones previas, lo que sugiere una buena oportunidad para implementar ajustes específicos que optimicen la red.	
Conclusión: El equipo, se encuentra en buenas condiciones para llevar a cabo configuraciones que aseguren una calidad de servicio.	

Tabla 15. Resultados obtenidos de la ficha de observación del FortiGate

Ficha de observación
Tipo de Observación: Semiestructurada **Fecha:** 20/08/2024 **Observador:** Aida Cocha

Objetivo: Evaluar la capacidad y configuración de los equipos de red del Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana para garantizar la Calidad de Servicio (QoS)	
Detalles del Equipo	
Nombre de equipo	FORTIGATE
Tipo de equipo	Firewall
Marca	Fortinet
Modelo	FortiGate-40F
Sistema Operativo	FortiOS
Configuración previa	Si
Ubicación	CIDFAE-Comando
Capacidad de hardware	
RAM	4GB
Memoria FLASH	16GB
Procesador	ARMv8
Número de puertos	5
Tipo de puerto	UTP
Capacidad de QoS	
Soporta QoS	Si
Protocolos	IPv4, IPv6, OSPF, BGP, RIP, PIM, IPsec y SSL/TLS, DPI, Web Filtering, DNS, VLANs, DSCP, Telnet, SSH, HTTP/HTTPS, NTP.
Observaciones Generales: El equipo se encuentra en buenas condiciones físicas y operativas, con funcionalidades de QoS.	
Conclusión: El equipo cumple con los requisitos para la gestión de tráfico en la red. Su capacidad de QoS y soporte para protocolos de enrutamiento y VLANs facilitan la administración del tráfico y aseguran su integración en una red con demandas de calidad de servicio. Además, su funcionalidad de inspección profunda de paquetes (DPI) permite analizar y clasificar el tráfico en tiempo real, lo que mejora la seguridad y optimiza el rendimiento al priorizar aplicaciones.	

Tabla 16. Resultados obtenidos de la ficha de observación MIKROBOARD

Ficha de observación	
Tipo de Observación: Semiestructurada **Fecha:** 20/08/2024 **Observador:** Aida Cocha **Objetivo:** Evaluar la capacidad y configuración de los equipos de red del Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana para garantizar la Calidad de Servicio (QoS)	
Detalles del Equipo	
Nombre de equipo	MIKROBOARD PRINCIPAL
Tipo de equipo	Router
Marca	MikroTik
Modelo	RB951UI-2HND
Sistema Operativo	RouterOS
Configuración previa	Si
Ubicación	CIDFAE-Comando
Capacidad de hardware	
RAM	128 MB
Memoria FLASH	16MB
Procesador	600 MHz AR9344-DC3A
Número de puertos	5
Tipo de puerto	UTP
Capacidad de QoS	
Soporta QoS	Si
Protocolos	OSPF, BGP, RIP
Observaciones Generales: El MikroTik RB951Ui-2HnD está en buen estado y ofrece funciones básicas de enrutamiento y QoS.	
Conclusión: El equipo cumple con los requisitos de conectividad y gestión de tráfico, proporcionando soporte básico para enrutamiento y QoS.	

Tabla 17. Resultados obtenidos de la ficha de observación de la ONT

Ficha de observación	
Tipo de Observación: Semiestructurada **Fecha:** 20/08/2024 **Observador:** Aida Cocha **Objetivo:** Evaluar la capacidad y configuración de los equipos de red del Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana para garantizar la Calidad de Servicio (QoS)	
Detalles del Equipo	
Nombre de equipo	ONT
Tipo de equipo	Terminal de Red Óptica
Marca	Huawei
Modelo	HG8245H5
Sistema Operativo	Versión integrada en el firmware
Configuración previa	Si
Ubicación	CIDFAE-Comando
Capacidad de hardware	
RAM	128MB
Memoria FLASH	16MB
Procesador	Dual-core
Número de puertos	4 GE, 2 POTS
Tipo de puerto	UTP
Capacidad de QoS	
Soporta QoS	Si
Protocolos	IEEE 802.1p, DSCP, VLAN
Observaciones Generales: El equipo ONT Huawei HG8245H5 está en buenas condiciones y es funcional para la entrega de servicios de Internet y telefonía	
Conclusión: El equipo cumple con los requisitos necesarios para la entrega de servicios de red y gestión de tráfico en la red.	

2.2.4 Procesamiento y análisis de datos

Con la información recopilada en el CIDFAE, se llevó a cabo un análisis estadístico basado en las encuestas realizadas al personal. Los resultados de la encuesta se representan mediante un gráfico Figura 11 en los que se tomó en cuenta los datos mayores o iguales a 5.

Datos encuesta

Tabla 18. Preguntas para el análisis de la encuesta

N°	Pregunta	Opciones
1	¿Alguna vez usted ha experimentado interrupciones en la conexión de Internet?	Siempre Casi siempre Casi nunca
2	¿Considera usted que una conexión a Internet se vuelve lenta cuando se realizan múltiples tareas al mismo tiempo?	Sí No
3	¿Qué aspecto cree que podría mejorar en la red del CIDFAE?	Velocidad de conexión Estabilidad de la conexión Seguridad
4	¿Considera que la red asegura suficiente ancho de banda para las aplicaciones esenciales de su trabajo?	Siempre Casi siempre Casi nunca
5	¿Alguna vez los problemas de conectividad han afectado la realización de tareas en su puesto de trabajo?	Siempre Casi siempre Casi nunca
6	¿Considera que la conexión de Internet es estable durante todo el día?	Casi siempre Casi nunca Nunca
7	¿En qué momentos del día suelen notar más problemas de conexión?	Mañana (de 8:00 a 12:00) Mediodía (de 12:00 a 14:00) Tarde (de 14:00 a 16:30)
8	¿Con qué frecuencia la velocidad de carga de las páginas web es satisfactoria?	Siempre Casi siempre Casi nunca
9	¿Qué tan a menudo puede realizar videoconferencias sin interrupciones?	Casi siempre Casi nunca
10	¿Qué beneficios cree que se obtendrán al implementar nuevas configuraciones para mejorar el rendimiento de la red?	Mejora del rendimiento de la red Mayor estabilidad en la red Aumento en la seguridad de la información

Gráfico encuesta

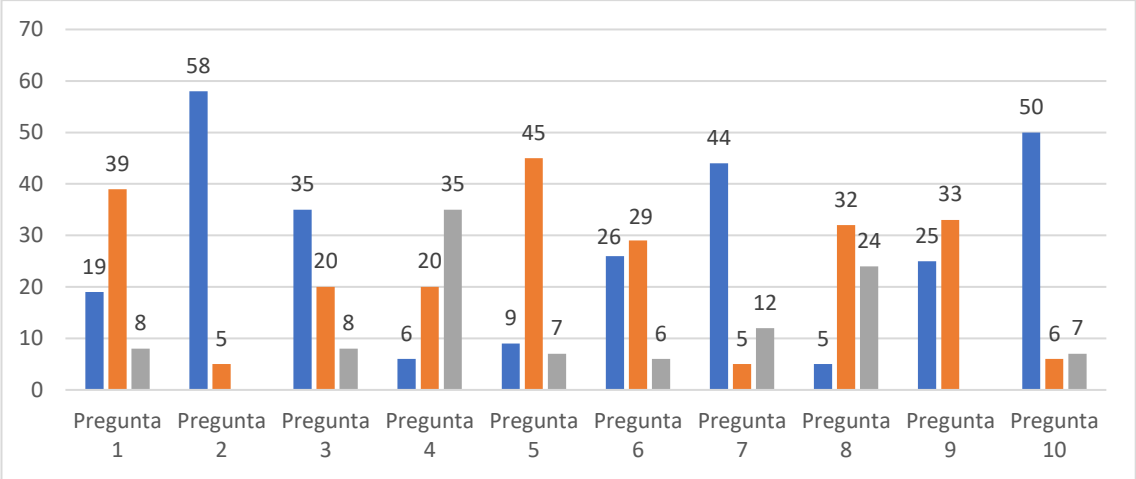


Figura 11. Estadísticas respuesta encuesta

En relación con los datos se agruparon en diferentes categorías basadas en el tipo de información: problemas de conectividad (Preguntas 1,5,6,7), rendimiento y uso de la red (Preguntas 2,4,8,9), mejoras y beneficios (Preguntas 3 y 10).

a. Problemas de conectividad

La gran mayoría del personal experimenta interrupciones frecuentes en la conexión a Internet, lo que afecta directamente su productividad y satisfacción laboral. Estos problemas de conectividad se presentan con mayor frecuencia durante las mañanas, un momento crítico para el inicio de las tareas, lo que sugiere una sobrecarga de la red en las horas pico.

b. Rendimiento y uso de la red

Una parte considerable del personal experimenta insuficiente ancho de banda, problemas de velocidad en la carga de páginas web y dificultades recurrentes en las videoconferencias, que son clave para la coordinación y comunicación en el entorno de trabajo.

c. Mejoras y uso de la red

La velocidad de conexión es el principal aspecto para mejorar en la red del CIDFAE. Implementar nuevas configuraciones es una prioridad, ya que optimizar la conectividad facilitaría el cumplimiento de las tareas diarias y mejoraría la eficiencia del trabajo.

De acuerdo con la información recolectada sobre la entrevista al personal se determina que:

- La red no está segmentada, lo que significa que no se han implementado técnicas de subnetting para dividir el rango de direcciones IP de manera eficiente.

- Las políticas de gestión de tráfico son insuficientes, lo que impide un control efectivo sobre la distribución del ancho de banda.

- La inexistencia de un plan de contingencia para abordar problemas imprevistos en la red expone al CIDFAE a riesgos adicionales, afectando la continuidad operativa y la seguridad de la información.

Con base en la información recopilada a través de la ficha de observación en la institución, se llegó a la determinación de:

- El switch SW_GOMAI presenta 10 puertos dañados, lo que limita su funcionalidad, la presencia de puertos inoperativos indica una necesidad de reparación o reemplazo para garantizar un servicio confiable.

- Se detectó la falta de configuraciones previas en los equipos evaluados, especialmente en los switches.

CAPÍTULO III. RESULTADOS Y DISCUSIÓN

3.1 Análisis y discusión de resultados

Mediante los instrumentos de recolección de la información llevados a cabo en el CIDFAE, se identifican varios problemas relacionados con la conectividad y el rendimiento de la red, estos problemas han sido detectados a través de la recopilación de información directa del personal y mediante el monitoreo y revisión de los equipos.

3.1.1 Análisis de los problemas y alternativas de solución

La Tabla 19 detalla cada problema identificado a partir de los instrumentos de recolección de información, su causa y la acción correctiva.

Tabla 19. Diagnóstico y Plan de Acción para la Red

Problema	**Causa**	**Acción**
Conexión lenta y caídas frecuentes	Sobrecarga de la red, problemas con el proveedor de servicios de Internet.	Segmentación de la red, implementación de calidad de servicio (QoS)
Bajo ancho de banda	Ancho de banda contratado insuficiente, configuraciones no realizadas, interferencias en la señal.	Aumentar contrato, optimizar configuración.
Red sin segmentación	Falta de planificación	Subnetting, VLANs, asignación IP.
Gestión de tráfico deficiente	Falta de control, priorización incorrecta.	Políticas de tráfico, monitoreo, QoS.
Daño en switch	Deterioro, falta de mantenimiento.	Reparar/reemplazar, mantenimiento preventivo.

3.1.2 Análisis de equipos de la red que soportan QoS

La red LAN del CIDFAE cuenta con tres switches Cisco 2960 WS-C2960-24LT-L, un switch Cisco 3750 WS-C3750G-24PS-S, switch TP-Link TL-SG1024DE y un FortiGate 40F. A continuación, se describen los equipos y sus características en términos de QoS.

a. Switch Cisco 2960

Los switches Cisco Catalyst 2960 son una gama de dispositivos que ofrecen conectividad rápida. A continuación, se detallan sus características [29].

- Permite clasificar el tráfico usando Class of Service (CoS) y DSCP, lo que facilita la priorización de diferentes tipos de datos según su importancia.
- Utiliza algoritmos como Weighted Tail Drop (WTD) para manejar la congestión, garantizando que el tráfico crítico sea tratado preferentemente.
- Admite listas de control de acceso (ACL) para controlar el tráfico, garantizando un uso adecuado de los recursos.

b. Switch Cisco 3750

Son una línea de productos innovadora que optimiza significativamente la eficiencia operativa en redes LAN, combinando facilidad de uso reconocida en el mercado con una alta fiabilidad en switches apilables. Sus características con respecto a QoS son [30]:

- Permite identificar y clasificar el tráfico según distintos parámetros, como las etiquetas DSCP y CoS.
- La capacidad de controlar el tráfico entrante para mantener la integridad del ancho de banda, en este modelo el tráfico puede ser medido y regulado a una velocidad específica.
- Se soportan acciones como el marcado y el control de tráfico, permitiendo una gestión efectiva de la calidad del servicio en función de las necesidades específicas de la red.

c. Switch TP-LINK

El switch TP-Link TL-SG1024DE es un modelo de 24 puertos que ofrece soporte para VLAN, lo que permite segmentar la red para una mejor gestión del tráfico,

proporciona QoS por puerto y basado en etiquetas, lo que posibilita que el tráfico sensible a la latencia fluya sin interrupciones [31].

d. FortiGate-40F

El QoS en FortiGate permite gestionar y optimizar el tráfico de red ajustando aspectos como la priorización de colas y el control del tráfico. A continuación, se destacan los aspectos más relevantes sobre trafic shapping [32].

- El Traffic Shaping en FortiGate utiliza políticas para identificar y controlar tráfico específico, ya sea por aplicación, dirección IP, servicios (puertos), categorías de URL.

- Los perfiles de Traffic Shaping permiten configurar parámetros, como el ancho de banda garantizado, que asegura un mínimo reservado para tráfico crítico, y el ancho de banda máximo, que establece un límite superior para evitar congestión.

- Se asignan prioridades a las clases de tráfico mediante niveles como “High”, “Medium” y “Low”, es posible definir hasta 30 clases de tráfico para diferenciar y manejar distintos tipos de datos en la red.

- Es compatible con el marcado DiffServ Code Point (DSCP) lo que facilita la priorización de paquetes, la coincidencia DSCP se utiliza para identificar las etiquetas DSCP en el tráfico que ingresa, mientras que el marcado DSCP permite modificar estas etiquetas en el tráfico que sale de la red.

- FortiGate utiliza dos métodos principales de Traffic Shaping: Policing, que descarta paquetes que exceden el ancho de banda configurado para evitar saturaciones y Queuing para retener tráfico excedente en una cola hasta que haya ancho de banda disponible, descartando paquetes si la cola se llena.

FortiGate fue elegido para implementar QoS debido a su capacidad para gestionar tráfico de manera centralizada, lo que simplifica la priorización de aplicaciones, su compatibilidad con técnicas avanzadas como Traffic Shaping, que garantiza un mínimo de ancho de banda y limita excesos. Además, integra QoS con políticas de seguridad, ofreciendo un control eficiente tanto para el tráfico LAN como WAN.

3.1.3 Parámetros de QoS

En la Tabla 20, se presenta los parámetros para evaluar el rendimiento de redes y sistemas de comunicación, los cuales son necesarios para garantizar una transmisión de datos eficiente y confiable [33], [34].

Tabla 20. Parámetros de QoS

Métrica	**Unidades**	**Descripción**
Retardo (Latencia)	ms	Tiempo que tarda en transmitirse la información desde el origen hasta el destino.
Ancho de Banda	Kb/s	Cantidad de datos que una interfaz puede transmitir, expresada en bits por segundo.
Jitter	ms	Variación en el retraso de los paquetes.
Pérdida de Paquetes	%	Proporción de paquetes que no alcanzan su destino.

3.1.4 Modelos para la obtención de QoS

Existen modelos de servicio que se pueden definir como un conjunto de capacidades de QoS de extremo a extremo. Dentro de estos modelos se identifican los siguientes niveles de servicio [33], [35] :

a. IntServ (Servicios Integrados)

El modelo IntServ (RFC 1633), fue creado por la Internet Engineering Task Force (IETF) con el objetivo de asegurar la calidad de servicio (QoS) de extremo a extremo en aplicaciones de tiempo real. En este modelo, la aplicación solicita un tipo específico de servicio según su perfil de tráfico y solo enviará los datos una vez que reciba confirmación de la red. IntServ reserva los recursos a lo largo de toda la ruta y exige que todos los nodos intermedios mantengan el estado de flujo, lo que genera un consumo significativo de recursos y por lo tanto, limita su escalabilidad.

b. DiffServ (Servicios Diferenciados)

El modelo DiffServ (RFC 2475) fue desarrollado como una solución a los problemas de escalabilidad presentes en IntServ para identificar los grupos de tráfico, se emplea un código DSCP. Cada paquete con el mismo código DSCP recibe el mismo tratamiento en cada nodo de la red; el comportamiento por salto (PHB) define cómo

se maneja cada clase de tráfico y las funciones de condicionamiento del tráfico, tales como medición, marcado, forma y vigilancia. La Tabla 21 presenta los 4 servicios disponibles de PHBs.

Tabla 21. Servicios de comportamiento por salto

Servicio	**RFC**	**Descripción**
Best Effort	2474	Este servicio se distingue por tener los tres primeros bits del DSCP en cero. Los dos bits restantes pueden usarse para asignar una prioridad, pero no ofrece ningún tipo de garantía.
Class-Selector (CS)	2474	Define un conjunto de siete valores DSCP, que van desde 001000 hasta 111000, los cuales se utilizan para clasificar y priorizar el tráfico de red.
Assured Forwarding (AF)	2597	Se definen cuatro clases posibles, a las cuales se puede asignar una cantidad determinada de recursos, como ancho de banda o espacio en los buffers.
Expedited Forwarding o Premium (EF)	2598	Tiene un valor DSCP de 101110 lo que permite ofrecer un servicio con bajo jitter, baja pérdida de datos, baja latencia y un ancho de banda garantizado.

Se eligió el modelo DiffServ porque es altamente escalable y flexible, permitiendo manejar grandes volúmenes de tráfico en redes complejas sin sobrecargar los nodos.

3.1.5 Tipos de encolamiento para gestión de congestión en la red

El encolamiento es una técnica utilizada para gestionar la congestión en una red, permitiendo asignar prioridades y reorganizar los paquetes antes de enviarlos hacia su destino. La Tabla 22 se presenta una comparación de los diferentes tipos de encolamiento, en la que se describen diversos parámetros que caracterizan a cada uno de ellos. Entre estos parámetros se incluyen la capacidad de priorización del tráfico, la eficiencia en el manejo de la congestión, los tiempos de respuesta, la complejidad asociada a su configuración, la asignación de ancho de banda según las necesidades de la red y se destacan las limitaciones específicas de cada algoritmo [33], [28], [36].

Tabla 22. Comparación de tipos de encolamiento

Algoritmo / Parámetro	First-In, First-Out (FIFO)	Priority Queuing (PQ)	Weighted Fair Queuing (WFQ)	Class Based Weighted Fair Queuing (CBWFQ)	Low Latency Queueing (LLQ)
Prioridad de tráfico	No ofrece prioridad a ningún tráfico, todos los paquetes se procesan en el orden en que llegan.	Proporciona prioridad estricta a ciertas clases de tráfico.	Asigna dinámicamente prioridad basada en pesos a diferentes clases de tráfico.	Amplía WFQ permitiendo definir clases específicas con prioridades personalizadas	Combina la prioridad estricta con un sistema de cola, asegurando que el tráfico prioritario reciba un tratamiento preferencial.
Eficiencia en manejo de congestión.	No tiene capacidad para manejar congestión.	Prioriza tráfico crítico, pero puede causar privación en otras clases.	Distribuye los recursos de manera justa y evita que una sola clase monopolice el ancho de banda.	Es capaz de manejar redes complejas.	Evita la congestión para tráfico sensible.
Tiempo de respuesta	Variable depende de la cantidad de tráfico en cola.	Bajos para alta prioridad; altos para baja prioridad.	Adecuado para escenarios que requieren rapidez en la entrega de datos, tanto para usuarios de alto como bajo consumo de red.	Tiempo de respuesta ajustado según prioridades de las clases.	El tráfico prioritario se procesa casi inmediatamente.
Complejidad de Configuración	Es fácil de implementar y entender, lo que facilita su gestión.	Requiere clasificar tráfico y asignar prioridades manualmente	Requiere de un análisis para configurar pesos para cada clase.	Definir políticas avanzadas y límites para clases puede ser complejo.	La configuración de LLQ es algo compleja porque requiere una planificación para identificar y clasificar el tráfico.
Asignación de Ancho de Banda	No asigna ancho de banda a clases específicas.	No permite asignar ancho de banda fijo.	Asigna ancho de banda proporcionalmente según los pesos establecidos para las clases de tráfico.	Control avanzado asigna ancho de banda explícito para cada clase definida.	Asigna ancho de banda eficiente y asegura prioridad absoluta para aplicaciones importantes.
Limitaciones	Puede introducir retrasos en la entrega de paquetes, especialmente si hay un gran volumen de tráfico.	Si el tráfico de alta prioridad se vuelve excesivo, las colas de menor prioridad pueden experimentar una escasez total de recursos.	Necesita llevar un registro detallado de varias categorías de servicio y revisar ese registro cada vez que llega un paquete.	CBWFQ utiliza un algoritmo sofisticado que necesita una cantidad considerable de estados de clases de servicio y realizar un seguimiento del estado de cada paquete entrante.	El seguimiento y la gestión de múltiples colas pueden incrementar la carga en los dispositivos de red, afectando su rendimiento general.

Weighted Fair Queuing WFQ es la opción que más se acomoda al proyecto porque permite clasificar el tráfico en clases y asignarles un peso específico para un uso eficiente del ancho de banda. Al combinarlo con Low Latency Queuing (LLQ), prioriza tráfico sensible al retraso, garantizando baja latencia sin afectar otros datos.

3.1.6 Mecanismo de regulación de tráfico

Traffic Policing y Traffic Shaping son modelados de QoS que controlan el flujo de datos utilizando un medidor de tráfico Token Bucket. Policing limita el tráfico descartando o marcando los datos que exceden la tasa configurada mientras que Shaping retiene los paquetes excedentes en una cola para enviarlos gradualmente, suavizando el flujo. En la Tabla 23, se describen las diferencias entre cada modelado [37].

Tabla 23. Comparativa entre Traffic Shapping y Policing

Criterio	**Shapping**	**Policing**
Propósito	Guarda en un búfer y organiza en cola los paquetes que excedan las velocidades acordadas.	Descarta los paquetes que superan las tasas establecidas, sin realizar almacenamiento en búfer.
Aplicación	Tráfico saliente	Tráfico entrante y saliente.
Tipo de encolamiento	PQ y WFQ	No utiliza encolamiento, procesa directamente.

3.1.7 Metodología de desarrollo

Una metodología en redes proporciona un enfoque estructurado y sistemático para diseñar, implementar y gestionar infraestructuras, minimizando errores, optimizando recursos y asegurando que la red cumpla con los requisitos de rendimiento, seguridad y escalabilidad. En el presente proyecto, se eligió tres metodologías Cisco, Davis Etheridge y Errol Simón, y McCabe James. Cisco por su marco integral, que cubre cada fase del ciclo de vida de la red, facilitando tanto la construcción inicial como la mejora continua, para adaptarse a cambios tecnológicos y a las necesidades de tráfico, Davis Etheridge y Errol Simón es adaptable a proyectos medianos y pequeños, con bibliografía que describe sus fases, procesos y actividades y la de McCabe James, permite un análisis de necesidades específicas y de los flujos de transferencia ajustados

a los requerimientos de un sistema de telecomunicaciones [7], [38], [39]. La Tabla 24 presenta la comparativa en la que se centró la elección de metodología, aspectos como flexibilidad, capacidad para evolucionar y eficacia operativa, con el fin de identificar aquella que se ajuste a las necesidades específicas del estudio.

Tabla 24. Comparativas de metodologías

Metodología / **Características**	**Cisco**	**Davis Etheridge y Errol Simón**	**McCabe James**
Enfoque	Soluciones empresariales integrales y personalizadas.	Planeamiento estratégico a largo plazo.	Metodología detallada para redes y sistemas.
Escalabilidad	Ofrece alta escalabilidad para adaptarse a las necesidades crecientes de una empresa.	Escalabilidad media adecuada para empresas medianas y grandes.	Media, adaptable a medianas empresas.
Seguridad	Tiene encriptación y medidas de control de tráfico en tiempo real.	Adaptable, con medidas de seguridad escalables	Máxima, con enfoque en minimizar ataques y asegurar tráfico
Flexibilidad	Permite configuraciones personalizadas basadas en las necesidades específicas de la red.	Los modelos teóricos pueden no ser aplicables a todas las situaciones prácticas.	Se puede adaptar a diferentes tipos de redes y necesidades a través de simulaciones.
QoS	Soluciones avanzadas, con control sobre clases de servicio y priorización por tipo de tráfico.	Configurable, pero dependiente de estándares y adaptabilidad en función del tráfico.	Integración de QoS con auditorías de tráfico y medidas de seguridad proactivas.

Tras analizar las características de cada metodología se decidió seleccionar Cisco, el mayor fabricante de equipos de red que describe las múltiples fases por las que una red atraviesa mediante el ciclo de vida de redes Preparar, Planear, Diseñar, Implementar, Operar, Optimizar (PPDIOO). Esta metodología fue elegida debido a su enfoque en soluciones empresariales integrales y personalizadas, permitiendo ajustar la red según las necesidades específicas de seguridad, tráfico y servicio en el entorno de la Fuerza Aérea.

Cisco ofrece alta escalabilidad, aspecto importante en un entorno militar donde la infraestructura de red puede crecer. Además, su enfoque en seguridad para proteger datos sensibles con respecto a QoS, Cisco proporciona soluciones que permiten

priorizar el tráfico y su flexibilidad en las configuraciones garantiza la implementación de políticas personalizadas.

a. Descripción de las fases de la metodología

Para poder definir una mejor estructura del proyecto en la Tabla 25, se detallan las fases principales del proceso. Cada fase incluye las actividades a realizarse, permitiendo un enfoque ordenado y progresivo.

Tabla 25. Fases del proyecto

Fases	Descripción	Actividades
Preparar	Identificación de requisitos y objetivos.	• Identificar requerimientos de la red. • Definir restricciones o limitaciones de la institución
Planear	Elaboración de un plan detallado para las configuraciones en la red y monitoreo preliminar.	• Evaluar el rendimiento actual utilizando herramientas de monitoreo y capturar de paquetes. • Elaborar una tabla con los hallazgos encontrados mediante el monitoreo. • Elaborar una tabla con los parámetros que se configurarán para la gestión de QoS
Diseñar	Esquema de bloques de la planificación, creación de un diseño de la red.	• Diseñar esquema de bloques planificación. • Diseñar la topología de la red.
Implementar	Despliegue de la red conforme al diseño.	• Configurar equipos de red. • Implementar VLANs y QoS. • Probar la conectividad inicial. • Documentar la nueva configuración
Operar	Monitoreo de la red para garantizar su funcionalidad.	• Monitorear tráfico y rendimiento. Identificar posibles problemas.
Optimizar	Evaluación continua para mejorar el rendimiento y corrección de errores	• Corregir errores identificados.

3.2 Desarrollo de la propuesta

3.3 Aplicación de la metodología de trabajo

Para el desarrollo del proyecto se examinaron las diferentes fases de la metodología Cisco, con lo cual se busca asegurar que el proyecto se realice de manera estructurada y eficiente maximizando el valor y minimizando los riesgos.

3.3.1 Fase I: Preparar

Durante la fase de preparación, se estableció una base para abordar los problemas de conectividad y rendimiento de la red estableciendo los requisitos. Para ello, se tomarán las siguientes acciones:

a) Requisitos de la red

- Se identificaron varios problemas en la red del CIDFAE que afectan la conectividad y el rendimiento general como se mostró en la Tabla 19.
- La elaboración de una lista de parámetros bajo lo que se regirá la implementación de QoS.
- Se utilizará herramientas para monitorear el rendimiento de la red y evaluar la efectividad de las soluciones implementadas.

b) Restricciones o desafíos

- Bajo presupuesto.
- Documentación sobre claves en los equipos.
- Establecer un cronograma claro para la implementación, asegurando que el personal no se vea afectado sin la conexión a Internet

3.3.2 Fase II: Planear

En esta etapa, se identificaron las herramientas necesarias para el monitoreo del tráfico de la red, se planificó la implementación de políticas de QoS y se seleccionó los parámetros y valores dscp para el consumo de ancho de banda identificando áreas que necesitaban atención.

b. Monitoreo de la red actual

La Tabla 26 presenta las características de diversas herramientas utilizadas para el monitoreo de redes, considerando su aplicabilidad en el contexto del CIDFAE. Aunque no todas estas herramientas fueron implementadas directamente en el monitoreo, se incluyen en el análisis por su relevancia y potencial en el diagnóstico y gestión de redes [40],[41], [42], [7], [43].

Tabla 26. Características herramientas de monitoreo

Herramienta	Capacidades de Monitoreo	Fortalezas	Caso de Uso	Limitaciones	Nivel de confiabilidad
FortiGate	Monitoreo en tiempo real del tráfico de red con Dashboard con métricas de ancho de banda.	Visualización de picos de tráfico, gestión de ancho de banda e integración con análisis de aplicaciones.	Monitoreo de tráfico empresarial.	Requiere licencias específicas para acceso completo a funciones avanzada	Alta: Plataforma empresarial con integración de seguridad y gestión de tráfico.
Palo Alto Networks	Monitoreo en tiempo real del tráfico de red. Detecta patrones anómalos.	Capacidad de identificar patrones de tráfico y momentos críticos.	Monitoreo y seguridad avanzada de red y análisis detallado de aplicaciones.	Altos costos de licencias para configuraciones completas.	Alta: Seguridad avanzada y análisis detallado de tráfico.
PingPlotter	Visualización gráfica de la latencia y la pérdida de paquetes en cada salto de la ruta.	Ideal para identificar puntos de conectividad en la red y es fácil de usar para monitorear.	Monitoreo de estabilidad en tiempo real.	Enfoque limitado al diagnóstico, no a la optimización.	Media: Útil para diagnóstico de latencia, pero sin optimización.
SpeedTest	Prueba de velocidad de conexión.	Rápido y fácil de usar para verificar la velocidad real de conexión.	Pruebas rápidas de velocidad de Internet.	Mide solo el estado de la red en ese momento	Media: Solo mide velocidad de conexión, sin análisis de red.
Nperf	Test de velocidad de Internet con análisis detallado.	Ofrece información detallada sobre latencia y estabilidad	Evaluación de la estabilidad y calidad de conexión a Internet.	Mide solo el estado de la red en ese momento	Media-Alta: Ofrece más detalles sobre latencia y estabilidad.
Wireshark	Captura y análisis detallado de paquetes de red.	Proporciona monitoreo de tráfico por protocolo, pérdida de paquetes.	Ideal para análisis técnico profundo de la red.	No es útil para análisis rápidos o generales.	Alta: Análisis profundo de tráfico, pero requiere conocimiento técnico.

En base a las características analizadas, las herramientas seleccionadas para el monitoreo de la red en el CIDFAE fueron FortiGate, Palo Alto Networks, PingPlotter,

Nperf y Wireshark. Estas herramientas fueron elegidas debido a su capacidad para abordar distintos aspectos del monitoreo y diagnóstico de redes.

- ***Herramienta Fortigate***

La Figura 12 y Figura 13 muestran la interfaz de FortiGate en la sección FortiView Destinations, donde se analiza el tráfico de red según los destinos y el consumo de datos para acceder al equipo se utilizó la IP de administración. La gráfica, abarca 7 días de monitoreo, se observa que los picos de tráfico más altos ocurren en martes, miércoles y viernes, con una disminución significativa durante el fin de semana. La tabla inferior revela que los patrones de tráfico más utilizados corresponden a los protocolos QUIC, SSH, HTTPS y HTTP, lo que indica una combinación de navegación segura, streaming de video y descargas de archivos. Además, se observa un uso de plataformas de videoconferencias.

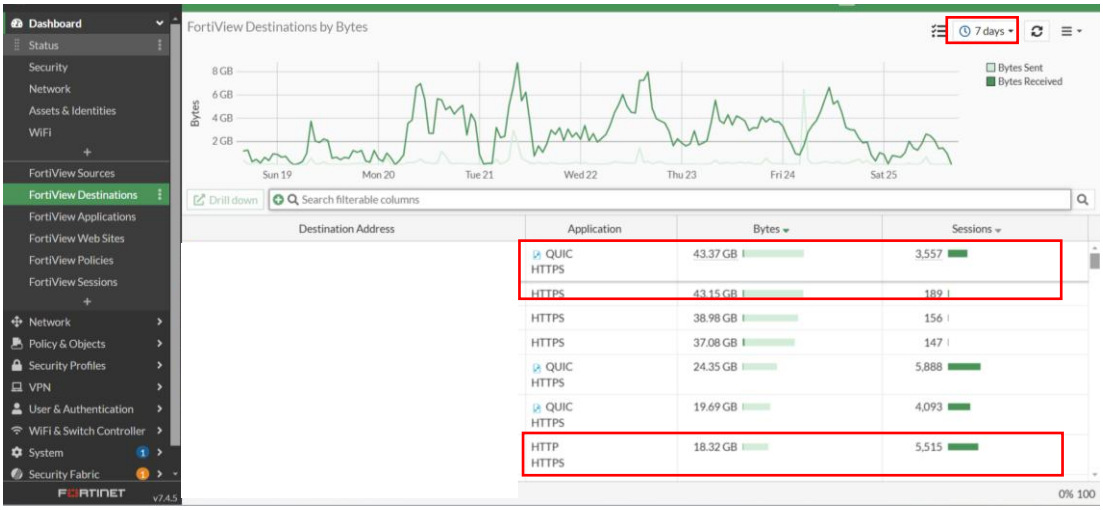


Figura 12. Monitoreo y patrones de uso Fortigate 7 días (Parte 1)

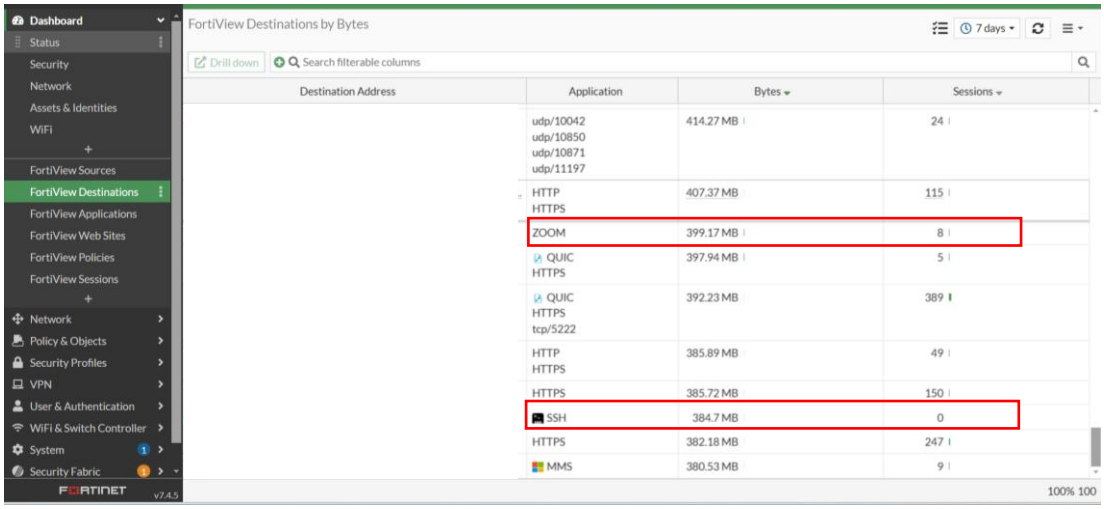


Figura 13. Monitoreo y patrones de uso Fortigate 7 días (Parte 2)

En la Figura 14 muestra el monitoreo de la red durante siete días, se observa que los días con mayor tráfico fueron el lunes, martes, miércoles y viernes, ya que presentan los picos más altos y frecuentes. En contraste, el sábado y domingo registraron un tráfico considerablemente menor, manteniéndose más estable y con valores bajos en la transferencia de datos. Esto sugiere un patrón de mayor demanda en días laborales, posiblemente debido a un incremento en el uso de aplicaciones y servicios en línea.

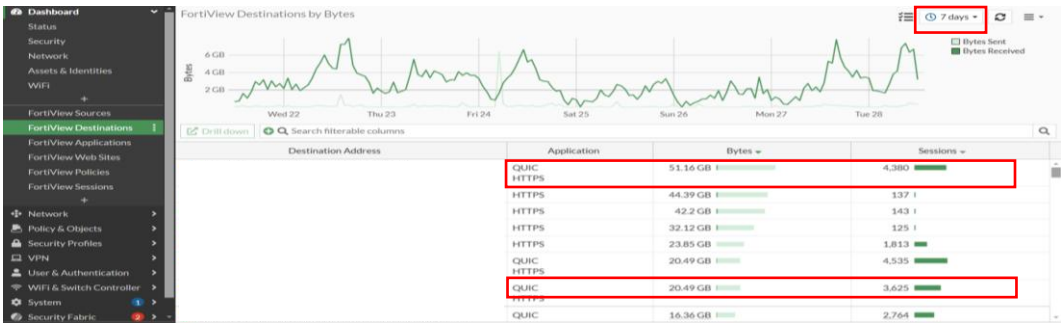


Figura 14. Monitoreo y patrones de uso Fortigate 7 días

La Figura 15 muestra el monitoreo del tráfico de la red durante las últimas 24 horas, destacando que los protocolos QUIC y HTTPS predominan en las conexiones. Esto sugiere un uso significativo de conexiones seguras, principalmente relacionadas con la navegación web, videoconferencias o descargas de contenido. Los momentos de

mayor tráfico se registran entre las 06:00 y las 08:00, de 09:00 a 12:00, y poco antes de las 18:00 horas.

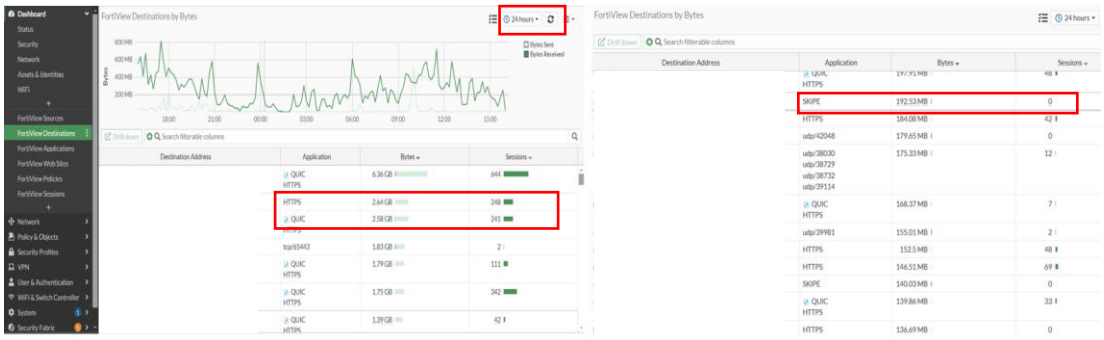


Figura 15. Monitoreo y patrones de uso Fortigate 24 horas

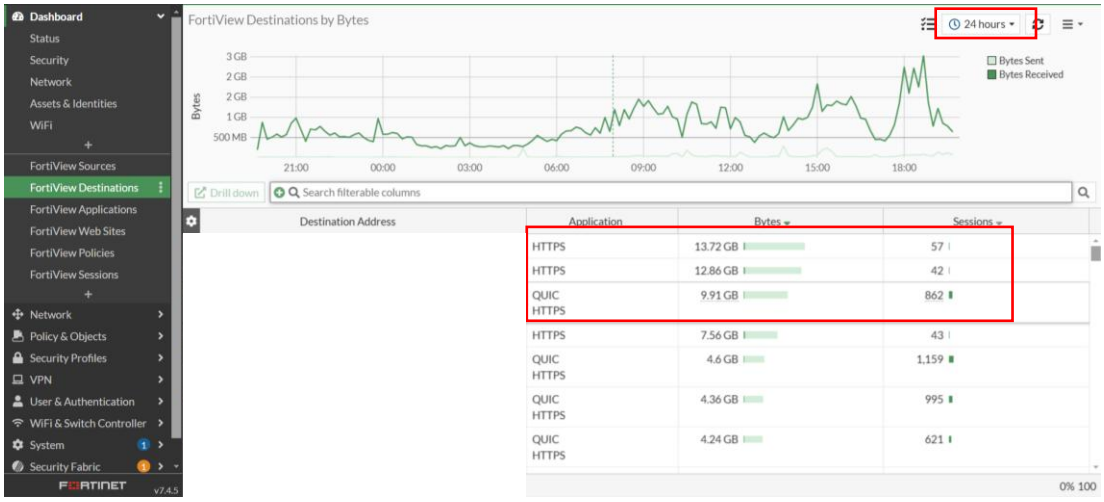


Figura 16. Monitoreo y patrones de uso Fortigate 24 horas

- ***Herramienta Palo Alto***

Como parte del monitoreo inicial y como complemento, se llevó a cabo un análisis utilizando la herramienta Palo Alto PA-440 al cual se accedió a través de su IP de administración. A continuación, se detallan los protocolos de red y las categorías asociadas al tráfico de aplicaciones [43], [44] .

unknown-udp: Se refiere al tráfico de red que utiliza el protocolo UDP. Puede incluir aplicaciones o servicios no reconocidos o no estándar.

ms-update: Son las actualizaciones de Microsoft, que incluyen parches de seguridad, mejoras y nuevas versiones de software.

Secure Sockets Layer (SSL): Es un protocolo de seguridad que establece comunicaciones encriptadas entre clientes y servidores.

Facebook-base: Este identificador del tráfico básico de Facebook, incluyendo actividades como la navegación.

WhatsApp-base: Es el tráfico de WhatsApp, que abarca el envío y recepción de mensajes de texto, imágenes, notas de voz y otras funciones.

Google-base: Este término engloba el tráfico de los servicios de Google, como búsquedas, acceso a Gmail, Google Drive y otras aplicaciones principales de Google.

TikTok-base: Es el tráfico básico de TikTok, incluyendo la visualización y carga de videos, interacción con contenido.

Real-time Transport Control Protocol (RTCP): Es un protocolo complementario al que se utiliza para supervisar la calidad de servicio.

Quick UDP Internet Connections (QUIC): Desarrollado por Google, QUIC es un protocolo de transporte que utiliza UDP para establecer conexiones más rápidas y seguras en comparación con TCP.

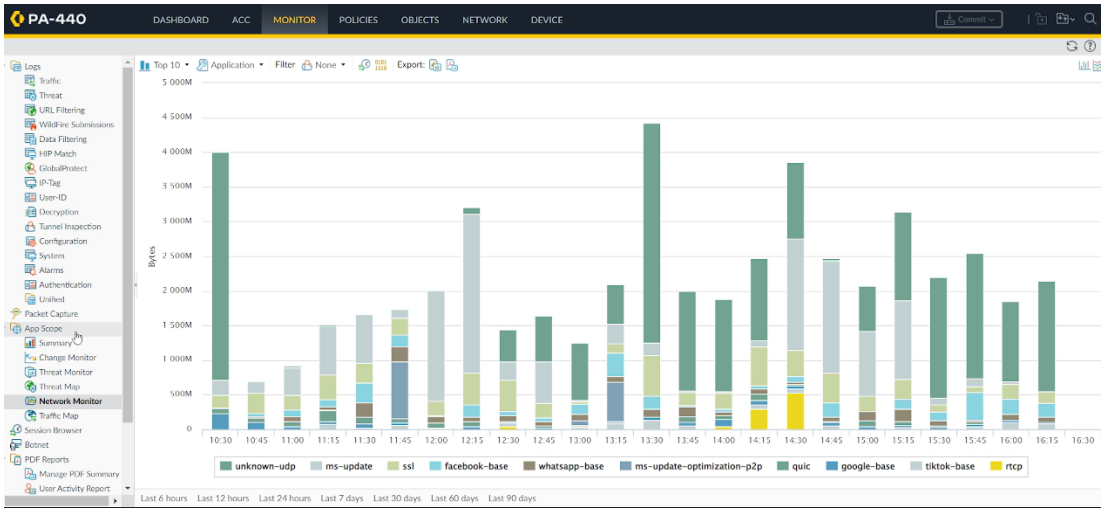


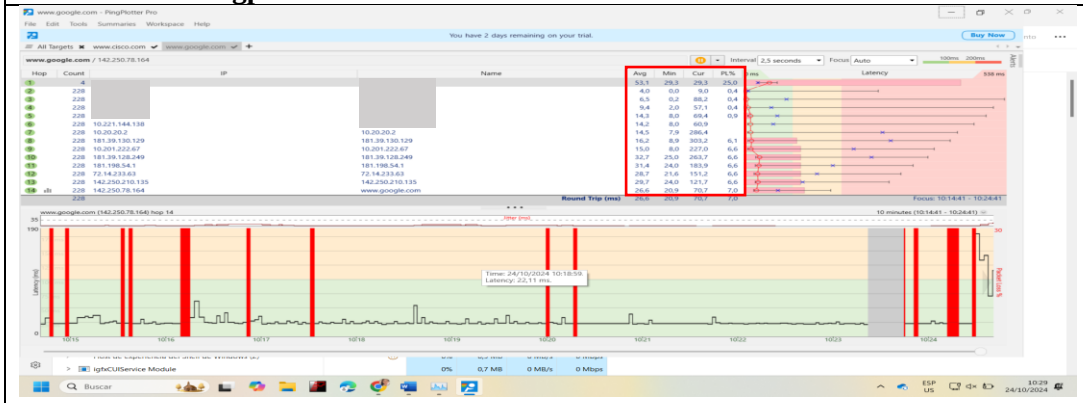
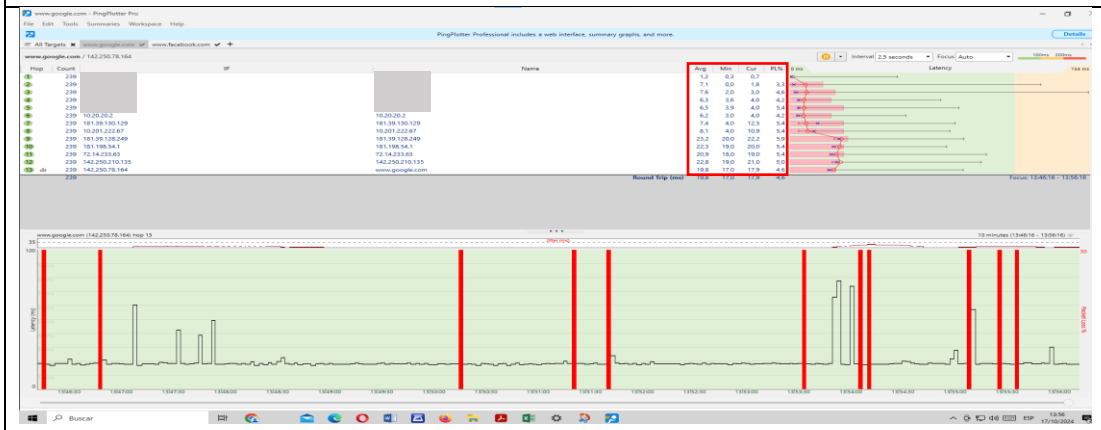
Figura 17. Monitoreo de tráfico de red en el firewall Palo Alto.

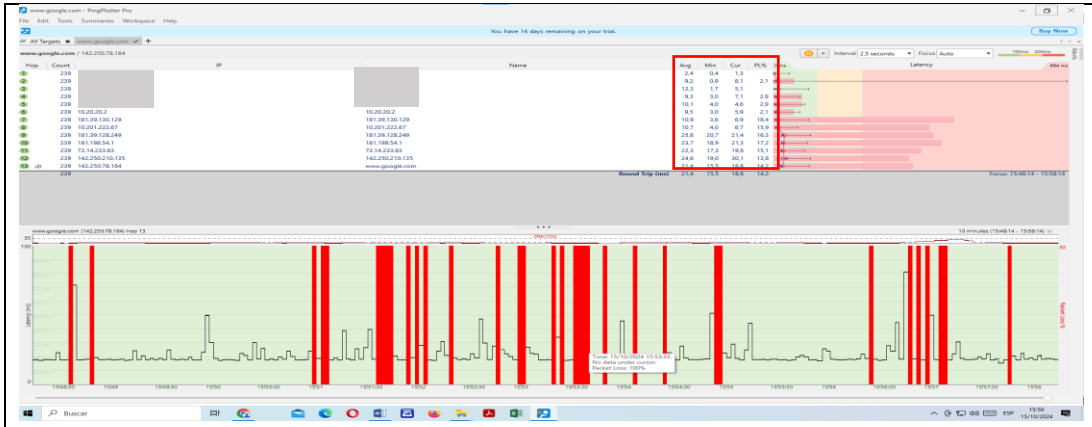
En la Figura 17, se muestra el tráfico en el firewall Palo Alto el cual revela que los momentos de mayor consumo de ancho de banda ocurrieron a las 10:30, 13:30 y 15:00, reflejando picos significativos en el uso de la red. Durante estos periodos, se identificó un alto tráfico asociado a Google, QUIC, SSL y actualizaciones de Microsoft, lo que sugiere actividades como navegación, transmisión de datos cifrados y descargas de software.

- ***Herramienta PingPlotter***

Para realizar esta prueba, se estableció el siguiente escenario: la conexión fue por cable Ethernet desde la computadora, la cual está equipada con una tarjeta de red de 1 Gbps, la ubicación fue en el área de comando. Se utilizó PingPlotter para evaluar la conectividad de la red y detectar posibles problemas de rendimiento, mediante el envío de pings a google.com. En la Tabla 27 se presentan las capturas obtenidas con la herramienta en distintos horarios de la jornada laboral.

Tabla 27. Monitoreo mediante Pingplotter

Herramienta Pingplotter	Descripción
 Figura 18. Monitoreo realizado en la mañana	La imagen refleja fluctuaciones en la latencia con momentos de pérdida de paquetes, lo que podría afectar la estabilidad de la conexión. Los colores representados en la gráfica simbolizan lo siguiente: • **Verde**: Indica una conexión estable con latencia baja y sin pérdida de paquetes significativa. • **Amarillo**: Representa una latencia moderada, lo que sugiere congestión leve en la red. • **Rojo**: Señala problemas de conectividad graves, ya sea alta latencia o pérdida de paquetes. • **Líneas verticales rojas**: Corresponden a momentos de pérdida de paquetes en la red, indicando interrupciones en la conectividad.
 Figura 19. Monitoreo realizado al medio día	La red experimenta pérdida de paquetes en varios momentos, lo que podría impactar la calidad del servicio. Este monitoreo se llevó a cabo al mediodía.

 Figura 20. Monitoreo realizado en la tarde	Se observa una latencia variable con picos de alto retraso y una significativa pérdida de paquetes, representada por numerosas líneas rojas en la gráfica inferior las pruebas se llevaron a cabo durante la tarde.

La Tabla 28 muestra la variación de latencia y pérdida de paquetes a lo largo del día, los valores fueron obtenidos de la Tabla 27. Asimismo, se encuentra la interpretación basada en los resultados obtenidos. Para ello, se calculó el promedio de la latencia y la pérdida de paquetes en cada jornada, para obtener una visión más clara y representativa del comportamiento de la red.

Tabla 28. Análisis de latencia y pérdida de paquetes según la jornada

Jornada	**Valores de Latencia**	**Avg (Latencia promedio) en ms**	**PL% (Pérdida de paquetes)**	**Promedio pérdida de paquetes en %**	**Interpretación**
Mañana	53.1, 4.0, 6.5, 9.4, 14.3, 14.2, 14.5, 16.2, 15.0, 32.7, 31.4, 28.7, 29.7, 26.6	21.16	25.0, 0.4, 0.4, 0.4, 0.9, 0.9, 6.1, 6.6, 6.6, 6.6, 6.6, 6.6, 7.0	5.76	Existe una mayor congestión en la red. Esto puede deberse al incremento en el uso de aplicaciones de trabajo y videoconferencias en las primeras horas del día.
Medio día	1.2, 7.1, 7.6, 6.3, 6.5, 6.2, 7.4, 8.1, 23.2,	12.26	3.3, 3.3, 4.6, 4.2, 5.4, 4.2, 5.4, 5.4, 5.9, 5.4, 5.4, 5.0, 4.6	4.78	Presenta la menor latencia porque existe reducción del tráfico en la red debido a que el personal en este lapso sale al almuerzo.

	22.3, 20.9, 22.8, 19.8				
Tarde	2.4, 9.2, 12.3, 9.3, 10.1, 9.5, 10.9, 10.7, 25.8, 23.7, 22.3, 24.6, 21.4	14.78	2.1, 2.1, 2.9, 2.9, 2.9, 2.1, 18.4, 15.9, 16.3, 17.2, 15.1, 13.8, 14.2	9.68	La latencia se mantiene en un nivel intermedio, pero la pérdida de paquetes aumenta está relacionado con un mayor uso de la red

- ***Herramienta Wireshark***

Se utilizó Wireshark en la que se aplicó el filtro “tcp.analysis.retransmission || tcp.analysis.duplicate_ack || tcp.analysis.out_of_order” para detectar problemas en la calidad de la conexión TCP [46], representado con la barra roja específicamente pérdidas de paquetes, duplicación de ACKs y paquetes fuera de orden . La línea continua en color celeste representa la cantidad total de paquetes TCP capturados a lo largo del tiempo en la red. Cada vez que la línea sube, indica un aumento en la cantidad de paquetes TCP que están siendo enviados y recibidos en la red, mientras por que la línea color violeta representa los paquetes UDP. La Tabla 29 presenta capturas del monitoreo realizado con Wireshark en diferentes áreas y horarios, un aspecto importante a destacar es la presencia de zonas en rojo en algunas gráficas. Esto puede deberse a congestión en los dispositivos de red, saturación de ancho de banda o fluctuaciones en la conectividad.

Tabla 29. Capturas del tráfico utilizando Wireshark

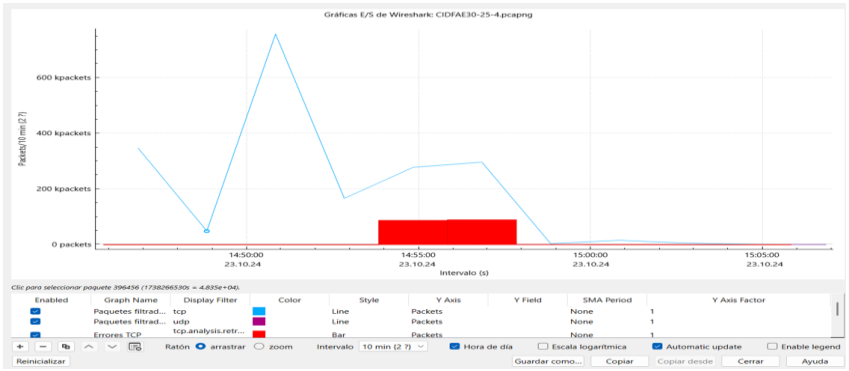


Figura 21. Captura en Wireshark - Tarde en el área PROYECTOS



Figura 22. Captura en Wireshark - Mañana en el área HANGAR



Figura 23. Captura en Wireshark - Mañana en el área COMANDO

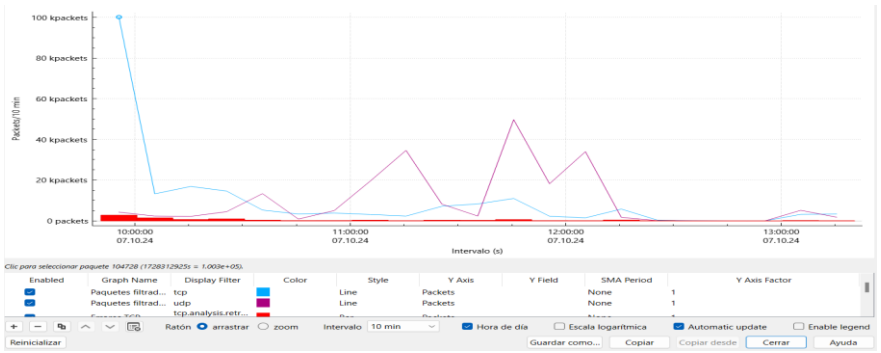


Figura 24. Captura en Wireshark - Tarde en el área GOMAI

La Tabla 30 presenta un resumen del comportamiento del tráfico en la red, basado en los datos obtenidos mediante FortiGate, Palo Alto, PingPlotter y Wireshark.

Tabla 30. Comportamiento de la red

Información obtenida mediante el análisis del tráfico	
Fortigate y Palo Alto	**Patrones de Uso:** Navegación web, videoconferencias, Datos.
	Protocolos: Https, UDP, QUIC, SSH
	Plataformas de comunicación: Zoom, Skipe, Teams.
	Días con mayor tráfico: martes y miércoles
	Horas pico: Generalmente los problemas son en la mañana.
Pingplotter	**Perdida de paquetes:** Mañana y tarde
	Mayor latencia: Mañana
Wireshark	**Problemas:** Congestión de la red
	Horas pico: Mañana y tarde

c. Requerimientos para QoS

En la Tabla 25, se describen las diferentes aplicaciones junto con los parámetros establecidos para sus requerimientos de ancho de banda [47], [48].

Tabla 31. Requerimiento de ancho de banda

Aplicación	**Descripción**	**Requerimiento**
Videoconferencia	La aplicación de videoconferencia requiere garantizar calidad de servicio mediante alta fiabilidad, bajo jitter, mínima latencia y suficiente ancho de banda para operar de manera óptima. Esta aplicación incluye cuatro flujos, distribuidos en dos por cada dirección: uno para audio y otro para video.	• MPEG-1: 500-1500 Kbps • MPEG-2: 5 a 10 Mbps • MPEG-4: 28.8 a 400 Kbps • H.261: 100 a 400 Kbps • Donde el video de alta calidad requiere aproximadamente 768 Kbps.
Navegación Web	Este cálculo se basa en una estimación promedio del uso de navegación.	160 Kbps
Datos	En comparación con aplicaciones como videoconferencias, que requieren un ancho de banda significativo, estos protocolos suelen consumir menos	30 Kbps

La Tabla 32 presenta el cálculo del ancho de banda para 63 usuarios, con información obtenida del DTIC y de una encuesta. Aunque no todos los usuarios se conectan al mismo tiempo, se consideró el total para garantizar un buen rendimiento en momentos de mayor demanda. En este centro de investigación, las actividades incluyen

navegación web, uso de plataformas como YouTube y comunicación interna. El ancho de banda se distribuyó según la prioridad de las aplicaciones: se asignaron valores máximos y garantizados para videoconferencias y navegación web debido a su necesidad de estabilidad y calidad. Para el tráfico de datos, solo se definió un valor máximo porque su demanda es menor, mientras que el tráfico por defecto utiliza el ancho de banda restante. En base a la siguiente formula se determinó la cantidad de ancho de banda máximo para las aplicaciones [48], [49]:

$$Aplicación = usuarios\ simultáneos\ x\ ancho\ de\ banda$$

Fórmula para las videoconferencias:

$$Aplicación = usuarios\ simultáneos\ x\ 0.768Mbps$$

Fórmula para la navegación web:

$$Aplicación = usuarios\ simultáneos\ x\ 0.16Mbps$$

Fórmula para datos:

$$Aplicación = usuarios\ simultáneos\ x\ 0.03Mbps$$

En base a la siguiente fórmula, se determinó la cantidad de ancho de banda mínimo [48], [49]. El valor de simultaneidad corresponde al 80%, puesto que este porcentaje refleja el número máximo de usuarios que, en promedio, utilizan la red de manera concurrente:

$$Aplicación = usuarios\ simultáneos\ x\ ancho\ de\ banda\ x\ simultaneidad$$

Fórmula para las videoconferencias:

$$Aplicación = usuarios\ simultáneos\ x\ 0.768Mbps\ x\ 80\%$$

Fórmula para la navegación web:

$$Aplicación = usuarios\ simultáneos\ x\ 0.16Mbps\ x\ 80\%$$

Fórmula para datos:

$$Aplicación = usuarios\ simultáneos\ x\ 0.03Mbps\ x\ 80\%$$

Tabla 32. Cálculo de ancho de banda

Aplicación	Distribución del Ancho de Banda	Usuarios simultáneos	Ancho de banda por usuario en Mbps	Total
Videoconferencia	Máximo	15	0.768	12 Mbps
	Garantizado	15	0.768	10 Mbps
Navegación Web	Máximo	63	0.16	10 Mbps
	Garantizado	63	0.16	8 Mbps
Datos	Máximo	63	0.03	2 Mbps
Default	----------	63	----------	----------

d. Elección de parámetros y valores dscp para QoS

Tras analizar las características de cada uno de los mecanismos, modelado, tipos de encolamiento para QoS, se presenta en la Tabla 33 los parámetros para llevar a cabo el proceso de implementación.

Tabla 33. Parámetros de QoS

Parámetros	Características de QoS asociadas	Aplicación
Mecanismos de regulación de tráfico.	• Shapping	Asignación al puerto de salida del tráfico
Marcado de tráfico	• DSCP	Asignación de prioridad y administración de congestión
Administración de Congestión del tráfico	• WFQ • LLQ	

El DSCP es un valor decimal que puede variar entre 0 y 63. Este valor se utiliza en las redes de comunicación para etiquetar un paquete IP con el objetivo de clasificarlo según su clase de tráfico permitiendo que los dispositivos de red, como enrutadores y switches, identifiquen la prioridad del tráfico y apliquen políticas específicas de QoS. La Tabla 34 define cómo se relacionan las clases de servicio con las etiquetas DSCP.

Tabla 34. Valores DSCP

Decimal Value	DSCP Value	DSCP Name	Service Class Name
10	001 010	AF11	High-Throughput Data
12	001 100	AF12	
14	001 110	AF13	
18	010 010	AF21	Low-Latency Data
20	010 100	AF22	
22	010 110	AF23	

26	011 010	AF31	Multimedia Streaming
28	011 100	AF32	
30	011 110	AF33	
34	100 010	AF41	Multimedia Conferencing
36	100 100	AF42	
38	100 110	AF43	
0	000 000	CS0	Standard (Default/Best Effort)
8	001 000	CS1	Low-Priority Data
16	010 000	CS2	OAM (Operations, Administration, and Management)
24	011 000	CS3	Broadcast Video
32	100 000	CS4	Real-Time Interactive
40	101 000	CS5	Signaling
48	110 000	CS6	Network Control
56	111 000	CS7	Reserved
46	101 110	EF	Telephony

En la Tabla 35 se presentan los valores de DSCP utilizados para clasificar cada tipo de tráfico, destacando las clases AF y sus variaciones. Además, se detalla el tipo de aplicación correspondiente a cada clase, los puertos asociados plataformas de videoconferencia como Zoom, Jitsi, Google Meet, Microsoft Teams y Skype, así como protocolos de navegación web HTTP y HTTPS y transferencia de datos (FTP, SSH y TFTP y el ancho de banda asignado según su prioridad. Las prioridades se determinaron con base en estudios previos [47], [50] y entrevistas con el personal del DTIC. Las videoconferencias tienen prioridad alta debido a su sensibilidad a la latencia. Las aplicaciones web tienen prioridad media, ya que, aunque son esenciales, toleran ciertas demoras. El tráfico de datos se clasifica con prioridad baja porque no requiere entrega inmediata.

Tabla 35. Aplicaciones, valores de DSCP y ancho de banda para configuración de QoS

Prioridad	**Aplicación**	**DSCP**	**Puertos**	**Ancho de banda**
Alta	Videoconferencia	AF43 100110	TCP: 443, 8801-8802, 16000-26000 UDP: 443, 3478-3481, 8801-8802, 50000-60000, 10000, 19302-19309	Min: 10 Mbps Max: 12 Mbps
Media	Aplicaciones web	AF33 011110	TCP: 80, 443	Min: 8 Mbps Max: 10 Mbps
Baja	Datos	AF22 010100	21, 22, 69	Max: 2 Mbps
Default	Cualquier otro	Default	-------	----------

3.3.3 Fase III: Diseñar

a. Esquema de planificación para cumplimiento de objetivos

La Figura 24 muestra la planificación estructurada que servirá como guía para la implementación de QoS, permitiendo organizar cada fase del proceso.

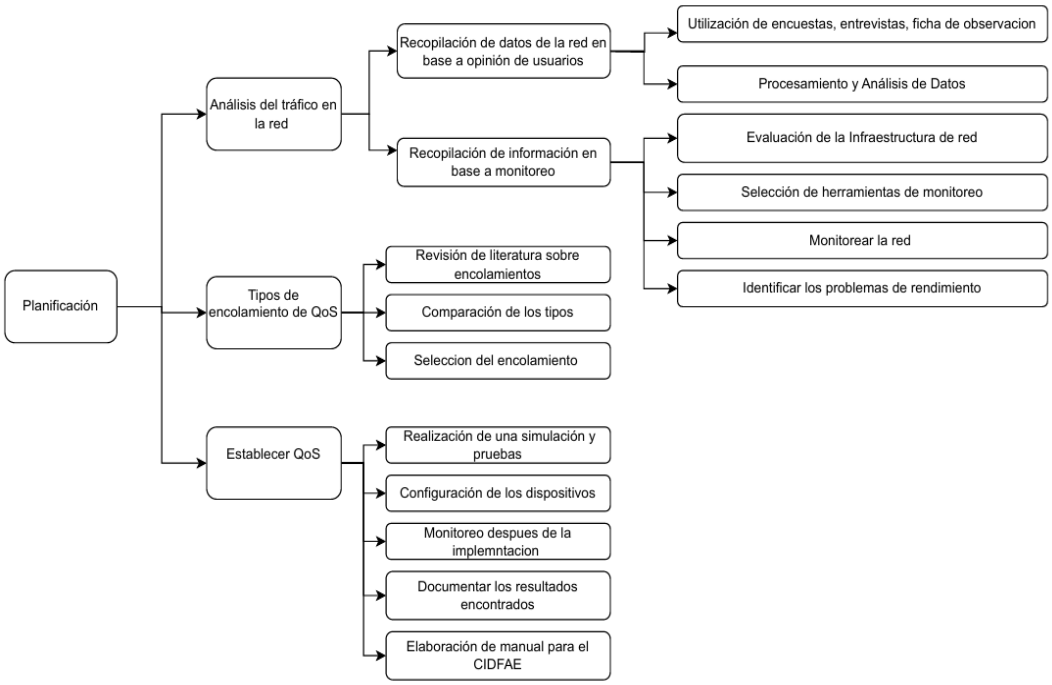


Figura 25. Diseño de planificación

b) Diseño de la red CIDFAE

El diseño de la red del CIDFAE tiene una infraestructura de tamaño mediano que conecta diversos dispositivos, como computadoras y cámaras, a través de switches Cisco y TP-Link, además de un firewall para la seguridad de la red. La red opera con una IP principal que gestiona todas las conexiones y facilita la comunicación entre los diferentes equipos.

Por motivos de seguridad y confidencialidad no es posible revelar la dirección IP real asignada al CIDFAE, para efectos de este documento y de las configuraciones realizadas se utilizará una dirección IP alternativa de ejemplo garantizando que no comprometa la integridad ni la seguridad de la red original.

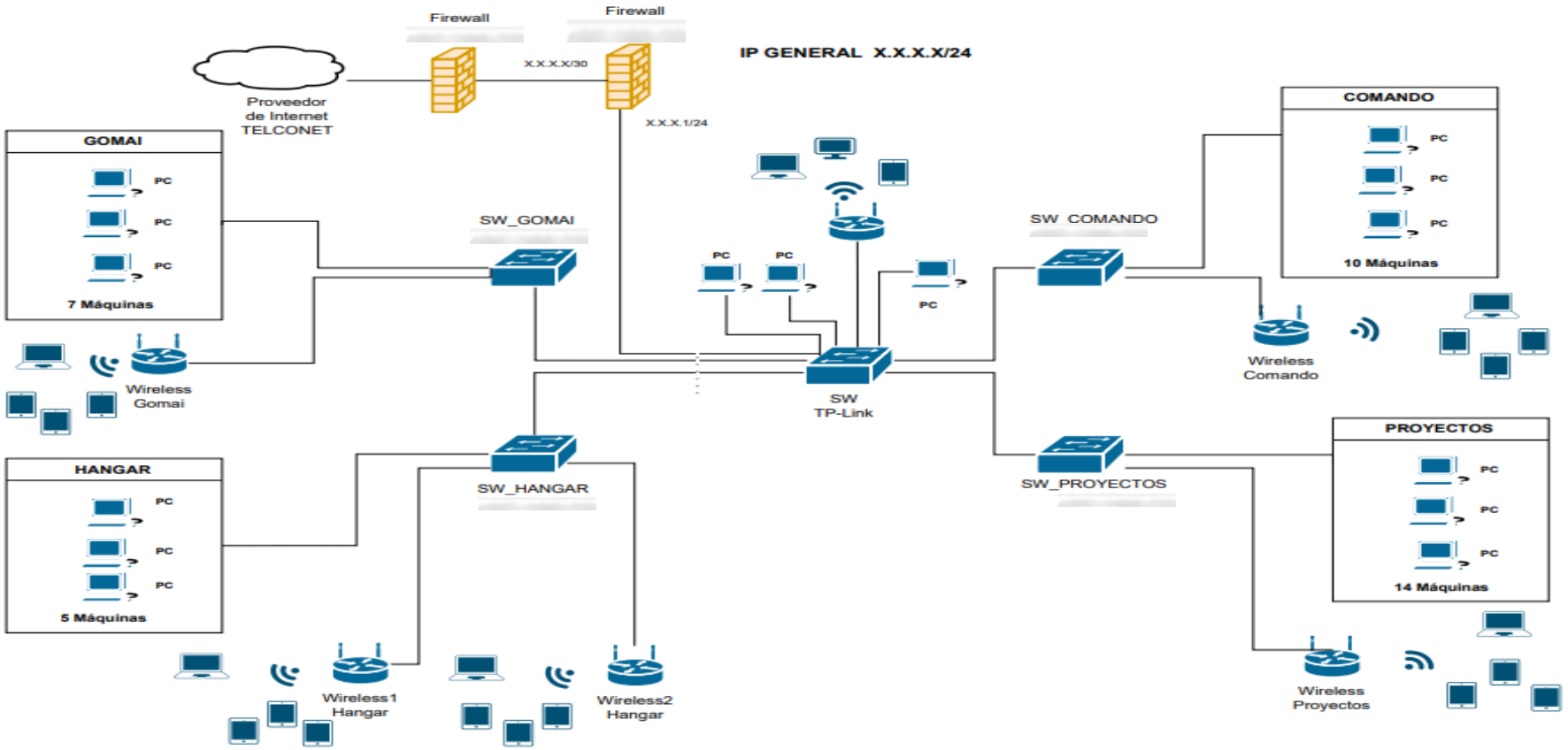


Figura 26. Diagrama de la red CIDFAE

En el diagrama de red de la Figura 26, se evidencia la falta de segmentación entre las diferentes áreas, como Gomai, Comando, Hangar y Proyectos. Esta ausencia de segmentación puede afectar el rendimiento de la red, ya que el tráfico de un área puede interferir con el de otras, provocando congestión y latencias indeseadas. Por lo tanto, se ha diseñado una nueva topología que incluye la segmentación de la red como se aprecia en la Tabla 36. Además, el CIDFAE ha decidido cambiar de proveedor de Internet, lo que implicó la adquisición de nuevos equipos para complementar su infraestructura puesto que la anterior empresa se llevó los equipos que le pertenecían.

b. Diseño de la red con los respectivos cambios

- ***Subnetting***

El CIDFAE tiene asignado la dirección de red 10.20.30.0/24 se ha tomado esta IP como ejemplo para lo cual realizo el subneteo en base a las áreas de la institución con los siguientes requisitos de direccionamiento:

- Comando requiere de 25 dispositivos
- Proyectos requiere de 25 dispositivos
- Hangar requiere de 25 dispositivos
- GOMAI requiere de 25 dispositivos
- Impresoras requiere de 25 dispositivos
- Extra requiere de 25 dispositivos
- Administración de dispositivos requiere de 4 Ips
- El enlace l enlace desde Fortigate a SW3 requerirá una dirección IP para cada extremo del enlace.

Tabla 36. Segmentación en subredes

Subred	**Dirección de red**	**Rango Ip's**	**Dirección de Broadcast**	**Máscara**
0	10.20.30.0	10.20.30.1-10.20.30.30	10.20.30.31	255.255.255.224
1	10.20.30.32	10.20.30.33-10.20.30.62	10.20.30.63	255.255.255.224
2	10.20.30.64	10.20.30.65-10.20.30.94	10.20.30.95	255.255.255.224
3	10.20.30.96	10.20.30.97-10.20.30.126	10.20.30.127	255.255.255.224
4	10.20.30.128	10.20.30.129-10.20.30.158	10.20.30.159	255.255.255.224
5	10.20.30.160	10.20.30.161-10.20.30.190	10.20.30.191	255.255.255.224
6	10.20.30.192	10.20.30.193-10.20.30.198	10.20.30.199	255.255.255.248
7	10.20.30.200	10.20.30.201-10.20.30.202	10.20.30.203	255.255.255.252

En la Tabla 37, se describe las IP's de administración que tendrán los equipos, su máscara y default Gateway mientras que en la Tabla 38, se especifican los puertos que se utilizarán para establecer la conexión entre el switch y el FortiGate.

Tabla 37. Ip´s de administración de los equipos

Dispositivo	**#Vlan**	**Puerto**	**Dirección IP**	**Mascara**	**Default Gateway**
SW_PROYECTOS	1	1	10.20.30.193	255.255.255.248	10.20.30.198
SW_HANGAR	1	1	10.20.30.194	255.255.255.248	10.20.30.198
SW_GOMAI	1	1	10.20.30.195	255.255.255.248	10.20.30.198
SW_CORE	1	1	10.20.30.196	255.255.255.248	10.20.30.198

Tabla 38. Conexión enlaces

Equipo	**Puerto**	**Dirección**
SW-CORE	F1/0/24	10.20.30.201/30
FortiGate	Port2	10.20.30.202/30
	Port1	10.20.30.205/30

La Tabla 39 muestra el direccionamiento IP de una red segmentada en múltiples VLANs. Cada VLAN representa una subred lógica con su propia dirección y máscara de subred.

Tabla 39. Direccionamiento Ip en las VLANs

Dispositivo	**#Vlan**	**Nombre**	**Puertos**	**Dirección de Red**	**Mascara**	**Default Gateway**
SW_COMANDO	10	COMANDO	2-19	10.20.30.0	255.255.255.224	10.20.30.30
	50	IMPRESORA	20-23	10.20.30.128		10.20.30.158
SW_PROYECTOS	20	PROYECTOS	2-19	10.20.30.32	255.255.255.224	10.20.30.62
	50	IMPRESORA	20-23	10.20.30.128		10.20.30.158
SW_HANGAR	30	HANGAR	2-19	10.20.30.64	255.255.255.224	10.20.30.94
	50	IMPRESORA	20-23	10.20.30.128		10.20.30.158
SW_GOMAI	40	GOMAI	2-19	10.20.30.96	255.255.255.224	10.20.30.126
	50	IMPRESORA	20, 22	10.20.30.128		10.20.30.158

- ***Descripción de la segmentación***

Los dispositivos para su administración tendrán asignadas 6 IPs, utilizando una máscara de subred /29 (255.255.255.248) y un gateway de 10.20.30.198. El rango de direcciones IP disponibles para estos dispositivos va de 10.20.30.193 a 10.20.30.197.

La VLAN 10 (Comando) tiene asignadas 30 IPs para uso, con una máscara de subred de /27 (255.255.255.224) y el gateway para esta VLAN es 10.20.30.30. Los dispositivos conectados a esta VLAN pueden usar cualquier IP del rango 10.20.30.1 - 10.20.30.29.

La VLAN 20 (Proyectos) tiene asignadas 30 IPs para uso, con una máscara de subred de /27 (255.255.255.224) y el gateway para esta VLAN es 10.20.30.62. Los dispositivos conectados a esta VLAN pueden usar cualquier IP del rango 10.20.30.33 - 10.20.30.61.

La VLAN 30 (Hangar) tiene asignadas 30 IPs para uso, con una máscara de subred de /27 (255.255.255.224) y el gateway para esta VLAN es 10.20.30.94. Los dispositivos conectados a esta VLAN pueden usar cualquier IP del rango 10.20.30.65 - 10.20.30.93.

La VLAN 40 (GOMAI) tiene asignadas 30 IPs para uso, con una máscara de subred de /27 (255.255.255.224) y el gateway para esta VLAN es 10.20.30.126. Los dispositivos conectados a esta VLAN pueden usar cualquier IP del rango 10.20.30.97 - 10.20.30.125.

La VLAN 50 (Impresoras) tiene asignadas 30 IPs para uso, con una máscara de subred de /27 (255.255.255.224) y el gateway para esta VLAN es 10.20.30.158. Los dispositivos conectados a esta VLAN pueden usar cualquier IP del rango 10.20.30.129 - 10.20.30.157.

La Figura 27 muestra el rediseño de la red, incorporando los cambios y la integración de los nuevos equipos adquiridos.

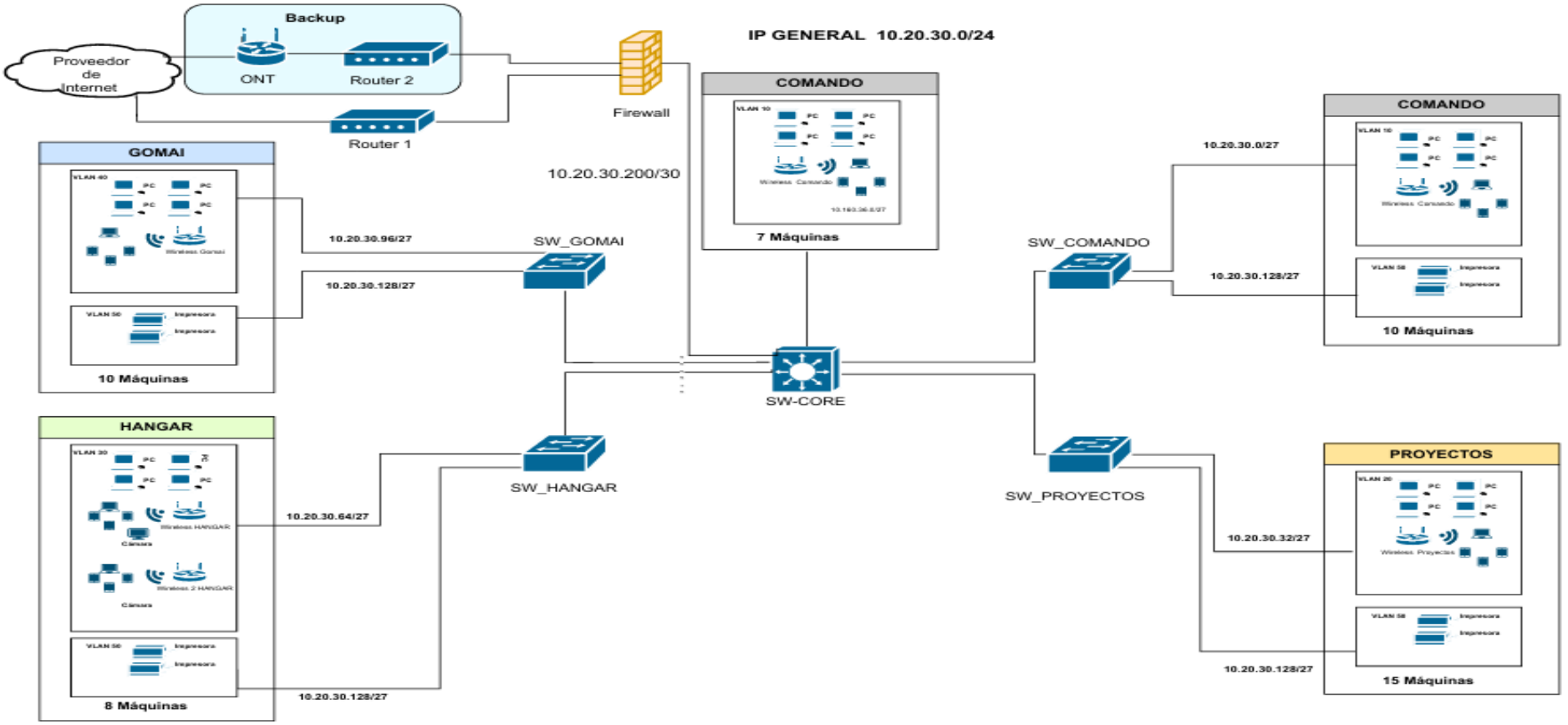


Figura 27. Diseño de la red CIDFAE

3.3.4 Fase IV: Implementar

En esta etapa se configuraron los equipos disponibles en el centro de investigación. Para ello, se creó un prototipo en un simulador de redes que permitió replicar el comportamiento de un sistema real. Con el fin de no evidenciar las IPs reales del CIDFAE, se utilizarán imágenes del simulador para ilustrar la segmentación de la red. Sin embargo, para la implementación de QoS, se presentarán imágenes reales del equipo configurado.

a) Herramienta de simulación GNS3

GNS3 es una herramienta usada en todo el mundo para crear y probar redes, ya sean virtuales o reales, aunque es muy conocida por su compatibilidad con equipos Cisco también funciona con dispositivos de otros fabricantes lo que la hace útil para aprender y resolver problemas en diferentes tipos de redes [37]. La Figura 28 muestra el logo de GNS3.



Figura 28. Logo de GNS3

- ***Esquema de simulación en GNS3***

Para llevar a cabo un análisis detallado, se utilizó el software GNS3 para simular la red y evaluar si los equipos soportan funciones de QoS, la simulación se basó en la topología lógica de la red del CIDFAE. Como primer paso, se cargaron los IOS correspondientes para cada switch, firewall y router, con el fin de crear un entorno más realista al ejecutar las configuraciones y pruebas. En la Figura 29, se muestra la topología implementada en GNS3. La topología está compuesta por un router

MikroTik con la versión 7.2.3, un FortiGate con la versión 7.0.0, un switch Cisco 3750 con la versión 15.1 y un switch Cisco 2960 con la versión 15.1.

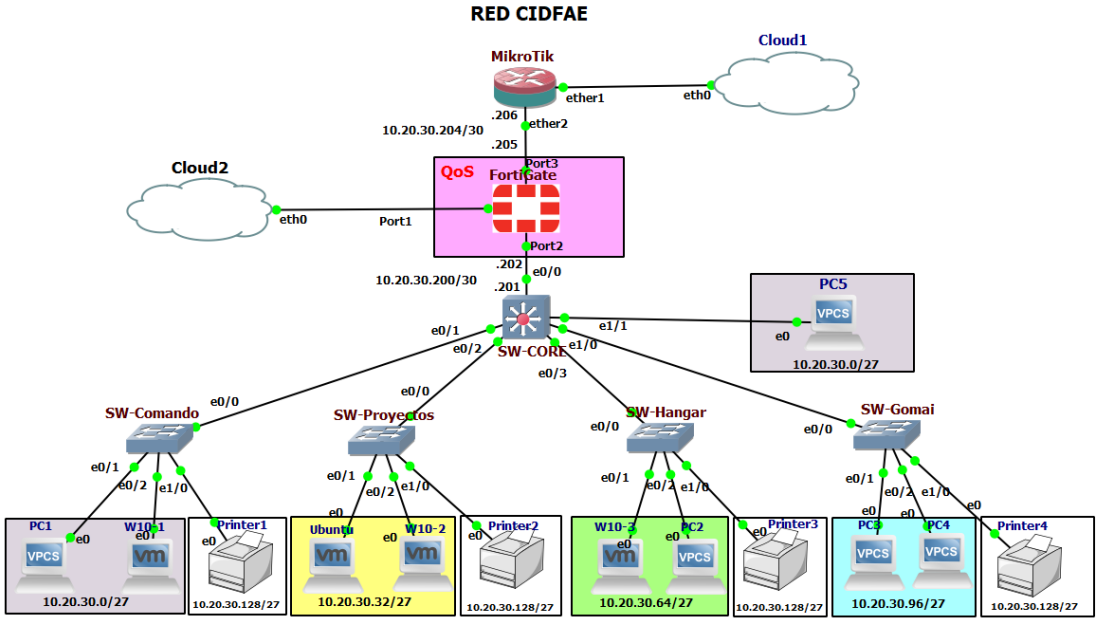


Figura 29. Red LAN CIDFAE en GNS3

- ***Configuración de VLANs en los switchs***

Se realizó InterVLAN configurando las diferentes VLANs en el switch capa 3 y se asignaron las direcciones correspondientes a cada una de ellas, se añadió una ruta estática hacia el FortiGate y se asignó la dirección IP correspondiente a la VLAN 16, que establece la conexión con el FortiGate y las interfaces como troncales para permitir la comunicación entre el switch de capa 3 y los diferentes switches de capa 2 como se muestra en la Figura 30.

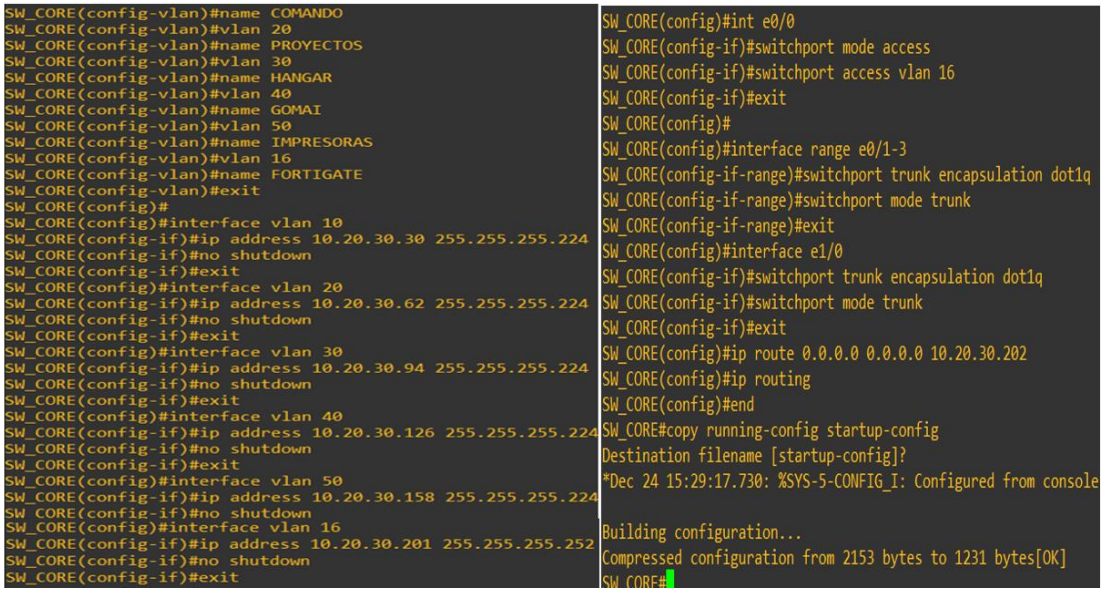


Figura 30. Configuración SW_CORE

En la Figura 31, se puede observar la configuración de VLANs en el switch COMANDO con sus respectivos nombres, se configuró un puerto como troncal y el acceso a las mismas, similar proceso se siguió para la configuración de los diferentes switchs (ver Anexo B). Para la simulación se configuro un generador de tráfico y verificar funcionalidad (ver Anexo E).

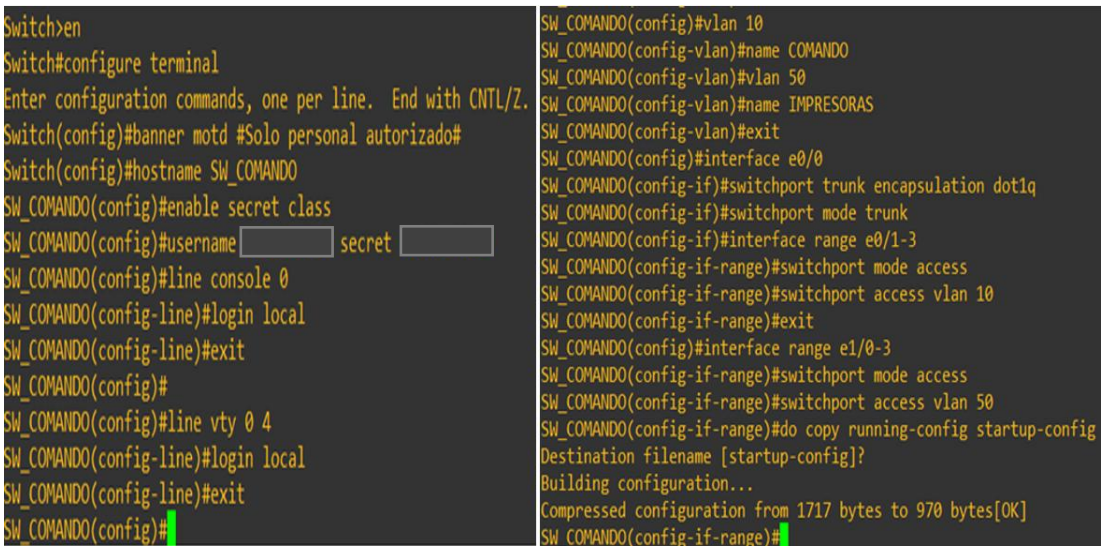


Figura 31. Configuración SW_COMANDO

- ***Configuración de VLANs Fortigate***

La Figura 32 presenta la configuración en el FortiGate está se llevó a cabo accediendo a su interfaz gráfica a través de un navegador web, utilizando su dirección IP asignada. Una vez dentro, en la sección “Policy & Objects” del menú, se ingresó al apartado de “Address” para crear las distintas VLAN. A cada una se le asignó su correspondiente dirección de red junto con su máscara.

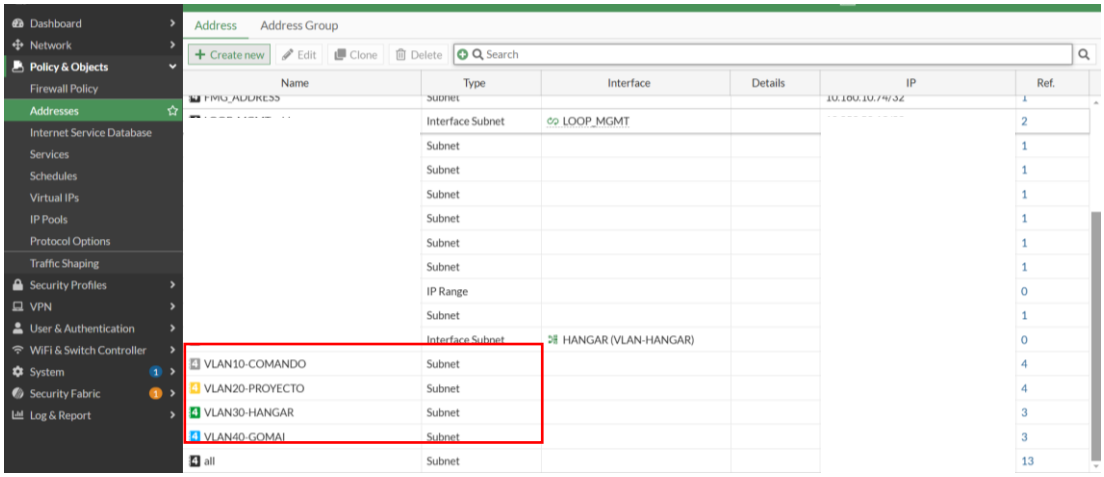


Figura 32. Creación de VLANs en FortiGate

Se utilizó el comando ping para comprobar la conectividad entre las diferentes direcciones IP asociadas a cada VLAN y salida a Internet como se observa en la Figura 33.

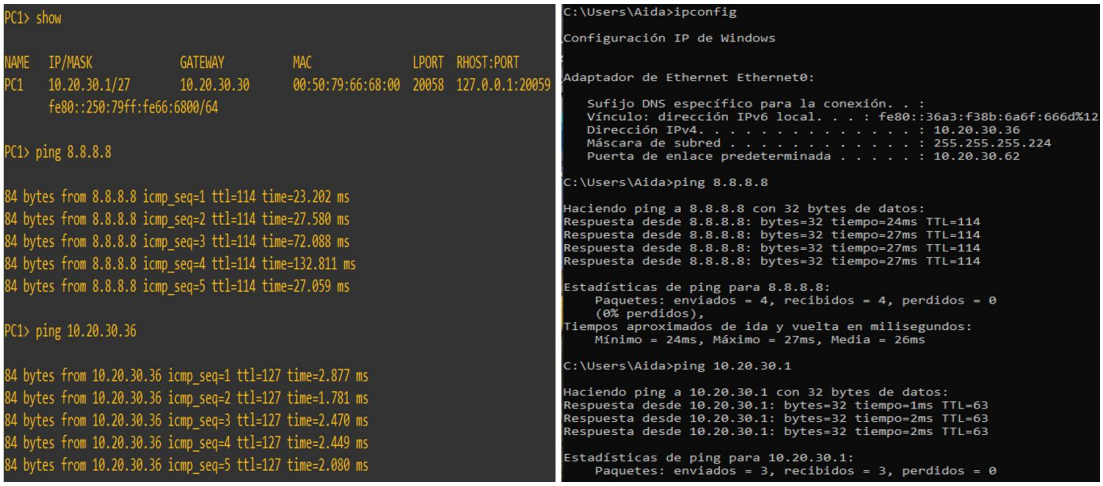


Figura 33. Verificación de conectividad

b) Configuración de QoS Fortigate

Para configurar QoS en el FortiGate, se establecieron los parámetros explicados en la Tabla 35, los cuales fueron aplicados. Para ello, se accedió al apartado “Traffic Shapers” donde se configuraron limitaciones o garantías de ancho de banda, se seleccionó la opción “Create New” para crear configuraciones personalizadas como se observa en la Figura 34.

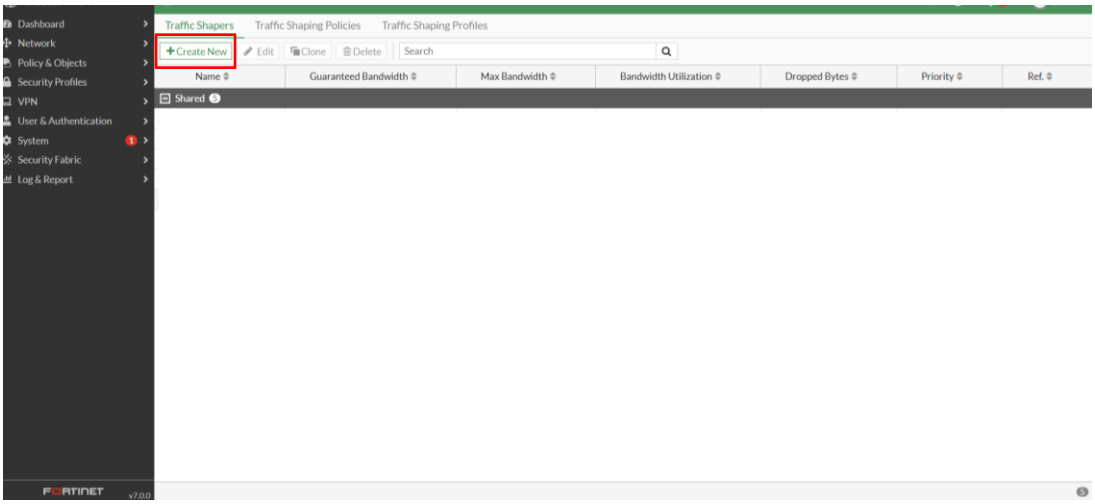


Figura 34. Sección de modelado de trafico

- ***Configuración de perfiles***

Para configurar el Traffic Shaper en FortiGate, es importante comprender los parámetros que permiten administrar el ancho de banda y la priorización del tráfico. En la Tabla 40, se presentan los valores recomendados para la configuración, y en la Figura 35, se muestra la implementación. A continuación, se describen cada uno de estos parámetros [51].

Nombre: Este campo identifica el Traffic Shaper y debe ser descriptivo para facilitar su administración. Se recomienda incluir la cantidad de ancho de banda en el nombre, para una identificación rápida.

Prioridad del tráfico: Define la importancia del tráfico que pasa a través del FortiGate, clasificándolo en Alta, Media o Baja.

Ancho de banda máximo: Establece el límite superior de velocidad en kilobits por segundo (kbps) para evitar que un tipo de tráfico consuma recursos excesivos.

Ancho de banda garantizado: Define el mínimo de ancho de banda reservado para el tráfico seleccionado.

DSCP: Permite marcar los paquetes con un valor DSCP específico para su priorización en la red esto se da a nivel de los demás dispositivos.

Tabla 40. Modelado de tráfico

Nombre del perfil	Ancho de banda garantizado en Kbps	Ancho de banda máximo en Kbps	DSCP	Prioridad interna FortiGate
12 Mbps	10000	12000	100110	High
10 Mbps	8000	10000	011110	Medium
2 Mbps	----------	2000	010100	Low
Default	6000	----------	001010	High

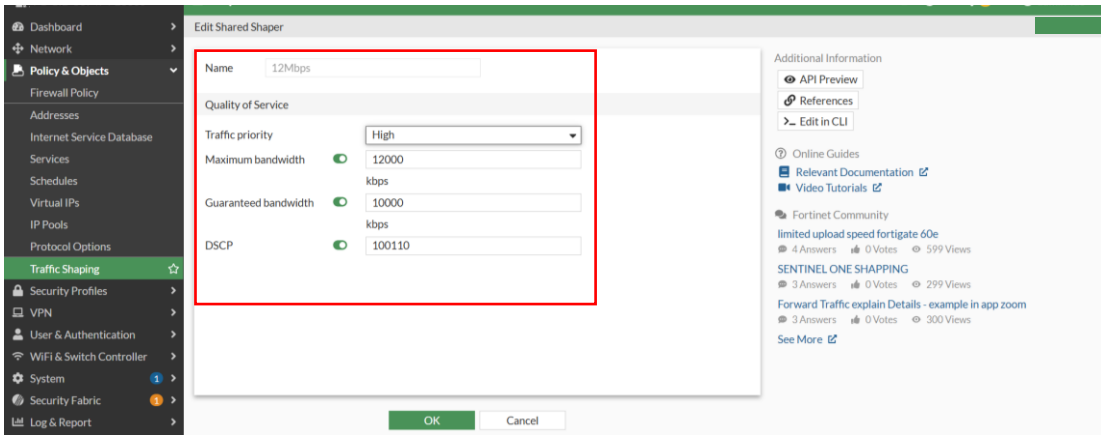


Figura 35. Configuración del perfil de tráfico 12 Mbps

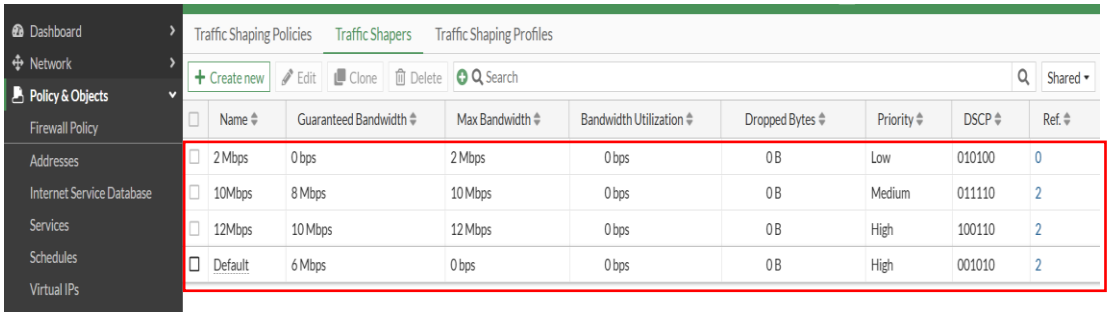


Figura 36. Visualización de los perfiles de tráfico

- ***Configuración de políticas***

Los parámetros utilizados para configurar las políticas de Traffic Shaping permiten ajustar el comportamiento del tráfico de red según las necesidades específicas de cada entorno [52]. A continuación, se los describe

Nombre: Permite asignar un identificador a la política de Traffic Shaping.

Status: Determina si la política está activa o inactiva. Solo las políticas habilitadas afectan el tráfico de la red, mientras que las deshabilitadas permanecen registradas sin aplicarse.

Source Interface: Define la interfaz desde la cual proviene el tráfico que será controlado.

Outgoing Interface: Especifica las interfaces de salida por donde se dirige el tráfico después de ser procesado.

Source: Permite restringir la aplicación de la política a un conjunto específico de direcciones IP, subredes o VLANs.

Destination: Determina hacia qué direcciones IP o dominios se aplicará la política.

Schedule: Permite establecer períodos de tiempo en los que la política estará activa.

Service: Especifica las aplicaciones o protocolos a los que se aplicará el Traffic Shaping.

Application: Permite definir aplicaciones específicas para aplicar la política, basándose en la identificación del tráfico dentro del FortiGate.

URL Category: Facilita la aplicación de Traffic Shaping a sitios web según su categoría, como redes sociales, streaming o videoconferencias, asegurando que ciertos tipos de tráfico tengan prioridad o limitaciones.

Apply Shaper: Asigna un Traffic Shaper previamente configurado, el cual define el ancho de banda máximo y garantizado para el tráfico seleccionado.

Reverse Shaper: Aplica un Traffic Shaper en la dirección opuesta, controlando el tráfico de respuesta o salida.

Per-IP Shaper: Permite aplicar las reglas de limitación o priorización a nivel individual por dirección IP, asegurando que cada usuario o dispositivo reciba un tratamiento específico dentro de la política de Traffic Shaping.

La Tabla 41 presenta una comparación entre los distintos métodos de Traffic Shaping en FortiGate, evaluando su precisión en el control del ancho de banda, flexibilidad para realizar ajustes y sus limitaciones

Tabla 41. Métodos de Traffic Shaping

Método de Traffic Shapping	**Precisión de control ancho de banda**	**Flexibilidad para ajustes**	**Limitaciones**
Servicios (puertos)	Alta: Permite definir límites exactos para cada puerto de servicio.	Ajustes inmediatos en puertos específicos sin afectar otros servicios	Requiere conocer la asignación de puertos en la red
Por IPs	Media: Depende de la asignación de IPs y su variabilidad.	Requiere administrar rangos de IP.	No es útil en redes con DHCP o IPs dinámicas
Aplicaciones	Media: Requiere identificación precisa del tráfico de la aplicación.	Depende de la correcta detección del tráfico por FortiGate.	Puede no identificar correctamente aplicaciones encriptadas
Por URL Category	Media: Filtra tráfico web según categoría, pero no afecta otros tipos de tráfico.	Rápida asignación de políticas a categorías de sitios web.	Solo afecta tráfico web, no otro tipo de comunicación en la red

La Figura 37 muestra el perfil generado incluido en una política accediendo al apartado “Traffic Shaping Policy”, donde se asignó el nombre de “Videoconferencias” y se configuraron los parámetros que puedan coincidir con el tráfico, especificando como origen las VLAN 10 y 20 y el tratamiento basado en servicios definidos por puertos Figura 38 (ver Anexo D). Además, se agregó un horario acorde a la duración de la jornada laboral en la institución Figura 39, y en la salida se aplicó la política a la interfaz WAN1 y WAN2 que conecta a Internet. Se habilitó “Shared Shaper” para controlar el ancho de banda de subida y “Reverse Shaper” para la velocidad de descarga, configurando ambos con el perfil de 12 Mbps.

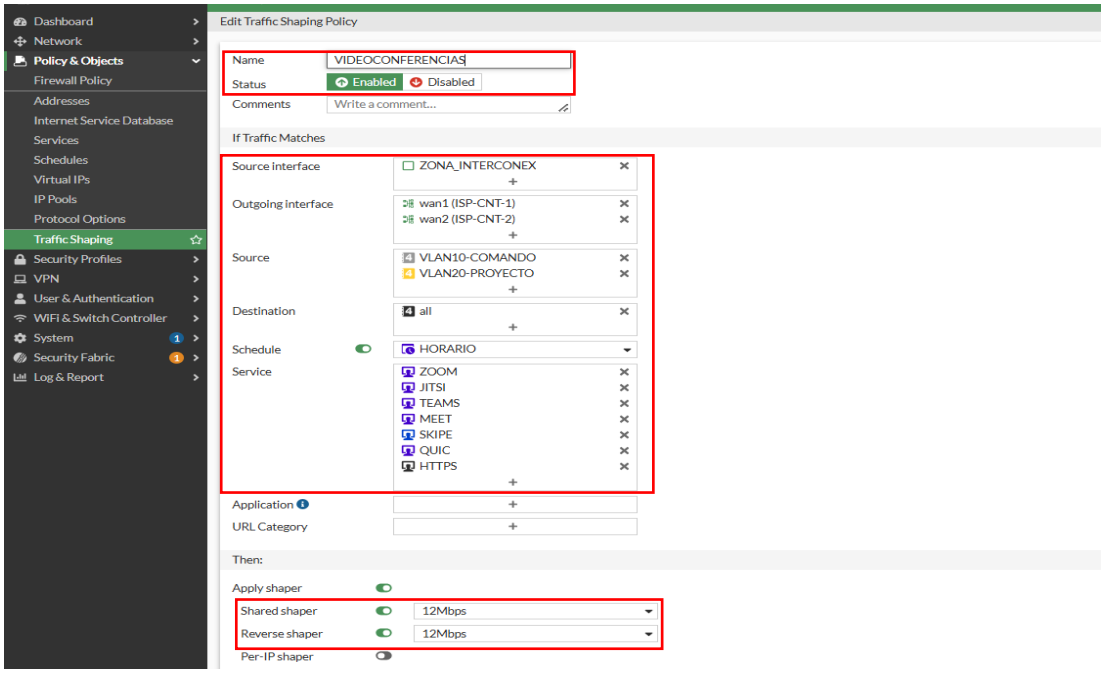


Figura 37. Creación de la política para videoconferencia

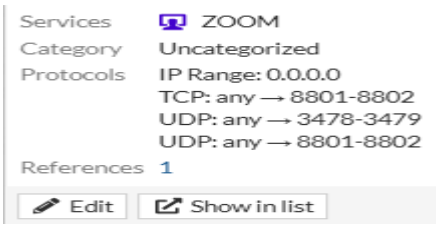


Figura 38. Configuración de puertos

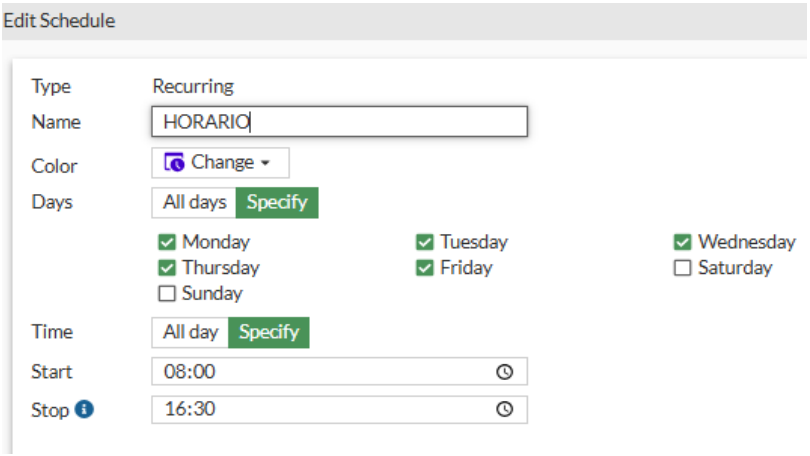


Figura 39. Horario para manejar las políticas

En las políticas de Traffic Shaping, se priorizó tráfico de videoconferencias, navegación web y datos mediante anchos de banda, cada política está habilitada con un shaper y servicios definidos como se muestra en la Figura 40.

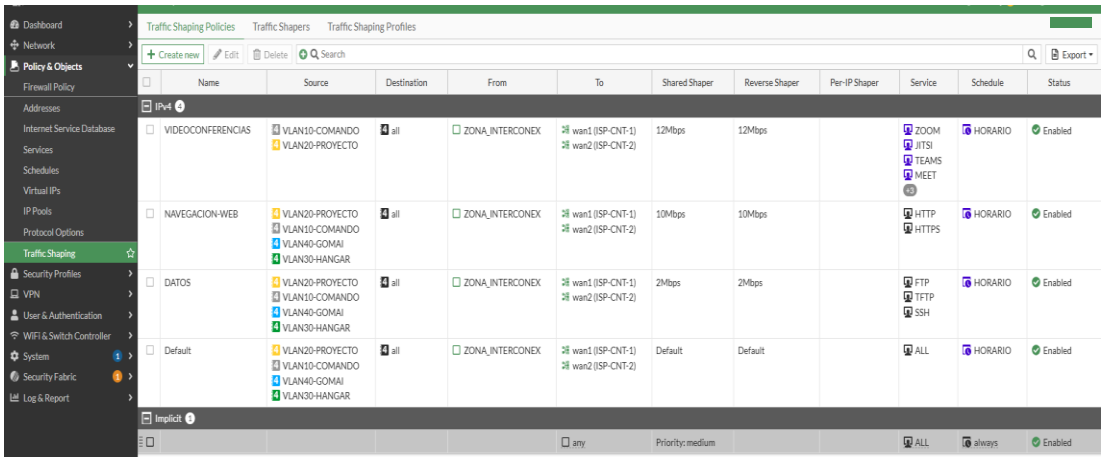


Figura 40. Políticas de tráfico

3.3.5 Fase V: Operar

Una vez implementada la red, se realizan pruebas para garantizar su funcionalidad y estabilidad en un entorno productivo.

a. Instalación de widget en fortigate

En la Figura 41, se puede observar el panel de configuración del Dashboard en un FortiGate, donde se puede agregar widgets para monitorear diferentes aspectos del sistema y la red como ancho de banda por interfaz, uso y actividad del sistema.

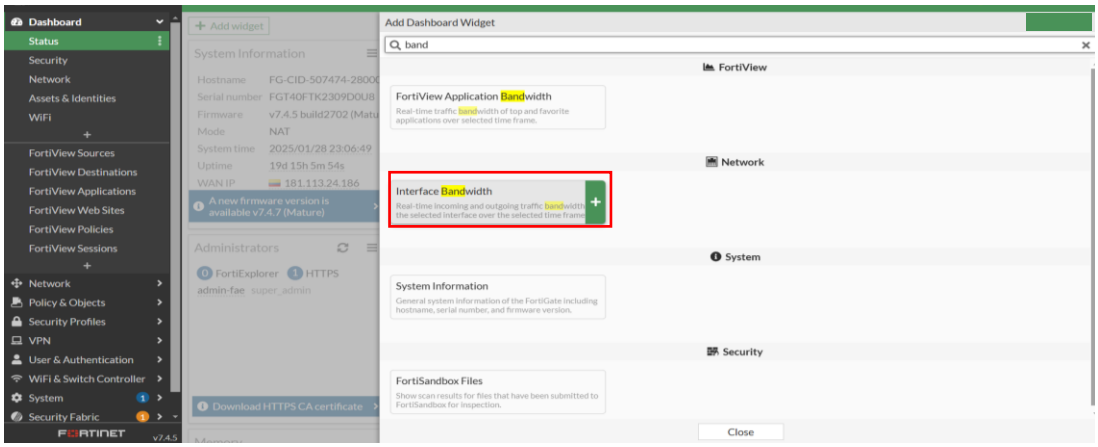


Figura 41. Adición de widget

La Figura 42 muestra cómo se añadió el monitoreo del tráfico en las interfaces WAN para obtener una visión del comportamiento de la red.

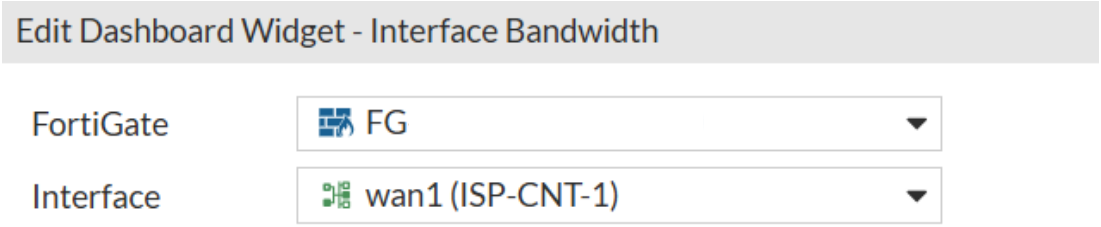


Figura 42. Interfaz para gráfica de ancho de banda

El panel de monitoreo de FortiGate, Figura 43 muestra un uso de memoria del 55%, indicando un rendimiento estable sin saturación. Actualmente, hay 1919 sesiones activas, con 0% de SPU y un 54.8% de nTurbo, lo que sugiere que más de la mitad del tráfico se procesa con aceleración de hardware. En cuanto al uso de ancho de banda, la interfaz WAN1 (ISP-CNT-1) tiene un tráfico de entrada de 704.37 kbps y de salida de 148.26 kbps, con picos máximos de hasta 30.3 Mbps, mientras que la interfaz WAN2 (ISP-CNT-2) presenta un tráfico de entrada de 3.46 Mbps y de salida de 421.11 kbps, con patrones de uso más elevados, lo que indica que esta interfaz está manejando una mayor carga. Dado que WAN2 tiene más tráfico que WAN1, se podría evaluar la configuración de balanceo de carga para distribuir mejor el tráfico y optimizar el rendimiento de la red.

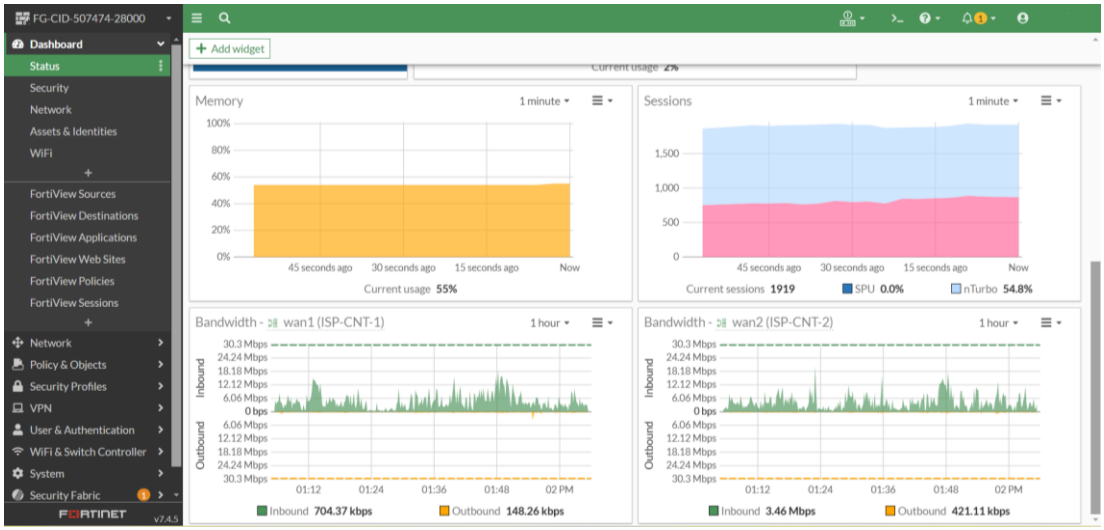


Figura 43. Dashboard FortiGate

La Figura 44 muestra la utilización de los perfiles configurados en el FortiGate, donde los valores de utilización de ancho de banda son 0 bps para el perfil de 2 Mbps, 776 bps para el de 10 Mbps, 49.47 kbps para el de 12 Mbps y 43.23 kbps para el perfil por default, sin que se hayan descartado bytes en ningún caso. Esto se debe a que el tráfico actual es muy bajo en comparación con los límites configurados, por lo que aún no se ha alcanzado un nivel que requiera la aplicación de políticas de descarte de paquetes.

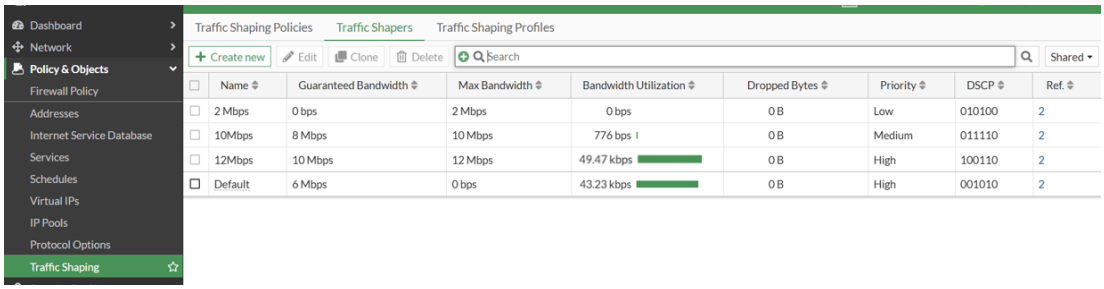


Figura 44. Consumo de ancho de banda

Revisión de los logs para verificar que la política se está aplicando correctamente. Figura 45

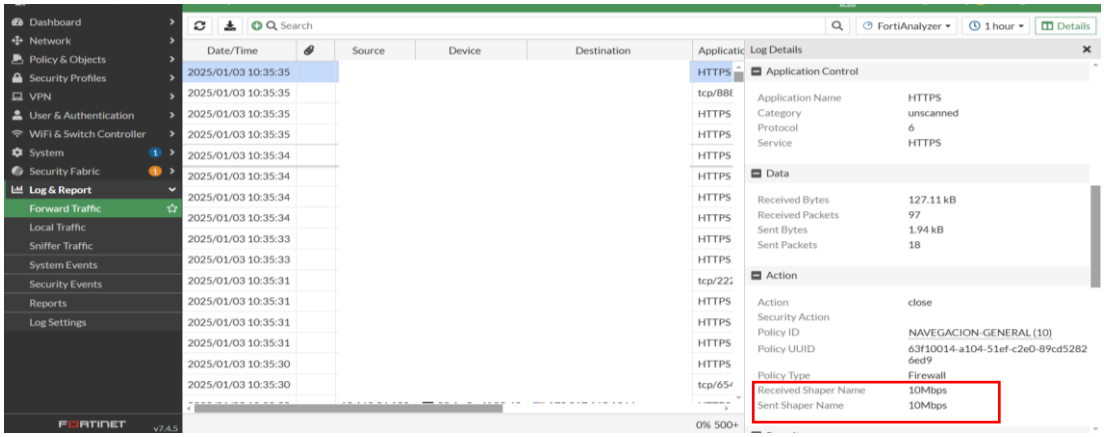
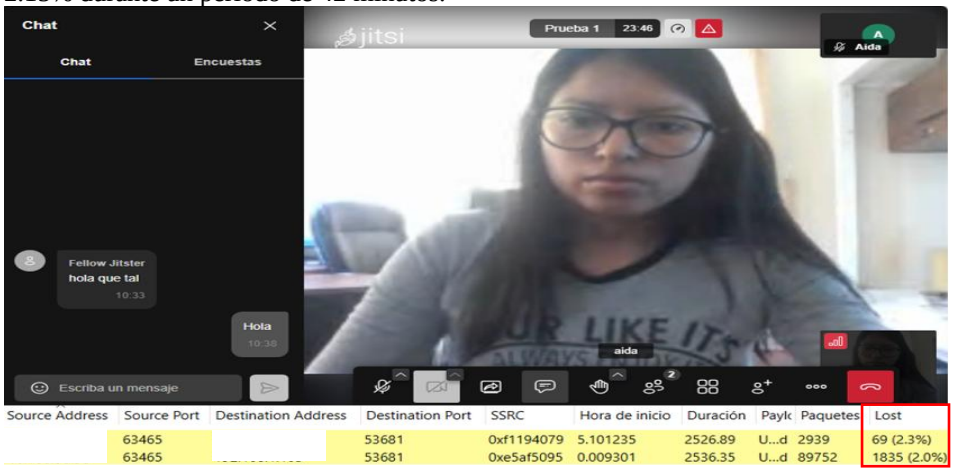


Figura 45. Logs del tráfico

Para analizar el rendimiento de la red, se realizaron pruebas utilizando Wireshark para monitorear y capturar el tráfico en dos escenarios: sin QoS y con QoS habilitado en la mañana, medio día y tarde. La calidad del servicio se analizó mediante Jitsi, que se usó para simular videoconferencias como se detalla en la Tabla 42.

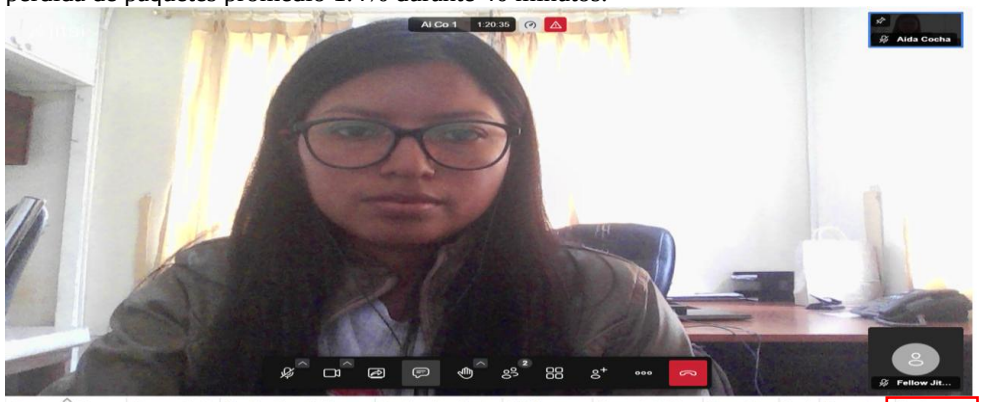
Tabla 42. Resultado de la videoconferencia

Sin QoS	Con QoS
En la Figura 40 se observa una imagen pixelada con una pérdida de paquetes promedio de 2.15% durante un período de 42 minutos.	En la Figura 41, se puede observar una mejora en la calidad de la imagen con una menor pérdida de paquetes promedio 1.4% durante 40 minutos.



Source Address	Source Port	Destination Address	Destination Port	SSRC	Hora de inicio	Duración	Paylc	Paquetes	Lost
	63465		53681	0xf1194079	5.101235	2526.89	U...d	2939	69 (2.3%)
	63465		53681	0xe5af5095	0.009301	2536.35	U...d	89752	1835 (2.0%)

Figura 46. Videoconferencia sin QoS



Source Address	Source Port	Destination Address	Destination Port	SSRC	Hora de inicio	Duración	Paylc	Paquetes	Lost
	55574		50409	0x4b071f9c	16.398034	2371.66	U...d	1956	9 (1.3%)
	55574		50409	0x56ebcbbe	0.110380	2399.28	U...d	69064	1077 (1.5%)

Figura 47. Videoconferencia con QoS

Source Address	Source Port	Destination Address	Destination Port	SSRC	Hora de inicio	Duración	Paylc	Paquetes	Lost
	63463		58185	0x26461be4	6.330949	1006.33	U...d	2902	74 (2.5%)
	63463		58185	0x792d98ca	0.000000	1015.66	U...d	42973	1151 (2.6%)
	55119		62407	0xa6d5b9c5	1.468856	2449.73	U...d	6036	185 (3.0%)
	55119		62407	0x28148529	1.119888	2450.10	U...d	92207	4166 (4.3%)
	55574		50409	0x4b071f9c	16.398034	2371.66	U...d	1956	9 (0.5%)
	55574		50409	0x56ebcbbe	0.110380	2399.28	U...d	69064	1077 (1.5%)
	50666		52188	0xcec0a92	7.294251	1882.28	U...d	3180	109 (3.3%)
	50666		52188	0xedcb9e49	0.277859	1932.58	U...d	56635	2106 (3.6%)
	52706		62407	0xa6d5b9c5	1.468856	2449.73	U...d	2110	63 (2.9%)
	52706		62407	0x28148529	1.119888	2450.10	U...d	41218	1103 (2.6%)

Figura 48. Capturas sin QoS -Mañana

Source Address	Source Port	Destination Address	Destination Port	SSRC	Hora de inicio	Duración	Payl	Paquetes	Lost
	52706		2407	0xa6d5b9c5	1.468856	2449.73	U...d	2110	63 (2.9%)
	52706		2407	0x28148529	1.119888	2450.10	U...d	41218	1103 (2.6%)
	50260		0000	0x80de772a	20.086522	1845.92	R...1	75256	1872 (2.4%)
	50259		3597	0xfa0f11c2	20.086462	364.58	R...1	18426	113 (0.6%)
	54009		09	0x28f409cd	103.512448	1784.02	Unassigned	4340	143 (3.2%)
	54008		00	0x1ca798a9	99.586852	3.93	Unassigned	104	0 (0.0%)
	50276		62422	0x55713b3c	3.865504	662.11	R...1	34798	39 (0.1%)
	65329		10000	0xdcfe5df4	0.729894	1827.68	U...t	45912	569 (1.2%)
	64009		09	0xcf878cda	230.224308	54.46	RTPType-111	2545	2 (0.1%)
	64009		09	0x37a98ecc	103.542017	1787.40	Unassigned	43636	2307 (5.0%)

Figura 49. Capturas con QoS -Mañana



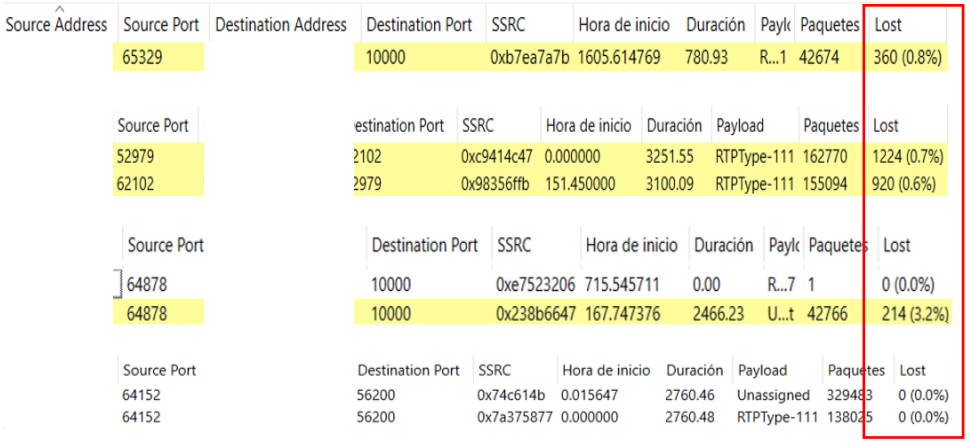
Source Address	Source Port	Destination Address	Destination Port	SSRC	Hora de inicio	Duración	Payload	Paquetes	Lost
	51251		49254	0x3a895294	32.255189	2476.62	RTPType-111	137837	882 (1.2%)
	60500		10000	0xce312fba	0.000000	32.15	RTPType-111	1777	8 (0.4%)

Source Port	ess	Destination Port	SSRC	Hora de inicio	Duración	Payl	Paquetes	Lost
64878		10000	0xeb0e7910	167.746311	0.00	U...7	597	2 (3.2%)
64878		10000	0xcf0fcd48	0.000110	2634.00	R...1	125181	486 (1.7%)

Source Port	ess	Destination Port	SSRC	Hora de inicio	Duración	Payl	Paquetes	Lost
51251		49254	0x3a895294	32.255189	2476.62	R...1	137837	882 (0.6%)
60500		10000	0xce312fba	0.000000	32.15	R...1	1777	8 (0.4%)

Source Port	ss	Destination Port	SSRC	Hora de inicio	Duración	Payl	Paquetes	Lost
65329		10000	0xb7ea7a7b	0.029216	1828.33	R...1	54898	1382 (2.5%)
65329		10000	0x1947324b	0.027417	1830.67	U...7	32689	295 (0.9%)

Figura 50. Capturas sin QoS – Medio día



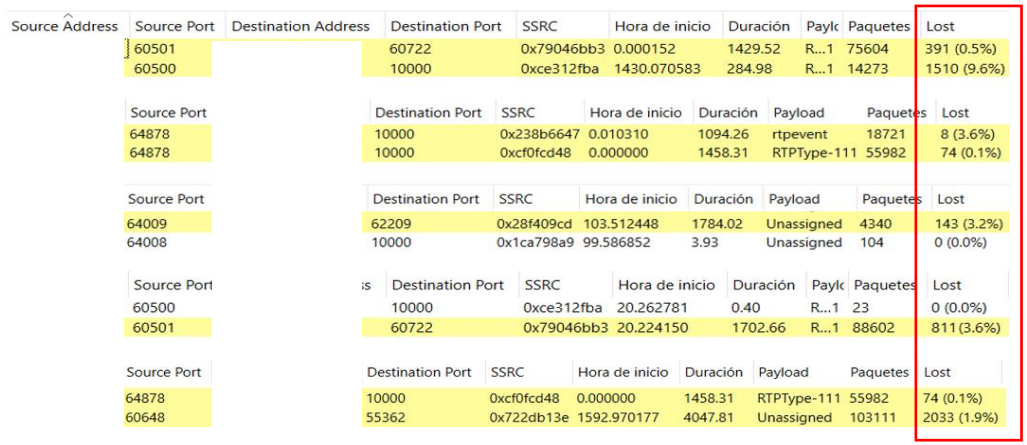
Source Address	Source Port	Destination Address	Destination Port	SSRC	Hora de inicio	Duración	Payl	Paquetes	Lost
	65329		10000	0xb7ea7a7b	1605.614769	780.93	R...1	42674	360 (0.8%)

Source Port	estination Port	SSRC	Hora de inicio	Duración	Payload	Paquetes	Lost
52979	2102	0xc9414c47	0.000000	3251.55	RTPType-111	162770	1224 (0.7%)
62102	2979	0x98356ffb	151.450000	3100.09	RTPType-111	155094	920 (0.6%)

Source Port	Destination Port	SSRC	Hora de inicio	Duración	Payl	Paquetes	Lost
64878	10000	0xe7523206	715.545711	0.00	R...7	1	0 (0.0%)
64878	10000	0x238b6647	167.747376	2466.23	U...t	42766	214 (3.2%)

Source Port	Destination Port	SSRC	Hora de inicio	Duración	Payload	Paquetes	Lost
64152	56200	0x74c614b	0.015647	2760.46	Unassigned	329483	0 (0.0%)
64152	56200	0x7a375877	0.000000	2760.48	RTPType-111	138025	0 (0.0%)

Figura 51. Capturas con QoS -Medio día



Source Address	Source Port	Destination Address	Destination Port	SSRC	Hora de inicio	Duración	Payl	Paquetes	Lost
	60501		60722	0x79046bb3	0.000152	1429.52	R...1	75604	391 (0.5%)
	60500		10000	0xce312fba	1430.070583	284.98	R...1	14273	1510 (9.6%)

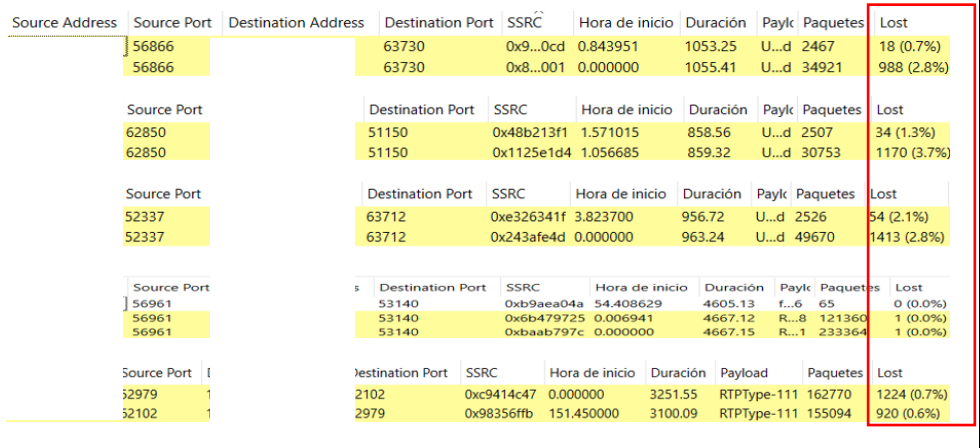
Source Port	Destination Port	SSRC	Hora de inicio	Duración	Payload	Paquetes	Lost
64878	10000	0x238b6647	0.010310	1094.26	rtpevent	18721	8 (3.6%)
64878	10000	0xcf0fcd48	0.000000	1458.31	RTPType-111	55982	74 (0.1%)

Source Port	Destination Port	SSRC	Hora de inicio	Duración	Payload	Paquetes	Lost
64009	62209	0x28f409cd	103.512448	1784.02	Unassigned	4340	143 (3.2%)
64008	10000	0x1ca798a9	99.586852	3.93	Unassigned	104	0 (0.0%)

Source Port	is	Destination Port	SSRC	Hora de inicio	Duración	Payl	Paquetes	Lost
60500		10000	0xce312fba	20.262781	0.40	R...1	23	0 (0.0%)
60501		60722	0x79046bb3	20.224150	1702.66	R...1	88602	811 (3.6%)

Source Port	Destination Port	SSRC	Hora de inicio	Duración	Payload	Paquetes	Lost
64878	10000	0xcf0fcd48	0.000000	1458.31	RTPType-111	55982	74 (0.1%)
60648	55362	0x722db13e	1592.970177	4047.81	Unassigned	103111	2033 (1.9%)

Figura 52. Capturas sin QoS -Tarde



Source Address	Source Port	Destination Address	Destination Port	SSRC	Hora de inicio	Duración	Payl	Paquetes	Lost
	56866		63730	0x9...0cd	0.843951	1053.25	U...d	2467	18 (0.7%)
	56866		63730	0x8...001	0.000000	1055.41	U...d	34921	988 (2.8%)

Source Port	Destination Port	SSRC	Hora de inicio	Duración	Payl	Paquetes	Lost
62850	51150	0x48b213f1	1.571015	858.56	U...d	2507	34 (1.3%)
62850	51150	0x1125e1d4	1.056685	859.32	U...d	30753	1170 (3.7%)

Source Port	Destination Port	SSRC	Hora de inicio	Duración	Payl	Paquetes	Lost
52337	63712	0xe326341f	3.823700	956.72	U...d	2526	54 (2.1%)
52337	63712	0x243afe4d	0.000000	963.24	U...d	49670	1413 (2.8%)

Source Port	s	Destination Port	SSRC	Hora de inicio	Duración	Payl	Paquetes	Lost
56961		53140	0xb9aea04a	54.408629	4605.13	f...6	65	0 (0.0%)
56961		53140	0x6b479725	0.006941	4667.12	R...8	121360	1 (0.0%)
56961		53140	0xbaab797c	0.000000	4667.15	R...1	233364	1 (0.0%)

Source Port	Destination Port	SSRC	Hora de inicio	Duración	Payload	Paquetes	Lost
52979	2102	0xc9414c47	0.000000	3251.55	RTPType-111	162770	1224 (0.7%)
52102	2979	0x98356ffb	151.450000	3100.09	RTPType-111	155094	920 (0.6%)

Figura 53. Capturas con QoS -Tarde

En la Tabla 43 se presentan los resultados obtenidos de las pruebas realizadas antes y después de implementar QoS, tomando como referencia los datos de la Tabla 42. Se detalla el promedio de pérdida de paquetes en cada escenario, el cual fue calculado sumando los valores y dividiéndolos entre el total. Asimismo, la duración de las pruebas, inicialmente registrada en segundos, fue convertida a minutos al dividir entre 60, se especifica el momento del día en que se llevaron a cabo las pruebas, categorizado como: Mañana (8:00 a 12:00), Mediodía (12:00 a 14:00) y Tarde (14:00 a 16:30) y se presenta el promedio general de pérdida de paquetes.

- **Antes de QoS**

Tabla 43. Pérdida de paquetes – Mañana (antes)

Escenario	**Duración en minutos**	**Horario**	**Pérdida de Paquetes**	**Promedio total de perdida de paquetes**
Antes de QoS	17	Mañana	2.55%	**2.59%**
	41	Mañana	3.65%	
	40	Mañana	1%	
	31	Mañana	3.45%	
	41	Mañana	2.15%	

Tabla 44. Pérdida de paquetes – Medio día (antes)

Escenario	**Duración en minutos**	**Horario**	**Pérdida de Paquetes**	**Promedio total de perdida de paquetes**
Antes de QoS	41	Medio día	0.80%	**1.36%**
	44	Medio día	2.45%	
	41	Medio día	0.50%	
	31	Medio día	1.70%	

Tabla 45. Pérdida de paquetes – Tarde (antes)

Escenario	**Duración en minutos**	**Horario**	**Pérdida de Paquetes**	**Promedio total de perdida de paquetes**
Antes de QoS	24	Tarde	5.05%	**2.26%**
	18	Tarde	1.85%	
	30	Tarde	1.60%	
	40	Tarde	1.8%	
	34	Tarde	1.00%	

- **Después de QoS**

Tabla 46. Pérdida de paquetes – Mañana (después)

Escenario	Duración en minutos	Horario	Pérdida de Paquetes	Promedio total de perdida de paquetes
Después de QoS	40	Mañana	2.75%	**1.81%**
	31	Mañana	1.50%	
	30	Mañana	1.6%	
	31	Mañana	0.65%	
	30	Mañana	2.55%	

Tabla 47. Pérdida de paquetes – Medio día (después)

Escenario	Duración en minutos	Horario	Pérdida de Paquetes	Promedio total de perdida de paquetes
Después de QoS	13	Medio día	0.80%	**0.79%**
	54	Medio día	0.65%	
	41	Medio día	1.60%	
	46	Medio día	0%	

Tabla 48. Pérdida de paquetes – Tarde (después)

Escenario	Duración en minutos	Horario	Pérdida de Paquetes	Promedio total de perdida de paquetes
Después de QoS	18	Tarde	1.75%	**1.47%**
	14	Tarde	2.5%	
	16	Tarde	2.45%	
	77	Tarde	0%	
	54	Tarde	0.65%	

- **Análisis de QoS**

La Tabla 49 muestra que el mayor tráfico ocurrió en la mañana, ya que antes de aplicar QoS, la pérdida de paquetes fue 2.59%, el valor más alto comparado con el 1.28% al medio día y el 2.24% en la tarde. Esto indica que en la mañana hubo más congestión en la red. Después de aplicar QoS, la pérdida las perdidas redujeron no en su totalidad, pero existió un cambio.

Tabla 49. Análisis de un antes y después

Escenario	Mañana	Medio día	Tarde
Antes de QoS	2.59%	1.36%	2.26%
Después de QoS	1.81%	0.79%	1.47%

3.3.6 Fase VI: Optimizar

En la fase de optimizar, se llevaron a cabo ajustes y mejoras tanto en la infraestructura de la red como en sus configuraciones, con el objetivo de maximizar su rendimiento y garantizar un funcionamiento eficiente como se presenta en la Tabla 50.

Tabla 50. Corrección de errores

Problema	**Detección**	**Impacto**	**Corrección**
Puertos dañados en el switch.	Se verificó la conexión a Internet puerto por puerto, observando que algunos permanecían en color ámbar sin cambiar de estado.	Sobrecarga en los puertos y posible fallo en la conectividad de la red.	Se reemplazó el switch por otro disponible en el CIDFAE y se realizó las configuraciones.
El perfil de 2 Mbps no utilizaba el ancho de banda reservado.	Se realizó un monitoreo durante 15 días para verificar el uso de las políticas configuradas y esta no tuvo utilización.	Desperdicio de ancho de banda reservado sin ser aprovechado.	Se aumentó el ancho de banda del perfil por defecto para cubrir puertos que no se habían tomado en cuenta.
Distancia mayor a 100 metros con cable UTP en el HANGAR.	Análisis realizado por la nueva empresa proveedora de Internet.	Pérdida de señal, reducción en la calidad de transmisión y baja velocidad en la red.	Se reemplazó el cable UTP por fibra óptica utilizando transceivers para mejorar la conectividad.
Falta de un esquema de red actualizado	Se solicitó información sobre el diagrama de la red, pero no se obtuvo respuesta.	Dificultad para gestionar la red.	Se elaboró un esquema actualizado junto con una tabla detallada sobre segmentación y políticas de QoS.
Computadoras con recursos insuficientes (procesador y memoria)	Se recopiló información sobre las características de cada equipo en la red.	Equipos con hardware limitado generan latencia alta, pérdida de paquetes y descargas lentas, afectando la conectividad y el rendimiento de aplicaciones en red.	Se envió una solicitud para evaluar la adquisición de nuevos equipos con mejor rendimiento.
Políticas de seguridad para restingir ciertos accesos	Mediante el ingreso a redes sociales.	Pueden consumir gran parte del ancho de banda, reduciendo la capacidad para aplicaciones críticas como sistemas de comunicación	El personal que maneja la seguridad de la fuerza aérea se encargó de implementar ciertas políticas.

En base a las correcciones realizadas, se presenta el siguiente test de velocidad con nPerf. La prueba se llevó a cabo en el área de comando, utilizando una laptop con tarjeta de red de 1 Gbps, conectada mediante cable Ethernet durante la tarde cabe mencionar que se realizó varias pruebas del mismo Figura 55, Figura 57, pero se colocó la imagen más representativa.

a. Pruebas antes con nPerf

La Figura 54, presenta la prueba de velocidad la cual mostró una velocidad de descarga máxima de 21.90 Mb/s, mientras que la velocidad de carga alcanzó 11.98 Mb/s con. La latencia fue de 15 ms, con un jitter de 11.70 ms, lo que indica una conexión funcional, pero con posibles fluctuaciones.



Figura 54. Prueba nPerf antes de las implementaciones



Figura 55. Pruebas realizadas

b. Pruebas después con nPerf

La Figura 56 presenta una velocidad de descarga máxima de 41.12 Mb/s, mientras que la velocidad de carga alcanzó 33.20 Mb/s. La latencia fue significativamente menor, con 5.800 ms y un jitter de 11.30 ms, lo que indica una conexión más estable y rápida.

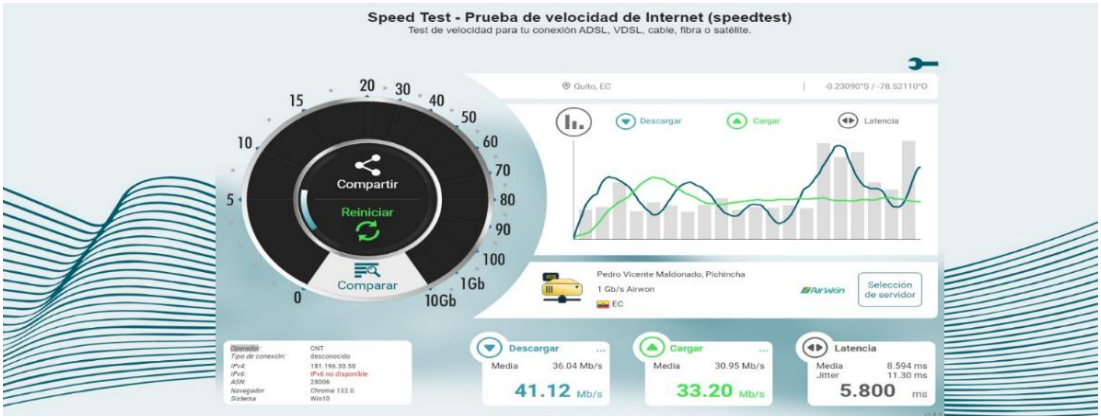


Figura 56. Prueba nPerf después de las implementaciones



Figura 57. Pruebas realizadas

CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- Mediante el análisis de la red y el monitoreo realizado con las herramientas de Fortigate, Palo Alto, PingPlotter, Wireshark, se identificaron los equipos y los patrones de uso, evidenciando que el tráfico proviene principalmente de navegación web, videoconferencias y transmisión de datos. Además, se determinó que las horas pico ocurren en la mañana y la tarde, con mayor congestión los días laborables.

- Se eligieron los algoritmos de Low Latency Queueing (LLQ) y Weighted Fair Queuing (WFQ) debido a su capacidad para manejar eficientemente la congestión y garantizar tiempos de respuesta óptimos. LLQ combina prioridad estricta con un sistema de colas, mientras que WFQ distribuye equitativamente el ancho de banda, evitando que una sola clase monopolice los recursos

- Para la configuración de QoS en el CIDFAE, se utilizó el FortiGate, ya que es compatible con estas funciones y ofrece una solución flexible. Además, QoS no está limitado a marcas específicas, lo que facilita su integración en infraestructuras de red heterogéneas. Se implementó Traffic Shaping basado en puertos debido a su precisión en la gestión del ancho de banda, permitiendo un mejor control del tráfico en la red.

- Los resultados muestran una mejora significativa en la pérdida de paquetes tras la implementación de QoS, reduciendo el promedio de 2.59% a 1.81%. Antes de QoS, las pérdidas fueron más altas, especialmente en la mañana. Después de QoS, se observa mayor estabilidad, con valores más bajos en los horarios.

- Las pruebas de velocidad reflejan una mejora significativa en la conexión tras las implementaciones realizadas, pasando de una descarga de 21.90 Mb/s y carga de 11.98 Mb/s con una latencia de 15 ms y jitter de 11.70 ms, a una descarga de 41.12 Mb/s y carga de 33.20 Mb/s, con una latencia reducida a 5.800 ms, lo que indica mayor estabilidad y eficiencia.

4.2 Recomendaciones

- Se recomienda contar con un esquema actualizado de la red, lo que permitirá una gestión eficiente de la infraestructura, agilizando la resolución de problemas. Mantener un esquema detallado facilita la identificación de la ubicación de los dispositivos, conexiones entre ellos, lo que contribuye a la detección de fallos, evitar redundancias innecesarias y prevenir posibles conflictos de direccionamiento IP, permitiendo así una administración más efectiva y organizada.

- Se sugiere que el rack de control esté ubicado en un lugar con temperatura controlada entre 21°C y 23°C o que cuente con un sistema de ventilación eficiente porque los equipos pueden recalentarse, lo que podría generar una disminución en su vida útil o incluso interrupciones en el servicio de red afectando la estabilidad y el rendimiento de la infraestructura tecnológica.

- Se recomienda realizar copias de seguridad de manera periódica para prevenir la pérdida de configuraciones o datos importantes en caso de fallos en algún equipo de la red ya que los imprevistos como errores en el hardware o fallos en la alimentación eléctrica pueden comprometer la información. Para firewalls y switches, se sugiere realizar respaldos al menos una vez por semana o después de cualquier cambio en la configuración, asegurando que cualquier ajuste reciente pueda restaurarse en caso de una falla.

- Es recomendable utilizar programas que permitan simular la red, ya que brindan la posibilidad de probar configuraciones, detectar errores y optimizar el rendimiento antes de aplicarlas en un entorno real. Estas simulaciones ayudan a evaluar el comportamiento del tráfico, ajustar parámetros y anticipar posibles problemas, evitando interrupciones en la infraestructura productiva.

REFERENCIAS BIBLIOGRÁFICAS

[1] Cisco, «Reporte de tendencias globales en redes 2020», Cisco. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://engage2demand.cisco.com/LP=18333

[2] D. Kim, «A 2020 perspective on "A dynamic model for the evolution of the next generation Internet – Implications for network policies": Towards a balanced perspective on the Internet's role in the 5G and Industry 4.0 era», *Electron. Commer. Res. Appl.*, vol. 41, p. 100966, may 2020, doi: 10.1016/j.elerap.2020.100966.

[3] C. E. para A. L. y el Caribe, *Infraestructura de Internet en América Latina: puntos de intercambio de tráfico, redes de distribución de contenido, cables submarinos y centros de datos*. Comisión Económica para América Latina y el Caribe, 2020. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://www.cepal.org/es/publicaciones/46388-infraestructura-internet-america-latina-puntos-intercambio-trafico-redes

[4] W. Liu, B. Yu, X. Liu, X. Chi, y J. Zhang, «Bandwidth abstraction and service rate instantiation for latency-bounded reliability provisioning in 5th generation wireless networks», *Comput. Commun.*, vol. 215, pp. 120-129, feb. 2024, doi: 10.1016/j.comcom.2023.12.017.

[5] C. R. Zapata, E. I. Rodriguez, y A. G. Zaballos, «Estado actual de las telecomunicaciones y la banda ancha en Ecuador», *IDB Publ.*, feb. 2020, doi: 10.18235/0002200.

[6] T. A. V. Peralta, A. K. A. Cedeño, y T. E. C. Macías, «Revisión de los mecanismos de QoS en las instituciones públicas del Ecuador», *Informática Sist. Rev. Tecnol. Informática Las Comun.*, vol. 6, n.º 1, Art. n.º 1, ene. 2022, doi: 10.33936/isrtic.v6i1.4565.

[7] A. M. Robalino Tubón, «Optimización de la infraestructura de red Lan mediante la aplicación de una metodología de diseño de redes en la Unidad Educativa Bolívar», Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Tecnologías de la Información, 2024. Accedido: 1

de diciembre de 2024. [En línea]. Disponible en: https://repositorio.uta.edu.ec/handle/123456789/40814

[8] N. E. Zapata Tapia, «Nodo de gestión y monitoreo de calidad de servicio de la empresa Ajnet en el cantón Latacunga.», Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Telecomunicaciones, 2023. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://repositorio.uta.edu.ec/handle/123456789/38409

[9] M. Yunga y C. Giovanny, «Análisis del impacto de un ataque DoS en la calidad de servicio de sistemas streaming multimedia en redes SDN.», masterThesis, Quito, 2021, 2021. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: http://bibdigital.epn.edu.ec/handle/15000/21663

[10] A. P. Silva García, «Laboratorio de telefonía IP : elaboración de prácticas de laboratorio aplicadas al aseguramiento y calidad de servicio de la infraestructura de voz sobre IP.», bachelorThesis, Quito : EPN, 2022., 2022. Accedido: 7 de diciembre de 2024. [En línea]. Disponible en: http://bibdigital.epn.edu.ec/handle/15000/23278

[11] J. D. Miranda Quishpe, «Sistema de comunicación en tiempo real con QOS para la integración de las unidades de salud de la provincia de Pastaza», Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Ingeniería en Electrónica y Comunicaciones, 2021. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://repositorio.uta.edu.ec/handle/123456789/33160

[12] H. Wang, J. Gu, y L. Xia, «Improved BEB Algorithm for Computer Network Optimization», en *2023 2nd International Conference for Innovation in Technology (INOCON)*, mar. 2023, pp. 1-5. doi: 10.1109/INOCON57975.2023.10101237.

[13] S. P. Badarla y V. P. Harigovindan, «Restricted Access Window-Based Resource Allocation Scheme for Performance Enhancement of IEEE 802.11ah Multi-Rate IoT Networks», *IEEE Access*, vol. 9, pp. 136507-136519, 2021, doi: 10.1109/ACCESS.2021.3117836.

[14] C. Sieber, S. Schwarzmann, A. Blenk, T. Zinner, y W. Kellerer, «Scalable Application- and User-aware Resource Allocation in Enterprise Networks Using End-

Host Pacing», *ACM Trans Model Perform Eval Comput Syst*, vol. 5, n.º 3, p. 11:1-11:41, may 2020, doi: 10.1145/3381996.

[15] E. Ayala y S. Gonzales Sánchez, «Tecnologías de la Información y la Comunicación», *Repos. Inst. - UIGV*, ago. 2015, Accedido: 14 de abril de 2024. [En línea]. Disponible en: http://repositorio.uigv.edu.pe/handle/20.500.11818/1189

[16] D. S. Pacheco, «Seguridad en redes de comunicaciones: Perspectivas y desafíos», *Ingeniare Rev. Chil. Ing.*, vol. 30, n.º 2, pp. 215-217, jun. 2022, doi: 10.4067/S0718-33052022000200215.

[17] F. E. Arévalo-Cordovilla, I. B. Ordoñez-Sigcho, M. F. Peñaherrera-Larenas, y V. J. Suárez-Matamoros, «Importancia de la seguridad de los sistemas de información frente el abuso, error y hurto de información», *Dominio Las Cienc.*, vol. 6, n.º 2, Art. n.º 2, abr. 2020, doi: 10.23857/dc.v6i2.1197.

[18] A. B. Martí, *Gestión de red*. Univ. Politèc. de Catalunya, 1999.

[19] A. Walton, «¿Qué es QoS? Cómo Usar QoS con Ejemplos » CCNA desde Cero», CCNA desde Cero. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://ccnadesdecero.es/que-es-qos/

[20] Villamarín, Erick José Alcívar; Herrera-Tapia, Jorge; Felipe, Marely Del Rosario Cruz, «Diseño de redes para Instituciones Académicas con criterios de QoS - ProQuest». Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://www.proquest.com/openview/937c0ffcf92bf2c246a4fa9621752df6/1?pq-origsite=gscholar&cbl=1006393

[21] «Infraestructura de red con Red Hat y sus partners». Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://www.redhat.com/es/partners/network-infrastructure

[22] «Descubriendo la Infraestructura de Red: Fundamentos y Funciones». Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://www.accessq.com.mx/infraestructura-de-red/

[23] Cisco, «What Is Network Switching?» Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://www.cisco.com/c/en/us/products/switches/what-is-network-switching.html

[24] Cisco, «What Is Routing?» Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://www.cisco.com/c/en/us/products/routers/what-is-routing.html

[25] G. Junco Romero y S. Rabelo Padua, «Los recursos de red y su monitoreo», *Rev. Cuba. Informática Médica*, vol. 10, n.º 1, pp. 76-83, jun. 2018.

[26] Cisco, «What Is Network Monitoring?», Cisco. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://www.cisco.com/c/en_uk/solutions/automation/what-is-network-monitoring.html

[27] A. F. Cumbajin Cumbajin, «Implementación de un sistema de control de acceso y video vigilancia a través de una red LAN interna en el laboratorio de comunicaciones de la Universidad de Fuerzas Armadas sede Latacunga para precautelar la integridad de equipos tecnológicos», Universidad de las Fuerzas Armadas ESPE Extensión Latacunga. Carrera de Tecnología en Redes y Telecomunicaciones., 2022. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: http://repositorio.espe.edu.ec/handle/21000/30405

[28] J. A. Estrella Onofa, «Diseño de red para empresas aplicando QoS para el tráfico de red y VLANs», PUCE - Quito, 2022. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://repositorio.puce.edu.ec/handle/123456789/27460

[29] Cisco, «Catalyst 2960, 2960-S, 2960-C, and 2960-Plus Switches Software Configuration Guide, Cisco IOS Release 15.0(2)SE and Later - Configuring QoS [Cisco Catalyst 2960 Series Switches]», Cisco. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: ttps://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/15-0_2_se/configuration/guide/scg2960/swqos.html

[30] Cisco, «Configure Catalyst 3750 QoS - Cisco». Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/91862-cat3750-qos-config.html

[31] TP-Link, «Switch Inteligente Sencillo de 24-Puertos Gigabit». Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://www.tp-link.com/ec/business-networking/easy-smart-switch/tl-sg1024de/

[32] «Traffic shaping | Administration Guide». Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/297431/traffic-shaping

[33] B. F. Simbaña Pineida, «Desarrollo de un prototipo de aplicación web interactiva para la simulación de las principales disciplinas de planificación de paquetes para la gestión de QoS.», bachelorThesis, Quito, 2022, 2022. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: http://bibdigital.epn.edu.ec/handle/15000/22156

[34] J. A. Arce Villacres, «Evaluación de parámetros de QOS en la transmisión de aplicaciones multimedia en una red FTTH utilizando el estándar ITU-T G987.X.», Escuela Superior Politécnica de Chimborazo, 2020. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: http://dspace.espoch.edu.ec/handle/123456789/20406

[35] Cisco, «QoS: DiffServ for Quality of Service Overview Configuration Guide, Cisco IOS Release 15M&T - Overview of DiffServ for Quality of Service [Support]», Cisco. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_dfsrv/configuration/15-mt/qos-dfsrv-15-mt-book/qos-dfsrv.html

[36] «QoS: Congestion Management Configuration Guide, Cisco IOS Release 15S - Congestion Management Overview [Support]», Cisco. Accedido: 27 de enero de 2025. [En línea]. Disponible en: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_conmgt/configuration/15-s/qos-conmgt-15-s-book/qos-conmgt-oview.html

[37] D. P. Quevedo Bravo y C. L. Vaca Nuñez, «Diseño e implementación de calidad de servicio (QoS) en la red de transporte de datos del Municipio del Distrito Metropolitano de Quito (MDMQ)», bachelorThesis, QUITO/EPN/2011, 2011. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: http://bibdigital.epn.edu.ec/handle/15000/4409

[38] J. C. Muñoz Alva, «Diseño de una red de interconexión de sedes para mejorar el flujo de información de la empresa Olva Courier - Trujillo», Universidad César Vallejo, 2021. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/78936

[39] C. A. A. Ortiz, A. D. Carhuamaca, M. A. Astucuri, y L. A. Huamán, «Implementación de Redes Virtuales Locales Fortaleciendo la Seguridad de la Información», *Sello Editor. CITSA*, pp. 1-71, nov. 2024, doi: 10.61286/edcitsa.vi.97.

[40] «Firewall Fortinet FortiGate 40F Protege contra amenazas cibernéticas», Neuronet. Accedido: 28 de enero de 2025. [En línea]. Disponible en: https://neuronet.cl/producto/firewall-fortinet-fortigate-40f/

[41] Ago 19 y 2020, «DESCRIPCIÓN GENERAL DEL FIREWALL», Palo Alto Networks. Accedido: 28 de enero de 2025. [En línea]. Disponible en: https://www.paloaltonetworks.lat/resources/datasheets/descripcion-del-firewall

[42] «The Complete Manual — Learn How to PingPlotter», Graphical Network Monitoring and Troubleshooting | PingPlotter. Accedido: 28 de enero de 2025. [En línea]. Disponible en: https://www.pingplotter.com/manual/

[43] «UCM-Proyecto de Innovación Software libre para ciencias e ingenierías». Accedido: 28 de enero de 2025. [En línea]. Disponible en: https://www.ucm.es/pimcd2014-free-software/wireshark

[44] «Cisco Secure Network Analytics», Cisco. Accedido: 28 de enero de 2025. [En línea]. Disponible en: https://www.cisco.com/site/au/en/products/security/security-analytics/secure-network-analytics/index.html

[45] «Blocking QUIC Application Leads to Impacted Performance for Cis... - Knowledge Base - Palo Alto Networks». Accedido: 28 de enero de 2025. [En línea]. Disponible en: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HCZOCA4&lang=en_US%E2%80%A9

[46] «Wireshark · Display Filter Reference: Transmission Control Protocol», Wireshark. Accedido: 28 de enero de 2025. [En línea]. Disponible en: https://www.wireshark.org/templates/dfref-protocol-page.html

[47] L. C. Azogue Talahua, «Calidad de servicio (QoS) en la Red MAN de la Empresa Eléctrica Ambato Regional Centro Norte S.A (EEASA) y sus sucursales», Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Ingeniería en Electrónica y Comunicaciones, 2015. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: http://repositorio.uta.edu.ec/handle/123456789/8603

[48] M. A. Viracucha Pilozo, «Implementación de técnicas de Calidad de Servicio (QoS) en un prototipo de red convergente de datos, video y telefonía usando IPv6 en una empresa PYME tipo», bachelorThesis, Quito, 2019., 2019. Accedido: 1 de diciembre de 2024. [En línea]. Disponible en: http://bibdigital.epn.edu.ec/handle/15000/20278

[49] Ivetec, *Determinación de ancho de banda que requiere una empresa*, (16 de mayo de 2020). Accedido: 28 de enero de 2025. [En línea Video]. Disponible en: https://www.youtube.com/watch?v=5kzKYJ4RHs0

[50] W. O. Chancosí Maldonado, «Implementación de políticas de calidad de servicio (QOS) para los servidores de internet de la empresa Saitel», bachelorThesis, 2017. Accedido: 28 de enero de 2025. [En línea]. Disponible en: https://dspace.uniandes.edu.ec/handle/123456789/5880

[51] «Limiting bandwidth with traffic shaping | Cookbook». Accedido: 29 de enero de 2025. [En línea]. Disponible en: https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/107907/docs.fortinet.com/document/fortigate/5.4.0/cookbook/107907/limiting-bandwidth-with-traffic-shaping

[52] «Traffic shaping policies | Administration Guide». Accedido: 29 de enero de 2025. [En línea]. Disponible en: https://docs.fortinet.com/document/fortigate/7.6.1/administration-guide/673634/docs.fortinet.com/document/fortigate/7.6.1/administration-guide/673634/traffic-shaping-policies

ANEXOS

Anexo A. Validación de encuesta

En las Figuras A1, A2 y A3 se muestran los resultados obtenidos a través de la encuesta realizada, evaluados mediante el coeficiente alfa de Cronbach.

Encuestados	Pregunta 1	Pregunta 4	Pregunta 5	Pregunta 6	Pregunta 8	Pregunta 9	Suma
1	2	3	2	2	2	2	13
2	1	1	1	2	2	2	9
3	1	3	1	2	1	2	10
4	1	2	2	4	2	2	13
5	2	2	1	3	3	2	13
6	1	3	2	3	2	3	14
7	2	2	1	3	3	3	14
8	2	3	2	3	3	3	16
9	3	3	3	2	3	4	18
10	2	2	2	2	2	2	12
11	2	3	2	3	3	3	16
12	2	3	2	3	3	3	16
13	2	3	2	3	3	3	16
14	2	3	2	3	3	3	16
15	2	3	2	2	2	2	13
16	3	2	2	2	2	2	13
17	2	2	2	2	2	2	12
18	2	3	2	2	3	3	15
19	1	3	2	2	3	3	14
20	1	2	2	2	2	2	11
21	1	4	1	4	4	4	18
22	2	3	2	2	2	2	13
23	1	3	2	3	2	3	14
24	1	1	2	3	2	1	10
25	3	2	3	2	2	3	15
26	2	3	2	3	2	2	14
27	2	2	2	3	3	3	15
28	2	2	2	3	2	2	13

Figura A1. Resultados de la encuesta

30	1	3	3	2	1	3	**13**
31	2	3	2	3	3	3	**16**
32	2	3	2	3	3	3	**16**
33	2	3	2	3	3	3	**16**
34	2	2	2	3	2	2	**13**
35	2	2	3	2	2	3	**14**
36	3	2	4	4	4	4	**21**
37	2	2	3	2	3	3	**15**
38	2	3	1	2	2	2	**12**
39	2	3	2	3	3	3	**16**
40	2	2	3	2	2	2	**13**
41	1	2	4	4	1	3	**15**
42	2	3	2	3	3	3	**16**
43	2	3	2	3	3	3	**16**
44	1	1	1	1	2	2	**8**
45	3	2	2	2	2	2	**13**
46	2	3	2	3	3	3	**16**
47	2	3	2	3	3	3	**16**
48	2	4	2	4	3	3	**18**
49	3	3	3	2	3	3	**17**
50	3	2	2	2	2	2	**13**
51	2	3	2	3	3	3	**16**
52	2	2	2	2	2	2	**12**
53	2	3	2	3	2	2	**14**
54	2	3	2	3	2	3	**15**
55	2	1	1	1	2	1	**8**
56	1	1	2	2	1	2	**9**
57	1	1	1	2	2	2	**9**

Figura A2. Resultados de la encuesta

57	1	1	1	2	2	2	**9**
58	2	3	2	2	2	2	**13**
59	1	3	2	3	1	3	**13**
60	2	3	2	3	2	3	**15**
61	1	3	2	3	2	3	**14**
62	2	3	2	4	2	3	**16**
63	2	3	2	3	3	3	**16**
Varianza	0,365	0,503	0,380	0,490	0,454	0,401	
Sumatoria de	2,593						
Varianza total	6,286						

$$\alpha = \left(\frac{k}{k-1}\right)\left(1 - \frac{\Sigma v_i}{v_t}\right)$$

Símbolo	**Signifcado**	**Valor**
α	Coeficiente de	0,705
k	Número de íte	6
ΣVi	Sumatoria de	2,593
vt	Varianza tota	6,286

Rango
0,9 - 1
0,8 - 0,9
0,7 - 0,8
0,6 - 0,7
0,5 - 0,6
< 0,5

Figura A3. Resultados de la encuesta

Anexo B. Configuración de SW_PROYECTOS, SW_HANGAR y SW_GOMAI

Las Figuras B1, B2 y B3 ilustran el proceso de creación de VLAN, la configuración de la troncalización de puertos, la asignación de puertos a las VLAN correspondientes e IPs de administración.

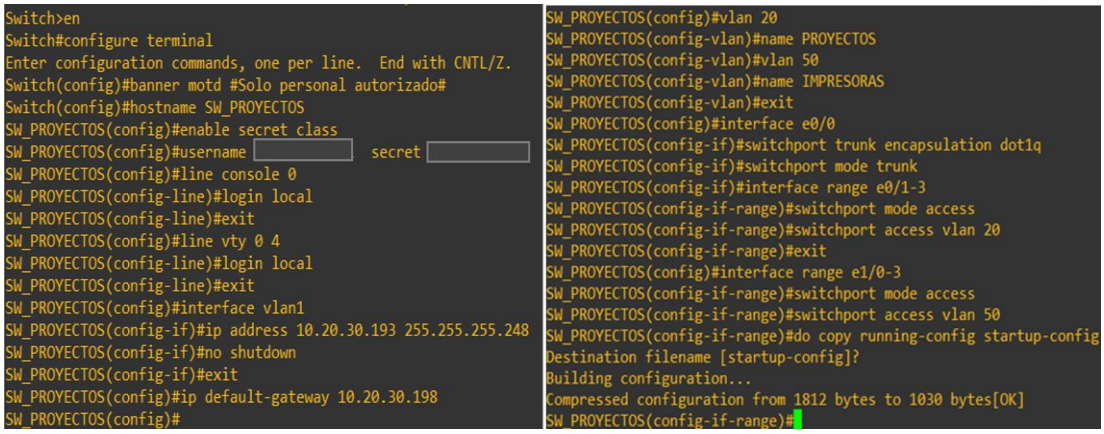


Figura B1. Configuración de SW_PROYECTOS

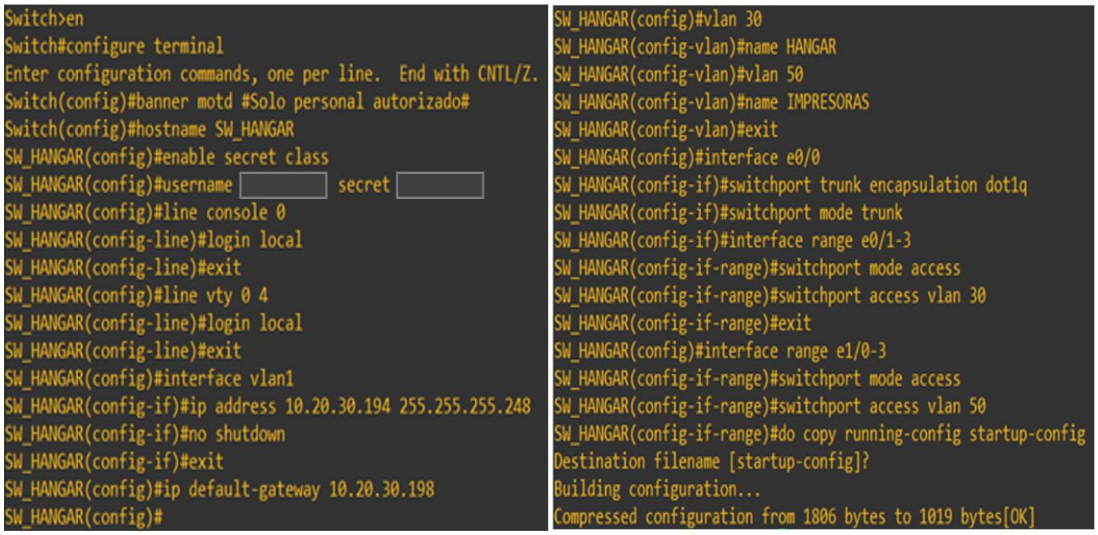


Figura B2. Configuración de SW_HANGAR

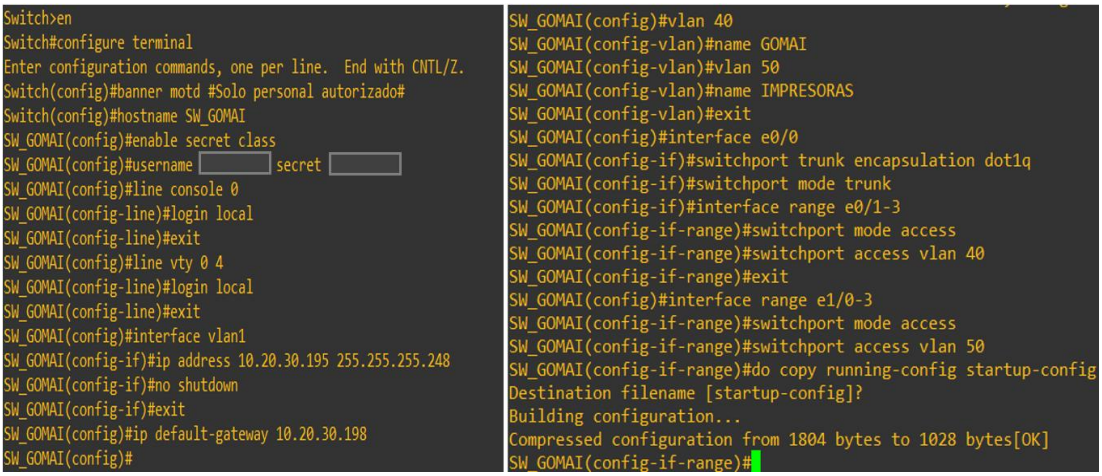


Figura B 3. Configuración de SW_GOMAI

Anexo C. Configuraciones de perfiles de tráfico

Las Figuras C1, C2 y C3 muestran el perfil de tráfico configurado en el sistema. En las figuras se presentan los nombres asignados a cada perfil, así como los valores correspondientes al ancho de banda máximo y mínimo definidos para cada uno. Además, se especifica el valor DSCP asignado a cada perfil lo que permite priorizar el tráfico en la red de acuerdo con las políticas de calidad de servicio establecidas.

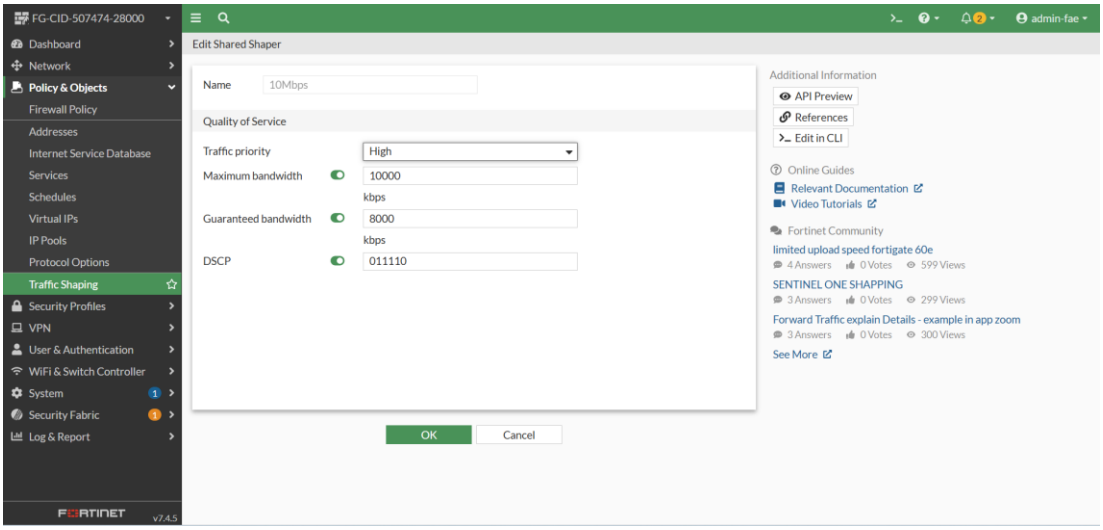


Figura C 1. Configuración del perfil

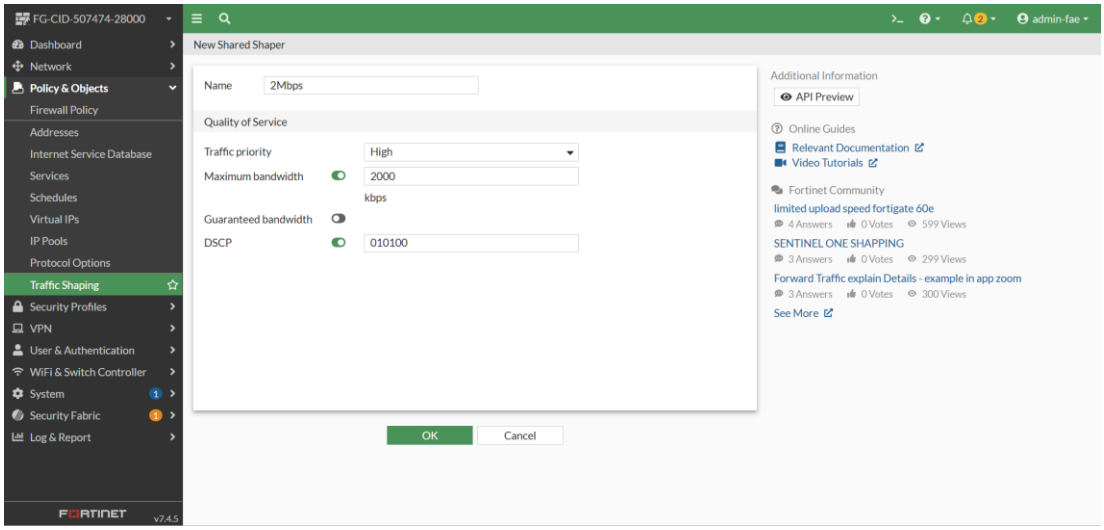


Figura C2. Configuración del perfil

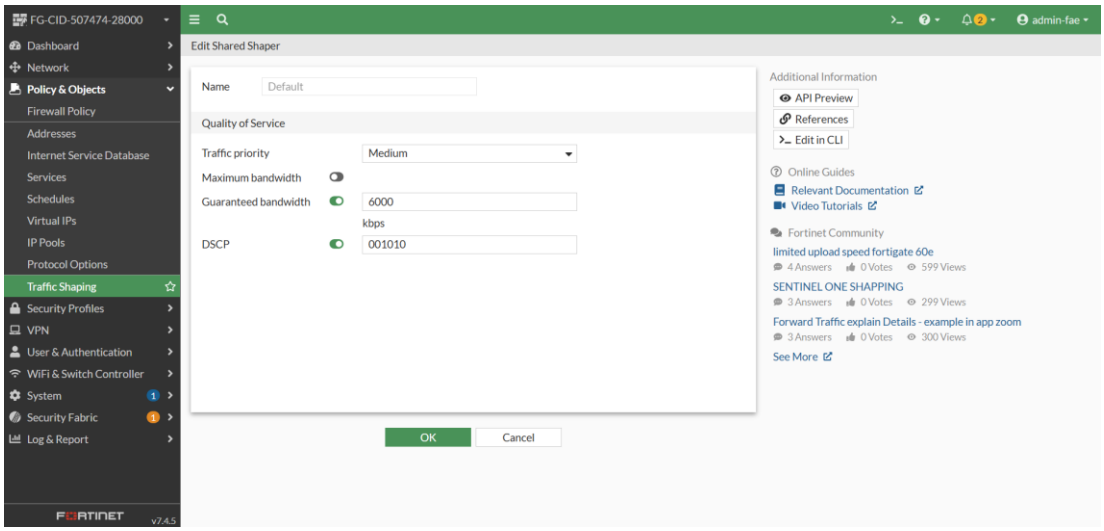


Figura C3. Configuración del perfil

Anexo D. Configuración de puertos

Las Figuras D1, D2, D3, D4 y D5 presentan la configuración de los puertos asignados para cada política implementada, mostrando tanto el nombre del servicio como el protocolo específico utilizado.



Figura D1. Puertos para videoconferencia

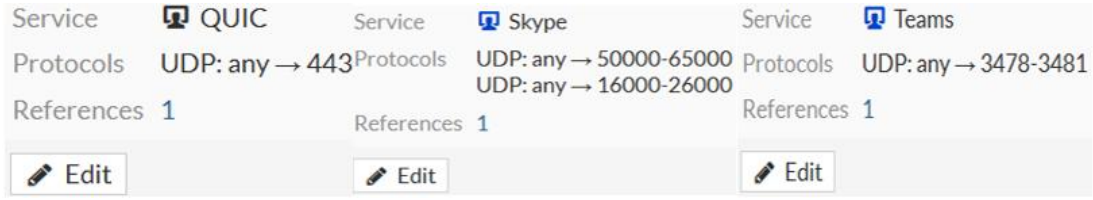


Figura D2. Puertos para videoconferencia

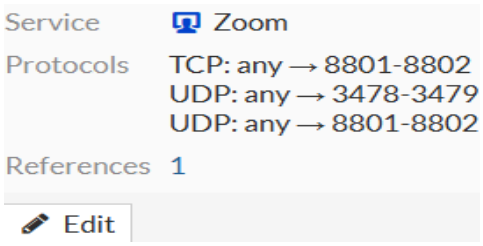


Figura D3. Puertos para videoconferencia



Figura D4. Puertos para navegación web

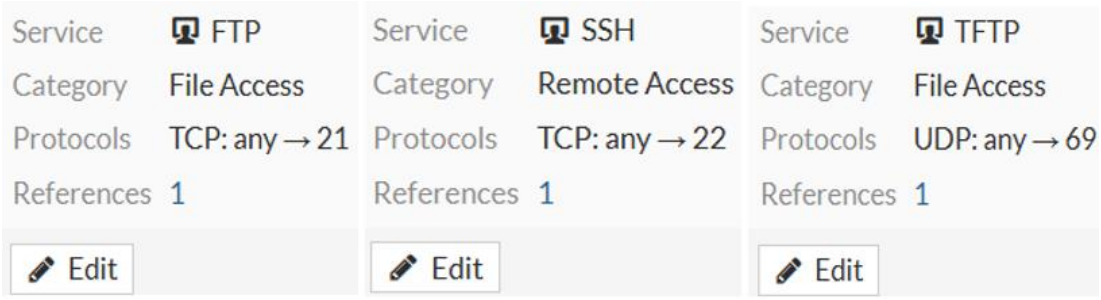


Figura D5. Puertos para Datos

Anexo E. Configuración del generador de tráfico

Para realizar la simulación de tráfico se configuro Ostinato una herramienta de software utilizada para generar, capturar y analizar tráfico en redes. La instalación se llevó a cabo en una máquina virtual con la distribución de Linux Ubuntu. En la Figura E1, se presenta el proceso de configuración de una dirección IP estática para la máquina y se verificación de conectividad a Internet.

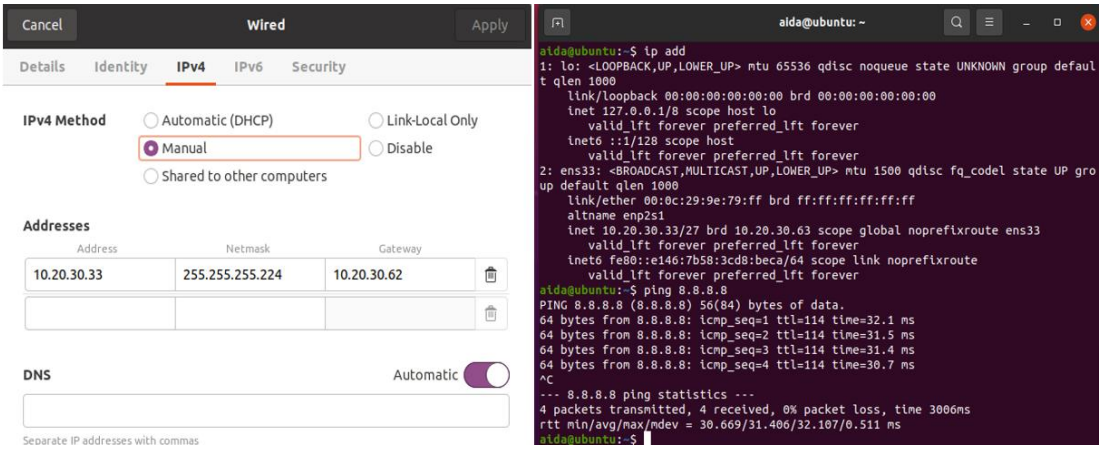


Figura E1. Conexión a Internet máquina Ubuntu

Para mantener el sistema sincronizado con los repositorios y evitar problemas al instalar el software se utilizó el comando “sudo apt update” y se procedió con la instalación “sudo apt-get install ostinato” y ejecución “sudo ostinato”. Figura E2

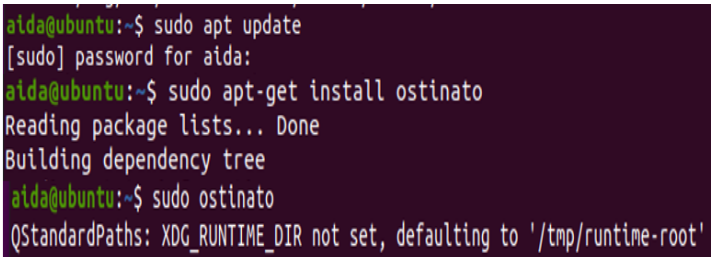


Figura E2. Instalación ostinato

En la ventana de Ostinato, se creó un nuevo flujo, se seleccionó la opción IPv4 como base para la configuración del tráfico y se configuró el tráfico a generar como ICMP como se presenta en la Figura E3.

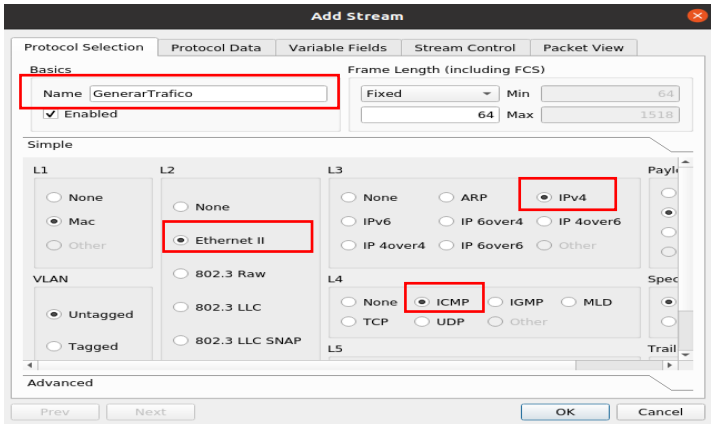


Figura E3. Selección de protocolo en Ostinato

En los “Datos de Protocolo”, se configuraron las direcciones IP correspondientes para el tráfico ICMP la IP de origen se estableció como la dirección asignada a la máquina virtual desde la cual se genera el tráfico, mientras que la IP de destino se configuró como la puerta de enlace predeterminada que conduce hacia el FortiGate como se muestra en la Figura E4.

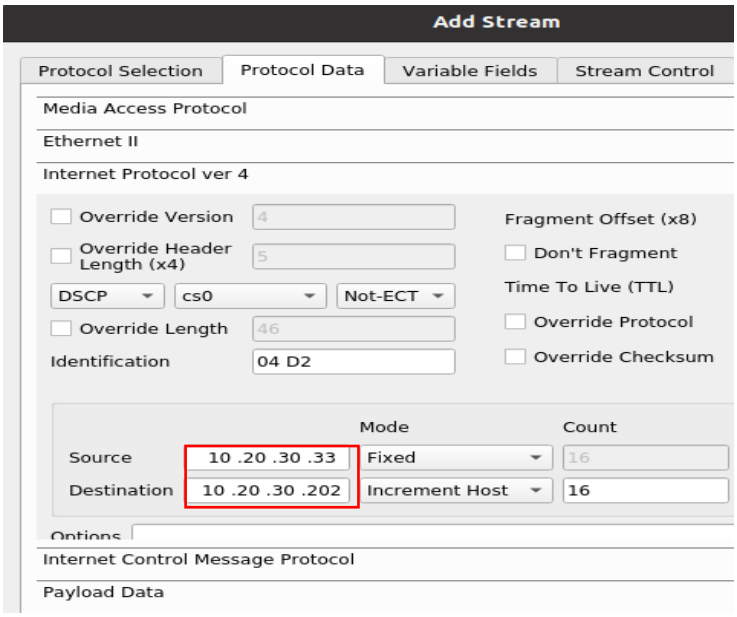


Figura E4. Configuración de IP origen y destino

La Figura E5 muestra la configuración del número total de paquetes enviados y la velocidad de transmisión en el cual, se estableció un volumen alto de paquetes.

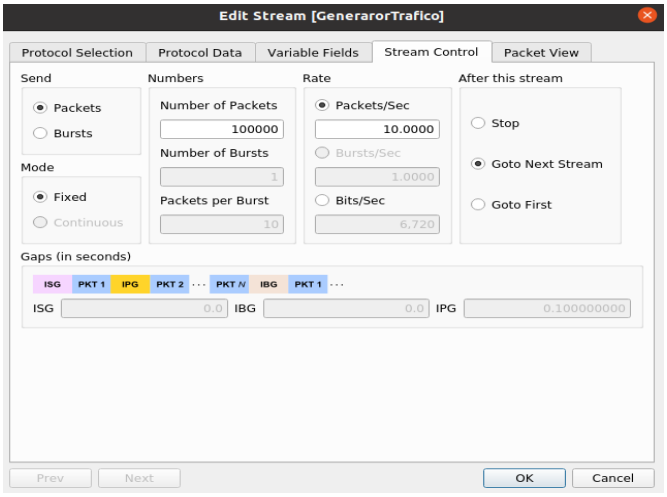


Figura E5. Configuración de paquetes

Finalizadas las configuraciones en Ostinato, se aplicaron los cambios realizados y se presionó el botón Play para iniciar la ejecución del tráfico configurado, se inició la captura del tráfico utilizando la herramienta Wireshark permitiendo observar y analizar el tráfico generado como se muestra en la Figura E6.

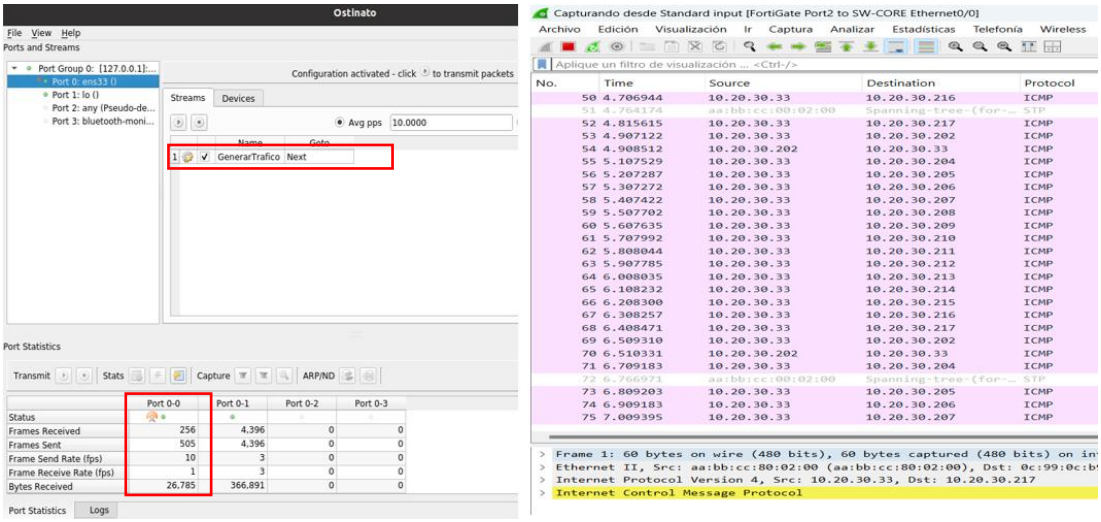


Figura E6. Ejecución del flujo en Ostinato

GNS3 está disponible para descargar en múltiples plataformas, incluyendo Windows, Linux y macOS. Para instalar y configurar imágenes en GNS3 integrando herramientas como Dynamips, que permite ejecutar imágenes IOS de Cisco, Dynagen que actúa como una interfaz de texto para Dynamips y Qemu utilizado para emular equipos de red como firewalls o routers, que no están disponibles fácilmente en el software lo que facilita la creación de laboratorios de redes realistas. A continuación, se proporcionarán los enlaces de descarga para las imágenes:

GNS3: https://gns3.com/marketplace/appliances

Cisco IOS: https://www.telectronika.com/descargas/cisco-imagenes-ios-para-gns3-dynamips-y-vm/

Varias imágenes: https://github.com/hegdepavankumar/Cisco-Images-for-GNS3-and-EVE-NG?tab=readme-ov-file

- **Requerimientos mínimos para equipos**

Los requisitos mínimos para ejecutar dispositivos de red en GNS3 como: routers Mikrotik, Fortigate y switches varían según el tipo de dispositivo y su complejidad Figura F1. A continuación, se muestran los requerimientos para la instalación de los equipos:

Dispositivo	**Versión**	**RAM Mínima**	**Procesador**	**Notas**
Router Mikrotik	7.2.3	384 MB	1 núcleo	Requiere imágenes compatibles con CHR para GNS3.
Firewall Fortigate	7.0.0	2048 MB	1 núcleo	La RAM depende de la imagen; FortiOS emula firewall y servicios complejos.
Switch Cisco	15.1	256 MB	1 núcleo	Para switches básicos. Los avanzados podrían requerir más RAM y CPU
Windows	Windows 7 (64 bit) o superior	4 GB	2 núcleo	Puede que requiera espacio de almacenamiento adicional para el sistema operativo y las imágenes de los dispositivos.
Linux	20.0.4	2 GB	2 núcleo	Es recomendable asignar recursos según los servicios que se planee ejecutar

Figura F1. Requerimientos para equipos

Una vez instalado en GNS3, se inició el programa para cargar la imagen del switch y se accedió a la sección de **“Preferences”.** Figura F2

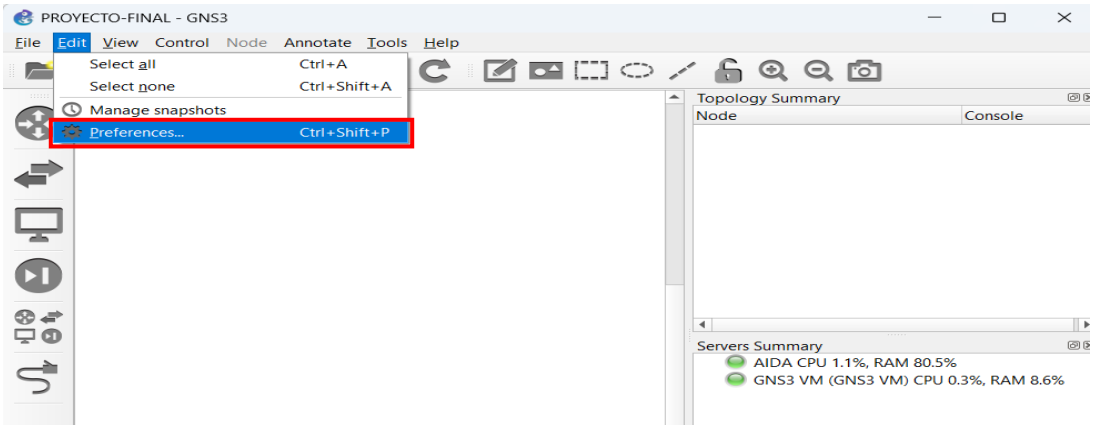


Figura F2. Interfaz de GNS3

En el menú se seleccionó “IOU Devices” y se creó un nuevo dispositivo, al cual se le asignó un “nombre”, se configuró el “tipo de imagen” y se especificó la “ruta” donde se encontraba la imagen del switch. Finalmente, se hizo clic en “Finish” para completar el proceso como se muestra en la Figura F3.

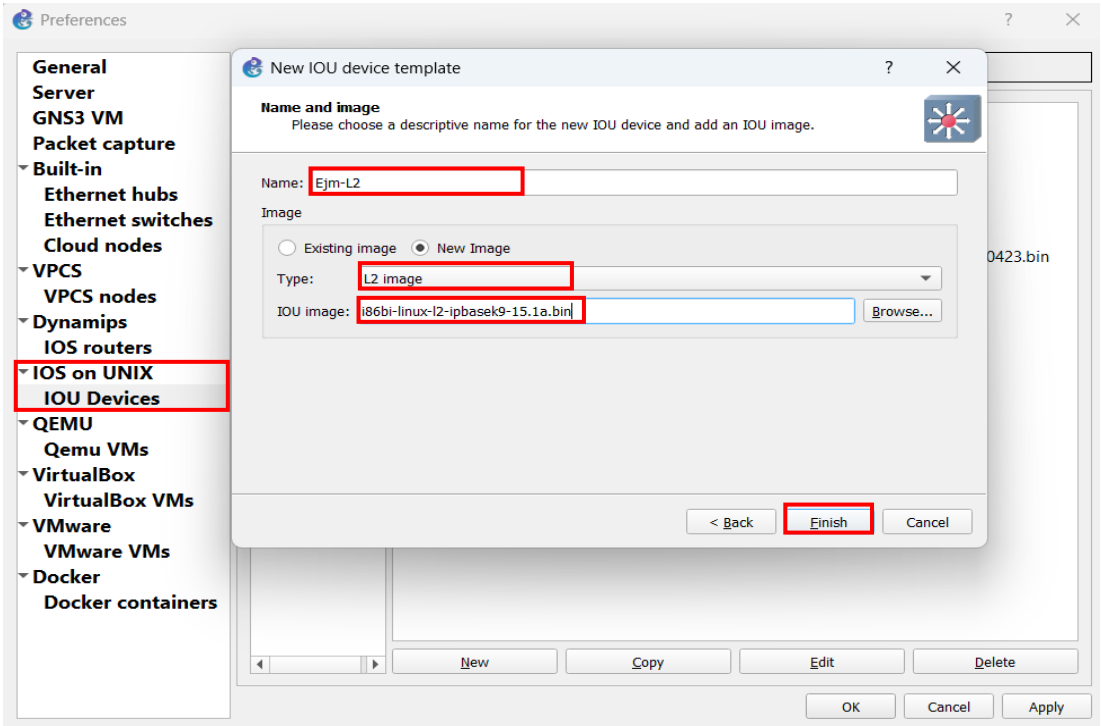


Figura F3. Instalación de la imagen del switch

Para la instalación del router MikroTik, se ingresó a “File > New Template”, se navegó hasta la sección de routers, se seleccionó “MikroTik CHR” y se hizo clic en “Install”. Luego, se agregó una nueva versión, especificando el disco de la imagen correspondiente. Posteriormente, se eligió la imagen correspondiente al router MikroTik buscándola en la ruta donde había sido guardada. Una vez encontrada, se seleccionó, se hizo clic en “Next” para continuar con el proceso de instalación y finalmente en “Finish”, como se muestra en las Figuras F4, Figura F5, Figura F6, Figura F7.

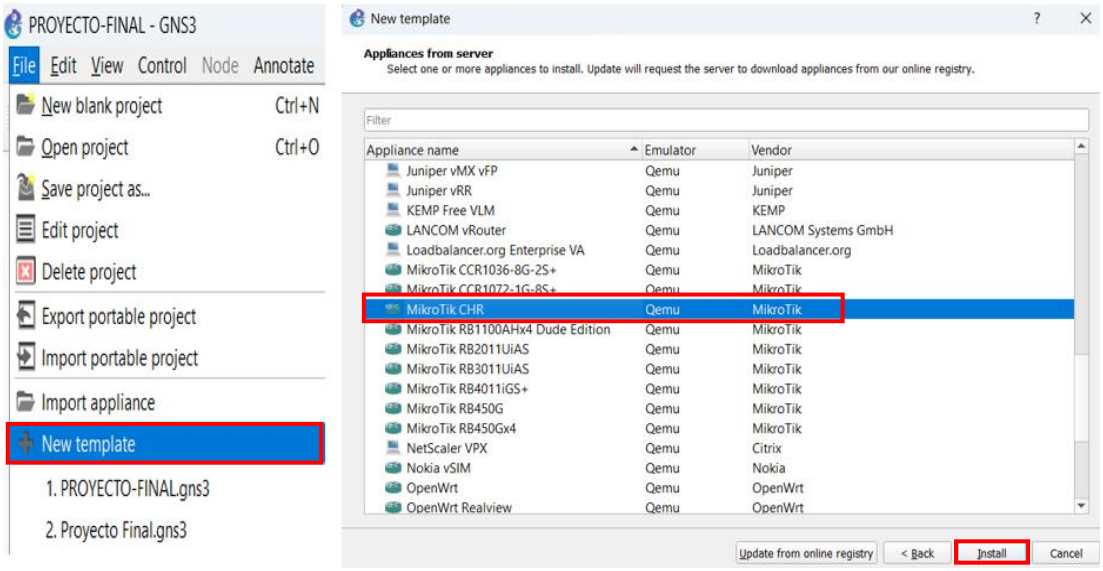


Figura F4. Creación de un nuevo template

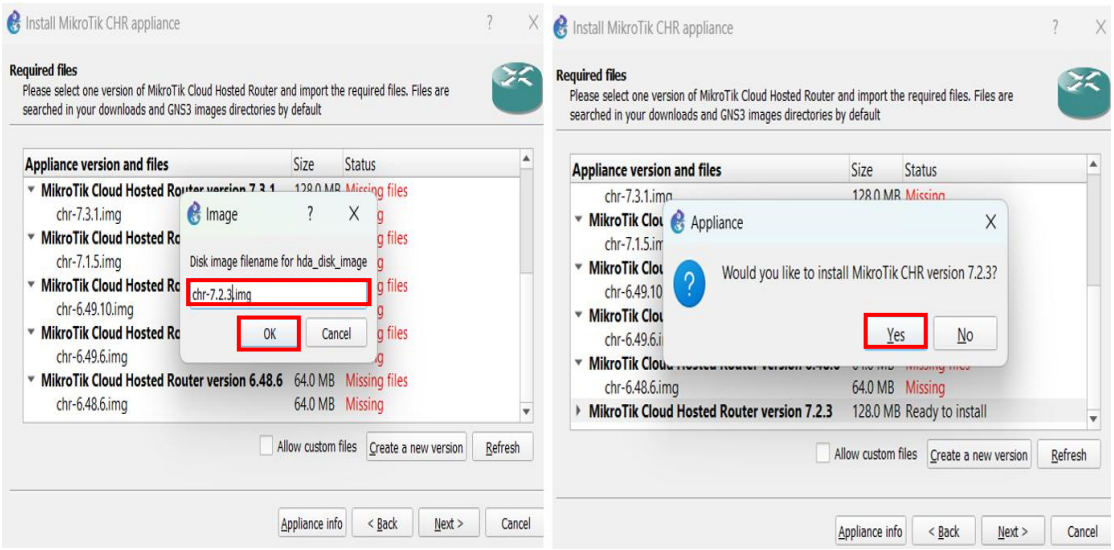


Figura F5. Asignación de nombre al archivo y agregación de la versión

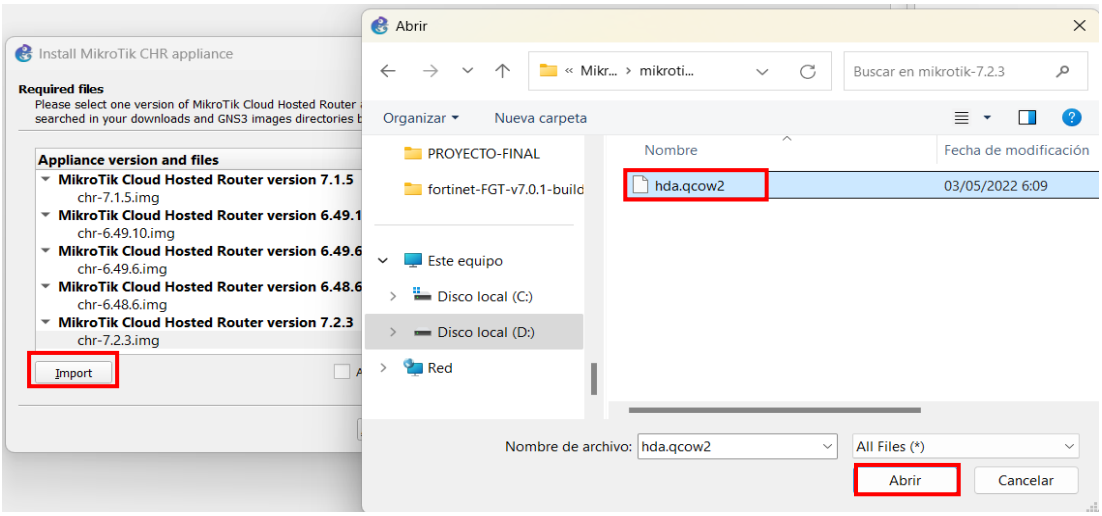


Figura F6. Importar la imagen desde su ruta correspondiente.

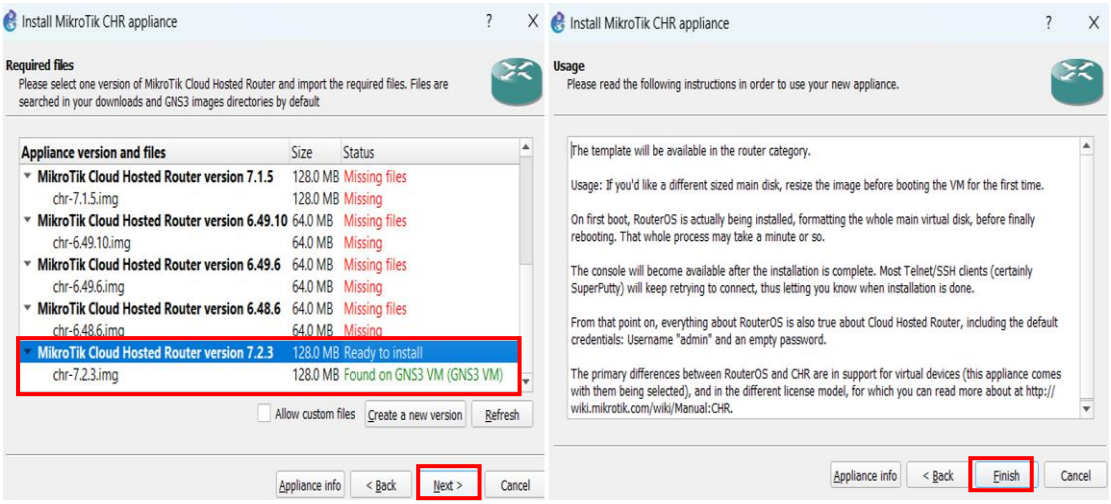


Figura F7. Instalación finalizada

Se utilizó un procedimiento similar para instalar el firewall FortiGate. Primero, se accedió a “Archivo > New Template” y, en la sección de firewalls, se seleccionó “FortiGate” para luego proceder con la opción “Instalar”. A continuación, se añadió una nueva versión especificando el disco correspondiente a la imagen del FortiGate. Posteriormente, se localizó la imagen en la ruta donde había sido almacenada, se seleccionó y se continuó el proceso haciendo clic en “Next”. Finalmente, se completó la instalación seleccionando “Finish”, como se muestra en las Figuras F8, Figura F9, Figura F10, Figura F11, Figura F12.

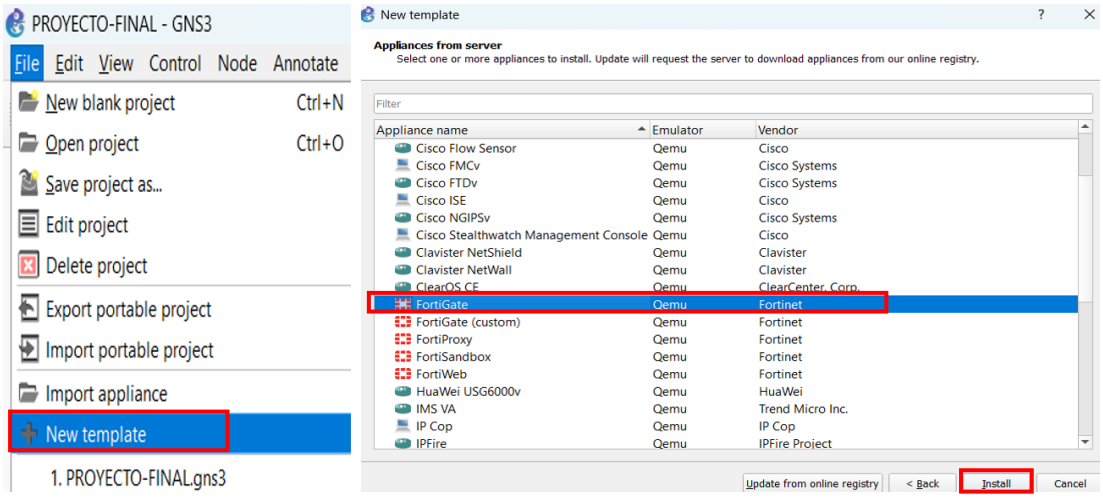


Figura F8. Creación de un nuevo template para el firewall

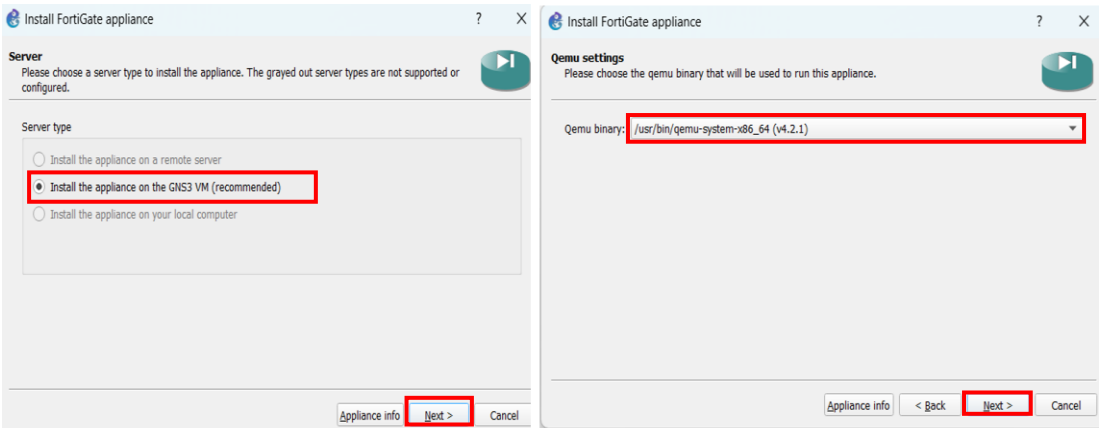


Figura F9. Elección del servidor y qemu

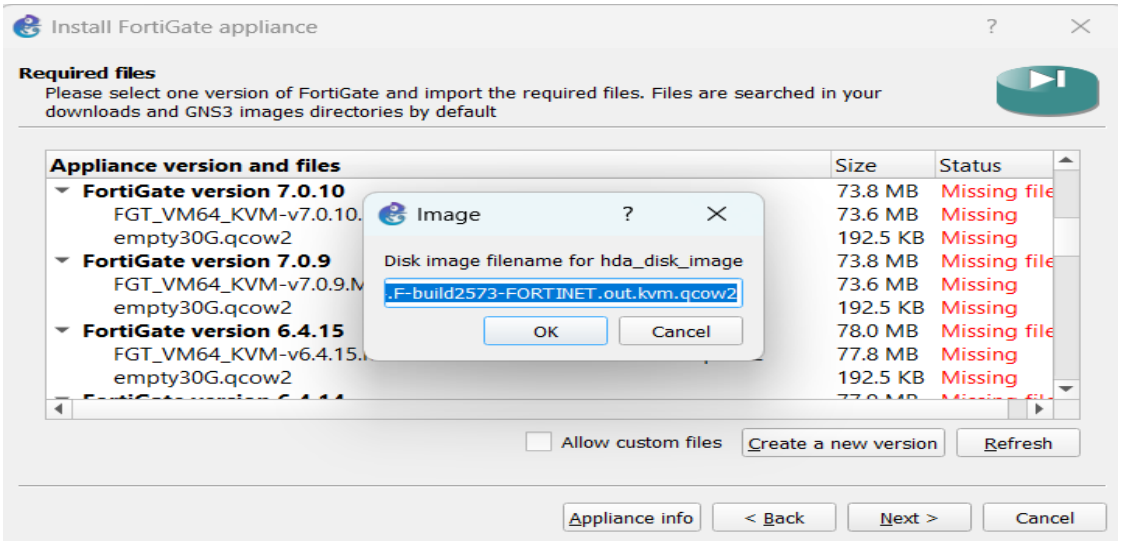


Figura F10. Asignación de un nombre de archivo al firewall

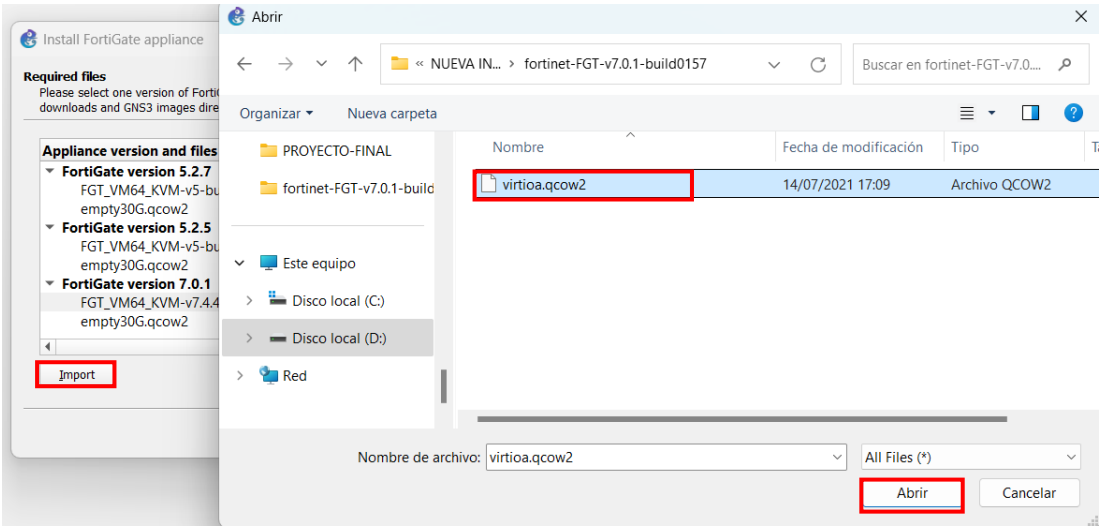


Figura F11. Importar la imagen desde su ruta correspondiente.

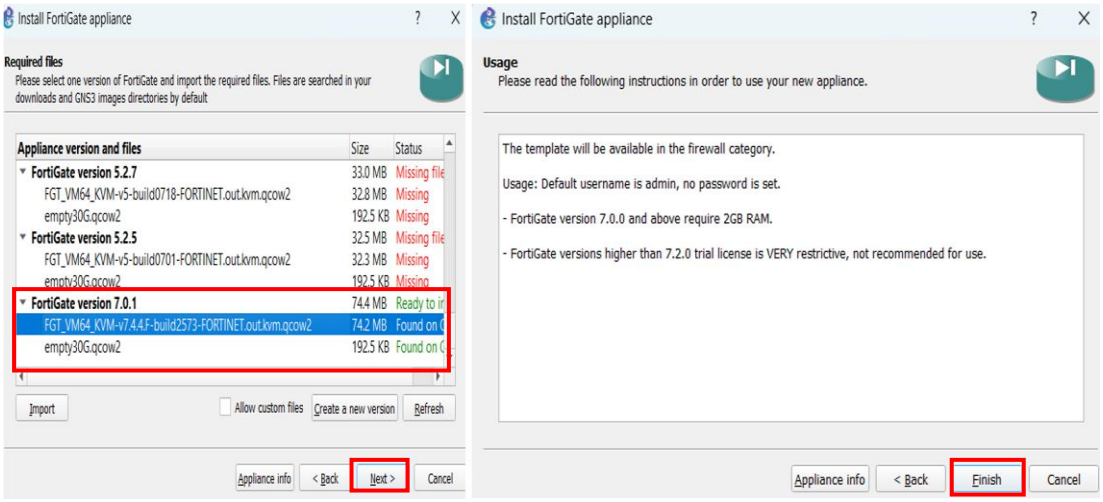


Figura F12. Instalación Finalizada

Después de completar la instalación de los equipos, se realiza una verificación de su configuración como se muestra en las Figura F13, Figura 14.

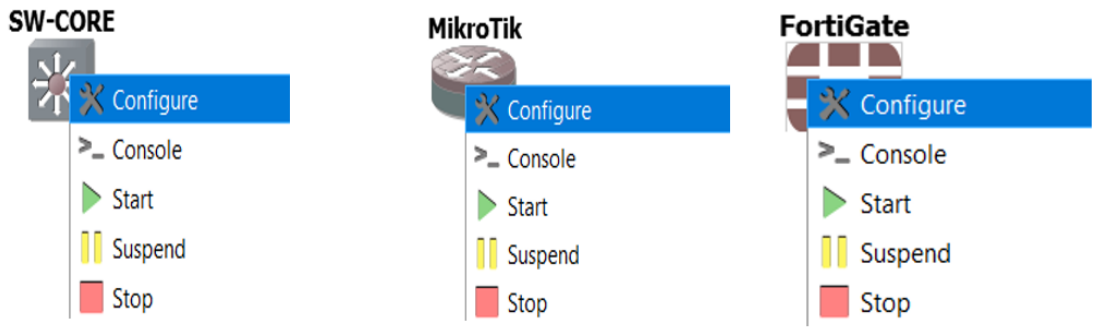


Figura F13. Configuración de los equipos

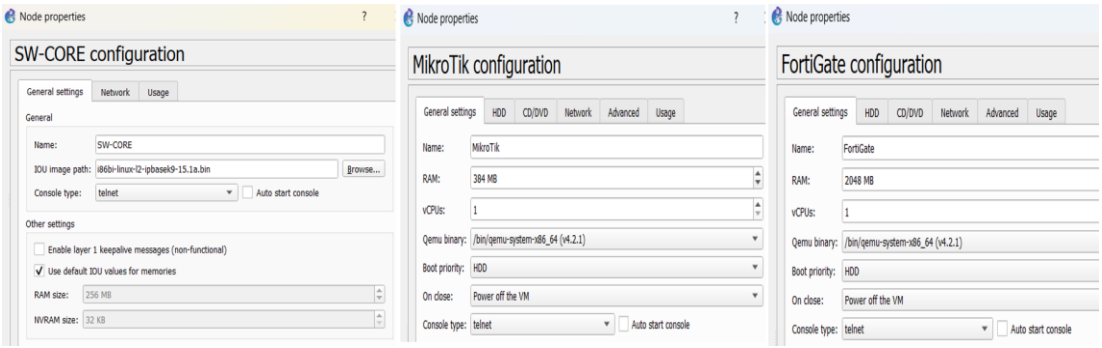


Figura F14. Verificación de configuración

En VMware, se procedió a instalar los sistemas operativos necesarios, incluyendo Windows 10 y Linux con Ubuntu. Figura F15

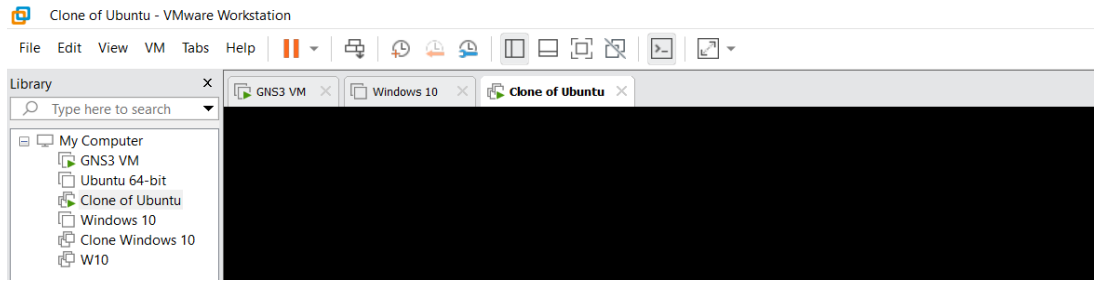


Figura F15. Instalación de máquinas virtuales en VMware

Para utilizar las máquinas virtuales en GNS3, es necesario ir a “Edit > Preferences”, seleccionar la sección de máquinas virtuales para VMware y luego hacer clic en “Next” como se muestra en la Figura F16 cabe mencionar que similar proceso se siguió para la utilización de las demás máquinas.

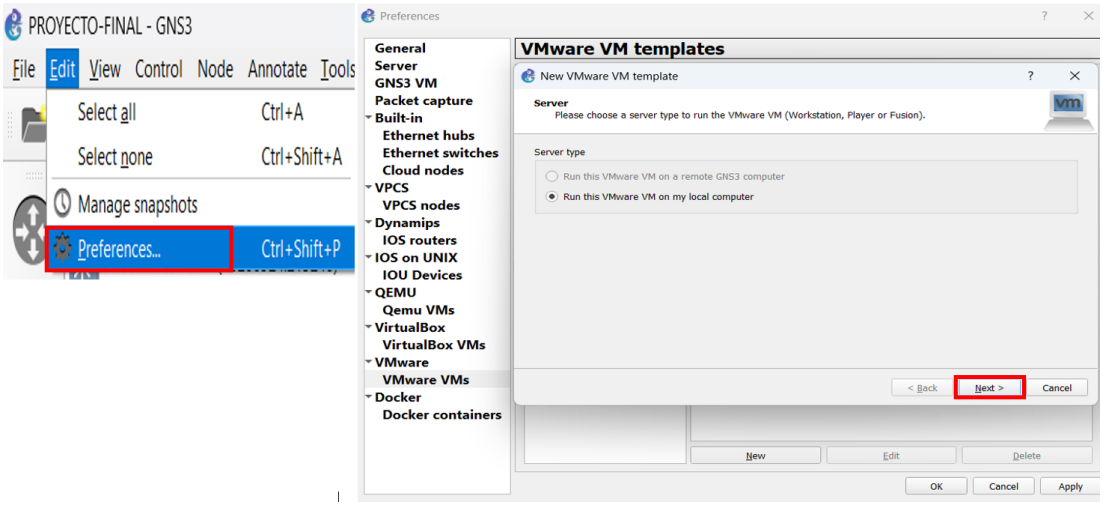


Figura F16. Añadir máquina virtual

A continuación, se selecciona la máquina virtual del listado y se completa el proceso haciendo clic en “Finish”.

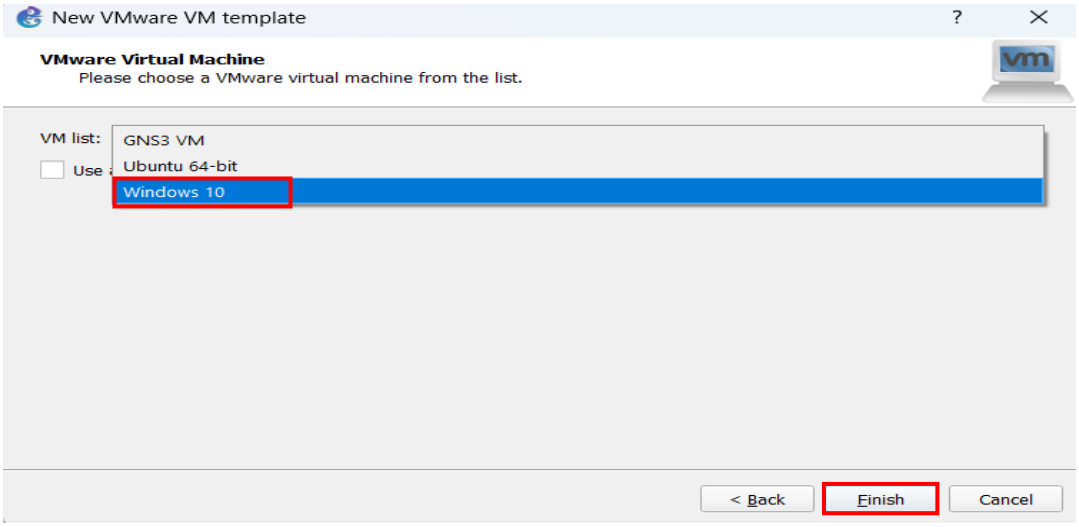


Figura F17. Listado de máquinas virtuales

Dirigirse a configuración y en red habilitar la casilla para asegurar que GNS3 pueda comunicarse de manera eficiente con la máquina virtual.

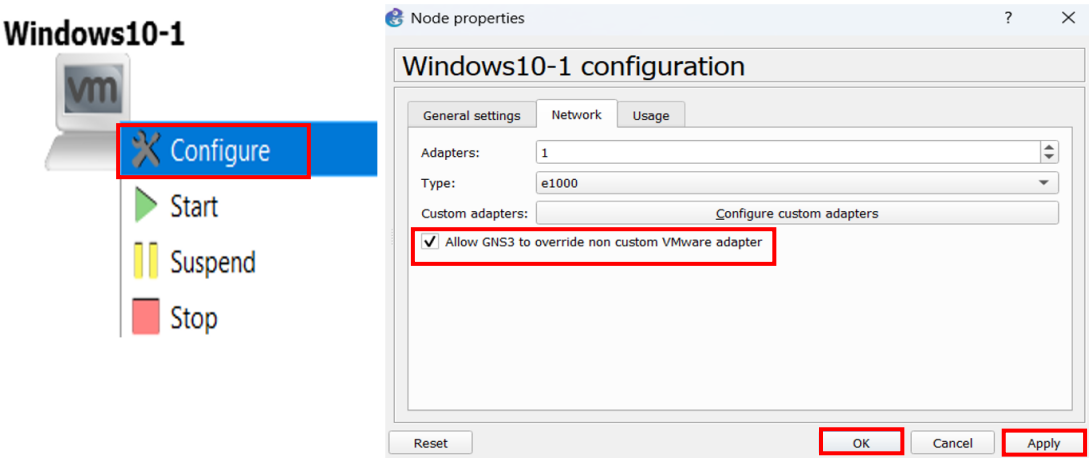


Figura F18. Configuración de un nodo

Después de instalar las imágenes de los equipos es necesario seleccionar aquellos que se utilizarán para la simulación Figura F19. Una vez elegidos, se procede a establecer las conexiones entre ellos como se aprecia en la Figura F20.

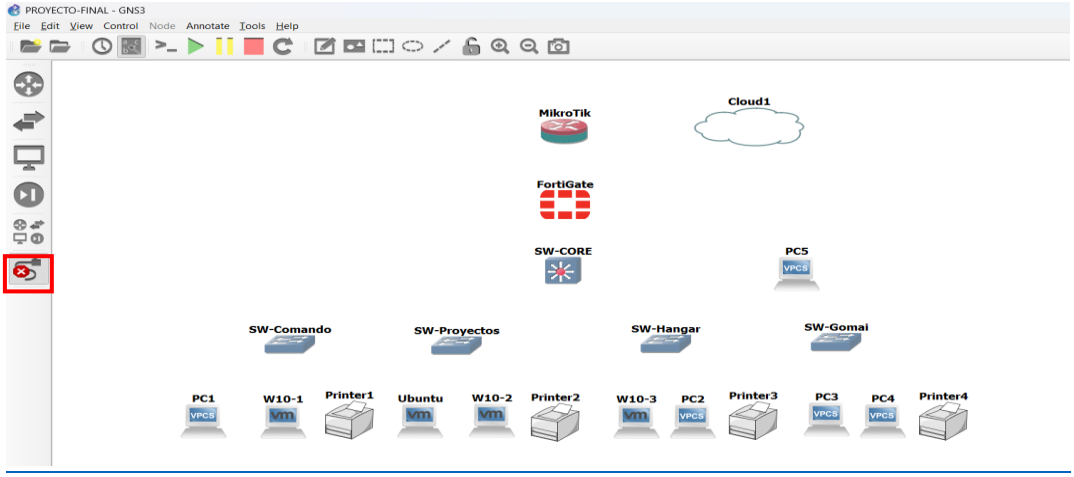


Figura F19. Equipos utilizados

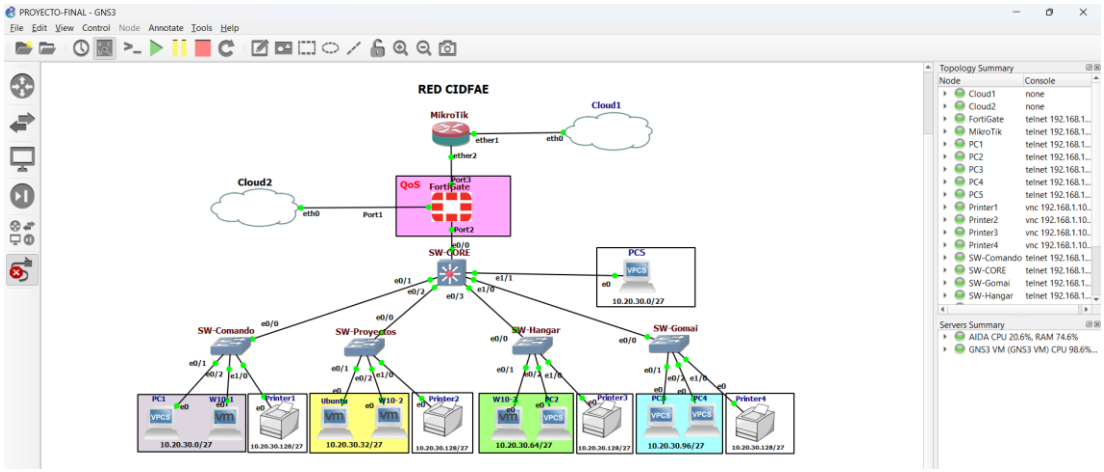


Figura F20. Establecimiento de conexiones