



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería Electrónica y Eléctrica

Escuela Profesional de Ingeniería Electrónica

**Diseño e implementación de monitoreo de conectividad
con Mikrotik y Zabbix entre DIRIS Lima Norte y
CSMC Samay**

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Ingeniero Electrónico

AUTOR

Luis Gabriel MORENO SOTELO

ASESOR

Jose VIDAL HUARCAYA

Lima, Perú

2026



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Moreno, L. (2026). *Diseño e implementación de monitoreo de conectividad con Mikrotik y Zabbix entre DIRIS Lima Norte y CSMC Samay*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería Electrónica y Eléctrica, Escuela Profesional de Ingeniería Electrónica]. Repositorio institucional Cybertesis UNMSM.

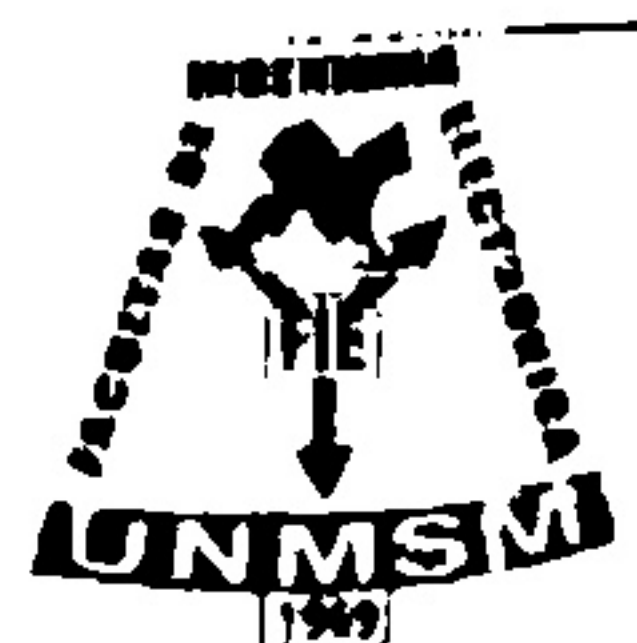
Metadatos complementarios

Datos de autor	
Nombres y apellidos	Luis Gabriel Moreno Sotelo
Tipo de documento de identidad	DNI
Número de documento de identidad	45077263
URL de ORCID	No Aplica
Datos de asesor	
Nombres y apellidos	Jose Vidal Huarcaya
Tipo de documento de identidad	DNI
Número de documento de identidad	09450859
URL de ORCID	https://orcid.org/0000-0002-7702-8162
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Jorge Elías Moscoso Sánchez
Tipo de documento	DNI
Número de documento de identidad	07206008
Miembro del jurado 1	
Nombres y apellidos	Wilbert Chavez Irazabal
Tipo de documento	DNI
Número de documento de identidad	08121733
Miembro del jurado 2	
Nombres y apellidos	Franklin Alfredo Cabezas Huerta
Tipo de documento	DNI
Número de documento de identidad	43809849
Datos de investigación	
Línea de investigación	Redes de datos (ODS 9: Industria, Innovación e Infraestructura)
Grupo de investigación	No Aplica

Agencia de financiamiento	No Aplica
Ubicación geográfica de la investigación	Edificio: Dirección de Redes Integradas de Salud Lima Norte País: Perú Departamento: Lima Provincia: Lima Distrito: Independencia Urbanización: Asociación Víctor Raúl Haya de la Torre Manzana y lote: Mz. 02, Lt. 03 Calle: Calle A Latitud: -11.9773437 Longitud: -77.0571246
Año o rango de años en que se realizó la investigación	2025 - 2026
URL de disciplinas OCDE	Ingeniería eléctrica, Ingeniería electrónica https://purl.org/pe-repo/ocde/ford#2.02.01 Ingeniería de sistemas y comunicaciones https://purl.org/pe-repo/ocde/ford#2.02.04 Telecomunicaciones https://purl.org/pe-repo/ocde/ford#2.02.05



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMÉRICA)
FACULTAD DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA
Teléfono 619-7000 Anexo 4226
Calle Germán Amezaga 375 – Lima 1 – Perú



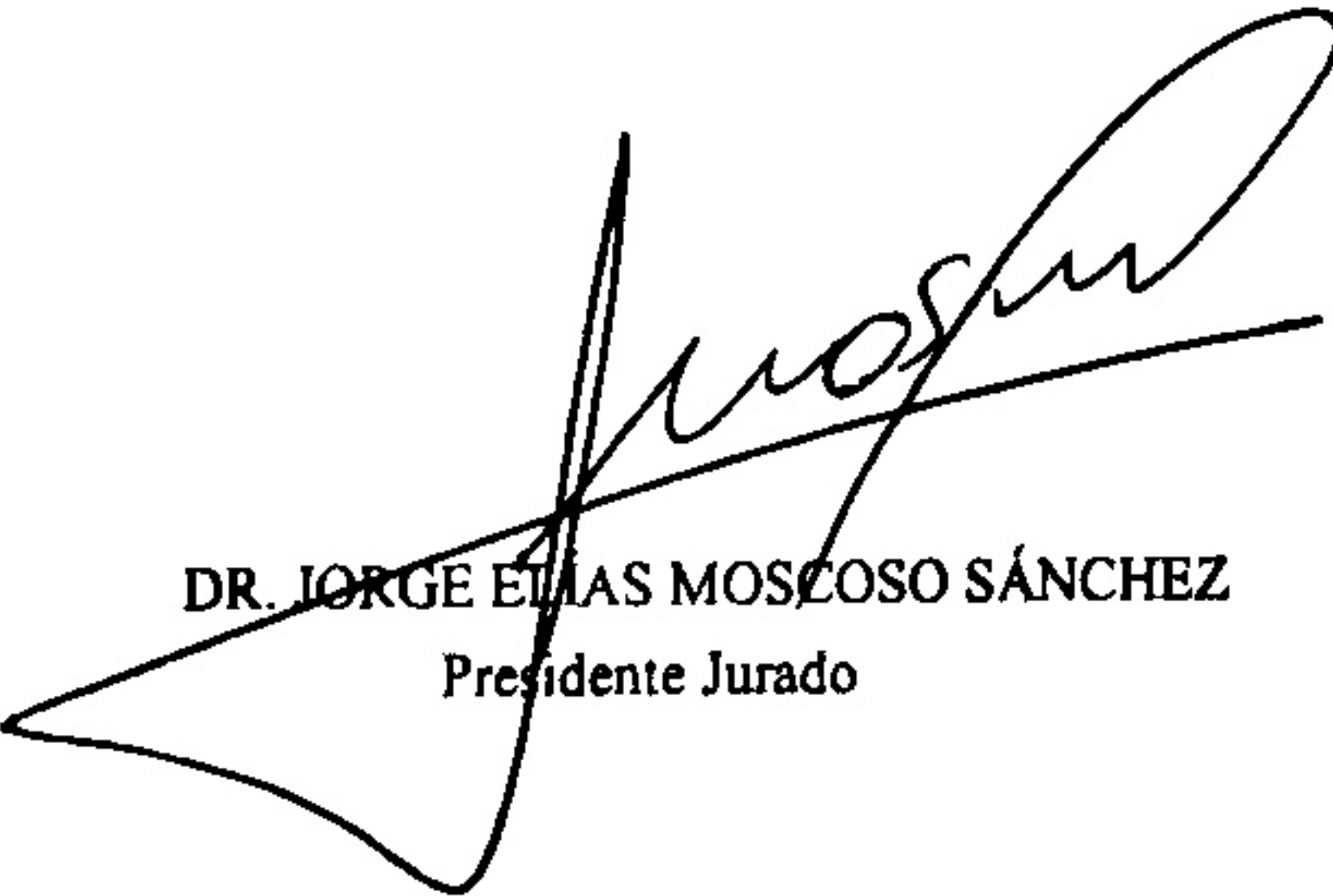
ACTA DE SUSTENTACIÓN
TRABAJO DE
SUFICIENCIA PROFESIONAL
ACTA N°44/FIEE-PPP/2026

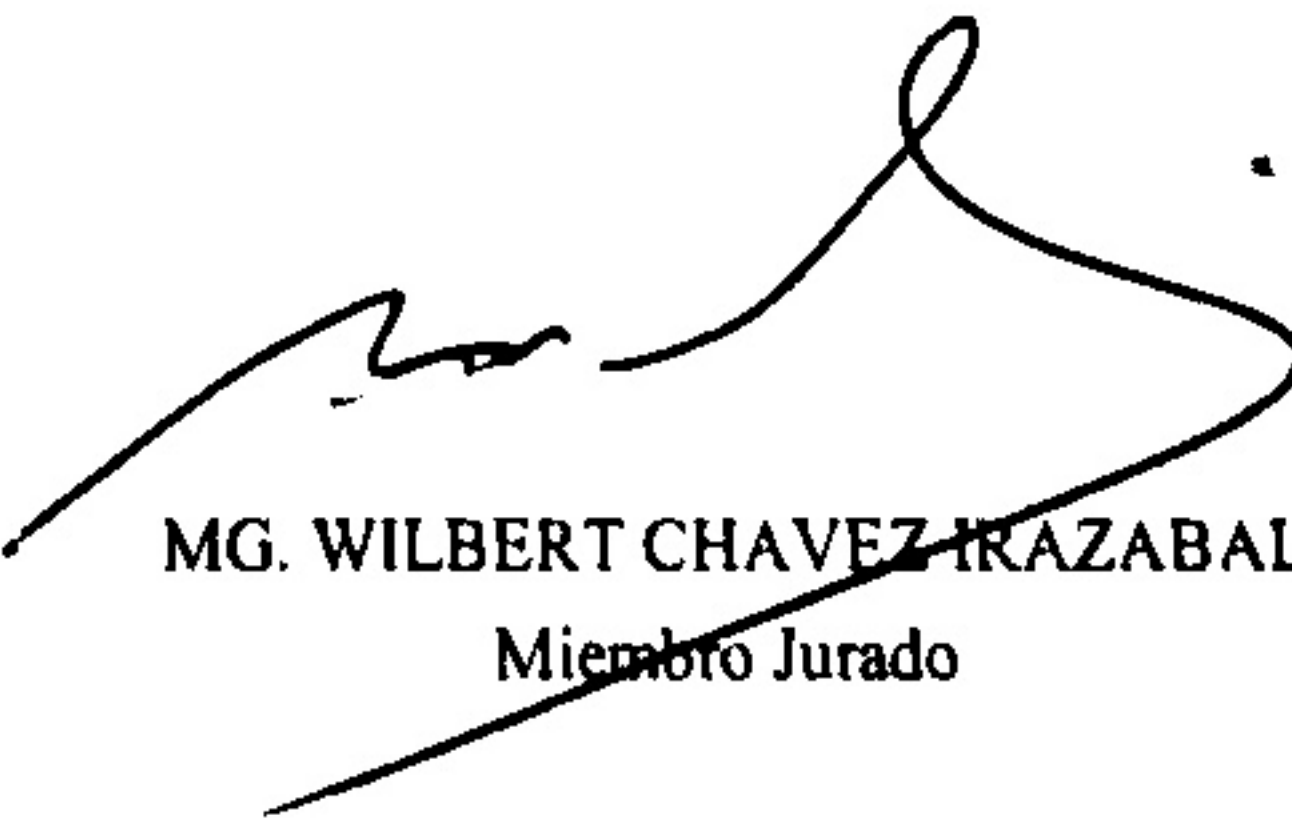
Los suscritos Miembros del Jurado, docentes permanentes de las Escuelas Profesionales de la Facultad de Ingeniería Electrónica y Eléctrica, reunidos en la fecha 26 de Junio del 2026, como presidente de Jurado el **DR. JORGE ELÍAS MOSCOSO SÁNCHEZ**, integrado por el Miembro de Jurado el **MG. WILBERT CHAVEZ IRAZABAL**, el Miembro de Jurado el **DR. FRANKLIN ALFREDO CABEZAS HUERTA** y Miembro Asesor el **ING. JOSE VIDAL HUARCAYA**.

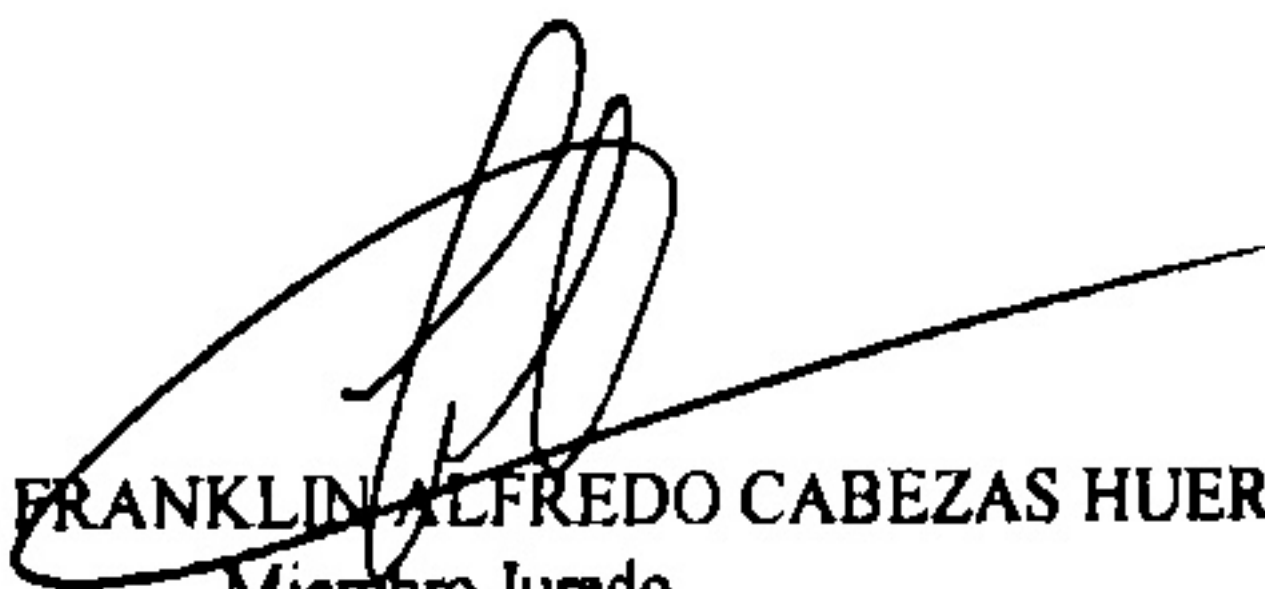
Después de escuchar la Sustentación Presencial del Trabajo de Suficiencia Profesional del Bachiller **LUIS GABRIEL MORENO SOTELO** con código 07190085 que para optar el Título Profesional de Ingeniero Electrónico sustentó el Trabajo de Suficiencia Profesional titulado **DISEÑO E IMPLEMENTACIÓN DE MONITOREO DE CONECTIVIDAD CON MIKROTIK Y ZABBIX ENTRE DIRIS LIMA NORTE Y CSMC SAMAY**.

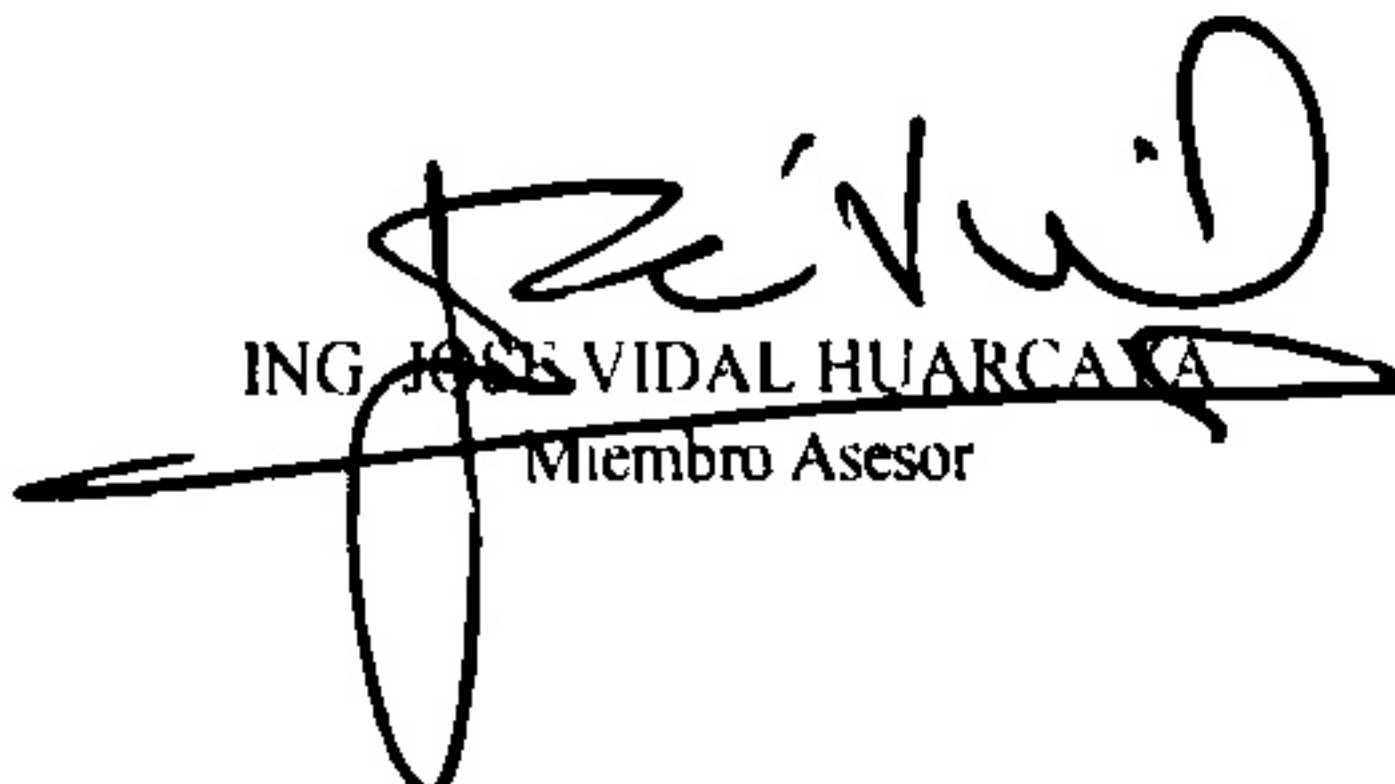
El jurado examinador procedió a formular las preguntas reglamentarias y, luego de una deliberación en privado, decidió otorgarle el calificativo de 15 (Buena).

Ciudad Universitaria, 26 de junio del 2026


DR. JORGE ELÍAS MOSCOSO SÁNCHEZ
Presidente Jurado


MG. WILBERT CHAVEZ IRAZABAL
Miembro Jurado


DR. FRANKLIN ALFREDO CABEZAS HUERTA
Miembro Jurado


ING. JOSE VIDAL HUARCAYA
Miembro Asesor



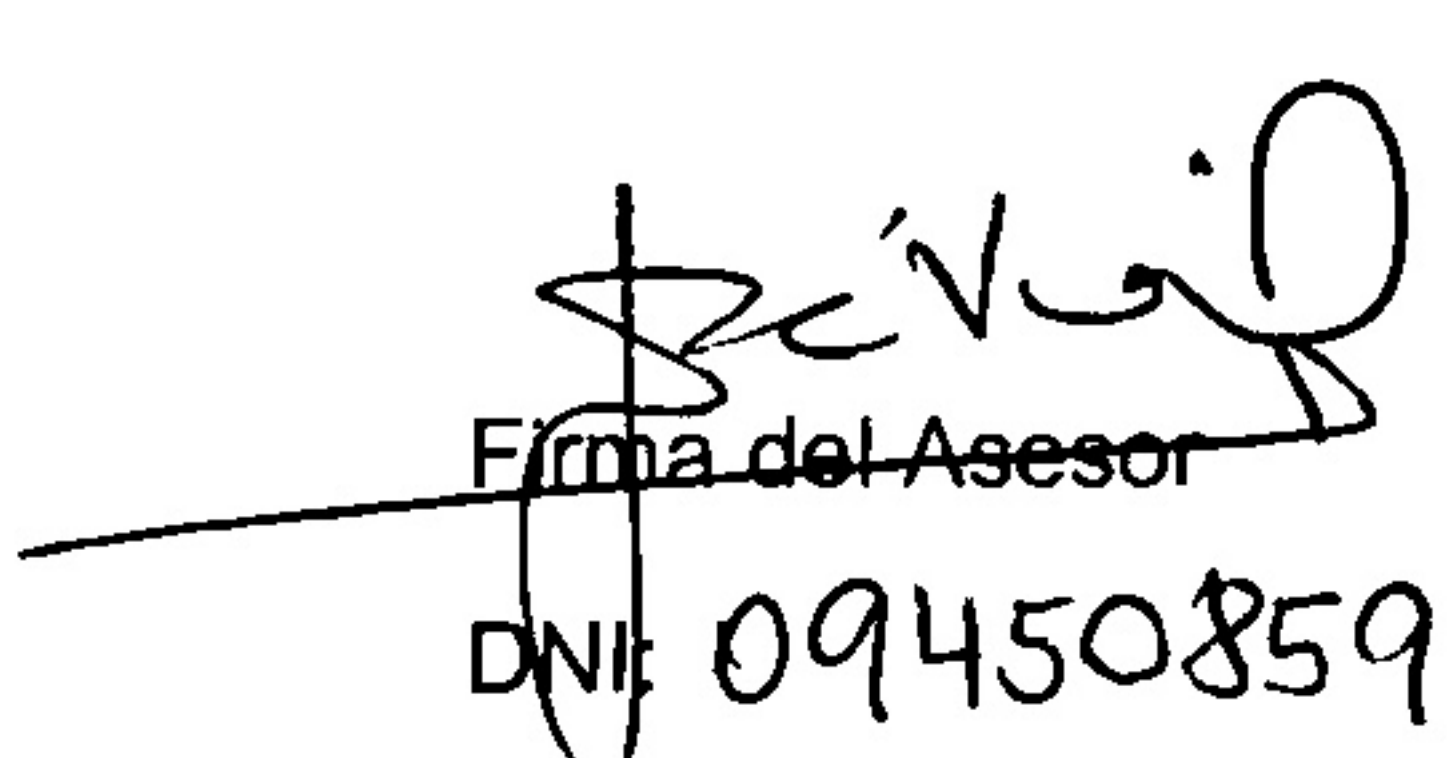
UNIVERSIDAD NACIONAL MAYOR DE
SAN MARCOS
Universidad del Perú, Decana de América

CERTIFICADO DE SIMILITUD

Yo, **JOSE VIDAL HUARCAYA** en mi condición de asesor acreditado con el Dictamen N°46/FIEE-PPP/2026 del Trabajo de Suficiencia Profesional titulado **DISEÑO E IMPLEMENTACIÓN DE MONITOREO DE CONECTIVIDAD CON MIKROTIK Y ZABBIX ENTRE DIRIS LIMA NORTE Y CSMC SAMAY**, presentado por el bachiller **LUIS GABRIEL MORENO SOTELO**, para optar el título profesional de Ingeniero Electrónico. CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante la plataforma PIDS, el documento evaluado cuenta con el 6% de similitud, nivel PERMITIDO para continuar con los trámites correspondientes y para su publicación en el repositorio institucional.

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del título profesional de Ingeniero Electrónico.

Lima, 26 de Junio del 2026


Firma del Asesor

DNI: 09450859

Nombres y apellidos del asesor:
JOSE VIDAL HUARCAYA

DEDICATORIA

Dedico este trabajo a mis padres, quienes siempre me han brindado su apoyo a lo largo de mi formación. Gracias por su esfuerzo constante, sus consejos y por los valores que me inculcaron desde pequeño, los cuales han sido fundamentales para seguir avanzando en mi vida personal y profesional. También les agradezco por la confianza que depositaron en mí y por motivarme a no rendirme en los momentos difíciles. Este logro es también de ustedes.

AGRADECIMIENTOS

Agradezco a la Universidad Nacional Mayor de San Marcos, en especial a la Facultad de Ingeniería Eléctrica y Electrónica, por brindarme la formación académica y profesional que me permitió llevar a cabo este trabajo. Asimismo, expreso mi agradecimiento a la Dirección de Redes Integradas de Salud Lima Norte, por darme la oportunidad de aplicar mis conocimientos en un entorno real y fortalecer mi experiencia profesional. De igual manera, agradezco a mis docentes por sus enseñanzas y orientación durante mi formación, así como a mis compañeros, con quienes compartí esta etapa académica. Finalmente, agradezco a mi asesor, José Vidal Huarcaya, por su orientación, apoyo y acompañamiento en el desarrollo del presente trabajo.

RESUMEN

El presente trabajo presenta el diseño e implementación de un sistema piloto para el monitoreo y acceso remoto de la red en el Centro de Salud Mental Comunitario Samay – Rímac, perteneciente a la Dirección de Redes Integradas de Salud Lima Norte. El objetivo principal fue mejorar la administración y continuidad del servicio de internet mediante una solución práctica y de bajo costo.

Para el desarrollo del proyecto se realizó la observación directa del funcionamiento de la red, revisión de información técnica y pruebas en el establecimiento. Como parte de la solución, se implementó un sistema de monitoreo utilizando Zabbix, además de la configuración de equipos MikroTik y una red privada virtual (VPN) mediante el protocolo WireGuard, permitiendo el acceso remoto y seguro a los dispositivos de red. Asimismo, se trabajó con dos proveedores de internet, utilizando GTD como enlace principal y Movistar como respaldo, configurando un cambio automático ante posibles fallas.

Durante las pruebas realizadas, se observó una mejora en el tiempo de atención de incidencias y en la continuidad del servicio. Finalmente, se concluye que la solución implementada puede aplicarse en otros establecimientos con características similares.

Palabras clave: monitoreo de red, gestión remota, VPN, WireGuard, Zabbix, MikroTik, redundancia.

ABSTRACT

This work presents the design and implementation of a pilot system for network monitoring and remote access at the Centro de Salud Mental Comunitario Samay – Rímac, belonging to the Dirección de Redes Integradas de Salud Lima Norte. The main objective was to improve the administration and continuity of the internet service through a practical and low-cost solution.

For the development of the project, direct observation of the network operation, review of technical information, and on-site testing were carried out. As part of the solution, a monitoring system using Zabbix was implemented, in addition to the configuration of MikroTik devices and a Virtual Private Network (VPN) through the WireGuard protocol, allowing secure remote access to network devices. Likewise, two internet providers were used, with GTD configured as the primary link and Movistar as the backup link, enabling automatic failover in case of service interruptions.

During the testing phase, improvements were observed in incident response time and service continuity. Finally, it is concluded that the implemented solution can be applied to other establishments with similar characteristics.

Keywords: network monitoring, remote management, VPN, WireGuard, Zabbix, MikroTik, redundancy.

INDICE GENERAL

RESUMEN	iv
ABSTRACT	v
TABLA DE CONTENIDO	vi
LISTA DE FIGURAS	ix
LISTA DE TABLAS	xii
CAPITULO I: INTRODUCCIÓN	1
1.1 Objetivo del informe	2
1.2 Estructura del informe	2
CAPITULO II: INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD	4
2.1 Institución – Actividad que desarrolla	4
2.2 Periodo de duración de la actividad.	6
2.3 Finalidad y objetivos de la entidad	7
2.4 Razón social	8
2.5 Dirección postal	8
2.6 Nombre y correo electrónico del profesional a cargo	9
CAPITULO III: DESCRIPCIÓN DE LA ACTIVIDAD	10
3.1 Organización de la actividad	10
3.2 Finalidad y objetivos de la Actividad	12
3.2.1 Finalidad	12
3.2.2 Objetivos	14
3.3 Problemática	15
3.3.1 Problema General	16
3.3.2 Problemas Específicos	16
3.3.3 Justificación e importancia de la investigación	17
3.4 Metodología	18
3.4.1 Bases teóricas	20

3.4.2	Marco conceptual	22
3.5	Procedimiento	24
3.5.1	Implementación del monitoreo con Zabbix	25
3.5.1.1	Situación inicial	25
3.5.1.2	Implementación	25
3.5.1.3	Pruebas realizadas	26
3.5.1.4	Resultado	28
3.5.2	Implementación de la VPN con Wireguard	28
3.5.2.1	Situación inicial	28
3.5.2.2	Descripción de la implementación	29
3.5.2.3	Pruebas realizadas	31
3.5.2.4	Resultado de la implementación	32
3.5.3	Implementación del mecanismo de conmutación automática (failover) en el router Mikrotik	33
3.5.3.1	Situación inicial	33
3.5.3.2	Implementación del mecanismo de failover	34
3.5.3.3	Pruebas realizadas	35
3.5.3.4	Resultados obtenidos	36
3.5.4	Evaluación de la solución implementada	37
3.5.4.1	Situación de evaluación	37
3.5.4.2	Pruebas de validación de la solución	38
3.5.4.3	Resultados de la evaluación	41
3.5.4.4	Resultado final de la evaluación	42
3.6	Resultado de la actividad	42
3.6.1	Resultados del monitoreo centralizado con Zabbix	43
3.6.2	Resultados de la conectividad mediante VPN WireGuard	44
3.6.3	Resultados del mecanismo de conmutación automática (failover)	45
3.6.4	Comparación de indicadores antes y después de la implementación	46
3.6.5	Impacto operativo de la solución implementada	47
3.6.6	Evaluación general de los resultados	47

CAPITULO IV: DISCUSION DE RESULTADOS	49
4.1 Descripción de la implementación	49
4.1.1 Discusión del objetivo de monitoreo con Zabbix	49
4.1.2 Discusión del objetivo de la VPN con Wireguard	50
4.1.3 Discusión del objetivo relacionado al failover en Mikrotik	50
4.1.4 Discusión del impacto en la disponibilidad del servicio	51
4.1.5 Discusión general de la solución implementada	52
4.1.6 Conclusión de la discusión	52
4.2 Evaluación Económica	53
CAPITULO V: CONCLUSIONES	55
CAPITULO VI: RECOMENDACIONES	58
6.1 Recomendaciones técnicas	58
6.2 Recomendaciones de continuidad del servicio	59
6.3 Recomendaciones de continuidad del servicio	59
6.4 Recomendaciones de escalabilidad e integración	59
CAPITULO VII: BIBLIOGRAFÍA	60
CAPITULO IX: ANEXOS	62

LISTA DE FIGURAS

Figura 1 Mapa de Lima Norte	5
Figura 2 Organigrama general de la DIRIS Lima Norte	11
Figura 3 Arquitectura de monitoreo y gestión remota de la conectividad	13
Figura 4 Panel de monitoreo en Zabbix mostrando el estado del router MikroTik del establecimiento del Rímac	26
Figura 5 Panel de alertas generado por el sistema Zabbix ante eventos de conectividad	27
Figura 6 Tráfico de red en la interfaz WireGuard del router MikroTik	27
Figura 7 Configuración de la interfaz WireGuard en el servidor VPN	30
Figura 8 Configuración de la interfaz WireGuard en el router MikroTik del establecimiento del Rímac	30
Figura 9 Pruebas de conectividad mediante comando ping entre la sede central y el establecimiento del Rímac	31
Figura 10 Estado de la conexión VPN y verificación de handshake en el servidor WireGuard.	32
Figura 11 Arquitectura de conectividad sin mecanismo de failover en el establecimiento de salud	33
Figura 12 Prueba de conectividad con enlace GTD activo	35
Figura 13 Validación del failover con conmutación automática hacia Movistar	36
Figura 14 Ruta de desplazamiento del personal técnico desde la DIRIS Lima Norte (Independencia) hacia el Centro de Salud Mental Comunitario Samay (Rímac).	38
Figura 15 Prueba de conectividad entre sede central y red del establecimiento mediante VPN WireGuard	39
Figura 16 Panel de monitoreo de Zabbix mostrando el estado del router del establecimiento	40

Figura 17 Prueba de conmutación automática de enlaces (failover) en el router MikroTik	40
Figura 18 Panel de monitoreo en Zabbix mostrando el estado del router MikroTik del establecimiento	43
Figura 19 Pruebas de conectividad mediante VPN entre sede central y establecimiento	44
Figura 20 Prueba de caída del enlace GTD y conmutación automática a Movistar	45
Figura A1 Arquitectura de red de la VPN implementada	63
Figura B1 Archivo de configuración del servidor VPN	64
Figura C1 Listado de peers en el servidor WireGuard	65
Figura D1 Configuración de WireGuard en el router MikroTik	66
Figura E1 Cliente VPN en la PC de monitoreo	68
Figura E2 Prueba de conectividad hacia el servidor VPN	68
Figura F1 Pruebas de conectividad mediante ping	69
Figura G1 Tráfico de red en la interfaz LAN del router MikroTik	70
Figura G2 Tráfico de red en la interfaz GTD del router MikroTik	70
Figura G3 Tráfico de red en la interfaz Movistar del router MikroTik	71
Figura G4 Tráfico de red en la interfaz WireGuard del router MikroTik	71
Figura G5 Uso de memoria del router MikroTik en Zabbix	72
Figura G6 Panel de alertas en Zabbix	72
Figura H1 Precio referencial del router MikroTik RB750Gr3	73
Figura H2 Plan de servidor VPS utilizado en la implementación	74
Figura I1 Reglas de firewall implementadas en MikroTik	75
Figura J1 Flujo de monitoreo mediante VPN	76
Figura K1 Sistema SIHCE – Registro de pacientes	78
Figura K2 Sistema de referencias médicas	78
Figura K3 Sistema HISMINSA – Registro estadístico	79
Figura K4 Sistema ARFSIS Web – Validación de seguros	79
Figura K5 Sistema de Gestión Documentario	80
Figura K6 Sistema DIGEMID – Módulo de farmacia	80
Figura K7 Correo institucional Zimbra	81
Figura L1 Verificación del estado de la VPN mediante comando wg	83

Figura M1 Estado de peers y handshake en el servidor WireGuard	84
Figura P1 Evidencia de conexión activa mediante handshake en WireGuard	87
Figura Q1 Panel de alertas en Zabbix	88
Figura R1 Diagrama de la red LAN del establecimiento (192.168.50.0/24)	89
Figura T1 Archivo de configuración wg0.conf del servidor Zabbix	92
Figura U1 Conexión remota al router MikroTik mediante Winbox a través de la VPN	93
Figura U2 Acceso al entorno de administración del router MikroTik del Rímac	93

LISTA DE TABLAS

Cuadro 1 Asignación de direcciones IP en la red VPN	29
Cuadro 2 Resultados de pruebas de conectividad en la VPN	31
Cuadro 3 Comparación del funcionamiento del acceso a Internet antes y después del failover	34
Cuadro 4 Impacto de la implementación del mecanismo de failover en la disponibilidad del servicio	37
Cuadro 5 Comparación del comportamiento de la red antes y después de la implementación	41
Cuadro 6 Comparación del desempeño de la red antes y después de la implementación	46
Cuadro 7 Costos de implementación de la solución	54
Cuadro C1 Clientes registrados en el servidor VPN	65
Cuadro F1 Resultados de pruebas de conectividad	69
Cuadro H1 Costos de implementación	73
Cuadro L1 Acciones de contingencia	84
Cuadro N1 Esquema de direccionamiento IP	85
Cuadro N2 Redes utilizadas	85
Cuadro O1 Cronograma de implementación	86

CAPÍTULO I: INTRODUCCIÓN

En los últimos años, el uso de tecnologías de la información en el sector salud se ha vuelto cada vez más importante, ya que muchos procesos dependen directamente de los sistemas informáticos. Actividades como el registro de historias clínicas, la validación de seguros o la referencia de pacientes requieren una conexión a Internet estable para funcionar correctamente.

En el caso de la Dirección de Redes Integradas de Salud Lima Norte (DIRIS Lima Norte), a través de la Oficina de Gestión de Tecnologías de la Información (OGTI), se tiene la responsabilidad de mantener operativa la infraestructura tecnológica en los distintos establecimientos de salud. Sin embargo, en la práctica, no siempre es posible supervisar o administrar de forma remota todos los equipos de red, sobre todo en centros que se encuentran alejados o que tienen limitaciones en su conectividad.

Uno de los principales inconvenientes identificados es que, ante una falla de Internet o de red, muchas veces es necesario que el personal técnico se traslade hasta el establecimiento para realizar el diagnóstico o la solución. Esto genera demoras que pueden afectar el uso de los sistemas y, en consecuencia, la atención a los pacientes. Además, la falta de monitoreo continuo dificulta detectar a tiempo problemas en los enlaces de Internet, especialmente cuando se cuenta con más de un proveedor, como es el caso de GTD y Movistar.

Frente a esta situación, en el presente trabajo se propone implementar una solución basada en una red privada virtual (VPN) utilizando el protocolo WireGuard. Esta solución permite interconectar de manera segura la sede de

monitoreo, un servidor en la nube y el router MikroTik del Centro de Salud Mental Comunitario Samay, ubicado en el distrito del Rímac, sin necesidad de contar con direcciones IP públicas ni realizar configuraciones complejas.

Asimismo, se incorpora la herramienta Zabbix como plataforma de monitoreo, lo que permite visualizar el estado de los enlaces de Internet y de los dispositivos de red en tiempo real. De esta manera, es posible detectar fallas de manera más rápida y generar alertas automáticas, mejorando la capacidad de respuesta ante incidencias.

1.1 Objetivo del Informe

El objetivo del presente informe es describir el diseño y la implementación de una solución de conectividad segura y monitoreo remoto aplicada al Centro de Salud Mental Comunitario Samay, perteneciente a la DIRIS Lima Norte. Con esta propuesta se busca mejorar la supervisión de la red, facilitar la detección de fallas y reducir los tiempos de atención, evitando en muchos casos la necesidad de desplazamiento del personal técnico.

1.2 Estructura del Informe

El presente informe está organizado de la siguiente manera:

Capítulo I: Introducción. Se presenta el contexto general del trabajo, el objetivo del informe y la estructura del documento.

Capítulo II: Información del lugar donde se desarrolló la actividad. Se describe la institución DIRIS Lima Norte, así como el entorno donde se llevó a cabo el proyecto.

Capítulo III: Descripción de la actividad. Se desarrollan los aspectos técnicos del trabajo, incluyendo la problemática identificada, la metodología aplicada, el procedimiento de implementación y los resultados obtenidos.

Capítulo IV: Discusión de resultados. Se analizan los resultados obtenidos, contrastándolos con los objetivos planteados y evaluando su impacto técnico y operativo.

Capítulo V: Conclusiones. Se presentan las conclusiones del trabajo en función de los objetivos establecidos.

Capítulo VI: Recomendaciones. Se plantean recomendaciones técnicas, operativas y estratégicas para la mejora y replicabilidad de la solución.

Capítulo VII: Referencias. Se incluyen las fuentes bibliográficas utilizadas en el desarrollo del trabajo.

Capítulo VIII: Anexos. Se presentan las capturas de pantalla y evidencias obtenidas durante la implementación, las cuales permiten visualizar los resultados de conectividad, acceso remoto y monitoreo de la red.

CAPITULO II: INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD

2.1 Institución – Actividad que desarrolla

La Dirección de Redes Integradas de Salud Lima Norte (DIRIS Lima Norte) es una entidad perteneciente al Ministerio de Salud encargada de la gestión, supervisión y organización de los servicios de salud en los establecimientos ubicados en la zona norte de Lima Metropolitana.

Esta institución administra una red de centros de salud, puestos de salud y establecimientos especializados distribuidos en diferentes distritos, lo que implica un manejo constante de recursos humanos, logísticos y tecnológicos. Debido a esta distribución geográfica, la conectividad de red y los sistemas informáticos cumplen un rol importante para el desarrollo de las actividades asistenciales y administrativas.

En la Figura 1 se muestra el ámbito territorial correspondiente a Lima Norte, donde se ubican los establecimientos que forman parte de la DIRIS Lima Norte, incluyendo los distritos de Ancón, Carabaylo, Comas, Independencia, Los Olivos, Puente Piedra, San Martín de Porres, Santa Rosa y Rímac.

En el área tecnológica, la Oficina de Gestión de Tecnologías de la Información (OGTI) es la encargada de administrar la infraestructura informática institucional. Dentro de sus funciones se incluyen la gestión de la conectividad de red, la configuración de equipos como routers y switches, la administración de servidores y el soporte técnico a los diferentes establecimientos.

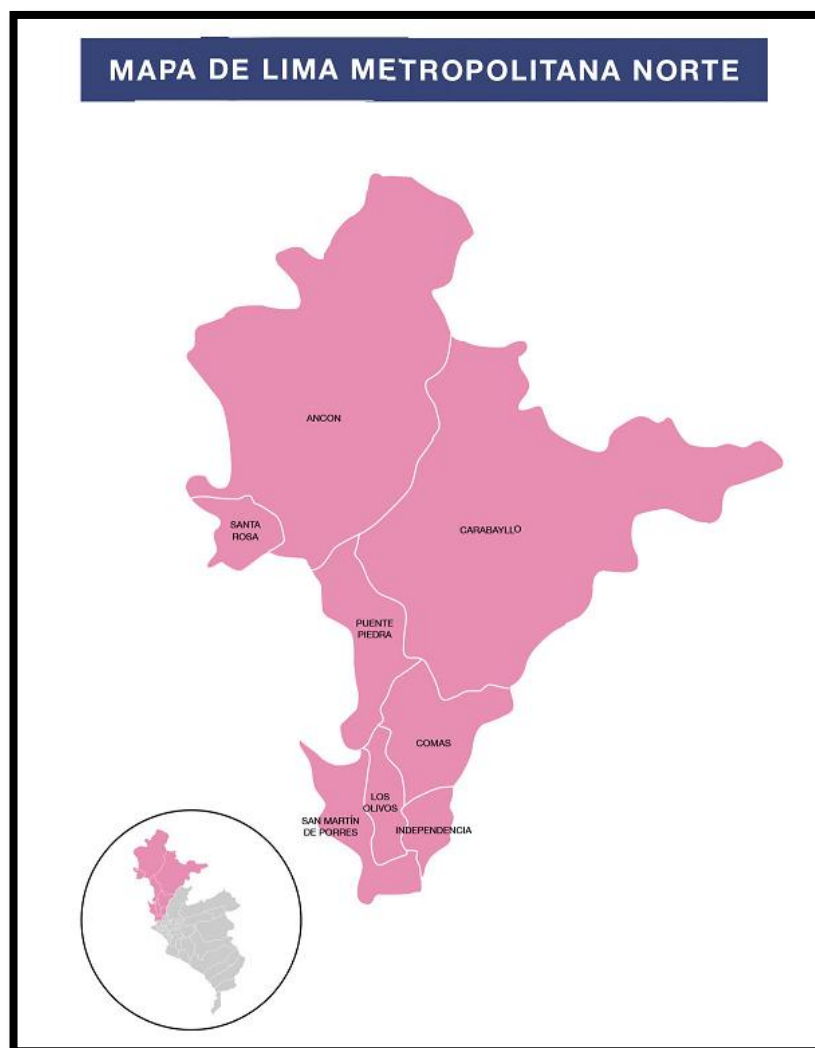


Figura 1 Mapa de Lima Norte. Fuente. Dirección de Redes Integradas de Salud Lima Norte (DIRIS Lima Norte)

En la práctica, gran parte de los servicios de salud dependen del uso de sistemas informáticos conectados a Internet. Por ejemplo, el registro de atenciones médicas, la validación de aseguramiento de pacientes y el uso de plataformas institucionales requieren una conexión estable. Cuando la conectividad presenta fallas, estos procesos se ven afectados, generando retrasos en la atención.

Uno de los principales problemas identificados es la dificultad para supervisar en tiempo real el estado de la red en todos los establecimientos, ya que muchos de ellos se encuentran distribuidos en distintas zonas. En varios casos, las fallas de conectividad son detectadas recién cuando el personal del

establecimiento reporta el problema, lo que genera demoras en la atención de incidencias.

Debido a esta situación, surge la necesidad de implementar soluciones que permitan mejorar el monitoreo de la red y facilitar la gestión remota de los equipos, reduciendo la dependencia de visitas presenciales del personal técnico. En ese contexto, se desarrolló el piloto en el Centro de Salud Mental Comunitario Samay, con el fin de evaluar una solución que permita mejorar la gestión de la conectividad y que pueda ser replicada en otros establecimientos.

2.2 Periodo de duración de la actividad

El desarrollo del presente trabajo se llevó a cabo durante los meses de agosto y septiembre de 2025, periodo en el cual se desarrollaron las actividades relacionadas con el diseño, implementación y validación de una solución de conectividad, ejecutada en modalidad piloto en el Centro de Salud Mental Comunitario Samay. Asimismo, el monitoreo se realiza de forma remota desde la sede principal de la DIRIS Lima Norte, ubicada en el distrito de Independencia.

En una primera etapa, se realizó la revisión de la infraestructura de red existente en el establecimiento, identificando la forma en que estaba configurada la conectividad, los equipos disponibles y las principales limitaciones en la gestión de la red.

Posteriormente, se procedió al diseño de la solución, en la cual se definió el uso de un router MikroTik para la gestión de red, un servidor de monitoreo Zabbix y la implementación de una red privada virtual (VPN) utilizando el protocolo WireGuard, con el objetivo de permitir el acceso remoto seguro.

La fase de implementación técnica se realizó los días 8 y 9 de septiembre de 2025, durante los cuales se llevaron a cabo las configuraciones necesarias en

el servidor VPN, el router MikroTik y el sistema de monitoreo. Asimismo, se realizaron pruebas de conectividad para verificar la comunicación entre los diferentes componentes.

Luego de la implementación, el sistema quedó en funcionamiento para realizar el monitoreo continuo de la red, lo que permitió observar su comportamiento en condiciones reales y evaluar la efectividad de la solución frente a problemas de conectividad.

Finalmente, los resultados obtenidos durante este periodo sirvieron como base para el análisis, conclusiones y evaluación de la viabilidad de replicar la solución en otros establecimientos de la DIRIS Lima Norte.

2.3 Finalidad y objetivos de la entidad

La Dirección de Redes Integradas de Salud Lima Norte tiene como finalidad asegurar que los establecimientos de salud de su jurisdicción brinden una atención adecuada a la población, lo cual implica no solo la disponibilidad de personal de salud, sino también el correcto funcionamiento de los sistemas tecnológicos que apoyan la atención.

Para cumplir con esta finalidad, la institución gestiona una red de establecimientos distribuidos en varios distritos, lo que requiere una adecuada coordinación de recursos y una infraestructura tecnológica que permita el funcionamiento continuo de los servicios.

En este contexto, la conectividad de red es un elemento fundamental, ya que permite el acceso a sistemas informáticos utilizados en la atención de los pacientes, así como la comunicación entre los diferentes establecimientos y la sede central.

Actualmente, los establecimientos cuentan con enlaces de Internet proporcionados por operadores como GTD y Movistar, los cuales permiten el

acceso a plataformas institucionales y servicios en línea. Sin embargo, cuando se presentan fallas de conectividad, la atención puede verse afectada si no se cuenta con mecanismos adecuados de supervisión y respuesta.

Por ello, la institución busca implementar mejoras en la gestión de su infraestructura tecnológica, incorporando soluciones que permitan monitorear la red, detectar problemas de manera oportuna y reducir los tiempos de atención ante incidencias.

El trabajo desarrollado en el Centro de Salud Mental Comunitario Samay se encuentra alineado con estos objetivos, ya que propone una solución basada en monitoreo y acceso remoto que permite mejorar la gestión de la conectividad, optimizar la atención de fallas y reducir la necesidad de desplazamiento del personal técnico.

2.4 Razón social

Dirección de Redes Integradas de Salud Lima Norte – DIRIS Lima Norte (MINSA)

2.5 Dirección postal

El piloto de monitoreo y gestión remota de la conectividad se implementó en el Centro de Salud Mental Comunitario Samay, establecimiento perteneciente a la Dirección de Redes Integradas de Salud Lima Norte (DIRIS Lima Norte).

El establecimiento se encuentra ubicado en la siguiente dirección:

Calle Virreyes N.º 205, sector El Manzano, distrito del Rímac, Lima – Perú.

Asimismo, la sede administrativa de la Dirección de Redes Integradas de Salud Lima Norte (DIRIS Lima Norte) se encuentra ubicada en:

Av. Túpac Amaru N.º 2245, distrito de Independencia, Lima – Perú.

2.6 Nombre y correo electrónico del profesional a cargo

Jaime Wilder Segura Santisteban – Jefe de Infraestructura de la Oficina de Gestión de Tecnologías de la Información (OGTI).

jaime.segura@dirisln.gob.pe

CAPITULO III: DESCRIPCIÓN DE LA ACTIVIDAD

3.1 Organización de la Actividad

La actividad desarrollada en el presente trabajo consistió en la implementación de una prueba piloto orientada al monitoreo y la gestión remota de la conectividad en el Centro de Salud Mental Comunitario Samay, perteneciente a la DIRIS Lima Norte.

Esta implementación se realizó únicamente en dicho establecimiento, con el fin de comprobar el funcionamiento de la solución en un entorno real. Los resultados obtenidos permitirán evaluar su posible aplicación en otros establecimientos de salud en una etapa posterior.

Para llevar a cabo esta actividad, fue necesaria la participación de diferentes áreas vinculadas a la gestión tecnológica y al funcionamiento del establecimiento de salud.

Por parte de la DIRIS Lima Norte, la Oficina de Gestión de Tecnologías de la Información (OGTI) cumple un rol importante, ya que es el área encargada de administrar la infraestructura tecnológica institucional. Dentro de sus funciones se incluyen la gestión de la conectividad de red, la configuración de equipos, la administración de servidores y el soporte técnico a los establecimientos.

En el caso del Centro de Salud Mental Comunitario Samay, ubicado en el distrito del Rímac, se brindaron las facilidades necesarias para la ejecución

del piloto, permitiendo realizar las configuraciones, pruebas y validaciones del sistema implementado.

Durante el desarrollo del trabajo, la coordinación se realizó principalmente con el área de tecnologías de la información de la DIRIS Lima Norte, desde donde se planificó, diseñó e implementó la solución. Asimismo, el personal del establecimiento apoyó en las pruebas de conectividad y en la verificación del funcionamiento del sistema.

La actividad se desarrolló de manera progresiva, iniciando con la evaluación de la situación actual del establecimiento, seguida del diseño de la solución, su implementación y finalmente la validación de resultados en un entorno real.

En la Figura 2 se muestra el organigrama general de la DIRIS Lima Norte

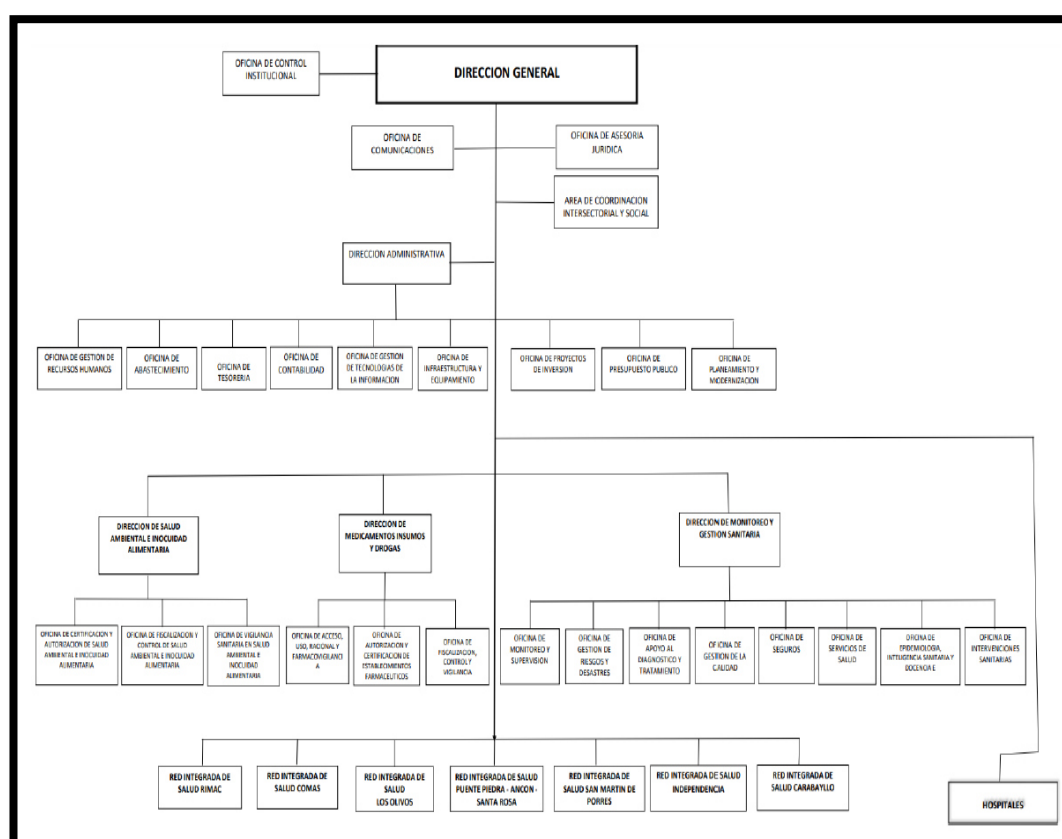


Figura 2 Organigrama general de la DIRIS Lima Norte. Fuente. Dirección de Redes Integradas de Salud Lima Norte (DIRIS Lima Norte).

3.2 Finalidad y objetivos de la Actividad

3.2.1 Finalidad

La finalidad de la presente actividad es implementar y validar un piloto que permita mejorar la gestión de la conectividad en el Centro de Salud Mental Comunitario Samay.

En la situación actual, cuando ocurre una falla en la red, muchas veces esta es detectada únicamente cuando el personal del establecimiento reporta la incidencia. Asimismo, la atención de estos problemas suele requerir la intervención del personal técnico, lo que puede generar retrasos en la identificación y solución de las fallas.

Frente a esta situación, la propuesta busca incorporar herramientas que permitan supervisar el estado de la red en tiempo real y acceder de manera remota a los equipos de comunicación, reduciendo la necesidad de desplazamientos y facilitando las labores de soporte técnico.

Para ello, se implementó una solución que integra el monitoreo mediante Zabbix, el acceso remoto a través de una VPN con WireGuard y un mecanismo de failover en el router MikroTik, el cual permite realizar el cambio automático entre los enlaces de Internet disponibles cuando se presenta una interrupción del servicio principal.

Esta solución permite detectar fallas de conectividad de forma más rápida, mantener la continuidad del servicio ante caídas del enlace principal y facilitar las tareas de administración y soporte desde la sede central.

Finalmente, la actividad busca demostrar que este tipo de implementación es viable y que puede aplicarse en otros establecimientos de salud con características similares, contribuyendo a mejorar la gestión de la infraestructura de red y la disponibilidad de los servicios informáticos.

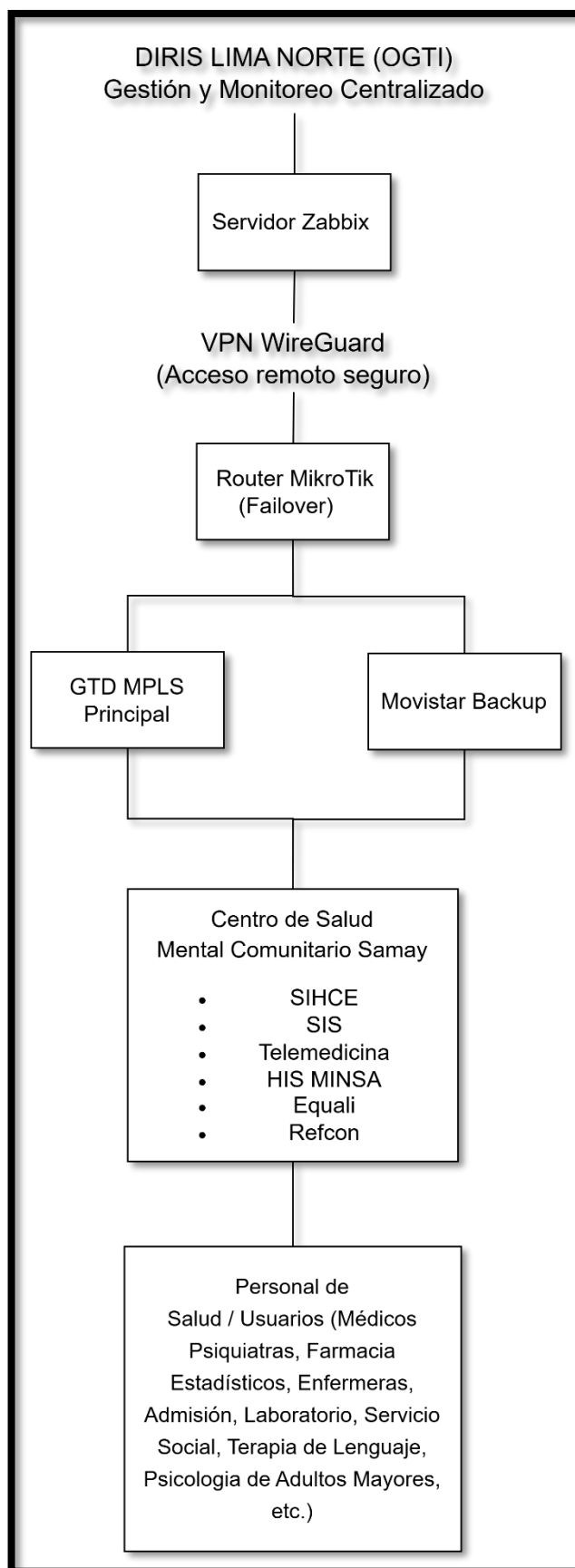


Figura 3 Arquitectura de monitoreo y gestión remota de la conectividad.
Fuente. Elaboración propia.

3.2.2 Objetivos

Implementar, en modalidad piloto, una solución de monitoreo y gestión remota de la conectividad en el Centro de Salud Mental Comunitario Samay, integrando Zabbix, VPN con WireGuard y failover en MikroTik, para la supervisión desde la sede central, con posibilidad de aplicación en otros establecimientos de la DIRIS Lima Norte.

Como objetivos específicos, se plantean los siguientes:

- Implementar una plataforma de monitoreo utilizando Zabbix para supervisar el estado de la conectividad del establecimiento, permitiendo identificar interrupciones, pérdidas de comunicación y otros eventos asociados a la red mediante la generación de alertas automáticas.
- Implementar una red privada virtual (VPN) mediante el protocolo WireGuard que permita la interconexión segura entre el servidor de monitoreo, el router MikroTik del establecimiento y el punto de administración, facilitando el acceso remoto a los dispositivos de red.
- Configurar un mecanismo de conmutación automática (failover) en el router MikroTik entre los enlaces de Internet disponibles, considerando a GTD como enlace principal y a Movistar como enlace de respaldo, permitiendo el cambio automático de ruta ante fallas del servicio principal.
- Evaluar el desempeño de la solución implementada verificando el funcionamiento del monitoreo, la conectividad mediante VPN y la conmutación automática de enlaces, así como determinar su contribución en la mejora de la gestión de la conectividad y la atención de incidencias desde la sede central y la continuidad de los servicios que dependen de la red informática del establecimiento.

3.3 Problemática

Actualmente, los establecimientos de salud dependen en gran medida del uso de sistemas informáticos para el desarrollo de sus actividades. En el caso del Centro de Salud Mental Comunitario Samay, estos sistemas son utilizados para el registro de atenciones, validación de seguros y otros procesos administrativos.

El funcionamiento de estos sistemas depende directamente de la conectividad a Internet. Cuando el servicio presenta fallas, se generan problemas en la atención, retrasos en el registro de información y dificultades en la gestión interna.

En el establecimiento se cuenta con dos enlaces de Internet: uno proporcionado por GTD y otro por Movistar. Sin embargo, a pesar de tener dos proveedores, no se disponía de un mecanismo que permita cambiar automáticamente entre ellos en caso de falla.

En la práctica, cuando el enlace principal dejaba de funcionar, era necesario realizar el cambio de forma manual, lo que implicaba que el personal técnico se trasladara al establecimiento. Este proceso podía tomar entre 60 y 90 minutos, dependiendo del tráfico y la distancia.

Además, no se contaba con herramientas que permitan monitorear la red en tiempo real. Esto hacía que muchas veces los problemas se detectaran cuando el personal del establecimiento reportaba la falla, lo que retrasaba la atención de incidencias.

Otro punto importante es que no existía acceso remoto a los equipos de red. Esto obligaba a realizar intervenciones presenciales incluso para tareas básicas como verificar el estado del router o reiniciar servicios, incrementando el tiempo de respuesta ante fallas y dificultando la atención oportuna de las incidencias de conectividad reportadas por el personal del establecimiento.

Estas limitaciones evidencian la necesidad de implementar una solución que permita mejorar la gestión de la conectividad, reducir los tiempos de atención y facilitar el monitoreo de la red desde la sede central.

3.3.1 Problema General

¿Cómo implementar, en modalidad piloto, una solución de monitoreo y gestión remota de la conectividad en el Centro de Salud Mental Comunitario Samay, integrando Zabbix, VPN con WireGuard y failover en MikroTik, para la supervisión desde la sede central, con posibilidad de aplicación en otros establecimientos de la DIRIS Lima Norte?

3.3.2 Problemas Específicos

1. ¿Cómo implementar una plataforma de monitoreo utilizando Zabbix para supervisar el estado de la conectividad del establecimiento, permitiendo identificar interrupciones, pérdidas de comunicación y eventos asociados a la red mediante la generación de alertas automáticas?
2. ¿Cómo implementar una red privada virtual (VPN) mediante el protocolo WireGuard que permita la interconexión segura entre el servidor de monitoreo, el router MikroTik del establecimiento y el punto de administración, facilitando el acceso remoto a los dispositivos de red?
3. ¿Cómo configurar un mecanismo de conmutación automática (failover) en el router MikroTik entre los enlaces de Internet disponibles, considerando a GTD como enlace principal y a Movistar como enlace de respaldo, para asegurar el cambio automático de ruta ante fallas del servicio principal y mantener la continuidad de la conectividad del establecimiento?

4. ¿Cómo evaluar el desempeño de la solución implementada verificando el funcionamiento del monitoreo, la conectividad mediante VPN y la conmutación automática de enlaces?

3.3.3 Justificación e importancia de la investigación

La DIRIS Lima Norte administra una gran cantidad de establecimientos de salud distribuidos en distintos distritos, lo que hace que la gestión de la conectividad sea un reto constante.

En muchos casos, estos establecimientos dependen de Internet para poder utilizar los sistemas informáticos necesarios en la atención de los pacientes. Por ello, cualquier interrupción en la conectividad afecta directamente el funcionamiento del servicio.

En el caso del Centro de Salud Mental Comunitario Samay, si bien se cuenta con dos enlaces de Internet, no existe un mecanismo automático que permita mantener la continuidad del servicio ante fallas. Esto genera interrupciones que pueden afectar tanto la atención médica como los procesos administrativos.

Además, la falta de monitoreo en tiempo real y de acceso remoto dificulta la gestión de la red, ya que el personal técnico debe trasladarse físicamente para resolver incidencias.

Ante esta situación, se plantea la implementación de una solución que combine monitoreo de red, acceso remoto y conmutación automática de enlaces, utilizando herramientas como Zabbix, WireGuard y Mikrotik.

La importancia de este trabajo radica en que propone una solución práctica, de bajo costo y aplicable a otros establecimientos con características similares. Asimismo, permite mejorar los tiempos de respuesta ante fallas,

optimizar la gestión de la red y reducir la necesidad de intervenciones presenciales.

Desde el punto de vista profesional, este trabajo también permite aplicar conocimientos de redes en un entorno real, lo que contribuye al desarrollo de soluciones orientadas a necesidades concretas del sector salud.

3.4 Metodología

La metodología utilizada en el presente Trabajo de Suficiencia Profesional tiene un enfoque aplicado, ya que busca dar solución a un problema real relacionado con la conectividad de red en un establecimiento de salud. Asimismo, presenta un componente práctico, debido a que la solución propuesta fue implementada y probada en un entorno real, permitiendo observar su funcionamiento en condiciones operativas.

El objetivo de esta metodología es evaluar una alternativa que permita mejorar el monitoreo, la gestión remota y la continuidad del servicio de conectividad en el Centro de Salud Mental Comunitario Samay, perteneciente a la Dirección de Redes Integradas de Salud Lima Norte.

El trabajo se desarrolló en etapas, con la finalidad de organizar de manera clara el proceso desde el análisis inicial hasta la validación de la solución implementada.

En una primera etapa se realizó el diagnóstico de la situación actual del establecimiento. Para ello, se revisó la infraestructura de red existente, identificando los equipos utilizados, los enlaces de Internet disponibles y la forma en que se atendían las incidencias. Como resultado, se observó que el establecimiento contaba con dos enlaces de Internet (GTD y Movistar), pero no existía un mecanismo automático que permitiera el cambio entre ellos en caso de falla. Además, no se disponía de herramientas de monitoreo en tiempo real ni de acceso remoto seguro desde la sede central.

En la segunda etapa se planteó el diseño de la solución. Se propuso utilizar un router MikroTik como equipo principal para la gestión de la red, implementar una red privada virtual (VPN) mediante el protocolo WireGuard para permitir el acceso remoto seguro, y utilizar la herramienta Zabbix para el monitoreo centralizado de la conectividad. Esta arquitectura fue planteada considerando su bajo costo, facilidad de implementación y posibilidad de replicarse en otros establecimientos.

En la tercera etapa se realizó la implementación del piloto. Se configuró el router MikroTik del establecimiento, definiendo las interfaces y estableciendo un esquema de failover entre los enlaces de Internet. Paralelamente, se implementó un servidor en la nube (VPS) donde se configuró la VPN con WireGuard, permitiendo la interconexión entre el establecimiento, el servidor de monitoreo y el equipo de administración.

Posteriormente, se integraron todos los componentes de la solución, logrando el acceso remoto al router del establecimiento y la supervisión de la conectividad mediante Zabbix.

En la etapa de pruebas, se realizaron diferentes validaciones para comprobar el funcionamiento del sistema. Estas incluyeron pruebas de conectividad entre los equipos, acceso remoto mediante la VPN y monitoreo del estado de los enlaces. Asimismo, se simuló la caída del enlace principal para verificar el funcionamiento del failover y el cambio automático al enlace de respaldo.

Finalmente, en la etapa de evaluación, se analizaron los resultados obtenidos durante las pruebas, observando el comportamiento del sistema ante fallas de conectividad, el tiempo de respuesta y la facilidad de acceso remoto. Esto permitió concluir que la solución implementada es funcional y puede ser considerada para su aplicación en otros establecimientos de la DIRIS Lima Norte, ya que durante las pruebas demostró un funcionamiento adecuado y permitió gestionar de manera más eficiente las incidencias relacionadas con la conectividad.

3.4.1 Bases teóricas

Las bases teóricas del presente trabajo se sustentaron en diversas investigaciones relacionadas con la implementación de redes de datos, el uso de tecnología MikroTik para la gestión de conectividad y balanceo de carga, así como la aplicación de sistemas de monitoreo de infraestructura de red. Estos estudios evidenciaron mejoras en la disponibilidad, estabilidad y administración del servicio de Internet en distintos entornos institucionales, especialmente en organizaciones donde la conectividad resulta crítica para el desarrollo de sus actividades.

a) Implementación de redes con tecnología MikroTik

Gonzales Rondan (2015) desarrolló una investigación de tipo cuantitativo, no experimental y descriptivo, en la que analizó la viabilidad de implementar un servicio de Internet inalámbrico mediante tecnología MikroTik en la ciudad de Recuay.

El estudio se realizó con una muestra de 341 pobladores, a quienes se les aplicó una encuesta para evaluar la aceptación del servicio y las condiciones del mercado local. Los resultados evidenciaron que el 100% de los encuestados manifestó disposición a contratar el servicio siempre que el costo fuera adecuado. Asimismo, se identificó que más del 50% de la población pertenecía a niveles socioeconómicos A, B y C, lo que representó un mercado potencial atractivo para la implementación.

Por otro lado, se observó que la población presentaba insatisfacción con la calidad del servicio de Internet existente y percibía los precios como poco accesibles. En base a estos resultados, el autor concluyó que existía viabilidad técnica y económica para la implementación del servicio, determinando además que la tecnología MikroTik permitió gestionar de manera eficiente redes de acceso en escenarios reales.

b) Balanceo de carga en redes con MikroTik

Muñoz López (2017) implementó una solución de balanceo de carga de Internet utilizando tecnología MikroTik en la Dirección de Red de Salud Conchucos Sur – Huari, bajo una arquitectura cliente–servidor.

El estudio tuvo como finalidad mejorar la administración del servicio de Internet mediante la distribución del tráfico entre varios enlaces disponibles. Los resultados obtenidos evidenciaron una mejora en la continuidad del servicio, reduciendo la saturación de la red y disminuyendo las interrupciones de conectividad.

Asimismo, se logró una distribución más eficiente del ancho de banda, permitiendo optimizar el uso de los recursos de red entre los usuarios institucionales. En conclusión, el estudio determinó que la implementación del balanceo de carga contribuyó directamente a mejorar la disponibilidad y estabilidad del servicio de Internet en la institución.

c) Balanceo de carga en instituciones públicas

Huane Solórzano (2020) realizó un estudio en la Dirección Regional de Transportes y Comunicaciones de Áncash con el objetivo de evaluar la calidad del servicio de Internet y la necesidad de implementar una solución de balanceo de carga con tecnología MikroTik.

Los resultados del estudio mostraron que el 86.96% de los trabajadores no se encontraba satisfecho con el servicio de Internet debido a problemas de estabilidad y calidad. Asimismo, el 95.65% de los encuestados consideró necesaria la implementación de una solución de balanceo de carga para mejorar la conectividad institucional.

A partir de estos resultados, se evidenció la existencia de deficiencias en la gestión del servicio de red. En conclusión, el autor determinó que la

implementación de MikroTik permitió mejorar la continuidad del servicio y optimizar el uso del ancho de banda, generando una mejor experiencia para los usuarios.

d) Sistemas de monitoreo de redes

Castro González (2020) implementó un sistema de monitoreo en la nube mediante la integración de herramientas como Zabbix, Grafana y Zammad, desplegadas sobre contenedores Docker en un entorno Linux.

El objetivo del proyecto fue integrar estas herramientas para lograr una supervisión centralizada de la infraestructura de red, permitiendo la visualización de métricas, generación de alertas y gestión de incidencias mediante tickets.

Los resultados demostraron que la integración de estas tecnologías permitió mejorar la capacidad de monitoreo de los sistemas, logrando una detección más rápida de fallas y una mejor gestión de eventos en tiempo real. Asimismo, se evidenció una mejora en los tiempos de respuesta ante incidentes, lo que permitió optimizar la administración de los servicios de red.

3.4.2 Marco conceptual

El marco conceptual del presente trabajo reúne los principales conceptos relacionados con la gestión de redes, la continuidad del servicio y la seguridad en la comunicación de datos, los cuales permiten comprender el funcionamiento de la solución propuesta en los establecimientos de salud de la DIRIS Lima Norte.

La conectividad de red es un componente fundamental en el sector salud, ya que permite el funcionamiento continuo de sistemas informáticos como HIS MINSA, ARFSIS, SIHCE, REFCON, telemedicina, SISMED y otras plataformas institucionales. Desde el punto de vista operativo, estos sistemas

dependen de la disponibilidad permanente del servicio de internet para registrar atenciones, consultas y procesos administrativos en tiempo real.

En este contexto, la interoperabilidad de los sistemas de información en salud se basa en la capacidad de intercambio de datos entre diferentes plataformas, lo cual permite una gestión integrada de la información clínica y administrativa, asegurando la continuidad del flujo de información entre establecimientos y servidores centrales.

Por otro lado, la gestión de redes mediante MikroTik RouterOS se fundamenta en su capacidad para administrar el tráfico de datos a través de reglas de enrutamiento, firewall, NAT y control de ancho de banda. Su funcionamiento permite optimizar la comunicación entre redes internas y externas, facilitando la administración de infraestructuras de red en entornos institucionales (Dávila Llimpe, 2019; Mejía Valverde, 2021).

En relación con la seguridad perimetral, la implementación de firewalls en equipos MikroTik permite fortalecer la protección de la red frente a accesos no autorizados. Estos mecanismos funcionan mediante la aplicación de reglas que controlan el tráfico entrante y saliente, reduciendo riesgos de ataques o accesos indebidos (Montaño, 2025).

Por otro lado, la redundancia de enlaces se basa en principios de alta disponibilidad, donde se utilizan múltiples rutas de conexión para asegurar la continuidad del servicio. En este modelo, un enlace principal opera activamente mientras otros permanecen como respaldo ante posibles fallas.

El failover corresponde al mecanismo automático de conmutación entre enlaces de red. Su funcionamiento se basa en la detección de fallas mediante pruebas constantes de conectividad, permitiendo que el tráfico se redirija automáticamente hacia un enlace secundario sin intervención del usuario, reduciendo así los tiempos de indisponibilidad.

Asimismo, el monitoreo de red se basa en la supervisión continua de la infraestructura tecnológica. Herramientas como Zabbix permiten recolectar información en tiempo real sobre el estado de los dispositivos y servicios, utilizando protocolos como SNMP e ICMP para la detección de fallas y generación de alertas (Castro González & Álvarez, 2020; Mármol Proaño, 2025).

En cuanto a la seguridad en la comunicación, las redes privadas virtuales (VPN) se basan en el principio de cifrado del tráfico de datos a través de redes públicas. Este mecanismo garantiza la confidencialidad de la información transmitida entre sedes remotas. En este proyecto se utilizó WireGuard, un protocolo VPN moderno que emplea criptografía eficiente, permitiendo conexiones seguras con menor consumo de recursos y mayor rendimiento (Ávila Coello, 2025; Luna Huamán & Zeta Núñez, 2021).

Asimismo, la teoría de alta disponibilidad en redes establece que los sistemas deben mantenerse operativos incluso ante fallas parciales de la infraestructura. Este principio se aplica mediante la implementación de enlaces redundantes, mecanismos de failover y sistemas de monitoreo centralizado.

Finalmente, la continuidad operativa se basa en la resiliencia tecnológica, la cual permite que los servicios institucionales sigan funcionando a pesar de interrupciones en la red, garantizando la disponibilidad permanente de los sistemas críticos del sector salud.

3.5 Procedimiento

El desarrollo del piloto de monitoreo y gestión remota en el Centro de Salud Mental Comunitario Samay se realizó considerando la situación inicial del establecimiento, la implementación de la solución propuesta y la validación mediante pruebas técnicas. Este enfoque permitió evaluar el cumplimiento de los objetivos planteados en el presente trabajo.

3.5.1 Implementación del monitoreo con Zabbix

3.5.1.1 Situación Inicial

Antes de la implementación, el establecimiento de salud no contaba con un sistema de monitoreo que permitiera supervisar el estado de la conectividad en tiempo real. La detección de fallas en el servicio de internet se realizaba de forma manual, lo que generaba retrasos en la identificación de incidentes y en la toma de acciones correctivas.

Asimismo, no existía visibilidad remota del estado del router MikroTik ni de los dispositivos de red del establecimiento, lo que limitaba la capacidad de gestión desde la sede central.

3.5.1.2 Implementación

Para dar solución a esta problemática, se implementó una plataforma de monitoreo basada en Zabbix, instalada en un servidor central, con el objetivo de supervisar de manera continua el estado de la conectividad del establecimiento.

Previamente, fue necesario establecer la conectividad entre el servidor de monitoreo y el establecimiento de salud mediante una red privada virtual (VPN) utilizando el protocolo WireGuard, lo cual permitió el acceso seguro a los dispositivos de la red interna.

Una vez establecida la VPN, se procedió a integrar el router MikroTik del establecimiento al sistema de monitoreo, configurando los parámetros necesarios para la supervisión de su estado.

Se implementaron ítems de monitoreo orientados a verificar la disponibilidad del equipo, la conectividad a internet, el tiempo de respuesta y el estado de los enlaces. Asimismo, se configuraron triggers

para la generación de alertas automáticas ante la detección de fallas en la conectividad.

En la Figura 4 se presenta el panel de monitoreo del sistema Zabbix, donde se evidencia el estado operativo del router MikroTik del establecimiento del Rímac, confirmando su correcta integración al sistema de supervisión.

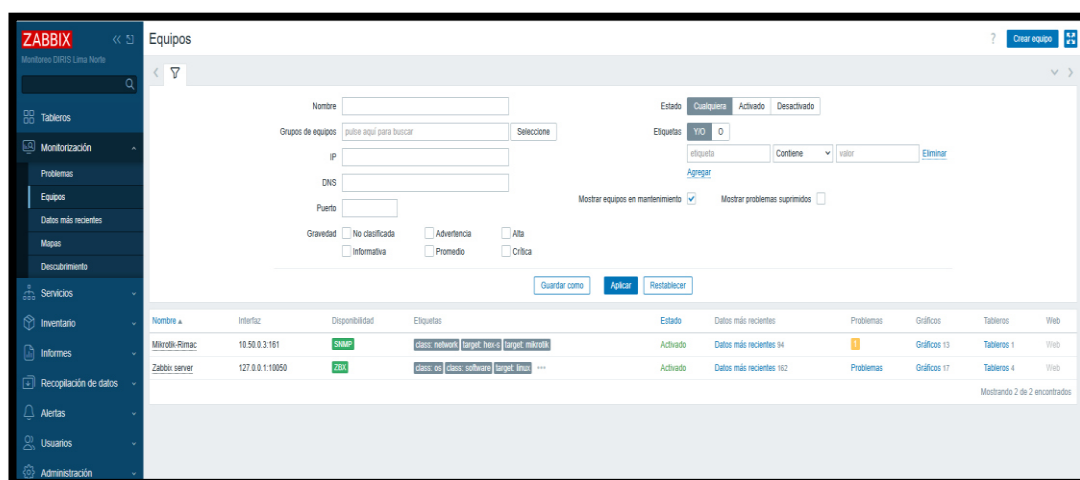


Figura 4 Panel de monitoreo en Zabbix mostrando el estado del router MikroTik del establecimiento del Rímac. Fuente. Elaboración propia.

3.5.1.3 Pruebas realizadas

Con la finalidad de validar el funcionamiento del sistema de monitoreo, se realizaron pruebas de conectividad desde el servidor Zabbix hacia el router MikroTik mediante la red VPN.

Se ejecutaron pruebas de tipo ping, verificando la comunicación con la dirección IP del router dentro de la red privada virtual. Asimismo, se simuló la interrupción del servicio de internet con el objetivo de comprobar la correcta generación de alertas en el sistema.

En la Figura 5 se muestra el panel de alertas del sistema Zabbix, donde se visualizan los eventos generados ante condiciones de falla, permitiendo la detección oportuna de incidentes en la red.

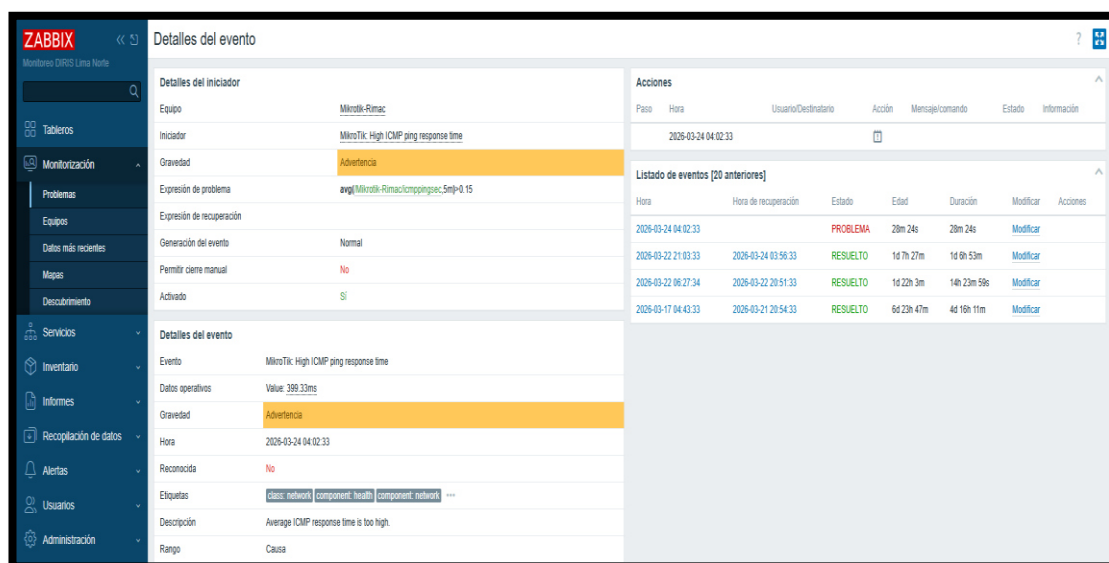


Figura 5 Panel de alertas generado por el sistema Zabbix ante eventos de conectividad. Fuente. Elaboración propia.

Adicionalmente, en la Figura 6 se observa el tráfico de la interfaz WireGuard, evidenciando la comunicación activa entre el servidor de monitoreo y el router MikroTik a través de la VPN. Esto permitió confirmar que la conexión se mantenía operativa durante las pruebas realizadas y que el acceso remoto al equipo podía efectuarse de forma satisfactoria.

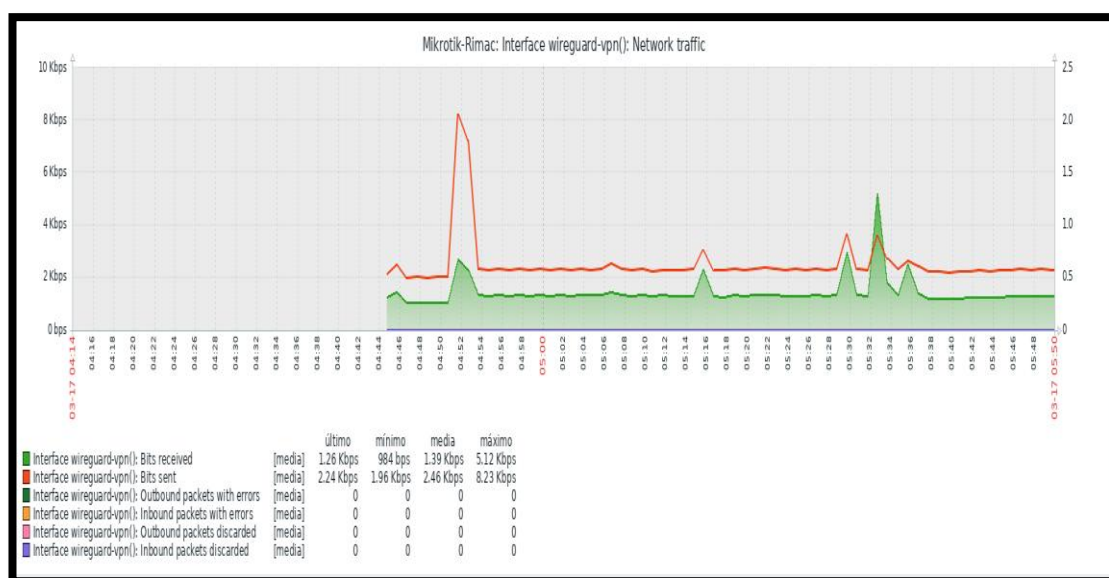


Figura 6 Tráfico de red en la interfaz WireGuard del router MikroTik. Fuente. Elaboración propia.

3.5.1.4 Resultado

Como resultado de la implementación, se logró contar con un sistema de monitoreo centralizado capaz de supervisar en tiempo real el estado de la conectividad del establecimiento de salud.

El servidor Zabbix permitió visualizar la disponibilidad del router MikroTik, así como detectar de manera oportuna interrupciones del servicio de internet mediante la generación automática de alertas.

Asimismo, la integración con la red privada virtual (VPN) posibilitó la gestión remota de los dispositivos de red desde la sede central, mejorando significativamente los tiempos de respuesta ante incidentes y fortaleciendo la continuidad operativa del servicio. Esto permitió realizar diversas verificaciones y tareas de soporte sin necesidad de acudir al establecimiento en todos los casos.

3.5.2 Implementación de la VPN con WireGuard

3.5.2.1 Situación inicial

Antes de la implementación, el establecimiento de salud no contaba con un mecanismo que permitiera la interconexión segura entre la sede central de monitoreo y los dispositivos de red ubicados en el establecimiento del distrito del Rímac.

El acceso a los equipos se realizaba únicamente de manera local, lo que dificultaba la administración remota, el diagnóstico oportuno de fallas y el monitoreo centralizado. Asimismo, no se disponía de un canal de comunicación cifrado, lo cual representaba un riesgo en la transmisión de información a través de la red. Como consecuencia, algunas tareas de verificación y soporte requerían la presencia del personal técnico en el establecimiento.

3.5.2.2 Descripción de la implementación

Con la finalidad de solucionar esta problemática, se implementó una red privada virtual (VPN) utilizando el protocolo WireGuard, permitiendo establecer una comunicación segura entre la sede central de monitoreo, el servidor Zabbix y el router MikroTik del establecimiento de salud.

Para ello, se desplegó un servidor VPN en la nube mediante un VPS, el cual fue configurado con el sistema operativo Ubuntu Server. Este servidor cumple la función de nodo central de la VPN, permitiendo la interconexión de todos los dispositivos participantes.

Se definió un esquema de direccionamiento privado para la red VPN utilizando el rango 10.50.0.0/24, asignando direcciones IP a cada uno de los nodos involucrados en la solución.

Cuadro 1 Asignación de direcciones IP en la red VPN

Dispositivo	Dirección IP VPN
Servidor VPN	10.50.0.1
PC sede Independencia	10.50.0.2
Router MikroTik Rímac	10.50.0.3
Servidor Zabbix	10.50.0.4

Fuente. Elaboración propia.

Posteriormente, se realizó la configuración del servidor VPN, donde se definieron los parámetros de la interfaz WireGuard, incluyendo la dirección IP, el puerto de escucha y las claves criptográficas necesarias para la autenticación de los clientes.

Una vez configurado el servidor, se procedió a la integración de los clientes VPN, los cuales corresponden a la estación de monitoreo ubicada en la sede de Independencia, el servidor Zabbix y el router MikroTik del establecimiento del Rímac

```

root@wireguard-vpn: ~
To see these additional updates run: apt list --upgradable
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

*** System restart required ***
Last login: Fri Apr 10 03:05:27 2026 from 190.42.17.17
root@wireguard-vpn:~# wg
interface: wg0
  public key: Jhq8iQK/a7XsYYt/vw8tgQq5eTJAmeYoOv6XSYIe/3c=
  private key: (hidden)
  listening port: 51820

peer: xweH5AyRHZfk0oxavwzXmgQVb5P+RPi03xPAP25Ijc=
  endpoint: 161.132.159.128:51820
  allowed ips: 10.50.0.3/32, 192.168.50.0/24
  latest handshake: 1 minute, 12 seconds ago
  transfer: 71.01 MiB received, 12.14 MiB sent

peer: AUCXPLUdnVNS1+IwH9CPH/QsibKRFZVOYJCMqToHcwU=
  endpoint: 181.66.157.132:6916
  allowed ips: 10.50.0.2/32
  latest handshake: 9 days, 22 hours, 59 minutes, 46 seconds ago
  transfer: 9.63 MiB received, 63.41 MiB sent

peer: 7+6VmGbGFU8XXR4yJOgc0XU060zoRp+kvkzD1QjmxSs=
  endpoint: 181.66.139.26:2048
  allowed ips: 10.50.0.4/32
  latest handshake: 34 days, 16 hours, 22 minutes, 14 seconds ago
  transfer: 1.35 MiB received, 2.68 MiB sent
root@wireguard-vpn:~#

```

Figura 7 Configuración de la interfaz WireGuard en el servidor VPN.
Fuente. Elaboración propia.

En el caso del router MikroTik, se creó una interfaz WireGuard, se asignó una dirección IP dentro de la red VPN y se configuró el servidor como peer, estableciendo así el túnel seguro de comunicación. Adicionalmente, se configuraron las rutas y reglas necesarias para permitir el acceso hacia la red local del establecimiento.

```

admin@10.50.0.3 (MikroTik) - WinBox (64bit) v7.20.4 on hEX (mmips)
Session Settings Dashboard
Safe Mode Session: 10.50.0.3

Terminal <1>
MMM MMM KKK TTTTTTTTTT KKK
MMM MMM KKK TTTTTTTTTT KKK
MMM MMM III KKK KKK RRRRRR OOOOOO TTT III KKK KKK
MMM MM III KKKKKK RRR RRR OOO OOO TTT III KKKKKK
MMM III KKK KKK RRRRRR OOO OOO TTT III KKK KKK
MMM MM III KKK KKK RRR RRR OOOOOO TTT III KKK KKK

MikroTik RouterOS 7.20.4 (c) 1999-2025 https://www.mikrotik.com/
Press F1 for help

[admin@MikroTik] > /interface wireguard print
Flags: X - disabled; R - running
0 R name="wireguard-vpn" mtu=1420 listen-port=51820
  private-key="wInICtLLH8STIEKcKdsogt8Fw5cyay2wIXrtjKd5GA="
  public-key="xweH5AyRHZfk0oxavwzXmgQVb5P+RPi03xPAP25Ijc="
[admin@MikroTik] > /interface wireguard peers print
Columns: INTERFACE, PUBLIC-KEY, ENDPOINT-ADDRESS
# INTERFACE PUBLIC-KEY ENDPOINT-ADDRESS
0 wireguard-vpn Jhq8iQK/a7XsYYt/vw8tgQq5eTJAmeYoOv6XSYIe/3c= 89.167.72.126
[admin@MikroTik] >

```

Figura 8 Configuración de la interfaz WireGuard en el router MikroTik del establecimiento del Rímac. Fuente. Elaboración propia.

3.5.2.3 Pruebas realizadas

Con la finalidad de validar el correcto funcionamiento de la VPN, se realizaron pruebas de conectividad entre los diferentes nodos de la red.

Se ejecutaron pruebas de tipo ping desde la estación de monitoreo hacia el servidor VPN, el router MikroTik y equipos dentro de la red local del establecimiento, verificando la correcta comunicación entre todos los puntos de la red.

Cuadro 2 Resultados de pruebas de conectividad en la VPN

Origen (Sede Independencia)	Destino	Resultado
PC monitoreo	10.50.0.1 (Servidor VPN)	Correcto
PC monitoreo	10.50.0.3 (MikroTik Rímac)	Correcto
PC monitoreo	192.168.50.1 (Gateway LAN)	Correcto
PC monitoreo	192.168.50.200 (Equipo LAN)	Correcto

Fuente. Elaboración propia.

```

Microsoft Windows [Versión 10.0.19045.6466]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\User>ping 10.50.0.3

Haciendo ping a 10.50.0.3 con 32 bytes de datos:
Respuesta desde 10.50.0.3: bytes=32 tiempo=404ms TTL=63
Respuesta desde 10.50.0.3: bytes=32 tiempo=421ms TTL=63
Respuesta desde 10.50.0.3: bytes=32 tiempo=400ms TTL=63
Respuesta desde 10.50.0.3: bytes=32 tiempo=399ms TTL=63

Estadísticas de ping para 10.50.0.3:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 399ms, Máximo = 421ms, Media = 406ms

C:\Users\User>ping 192.168.50.1

Haciendo ping a 192.168.50.1 con 32 bytes de datos:
Respuesta desde 192.168.50.1: bytes=32 tiempo=401ms TTL=63
Respuesta desde 192.168.50.1: bytes=32 tiempo=400ms TTL=63
Respuesta desde 192.168.50.1: bytes=32 tiempo=399ms TTL=63
Respuesta desde 192.168.50.1: bytes=32 tiempo=400ms TTL=63

Estadísticas de ping para 192.168.50.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 399ms, Máximo = 401ms, Media = 400ms

C:\Users\User>ping 192.168.50.190

Haciendo ping a 192.168.50.190 con 32 bytes de datos:
Respuesta desde 192.168.50.190: bytes=32 tiempo=400ms TTL=62
Respuesta desde 192.168.50.190: bytes=32 tiempo=401ms TTL=62
Respuesta desde 192.168.50.190: bytes=32 tiempo=403ms TTL=62
Respuesta desde 192.168.50.190: bytes=32 tiempo=400ms TTL=62

Estadísticas de ping para 192.168.50.190:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 400ms, Máximo = 403ms, Media = 401ms

C:\Users\User>
  
```

Figura 9 Pruebas de conectividad mediante comando ping entre la sede central y el establecimiento del Rímac. Fuente. Elaboración propia.

Adicionalmente, se verificó el estado de la conexión en el servidor VPN mediante la herramienta de administración de WireGuard, observando el intercambio de tráfico y el establecimiento del handshake entre los dispositivos conectados.

```

root@wireguard-vpn: ~
https://ubuntu.com/engage/secure-kubernetes-at-the-edge
Expanded Security Maintenance for Applications is not enabled.
19 updates can be applied immediately.
To see these additional updates run: apt list --upgradable
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

*** System restart required ***
Last login: Wed Apr 29 02:40:44 2026 from 181.66.138.152
root@wireguard-vpn:~# wg
interface: wg0
  public key: Jhq8iQK/a7XsYYt/vw8tgQq5eTJAmeYo0v6X5YIe/3c=
  private key: (hidden)
  listening port: 51820

peer: xweH5AyRHZfk0oxavwzXmgQVb5P+Rpi03xPAP25Ijc=
  endpoint: 161.132.159.128:51820
  allowed ips: 10.50.0.3/32, 192.168.50.0/24
  latest handshake: 5 seconds ago
  transfer: 71.56 MiB received, 12.21 MiB sent

peer: AUCXPLUdnVNS1+IwW9CPh/QsibKRFZVOYJCMqToHcwU=
  endpoint: 181.66.138.152:4173
  allowed ips: 10.50.0.2/32
  latest handshake: 57 seconds ago
  transfer: 9.71 MiB received, 63.96 MiB sent

peer: 7+6VmGbGFU8XXR4yJ0gc0XU060zoRp+kvkzD1QjmxSs=
  endpoint: 181.66.139.26:2048
  allowed ips: 10.50.0.4/32
  latest handshake: 34 days, 16 hours, 41 minutes, 45 seconds ago
  transfer: 1.35 MiB received, 2.68 MiB sent
root@wireguard-vpn:~#

```

Figura 10 Estado de la conexión VPN y verificación de handshake en el servidor WireGuard. Fuente. Elaboración propia.

3.5.2.4 Resultado de la implementación

Como resultado de la implementación, se logró establecer una red privada virtual segura y estable que permite la interconexión entre la sede central de monitoreo y el establecimiento de salud del Rímac.

La solución implementada mediante WireGuard permitió el acceso remoto a los dispositivos de red del establecimiento sin necesidad de

intervención presencial, garantizando la confidencialidad e integridad de la información mediante el uso de cifrado.

Asimismo, la VPN permitió la integración con el servidor Zabbix, facilitando el monitoreo centralizado de la infraestructura de red y mejorando significativamente la capacidad de respuesta ante incidentes de conectividad.

3.5.3 Implementación del mecanismo de conmutación automática (failover) en el router MikroTik

3.5.3.1 Situación inicial

Antes de la implementación del mecanismo de conmutación automática, el Centro de Salud Mental Comunitario Samay contaba con dos enlaces de Internet proporcionados por los operadores GTD (enlace principal) y Movistar (enlace secundario). Sin embargo, no existía un sistema automatizado de respaldo que permitiera la conmutación inmediata ante fallas del servicio.

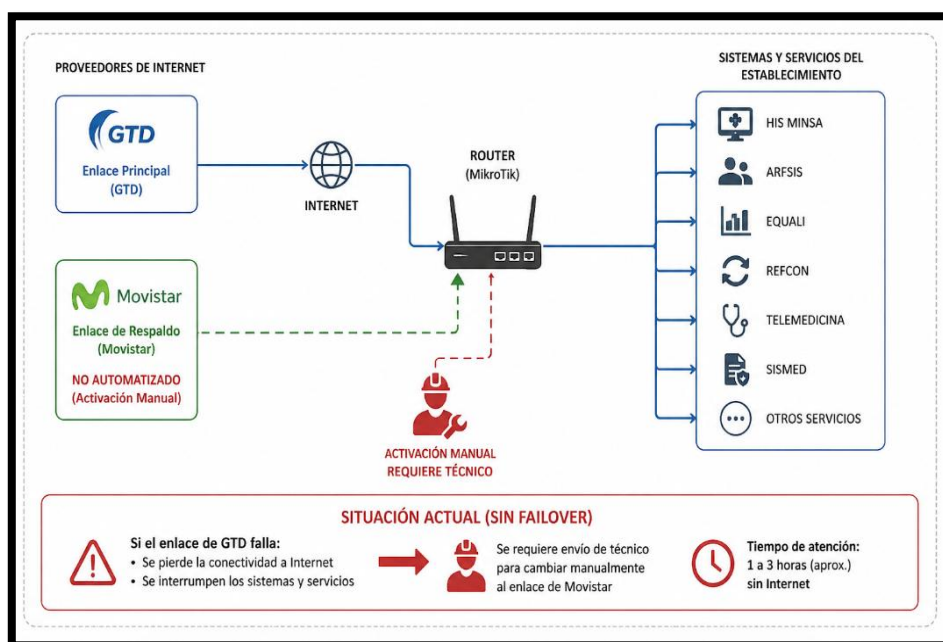


Figura 11 Arquitectura de conectividad sin mecanismo de failover en el establecimiento de salud. Fuente. Elaboración propia.

Cuando el enlace principal GTD presentaba interrupciones, la continuidad del servicio de Internet se veía afectada, ya que el cambio hacia el enlace secundario requería intervención manual de un técnico especializado, con un tiempo de respuesta aproximado entre 1 a 3 horas.

Durante este periodo, el establecimiento de salud quedaba sin acceso a servicios críticos como HIS MINSA, ARFSIS, SIHCE, REFCON, telemedicina, SISMED y otras plataformas institucionales, afectando la operatividad asistencial y administrativa.

3.5.3.2 Implementación del mecanismo de failover

Se configuró el router MikroTik RB750Gr3 para implementar la conmutación automática entre enlaces de Internet, estableciendo a GTD como enlace principal y a Movistar como respaldo.

El mecanismo de failover permite que, ante la caída del enlace principal, el sistema redirija automáticamente el tráfico hacia el enlace de respaldo sin intervención humana, garantizando la continuidad operativa de los servicios institucionales. De esta manera, se reduce el impacto de las interrupciones del servicio de Internet y se mantiene la disponibilidad de los sistemas utilizados por el personal del establecimiento para el desarrollo de sus actividades diarias.

Cuadro 3 Comparación del funcionamiento del acceso a Internet antes y después del failover.

Condición	Sin failover	Con failover
Tipo de cambio de enlace	Manual	Automático
Tiempo de recuperación	1 a 3 horas	1 a 3 minutos
Intervención técnica	Requerida	No requerida
Disponibilidad de servicios HIS, ARFSIS, eQhali, REFCON, telemedicina, SISMED	Interrumpida	Continua (breve interrupción)

Fuente. Elaboración propia.

3.5.3.3 Pruebas realizadas

Se realizaron pruebas de conectividad simulando la caída del enlace principal GTD, con el objetivo de validar el comportamiento del sistema de conmutación automática.

En el escenario sin failover, la caída del servicio requería la intervención de un técnico para la reconexión manual hacia el enlace Movistar, generando tiempos prolongados de indisponibilidad.

En contraste, con la implementación del failover, al producirse la caída del enlace GTD, el router MikroTik redirigió automáticamente el tráfico hacia el enlace Movistar.

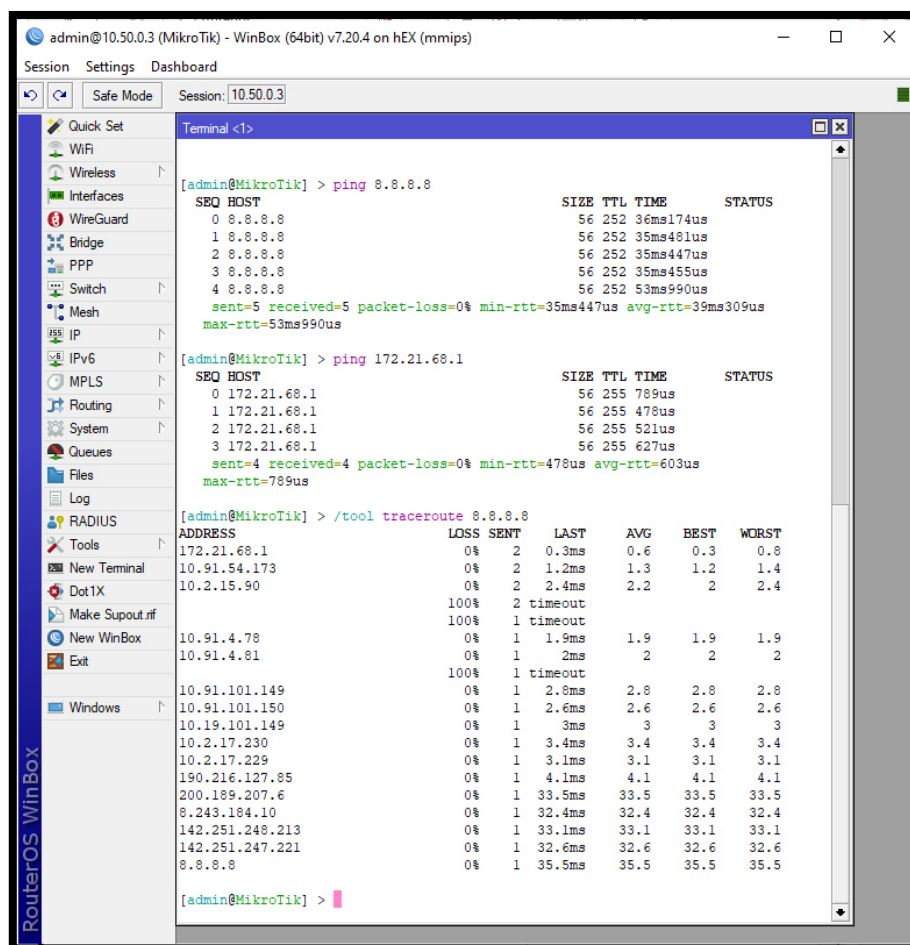


Figura 12 Prueba de conectividad con enlace GTD activo. Fuente. Elaboración propia.

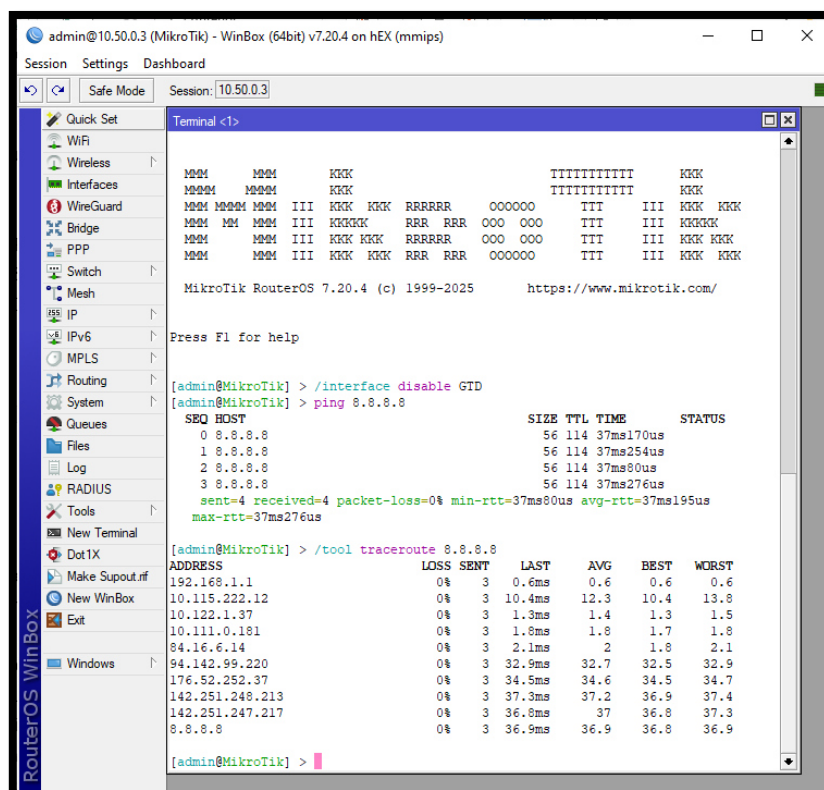


Figura 13 Validación del failover con conmutación automática hacia Movistar. Fuente. Elaboración propia.

3.5.3.4 Resultados obtenidos

La implementación del mecanismo de conmutación automática permitió reducir significativamente el tiempo de indisponibilidad del servicio de Internet en el establecimiento de salud.

Mientras que anteriormente la recuperación del servicio dependía de la llegada de un técnico con tiempos de 1 a 3 horas, con la solución implementada la conmutación hacia el enlace de respaldo se realiza de manera automática en un tiempo aproximado de 1 a 3 minutos.

Esto garantiza la continuidad operativa de los sistemas críticos utilizados en el establecimiento de salud, tales como HIS MINSA, ARFSIS, SIHCE, REFCON, telemedicina, SISMED y otras plataformas institucionales, evitando interrupciones prolongadas en la atención y gestión asistencial.

Cuadro 4 Impacto de la implementación del mecanismo de failover en la disponibilidad del servicio.

Indicador	Antes de la implementación	Después de la implementación
Tiempo de recuperación	1 a 3 horas	1 a 3 minutos
Tipo de conmutación	Manual	Automática
Disponibilidad de sistemas clínicos	Interrumpida	Casi continua
Dependencia de técnico	Alta	Nula

Fuente. Elaboración propia.

3.5.4 Evaluación de la solución implementada

3.5.4.1 Situación de evaluación

Una vez implementadas las soluciones de monitoreo con Zabbix, la red privada virtual mediante WireGuard y el mecanismo de conmutación automática (failover) en el router MikroTik, se procedió a realizar la evaluación integral del sistema en condiciones reales de operación del Centro de Salud Mental Comunitario Samay.

Antes de la implementación, el establecimiento presentaba las siguientes limitaciones, las cuales afectaban la capacidad de respuesta ante incidencias de conectividad y dificultaban la gestión eficiente de la red:

- Dependencia de intervención técnica presencial para resolver caídas de Internet
- Tiempo de atención entre 1 a 3 horas en caso de fallas del enlace principal GTD
- Ausencia de visibilidad centralizada del estado de la red
- Interrupción de servicios críticos como HIS MINSA, ARFSIS, SIHCE, REFCON, telemedicina y SISMED durante caídas de conectividad

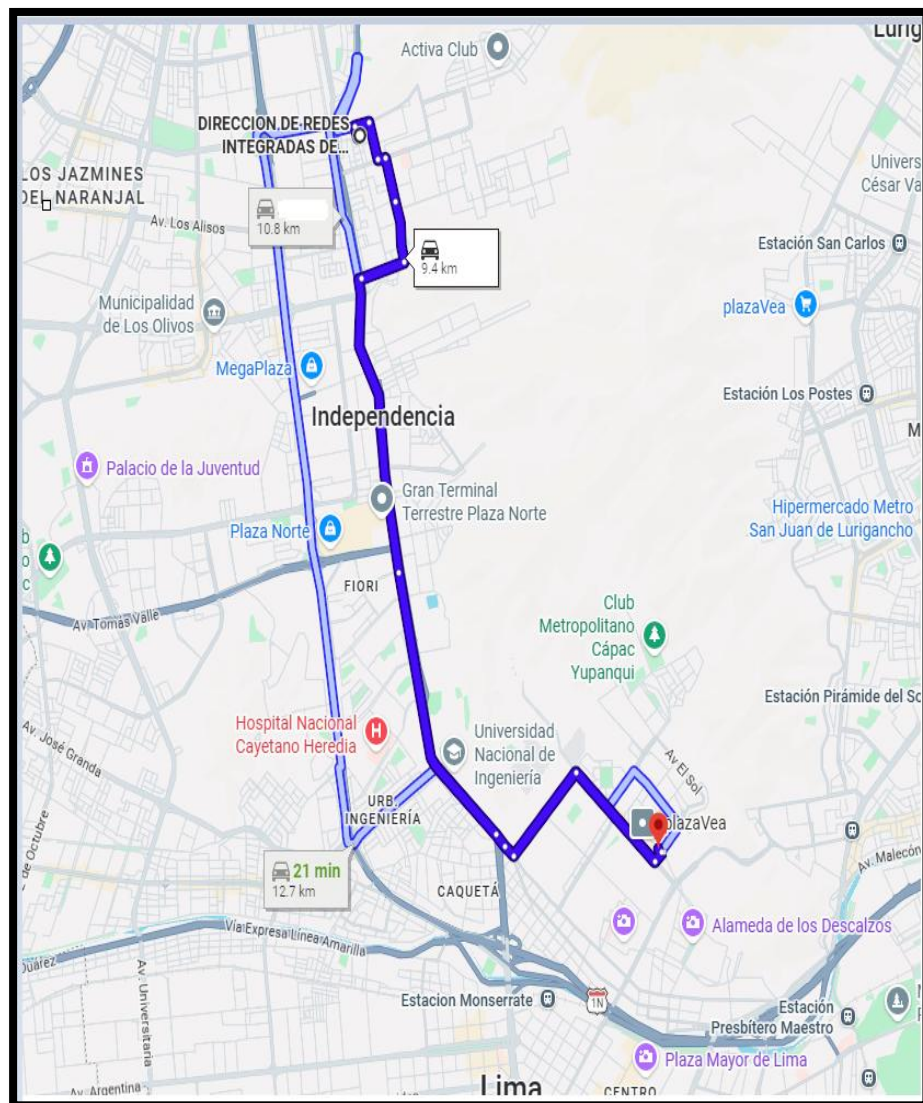


Figura 14 Ruta de desplazamiento del personal técnico desde la DIRIS Lima Norte (Independencia) hacia el Centro de Salud Mental Comunitario Samay (Rímac). Fuente. Elaboración propia en base a Google Maps.

3.5.4.2 Pruebas de validación de la solución

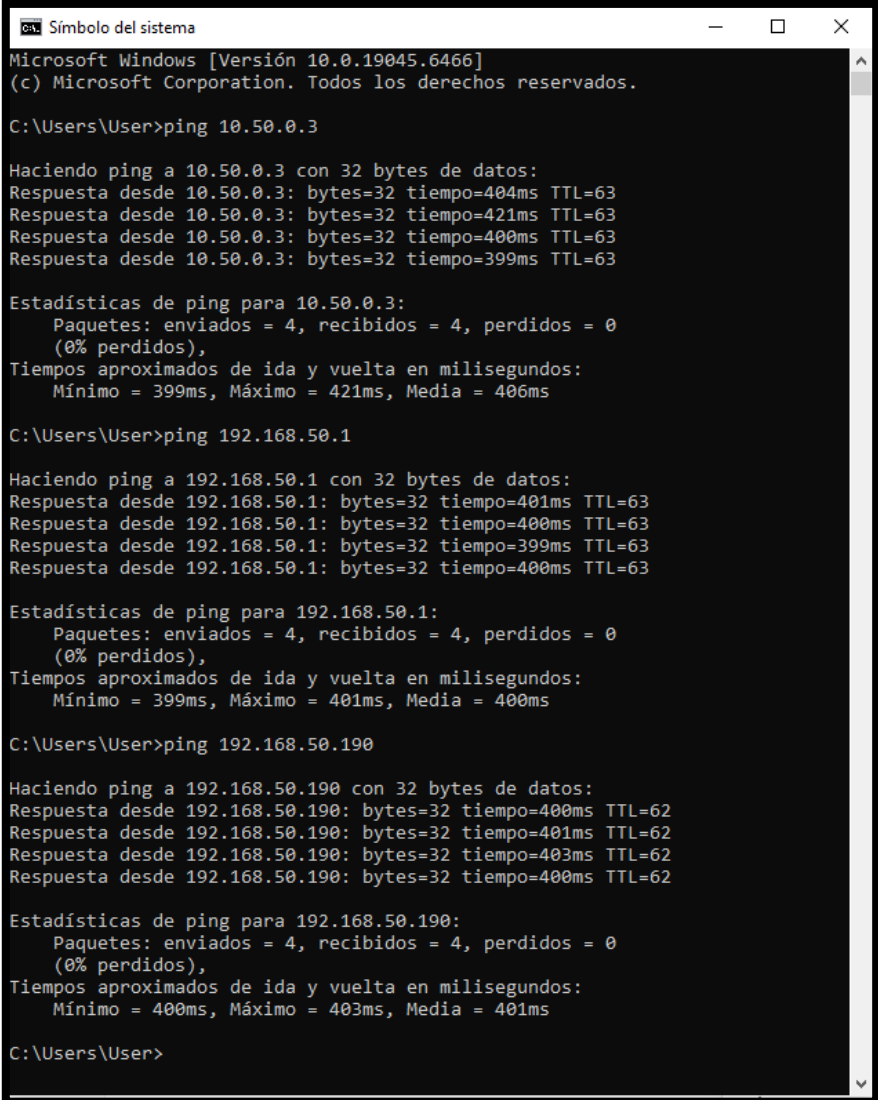
Se realizaron pruebas integrales para validar el funcionamiento conjunto de los tres componentes implementados:

1. Pruebas de conectividad mediante VPN

Ping desde sede central hacia:

- Mikrotik del establecimiento (10.50.0.3)

- Servidor VPN (10.50.0.1)
- Red interna del establecimiento (192.168.50.0/24)



```
Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.6466]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\User>ping 10.50.0.3

Haciendo ping a 10.50.0.3 con 32 bytes de datos:
Respuesta desde 10.50.0.3: bytes=32 tiempo=404ms TTL=63
Respuesta desde 10.50.0.3: bytes=32 tiempo=421ms TTL=63
Respuesta desde 10.50.0.3: bytes=32 tiempo=400ms TTL=63
Respuesta desde 10.50.0.3: bytes=32 tiempo=399ms TTL=63

Estadísticas de ping para 10.50.0.3:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 399ms, Máximo = 421ms, Media = 406ms

C:\Users\User>ping 192.168.50.1

Haciendo ping a 192.168.50.1 con 32 bytes de datos:
Respuesta desde 192.168.50.1: bytes=32 tiempo=401ms TTL=63
Respuesta desde 192.168.50.1: bytes=32 tiempo=400ms TTL=63
Respuesta desde 192.168.50.1: bytes=32 tiempo=399ms TTL=63
Respuesta desde 192.168.50.1: bytes=32 tiempo=400ms TTL=63

Estadísticas de ping para 192.168.50.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 399ms, Máximo = 401ms, Media = 400ms

C:\Users\User>ping 192.168.50.190

Haciendo ping a 192.168.50.190 con 32 bytes de datos:
Respuesta desde 192.168.50.190: bytes=32 tiempo=400ms TTL=62
Respuesta desde 192.168.50.190: bytes=32 tiempo=401ms TTL=62
Respuesta desde 192.168.50.190: bytes=32 tiempo=403ms TTL=62
Respuesta desde 192.168.50.190: bytes=32 tiempo=400ms TTL=62

Estadísticas de ping para 192.168.50.190:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 400ms, Máximo = 403ms, Media = 401ms

C:\Users\User>
```

Figura 15 Prueba de conectividad entre sede central y red del establecimiento mediante VPN WireGuard. Fuente. Elaboración propia.

2. Pruebas de monitoreo en Zabbix

- Verificación de disponibilidad del host MikroTik
- Generación de alertas ante desconexión
- Visualización del estado en tiempo real

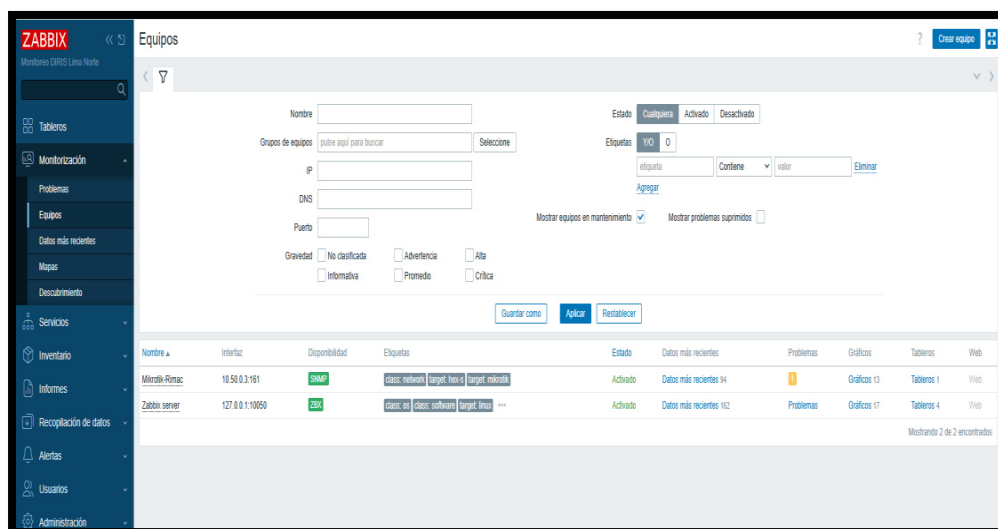


Figura 16 Panel de monitoreo de Zabbix mostrando el estado del router del establecimiento. Fuente. Elaboración propia.

3. Pruebas del mecanismo de failover

- Simulación de caída del enlace GTD
- Verificación de cambio automático a Movistar
- Validación de continuidad de Internet

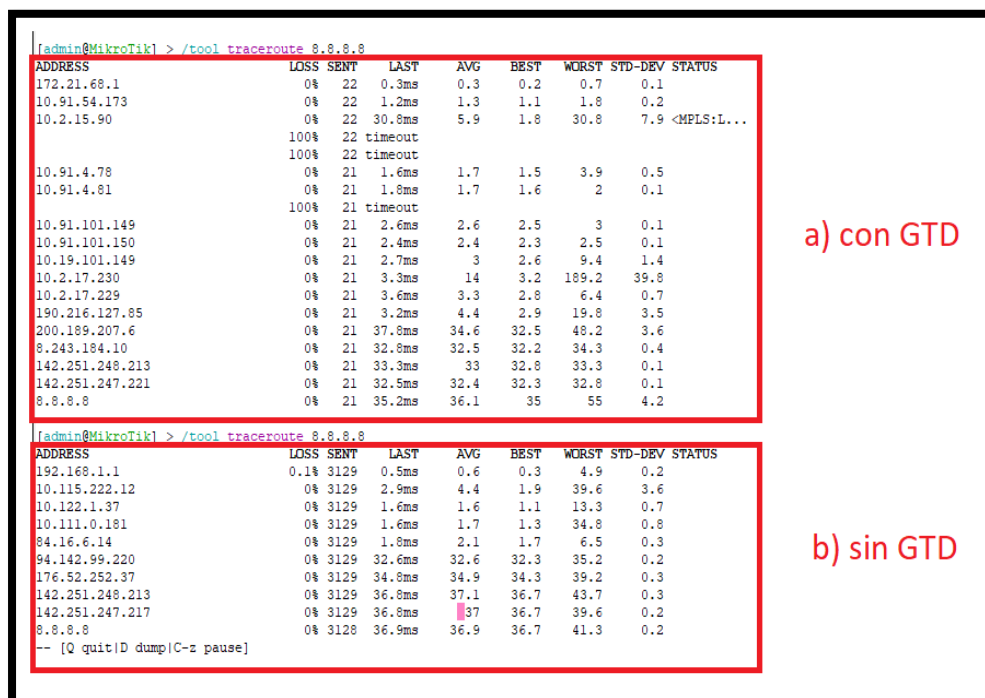


Figura 17 Prueba de conmutación automática de enlaces (failover) en el router MikroTik. Fuente. Elaboración propia.

3.5.4.3 Resultados de la evaluación

Como resultado de las pruebas realizadas, se evidenció que:

- El sistema de monitoreo con Zabbix permite visualizar el estado de la conectividad en tiempo real
- La VPN con WireGuard garantiza acceso remoto seguro a la red del establecimiento
- El mecanismo de failover permite la continuidad del servicio de Internet ante fallas del enlace principal
- La implementación del mecanismo de failover automático reduce el tiempo de interrupción del servicio de Internet de 1–3 horas a aproximadamente 1–3 minutos.
- Se garantiza la continuidad operativa de los sistemas críticos del establecimiento de salud

Cuadro 5 Comparación del comportamiento de la red antes y después de la implementación.

Indicador	Antes	Después
Tiempo de caída de Internet	1 a 3 horas (intervención manual)	1 a 3 minutos (restablecimiento total del servicio)
Acceso remoto	No disponible	Disponible mediante VPN
Monitoreo centralizado	No existente	Implementado con Zabbix
Continuidad de servicios	Interrumpida	Garantizada con failover automático

Fuente. Elaboración propia.

En relación con los tiempos mostrados en el Cuadro 5, es importante precisar que el tiempo de conmutación del mecanismo de failover en el router MikroTik es prácticamente inmediato, registrándose entre 1 a 5 segundos aproximadamente, debido a la detección automática de caída del enlace principal y la redirección del tráfico hacia el enlace secundario.

Sin embargo, el tiempo considerado en el presente trabajo (1 a 3 minutos) corresponde al tiempo de restablecimiento completo del servicio de conectividad en todos los dispositivos de la red del establecimiento de salud, incluyendo computadoras, impresoras de red y sistemas clínicos como HIS MINSA, ARFSIS, SIHCE, REFCON, telemedicina, SISMED y otras plataformas institucionales.

Este tiempo adicional se debe a procesos propios de la red local, tales como renovación de sesiones TCP/IP, reconexión de servicios activos, actualización de rutas en los dispositivos finales y restablecimiento de comunicación con servidores internos y externos.

En el entorno evaluado, aproximadamente 20 dispositivos entre estaciones de trabajo y equipos de impresión requieren reestablecer sus sesiones de red luego de la conmutación, lo que genera una ligera latencia hasta la normalización total del servicio.

3.5.4.4 Resultado final de la evaluación

La evaluación de la solución implementada demuestra que la integración de Zabbix, WireGuard y el failover en MikroTik permite una gestión centralizada, segura y altamente disponible de la conectividad del establecimiento de salud, mejorando significativamente la continuidad operativa de los servicios críticos de salud.

3.6 Resultados de la actividad

Como resultado de la implementación del sistema de monitoreo, la red privada virtual (VPN) y el mecanismo de conmutación automática (failover), se logró consolidar una solución integral para la gestión de la conectividad del Centro de Salud Mental Comunitario Samay, permitiendo mejorar la continuidad operativa de los servicios digitales críticos utilizados en el establecimiento.

La evaluación de los resultados se realizó en función de los objetivos específicos planteados, considerando aspectos de conectividad, disponibilidad, tiempos de respuesta, seguridad y monitoreo centralizado. Para ello, se realizaron pruebas en un entorno real de operación, simulando fallas de conectividad y verificando el comportamiento de la solución implementada.

3.6.1 Resultados del monitoreo centralizado con Zabbix

A partir de la implementación de la plataforma Zabbix, se logró obtener visibilidad en tiempo real del estado del router MikroTik del establecimiento, así como de los enlaces de comunicación.

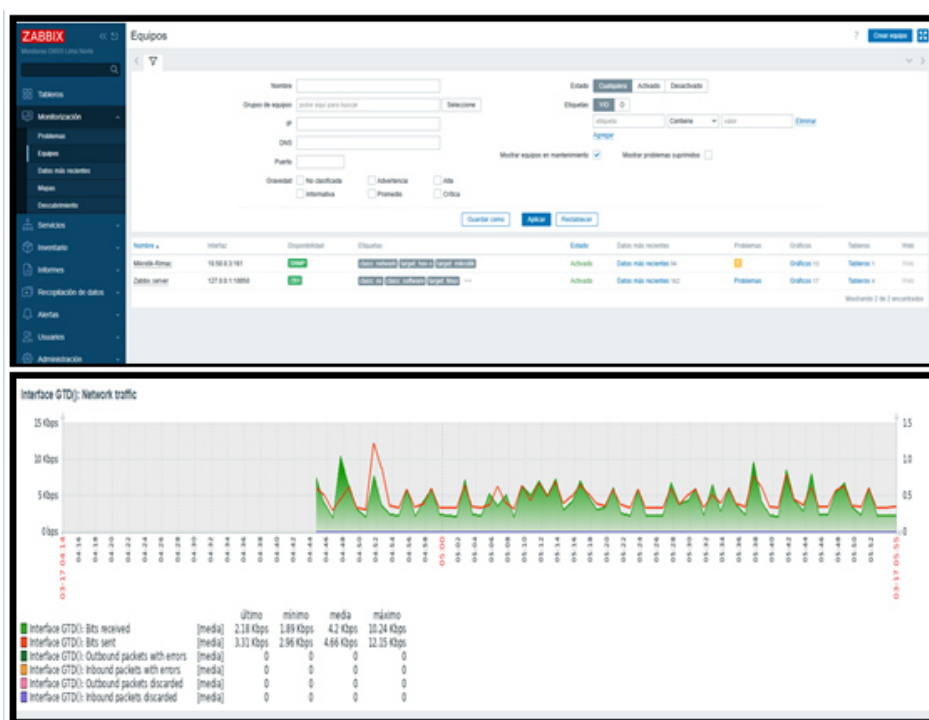


Figura 18 Panel de monitoreo en Zabbix mostrando el estado del router MikroTik del establecimiento. Fuente. Elaboración propia.

Se evidenció que el sistema permite detectar de manera inmediata cualquier evento relacionado con la caída del servicio de Internet o la pérdida de conectividad del equipo monitoreado. Esto representa una mejora importante frente al escenario anterior, donde la identificación de fallas dependía de reportes de los usuarios o validaciones manuales.

Durante las pruebas realizadas, el sistema generó alertas automáticas ante variaciones en la disponibilidad del equipo, permitiendo al personal técnico identificar incidentes sin necesidad de estar físicamente en el establecimiento.

En la práctica, esto permitió reducir el tiempo de detección de fallas, ya que ahora el evento es notificado automáticamente desde la sede central.

3.6.2 Resultados de la conectividad mediante VPN WireGuard

La implementación de la VPN permitió establecer un canal seguro de comunicación entre la sede central y el establecimiento de salud, facilitando el acceso remoto a la red interna.

```

Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.6466]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\User>ping 10.50.0.1

Haciendo ping a 10.50.0.1 con 32 bytes de datos:
Respuesta desde 10.50.0.1: bytes=32 tiempo=266ms TTL=64
Respuesta desde 10.50.0.1: bytes=32 tiempo=265ms TTL=64
Respuesta desde 10.50.0.1: bytes=32 tiempo=265ms TTL=64
Respuesta desde 10.50.0.1: bytes=32 tiempo=265ms TTL=64

Estadísticas de ping para 10.50.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 265ms, Máximo = 266ms, Media = 265ms

C:\Users\User>ping 10.50.0.3

Haciendo ping a 10.50.0.3 con 32 bytes de datos:
Respuesta desde 10.50.0.3: bytes=32 tiempo=461ms TTL=63
Respuesta desde 10.50.0.3: bytes=32 tiempo=485ms TTL=63
Respuesta desde 10.50.0.3: bytes=32 tiempo=460ms TTL=63
Respuesta desde 10.50.0.3: bytes=32 tiempo=460ms TTL=63

Estadísticas de ping para 10.50.0.3:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 460ms, Máximo = 485ms, Media = 466ms

C:\Users\User>ping 192.168.50.1

Haciendo ping a 192.168.50.1 con 32 bytes de datos:
Respuesta desde 192.168.50.1: bytes=32 tiempo=463ms TTL=63
Respuesta desde 192.168.50.1: bytes=32 tiempo=461ms TTL=63
Respuesta desde 192.168.50.1: bytes=32 tiempo=460ms TTL=63
Respuesta desde 192.168.50.1: bytes=32 tiempo=460ms TTL=63

Estadísticas de ping para 192.168.50.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 460ms, Máximo = 463ms, Media = 461ms

C:\Users\User>ping 192.168.50.191

Haciendo ping a 192.168.50.191 con 32 bytes de datos:
Respuesta desde 192.168.50.191: bytes=32 tiempo=460ms TTL=62
Respuesta desde 192.168.50.191: bytes=32 tiempo=460ms TTL=62
Respuesta desde 192.168.50.191: bytes=32 tiempo=460ms TTL=62
Respuesta desde 192.168.50.191: bytes=32 tiempo=465ms TTL=62

Estadísticas de ping para 192.168.50.191:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 460ms, Máximo = 465ms, Media = 461ms

C:\Users\User>
  
```

Figura 19 Pruebas de conectividad mediante VPN entre sede central y establecimiento. Fuente. Elaboración propia

Las pruebas de conectividad realizadas demostraron que es posible alcanzar los dispositivos internos del establecimiento (como el router MikroTik y otros equipos de red) utilizando direcciones IP privadas dentro del túnel VPN.

Esto eliminó la necesidad de depender de accesos físicos o configuraciones expuestas directamente a Internet.

En términos operativos, este resultado permitió que las tareas de administración y diagnóstico de red puedan ejecutarse de forma remota, reduciendo significativamente la dependencia del traslado de personal técnico.

3.6.3 Resultados del mecanismo de conmutación automática (failover)

Uno de los resultados más relevantes del proyecto fue la validación del funcionamiento del failover en el router MikroTik.

The screenshot shows the MikroTik RouterOS WinBox interface. The terminal window displays the following commands and output:

```

[admin@MikroTik] > /ip route disable [find gateway=172.21.68.1]
[admin@MikroTik] > ping 8.8.8.8

```

The ping output shows successful results:

SIZE	TTL	TIME	STATUS
0	8.8.8.8	56	115 35ms259us
1	8.8.8.8	56	115 34ms699us
2	8.8.8.8	56	115 34ms913us
3	8.8.8.8	56	115 34ms921us

Below the ping output, the following statistics are shown:

```

sent=4 received=4 packet-loss=0% min-rtt=34ms699us avg-rtt=34ms945us max-rtt=35ms259us

```

The terminal also shows the output of the `/tool traceRoute` command, which displays the route from the router to 8.8.8.8:

ADDRESS	LOSS	SENT	LAST	AVG	BEST	WORST	STD-DEV	STATUS
192.168.1.1	0%	5	0.6ms	0.6	0.6	0.6	0	
10.115.232.12	0%	5	5ms	2.9	2.6	3.2	0.2	
10.122.1.37	0%	5	1.6ms	1.4	1.3	1.6	0.1	
10.111.0.181	0%	5	1.6ms	1.7	1.6	1.8	0.1	
94.16.6.14	0%	5	1.9ms	2	1.8	2.3	0.2	
94.142.99.220	0%	5	35ms	34.9	34.8	35.1	0.1	
176.52.252.37	0%	5	39ms	37.7	37	39	0.7	
142.251.249.213	0%	5	34.5ms	34.6	34.5	34.7	0.1	
142.251.247.217	0%	5	38.4ms	38.5	38.3	38.8	0.2	
8.8.8.8	0%	5	34.5ms	34.7	34.4	34.9	0.2	

The terminal also shows the output of the `/ip route print` command, which displays the routing table:

```

[admin@MikroTik] > /ip route print
Flags: D - DYNAMIC, X - DISABLED, I - INACTIVE, A - ACTIVE; c - CONNECT, s - STATIC, d - DHCP
Columns: DST-ADDRESS, GATEWAY, ROUTING-TABLE, DISTANCE
# DST-ADDRESS GATEWAY ROUTING-TABLE DISTANCE
0 Xs 0.0.0.0/0 172.21.68.1 1
Dsd 0.0.0.0/0 192.168.1.1 main 2
Ddc 10.50.0.0/24 wireguard-vpn main 0
Ddc 172.21.68.0/24 GTD main 0
Ddc 192.168.1.0/24 Movistar main 0
Ddc 192.168.50.0/24 bridge-lan main 0

```

Red annotations on the image indicate:

- GTD deshabilitado** (GTD disabled) pointing to the `/ip route disable` command.
- Failover Movistar Activo** (Failover Movistar Active) pointing to the routing table output.

Figura 20 Prueba de caída del enlace GTD y conmutación automática a Movistar. Fuente. Elaboración propia.

Durante las pruebas, se simuló la caída del enlace principal proporcionado por GTD, observándose que el sistema realizó automáticamente la conmutación hacia el enlace de respaldo Movistar.

Este cambio ocurrió sin intervención manual, lo cual representa una mejora importante frente al escenario anterior, donde el cambio de enlace dependía del desplazamiento de un técnico al establecimiento.

Este comportamiento permitió mantener la continuidad de los servicios institucionales, reduciendo considerablemente el tiempo de indisponibilidad del servicio de Internet.

3.6.4 Comparación de indicadores antes y después de la implementación

A partir de las pruebas realizadas, se elaboró una comparación general del comportamiento de la infraestructura antes y después de la implementación de la solución.

Cuadro 6 Comparación del desempeño de la red antes y después de la implementación.

Indicador	Antes de la implementación	Después de la implementación
Detección de fallas	Manual	Automática (Zabbix)
Tiempo de recuperación de Internet	1 a 3 horas	1 a 3 minutos
Acceso a la red del establecimiento	Solo presencial	Remoto mediante VPN
Cambio de enlace (failover)	Manual con técnico	Automático en MikroTik
Disponibilidad de servicios (HIS, ARFSIS, eQhali, REFCON, SISMED)	Interrumpida en fallas	Alta continuidad operativa

Fuente. Elaboración propia.

3.6.5 Impacto operativo de la solución implementada

En el análisis general, se evidenció que la solución implementada tiene un impacto directo en la continuidad de los servicios de salud digital del establecimiento.

Sistemas como HIS MINSA, ARFSIS, SIHCE, REFCON, telemedicina, SISMED y otras plataformas institucionales, que anteriormente se veían afectados por caídas de Internet, ahora mantienen una mayor disponibilidad debido a la conmutación automática entre enlaces.

Asimismo, la capacidad de monitoreo remoto permite una reacción más rápida del equipo técnico, reduciendo la dependencia de desplazamientos físicos y mejorando la eficiencia operativa de la gestión de redes.

En términos prácticos, el establecimiento pasa de un modelo reactivo (esperar la falla y enviar técnico) a un modelo proactivo (detección automática y conmutación inmediata).

3.6.6 Evaluación general de resultados

En conjunto, los resultados obtenidos confirman que la integración de Zabbix, WireGuard y el mecanismo de failover en MikroTik constituye una solución viable, estable y replicable para otros establecimientos de la DIRIS Lima Norte.

La solución no solo mejora la visibilidad de la red, sino que también optimiza los tiempos de respuesta ante fallas y garantiza la continuidad de los servicios críticos de salud.

Finalmente, se concluye que la implementación piloto en el Centro de Salud Mental Comunitario Samay cumple con los objetivos planteados,

demostrando mejoras concretas en monitoreo, conectividad y disponibilidad del servicio.

CAPITULO IV: DISCUSION DE RESULTADOS

4.1 Descripción de la implementación

4.1.1 Discusión del objetivo de monitoreo con Zabbix

La implementación del sistema de monitoreo con Zabbix permitió contar con una supervisión continua del estado de los dispositivos de red del establecimiento, especialmente del router MikroTik y de los enlaces de Internet.

En la práctica, esto significó pasar de un escenario donde las caídas de servicio eran reportadas por los usuarios o detectadas de manera manual, a un entorno donde las alertas se generan automáticamente y pueden ser visualizadas desde la sede central.

Este resultado coincide con lo expuesto por Castro González, José Stalyn (2020), quien en su investigación sobre monitoreo en la nube con Zabbix, Grafana y Zammad, concluye que el monitoreo en tiempo real mejora la detección de fallas y reduce el tiempo de respuesta ante incidentes. En su caso, la integración de alertas automáticas permitió incluso la generación de tickets sin intervención humana, lo cual refuerza la utilidad de este tipo de soluciones.

En comparación, en este trabajo no se llegó a una automatización de tickets, pero sí se logró la detección temprana de caídas y la visualización del estado de la red, lo cual ya representa una mejora operativa importante para un entorno institucional de salud.

4.1.2 Discusión del objetivo de la VPN con WireGuard

El segundo objetivo específico consistió en implementar una red privada virtual mediante WireGuard para permitir la interconexión segura entre la sede central y el establecimiento de salud.

Los resultados evidencian que fue posible establecer un canal cifrado que permite el acceso remoto a la red interna del establecimiento, incluyendo el router MikroTik y otros dispositivos de red.

Este resultado mejora el escenario previo, donde el acceso solo era posible de forma presencial, limitando las tareas de soporte y diagnóstico.

En relación con estudios como el de MikroTik en redes institucionales, se confirma que el uso de tecnologías VPN permite mejorar la administración remota y la seguridad de la información, reduciendo la necesidad de desplazamiento físico del personal técnico.

4.1.3 Discusión del objetivo relacionado al failover en MikroTik

El mecanismo de conmutación automática implementado en el router MikroTik permitió mantener la continuidad del servicio de Internet ante la caída del enlace principal GTD, activando automáticamente el enlace de respaldo Movistar.

Este comportamiento es consistente con los resultados obtenidos por Muñoz López, Juan Orlando (2017), quien en su estudio sobre balanceo de carga en redes de salud concluye que la implementación de tecnologías MikroTik mejora la continuidad del servicio y reduce las interrupciones de conectividad en entornos institucionales.

De manera similar, Huane Solorzano, Julio Cesar (2020) señala que la implementación de balanceo de carga y mecanismos de control del tráfico

contribuye a mejorar la estabilidad del servicio de Internet, sobre todo en instituciones públicas donde la demanda de conectividad es constante durante la jornada de trabajo, lo cual permite asegurar una mejor continuidad en la disponibilidad de los servicios digitales.

En este trabajo, el failover permitió que la transición entre enlaces sea prácticamente automática, evitando la interrupción prolongada del servicio, lo cual es crítico en establecimientos de salud donde los sistemas dependen de conectividad permanente.

4.1.4 Discusión del impacto en la disponibilidad del servicio

Uno de los resultados más importantes observados fue la mejora en la disponibilidad de los servicios digitales del establecimiento, como HIS MINSA, ARFSIS, SIHCE, REFCON, telemedicina, SISMED y otras plataformas institucionales.

Antes de la implementación, estos servicios se veían afectados directamente por caídas del enlace principal, generando interrupciones operativas. Después de la implementación, la continuidad del servicio se mantiene gracias al failover y al monitoreo constante.

Esto se relaciona con lo indicado por Huane Solorzano, Julio Cesar (2020), quien resalta que la calidad del servicio de Internet influye directamente en el desempeño de las aplicaciones institucionales y en la eficiencia del personal.

En este sentido, los resultados del presente trabajo confirman que la disponibilidad de servicios no depende únicamente del ancho de banda, sino también de la arquitectura de redundancia y monitoreo implementada. Asimismo, evidencian la importancia de contar con mecanismos que permitan mantener la continuidad de la conectividad ante fallas de los proveedores de Internet.

4.1.5 Discusión general de la solución implementada

En términos generales, la solución integrada de Zabbix, WireGuard y MikroTik permitió transformar el modelo tradicional de gestión de conectividad hacia un enfoque más automatizado, centralizado y proactivo.

Este resultado es comparable con la propuesta de Castro González, José Stalyn (2020), quien plantea que la integración de herramientas open source en entornos virtualizados permite mejorar la gestión de infraestructura y reducir la carga operativa del personal técnico.

Asimismo, estudios como el de Gonzales Rondan, Nicanor Oswaldo (2015) y Muñoz López, Juan Orlando (2017) refuerzan la idea de que las soluciones basadas en MikroTik son viables, escalables y adecuadas para entornos donde se requiere optimizar recursos sin incrementar costos elevados.

En ese sentido, la solución implementada en este trabajo no solo responde a una necesidad puntual del establecimiento, sino que también puede ser replicada en otros establecimientos de la DIRIS Lima Norte con características similares.

4.1.6 Conclusión de la discusión

La discusión de resultados permite afirmar que los objetivos planteados han sido cumplidos de manera satisfactoria.

La solución implementada no solo es funcional a nivel técnico, sino que también es aplicable y escalable a otros establecimientos de la red DIRIS Lima Norte, lo que representa un aporte importante para la gestión de conectividad en el sector salud.

4.2 Evaluación Económica

La evaluación económica de la solución implementada se realizó considerando los costos de los equipos y servicios utilizados durante la implementación, así como los beneficios obtenidos en la administración y supervisión de la red.

La propuesta desarrollada utiliza herramientas de software libre y servicios en la nube de bajo costo, permitiendo implementar la solución sin realizar una inversión elevada en infraestructura o licenciamiento.

Para la implementación se utilizó un router MikroTik modelo RB750Gr3 en el establecimiento de salud del Rímac, con un costo aproximado de 340 soles. Este equipo permitió realizar la administración de la red local, la configuración del firewall y la conexión VPN mediante WireGuard.

Asimismo, se utilizó un servidor virtual privado (VPS) del proveedor Hetzner, con un costo mensual aproximado de 6.49 euros. Este servidor fue utilizado como nodo central de la VPN para permitir la conexión entre la sede de monitoreo y el establecimiento de salud.

Por otro lado, el sistema de monitoreo Zabbix utilizado en la solución es de código abierto y no requiere pago de licencias, ayudando a reducir costos de implementación.

Desde el punto de vista operativo, la solución implementada permitió reducir tiempos de atención y disminuir la necesidad de desplazamientos del personal técnico hacia el establecimiento de salud.

Antes de la implementación, muchas incidencias relacionadas con conectividad requerían revisiones presenciales. Después de la implementación, gran parte de estas incidencias pueden ser verificadas y

atendidas de manera remota mediante la VPN y el monitoreo realizado con Zabbix.

A continuación, se presenta el resumen de costos asociados a la solución implementada:

Cuadro 7 Costos de implementación de la solución.

Componente	Descripción	Costo aproximado
Router MikroTik RB750Gr3	Equipo de red para el establecimiento	S/ 340.00
Servidor VPS (Hetzner)	Nodo central de la VPN (mensual)	€ 6.49 (aprox. ~S/ 26.00)
Software Zabbix	Plataforma de monitoreo	Gratuito

Fuente. Elaboración propia.

Asimismo, la detección rápida de fallas y el mecanismo de failover implementado contribuyen a mantener la continuidad de servicios institucionales como HIS MINSA, SIHCE, REFCON, SISMED, ARFSIS y otros aplicativos institucionales.

En conjunto, la solución implementada representa una alternativa de bajo costo para mejorar la administración de la red y la continuidad de los servicios digitales del establecimiento.

Además, debido al uso de herramientas open source y equipos de costo accesible, la solución puede ser replicada en otros establecimientos de salud de la DIRIS Lima Norte sin requerir cambios importantes en la infraestructura existente.

CAPITULO V: CONCLUSIONES

Respecto al objetivo general, la implementación piloto de la solución de monitoreo y gestión de conectividad en el Centro de Salud Mental Comunitario Samay permitió integrar de forma funcional tres componentes clave: el sistema de monitoreo Zabbix, la red privada virtual con WireGuard y el mecanismo de conmutación automática en MikroTik.

En la práctica, esta integración no solo permitió centralizar la administración de la red desde la sede de la DIRIS Lima Norte, sino que también cambió la forma en que se gestionan las incidencias, pasando de una atención presencial y reactiva a una gestión remota mucho más rápida y controlada.

Se evidenció que la solución es técnicamente viable en entornos reales de salud, donde la continuidad del servicio es crítica, ya que permite mantener operativos los sistemas institucionales incluso ante fallas del proveedor principal de Internet.

Respecto al objetivo específico 1, la implementación de Zabbix permitió tener visibilidad constante del estado del router MikroTik y de los enlaces de comunicación del establecimiento, algo que anteriormente no existía.

Antes de esta implementación, los cortes de Internet eran reportados únicamente por los usuarios finales o detectados cuando ya existía afectación en los sistemas. Con Zabbix, este escenario cambia completamente, ya que ahora la detección es automática y casi inmediata.

Durante las pruebas realizadas, se observó que el sistema genera alertas cuando existe pérdida de conectividad, lo que facilita la intervención del personal técnico sin necesidad de estar físicamente en el establecimiento.

Esto representa una mejora importante en la gestión operativa, ya que reduce el tiempo de identificación del problema y permite actuar con mayor rapidez.

Respecto al objetivo específico 2, la implementación de la VPN con WireGuard permitió establecer un canal de comunicación seguro entre la sede central y el establecimiento de salud, utilizando cifrado moderno y eficiente.

Gracias a esta solución, fue posible acceder de forma remota a los equipos de red del establecimiento, incluyendo el router MikroTik y otros dispositivos de la red interna, sin exponer servicios directamente a Internet.

Este cambio tiene un impacto operativo importante, ya que antes cualquier configuración o diagnóstico requería desplazamiento físico del personal técnico hacia el establecimiento, lo cual implicaba tiempo, coordinación y dependencia del tráfico vehicular.

Con la VPN, estas tareas ahora se pueden realizar desde la sede central, lo que agiliza la atención de incidencias y mejora la capacidad de respuesta del área de soporte.

Respecto al objetivo específico 3, el mecanismo de conmutación automática configurado en el router MikroTik permitió asegurar la continuidad del servicio de Internet mediante el uso de dos enlaces: GTD como principal y Movistar como respaldo.

Durante las pruebas de validación, se comprobó que ante la caída del enlace principal, el sistema realiza el cambio de forma automática hacia el enlace secundario sin intervención manual.

Esto es especialmente importante en entornos como establecimientos de salud, donde una caída de Internet no solo afecta la navegación, sino también el funcionamiento de sistemas críticos como HIS MINSA, SIHCE, REFCON, SISMED, ARFSIS y otros aplicativos institucionales.

La solución reduce significativamente el impacto de las fallas del proveedor principal y permite mantener la operación del establecimiento de forma más estable.

Respecto al objetivo 4, la evaluación general de la solución implementada permitió verificar que los tres componentes trabajan de manera conjunta y coherente dentro del entorno real del establecimiento.

Las pruebas realizadas evidenciaron que el sistema no solo funciona a nivel técnico, sino que también tiene un impacto operativo directo, mejorando la continuidad del servicio y reduciendo la dependencia de atención presencial.

Asimismo, se observó que la solución permite una mejor organización del trabajo del personal técnico, ya que ahora las incidencias pueden ser detectadas, diagnosticadas y en muchos casos resueltas de manera remota.

CAPITULO VI: RECOMENDACIONES

En base a los resultados obtenidos durante la implementación de la solución de monitoreo con Zabbix, la red privada virtual mediante WireGuard y el mecanismo de conmutación automática (failover) en el router MikroTik, se formulan las siguientes recomendaciones orientadas a fortalecer la continuidad, seguridad y escalabilidad del sistema implementado en el Centro de Salud Mental Comunitario Samay.

6.1 Recomendaciones técnicas

Se recomienda mantener actualizados los equipos de red implementados, especialmente el router MikroTik y el servidor de monitoreo Zabbix, a fin de asegurar la estabilidad del sistema y evitar fallas por desactualización o configuración inadecuada.

Asimismo, se sugiere realizar revisiones periódicas de los registros generados por el sistema de monitoreo, lo cual permitirá detectar eventos de red de manera anticipada y mejorar la gestión preventiva de incidencias.

De igual manera, es importante conservar de forma segura la configuración de la VPN WireGuard, incluyendo claves y parámetros de conexión, para garantizar la continuidad del acceso remoto ante posibles fallas o reinstalaciones.

Finalmente, se recomienda reforzar las políticas de seguridad en el router MikroTik mediante la restricción de accesos no autorizados, protegiendo así la infraestructura de red del establecimiento.

6.2 Recomendaciones operativas

Se recomienda fortalecer la capacitación del personal técnico responsable de la administración de la red, con el objetivo de asegurar el correcto uso de las herramientas implementadas y mejorar la capacidad de respuesta ante incidencias.

Asimismo, es importante mantener documentación técnica actualizada que incluya configuraciones, diagramas de red y procedimientos de recuperación, facilitando la gestión del sistema sin dependencia de un solo responsable.

6.3 Recomendaciones de continuidad del servicio

Se recomienda realizar pruebas periódicas del mecanismo de failover entre los enlaces GTD y Movistar, con la finalidad de verificar su correcto funcionamiento ante posibles fallas del enlace principal.

Asimismo, se sugiere establecer un plan de contingencia básico que permita mantener la operatividad del establecimiento ante interrupciones del servicio de Internet.

6.4 Recomendaciones de escalabilidad e integración

Se recomienda evaluar la implementación de esta solución en otros establecimientos de salud de la DIRIS Lima Norte que presenten problemas similares de conectividad.

Del mismo modo, se sugiere considerar la integración futura con sistemas institucionales como telemedicina, historias clínicas electrónicas y plataformas administrativas, con el fin de mejorar la gestión centralizada de la infraestructura tecnológica.

CAPITULO VII: BIBLIOGRAFÍA

Ávila Coello, A. A. (2025). *Red virtual segura («VPN») con Mikrotik en sistemas operativos Windows. Arandu UTIC*, 12(2), 2972–2982.
<https://doi.org/10.69639/arandu.v12i2.1122>

Castro González, J. S. (2020). *Implementación en la nube de un sistema de monitoreo de eventos de fallas para infraestructura de redes y de seguridad informática utilizando la integración de Zabbix, Grafana y Zammad* [Tesis de grado, Escuela Superior Politécnica del Litoral].
<http://www.dspace.espol.edu.ec/handle/123456789/56359>

Dávila Llimpe, Y. T. (2019). *Modelo de gestión de servicios de red con RouterOS MikroTik en la disponibilidad de información de la red de datos de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica* [Tesis de título profesional, Universidad Nacional de Huancavelica].
<https://hdl.handle.net/20.500.14597/2618>

Gonzales Rondan, N. O. (2017). *Diseño e implementación de un proveedor de servicio de internet inalámbrico utilizando la tecnología Routerboard MikroTik, en la ciudad de Recuay en el año 2015* [Tesis de pregrado, Universidad Católica Los Ángeles de Chimbote].
<https://hdl.handle.net/20.500.13032/894>

Huane Solórzano, J. C. (2020). *Propuesta de implementación de balanceo de carga con tecnología MikroTik para la Oficina de Informática de la Dirección Regional de Transportes y Comunicaciones Región Áncash - Huaraz* [Tesis de título profesional, Universidad Católica Los Ángeles de Chimbote].

https://repositorio.uladech.edu.pe/bitstream/handle/20.500.13032/18434/BALANCEO_MIKROTIK_HUANE_SOLORIZANO_JULIO_CESAR.pdf

Luna Huamán, A., & Zeta Núñez, C. D. (2021). *Implementación de redes VPN MikroTik para los servidores entre ciudades de Lima y Pisco* [Tesis de título profesional, Universidad César Vallejo]. <https://hdl.handle.net/20.500.12692/82658>

Mármol Proaño, D. S. (2025). *Implementación de una aplicación de monitoreo de red sobre una red virtualizada* [Trabajo de integración curricular, Escuela Politécnica Nacional]. <https://bibdigital.epn.edu.ec/handle/15000/27127>

Mejía Valverde, L. D. (2023). *Propuesta de implementación de red inalámbrica con tecnología Routerboard MikroTik en centro poblado Unchus – Huaraz; 2021* [Tesis de título profesional, Universidad Católica Los Ángeles de Chimbote]. <https://hdl.handle.net/20.500.13032/31692>

Muñoz López, J. O. (2018). *Implementación de balanceo de carga de internet con MikroTik en la Dirección de Red de Salud Conchucos Sur - Huari; 2017* [Tesis de título profesional, Universidad Católica Los Ángeles de Chimbote]. <https://hdl.handle.net/20.500.13032/1983>

Sánchez Cumanicho, G. J. (2025). *Implementación de firewall en equipo MikroTik para el fortalecimiento de la seguridad en redes con acceso a internet* [Tesis de pregrado, Universidad Estatal Península de Santa Elena]. <https://repositorio.upse.edu.ec/handle/46000/12836>

CAPITULO IX: ANEXOS

En el presente capítulo se incluyen los documentos y evidencias que complementan el desarrollo del trabajo de suficiencia profesional. Estos anexos permiten sustentar la implementación de la solución basada en VPN con WireGuard, así como verificar los resultados obtenidos durante la interconexión entre la sede de Independencia (DIRIS Lima Norte) y el Centro de Salud Mental Comunitario Samay del distrito del Rímac.

Asimismo, se presentan configuraciones reales de los equipos, capturas de pantalla, diagramas de red y resultados de pruebas de conectividad, los cuales respaldan el funcionamiento de la solución implementada y facilitan su posible replicación en otros establecimientos.

Anexo A: Diagrama general de la arquitectura de red implementada

En este anexo se muestra el diagrama general de la arquitectura de red implementada, donde se observa la interconexión entre la sede de Independencia, el servidor VPN en la nube y el Centro de Salud Mental Comunitario Samay del Rímac.

La comunicación entre los nodos se realiza mediante un túnel VPN basado en el protocolo WireGuard, lo que permite el acceso seguro a la red interna del establecimiento (192.168.50.0/24) a través de Internet. Esta arquitectura facilita la administración remota de los equipos de red y el monitoreo centralizado de la conectividad desde la sede principal. Asimismo, permite realizar tareas de verificación, diagnóstico y soporte de manera más eficiente, contribuyendo a una mejor gestión de la infraestructura tecnológica del establecimiento.

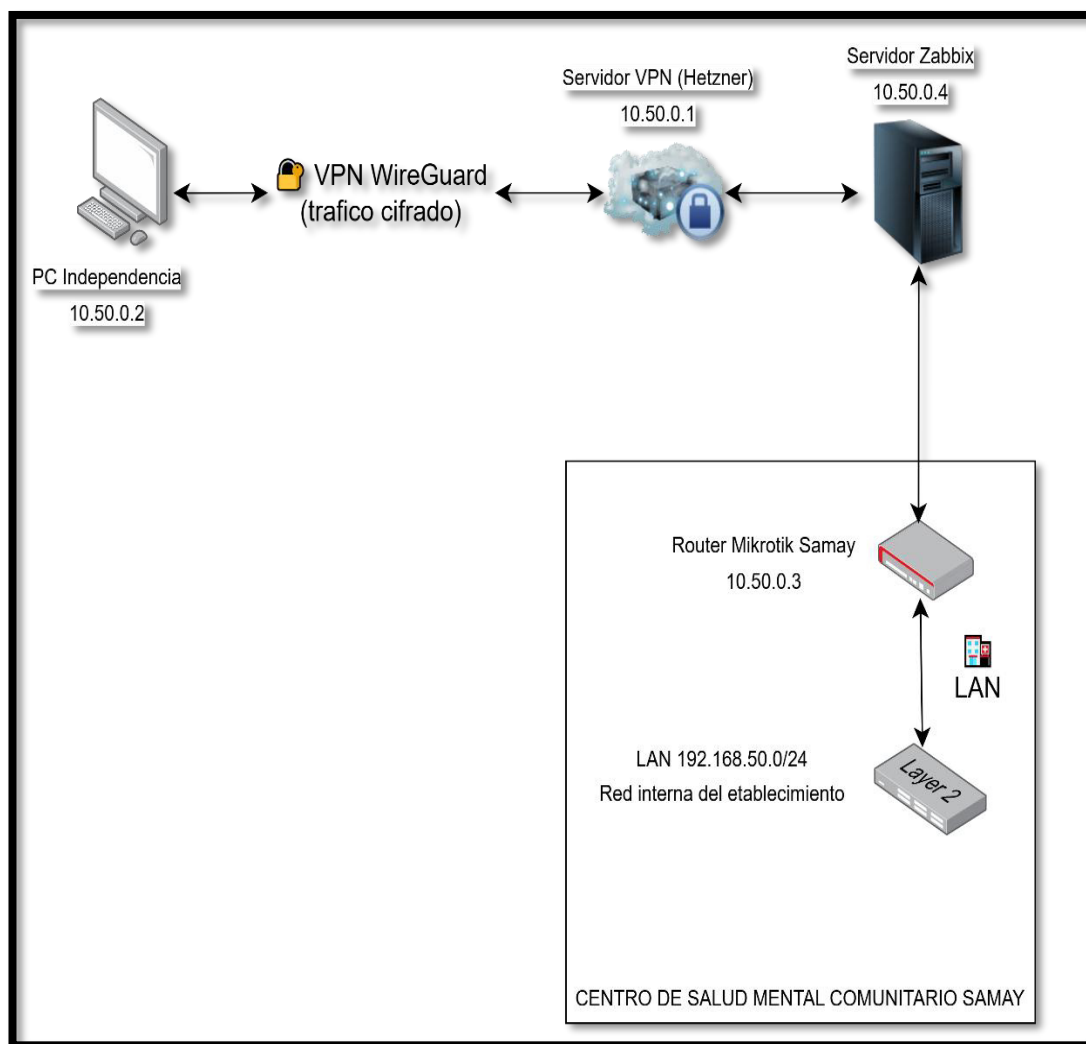
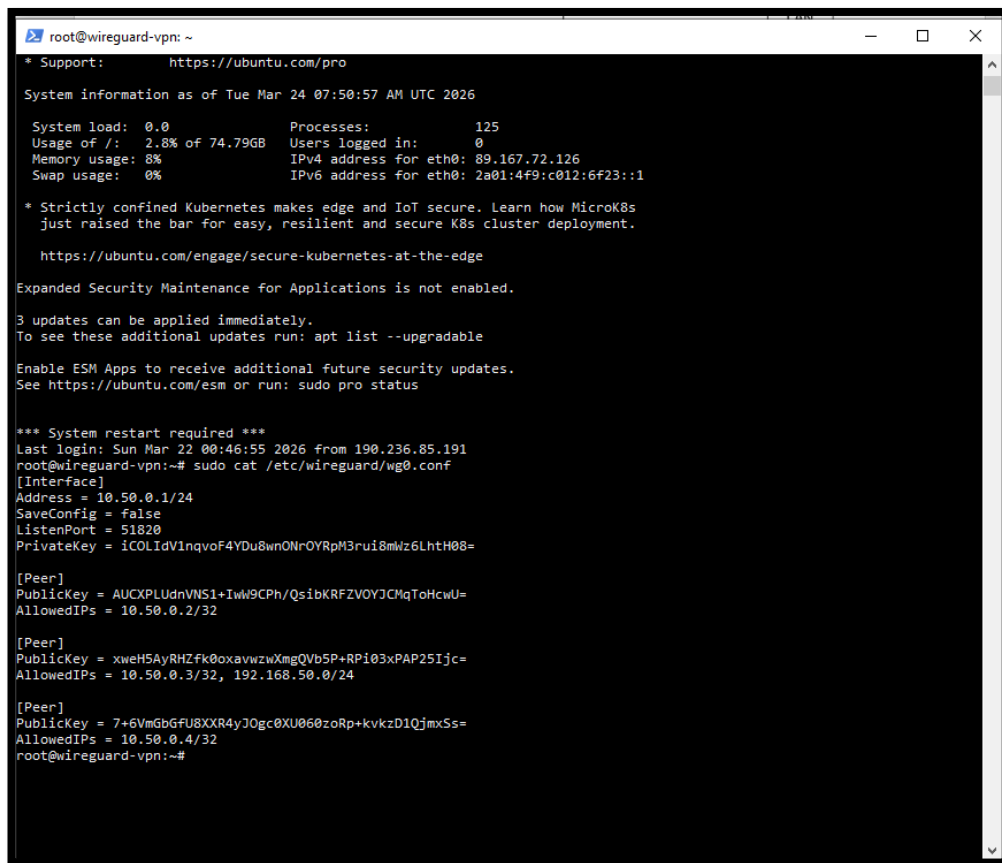


Figura A1 Arquitectura de red de la VPN implementada. Fuente. Elaboración propia

Anexo B: Configuración del servidor VPN (archivo wg0.conf)

Se muestra la estructura del archivo de configuración principal del servidor WireGuard, omitiendo las claves privadas por motivos de seguridad.

```
[Interface]
Address = 10.50.0.1/24
ListenPort = 51820
PrivateKey = <CLAVE_PRIVADA_SERVIDOR>
SaveConfig = false
```



```

root@wireguard-vpn: ~
* Support: https://ubuntu.com/pro

System information as of Tue Mar 24 07:50:57 AM UTC 2026

System load: 0.0          Processes: 125
Usage of /: 2.8% of 74.79GB Users logged in: 0
Memory usage: 8%         IPv4 address for eth0: 89.167.72.126
Swap usage: 0%           IPv6 address for eth0: 2a01:4f9:c012:6f23::1

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
  just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

3 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

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

*** System restart required ***
Last login: Sun Mar 22 00:46:55 2026 from 190.236.85.191
root@wireguard-vpn:~# sudo cat /etc/wireguard/wg0.conf
[Interface]
Address = 10.50.0.1/24
SaveConfig = false
ListenPort = 51820
PrivateKey = iCOLIdV1nqvoF4YDu8wnONrOYRpM3rui8mWz6Lhth08=

[Peer]
PublicKey = AUCXPLUdnVNS1+IwW9CPh/QsibKRFZVOYJCMqToHcwU=
AllowedIPs = 10.50.0.2/32

[Peer]
PublicKey = xweH5AyRHZfk0oxavwzWxmgQVb5P+RPi03xPAP25Ijc=
AllowedIPs = 10.50.0.3/32, 192.168.50.0/24

[Peer]
PublicKey = 7+6VmGbGfU8XXR4yJ0gc0XU060zoRp+kvkzD1QjmxSs=
AllowedIPs = 10.50.0.4/32
root@wireguard-vpn:~#

```

Figura B1 Archivo de configuración del servidor VPN. Fuente. Elaboración propia.

Se muestra la estructura del archivo de configuración del servidor WireGuard (wg0.conf), donde se definen los parámetros de la interfaz, el puerto de escucha y los peers registrados dentro de la red VPN, omitiendo las claves privadas por motivos de seguridad.

El archivo de configuración permite gestionar la autenticación de los clientes mediante claves públicas y privadas, así como definir las direcciones IP asignadas dentro de la red VPN.

Anexo C: Registro de clientes (peers) en el servidor VPN

Se presenta la relación de clientes (peers) registrados en el servidor VPN, indicando la dirección IP asignada dentro de la red privada virtual y las redes asociadas a cada nodo.

Cuadro C1 Clientes registrados en el servidor VPN.

Cliente	Dirección VPN	Red asociada
PC Independencia	10.50.0.2	-
Router MikroTik Rímac	10.50.0.3	192.168.50.0/24
Servidor Zabbix	10.50.0.4	-

Fuente. Elaboración propia.

Cada cliente registrado en el servidor VPN cuenta con un identificador único mediante su clave pública, lo cual permite controlar el acceso y enrutar el tráfico de forma segura dentro de la red privada virtual.

```

root@wireguard-vpn: ~
root@wireguard-vpn:~# wg
interface: wg0
  public key: Jhq8iQK/a7XsYYt/vw8tgQq5eTJAmeYo0v6X5YIe/3c=
  private key: (hidden)
  listening port: 51820

peer: xweH5AyRHZfk0oxavwzWmgQVb5P+RPi03xPAP25Ijc=
  endpoint: 161.132.159.128:51820
  allowed ips: 10.50.0.3/32, 192.168.50.0/24
  latest handshake: 15 seconds ago
  transfer: 14.81 MiB received, 8.01 MiB sent

peer: AUCXPLUdnVNS1+IwW9CPh/QsibKRFZVOYJCHqToHcwU=
  endpoint: 132.157.129.45:7390
  allowed ips: 10.50.0.2/32
  latest handshake: 1 day, 39 minutes, 4 seconds ago
  transfer: 3.07 MiB received, 4.03 MiB sent

peer: 7+6VmGbGfU8XXR4yJOgc0XU060zoRp+kvkzD1QjmxSs=
  endpoint: 132.157.129.45:16262
  allowed ips: 10.50.0.4/32
  latest handshake: 1 day, 39 minutes, 6 seconds ago
  transfer: 5.21 MiB received, 10.46 MiB sent
root@wireguard-vpn:~#

```

Figura C1 Listado de peers en el servidor WireGuard. Fuente. Elaboración propia.

Anexo D: Configuración del router MikroTik (WireGuard)

Se detallan los comandos aplicados en el router MikroTik del establecimiento para la implementación del túnel VPN mediante el protocolo WireGuard, permitiendo la comunicación segura con el servidor VPN central.

Configuración aplicada

```

/interface wireguard add \
name=wireguard-vpn \

```

```
listen-port=51820 \
Private-key="<CLAVE_PRIVADA_MIKROTIK>"

/interface wireguard peers add \
interface=wireguard-vpn \
public-key="<CLAVE_PUBLICA_SERVIDOR>" \
endpoint-address=89.167.72.126 \
endpoint-port=51820 \
allowed-address=10.50.0.0/24 \
persistent-keepalive=25

/ip route add \
dst-address=10.50.0.0/24 \
gateway=wireguard-vpn
```

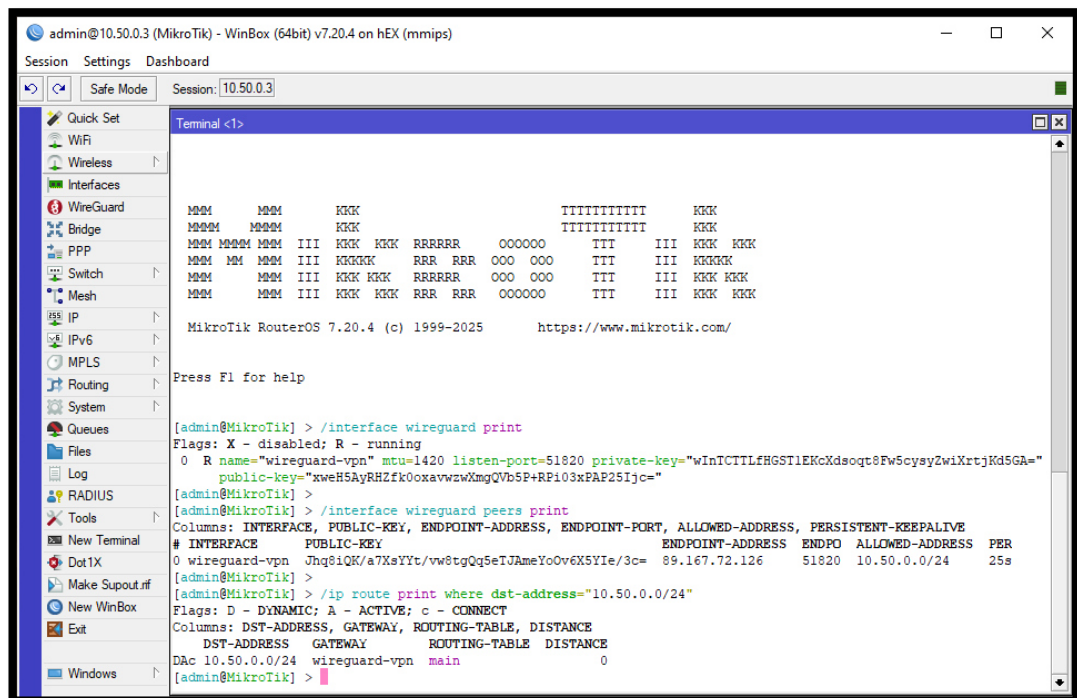


Figura D1 Configuración de WireGuard en el router MikroTik. Fuente. Elaboración propia.

Se muestra la configuración de la interfaz WireGuard, el registro del servidor VPN como peer y la ruta estática establecida para el enrutamiento del tráfico hacia la red privada virtual.

La configuración del router MikroTik permite establecer el túnel VPN hacia el servidor central, habilitando el enrutamiento del tráfico hacia la red 10.50.0.0/24 y garantizando la conectividad con los demás nodos de la VPN.

Anexo E: Configuración del cliente VPN en la PC de Independencia

Se presenta la configuración del cliente WireGuard instalada en la estación de monitoreo ubicada en la sede de Independencia, la cual permite establecer la conexión segura hacia el servidor VPN y acceder a la red interna del establecimiento.

Configuración del cliente

[Interface]

PrivateKey = <CLAVE_PRIVADA_PC>

Address = 10.50.0.2/24

DNS = 8.8.8.8

[Peer]

PublicKey = <CLAVE_PUBLICA_SERVIDOR>

Endpoint = 89.167.72.126:51820

AllowedIPs = 10.50.0.0/24, 192.168.50.0/24

PersistentKeepalive = 25

Se muestra la configuración activa del cliente WireGuard en la estación de monitoreo de la sede de Independencia, evidenciando la conexión establecida con el servidor VPN y el intercambio de tráfico dentro de la red privada virtual.

Se muestra la ejecución del comando ping desde la estación de monitoreo en la sede de Independencia hacia la dirección IP 10.50.0.1, correspondiente al servidor VPN, evidenciando una respuesta exitosa y la correcta conectividad dentro de la red privada virtual.

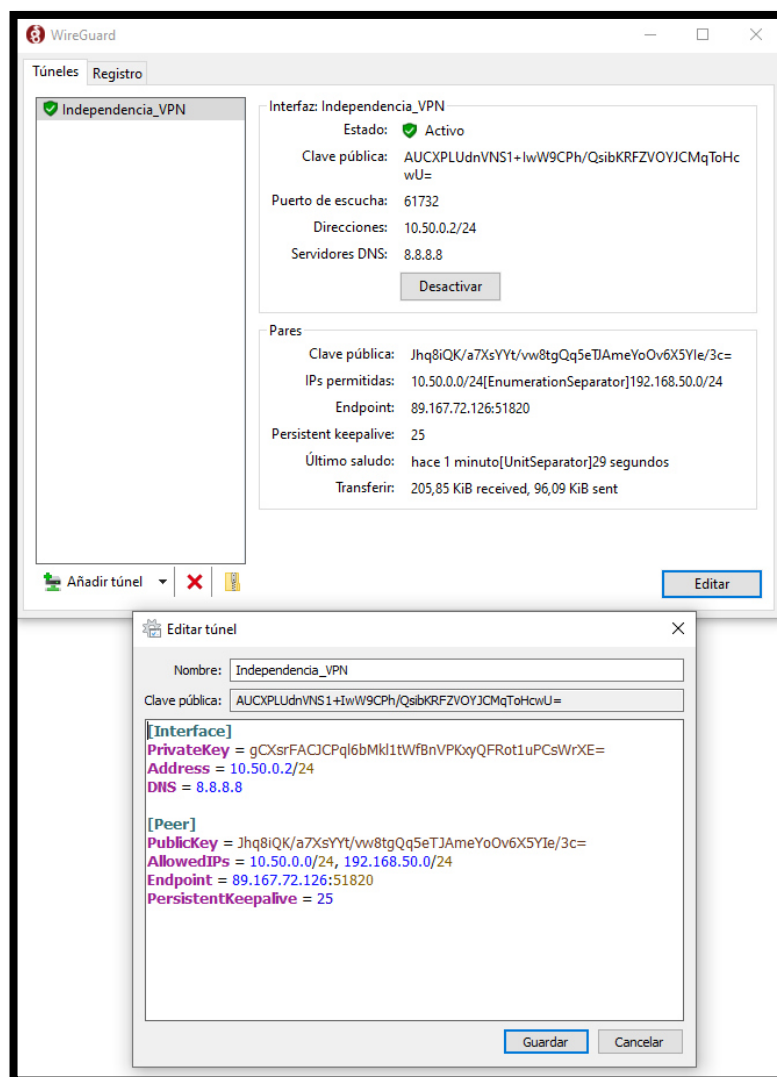


Figura E1 Cliente VPN en la PC de monitoreo. Fuente. Elaboración propia.

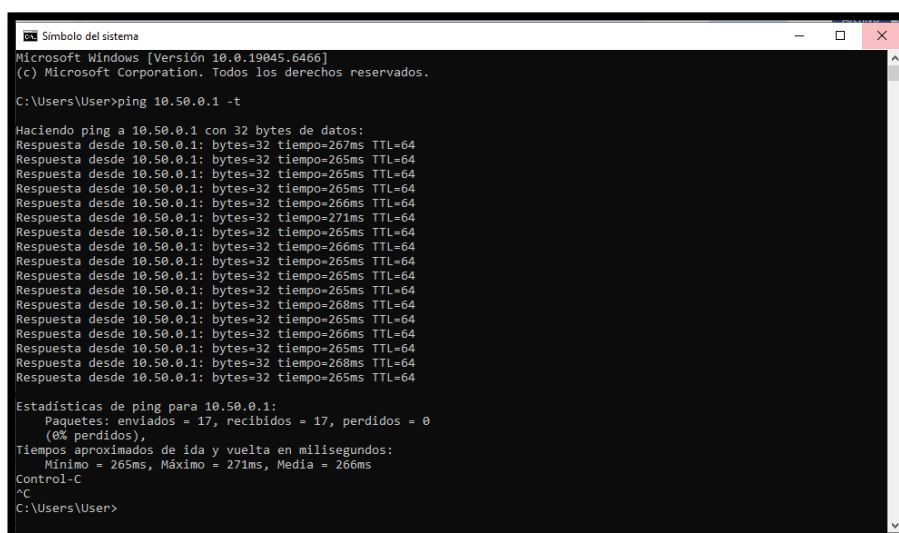


Figura E2 Prueba de conectividad hacia el servidor VPN. Fuente. Elaboración propia.

Anexo F: Resultados de pruebas de conectividad

Se presentan los resultados de las pruebas de conectividad realizadas desde la estación de monitoreo en la sede de Independencia hacia los distintos nodos de la red VPN y la red local del establecimiento, con el fin de verificar la correcta comunicación entre los dispositivos.

Cuadro F1 Resultados de pruebas de conectividad.

Destino	Dirección IP	Resultado
Servidor VPN	10.50.0.1	Correcto
Router MikroTik Rímac	10.50.0.3	Correcto
Gateway LAN	192.168.50.1	Correcto
Equipo interno	192.168.50.191	Correcto

Fuente. Elaboración propia.

Las pruebas realizadas mediante el comando ping evidenciaron una comunicación exitosa sin pérdida de paquetes, confirmando la correcta implementación del túnel VPN y el acceso a la red interna del establecimiento.

```

Microsoft Windows [Versión 10.0.19045.6466]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\User>ping 10.50.0.1

Haciendo ping a 10.50.0.1 con 32 bytes de datos:
Respuesta desde 10.50.0.1: bytes=32 tiempo=266ms TTL=64
Respuesta desde 10.50.0.1: bytes=32 tiempo=265ms TTL=64
Respuesta desde 10.50.0.1: bytes=32 tiempo=265ms TTL=64
Respuesta desde 10.50.0.1: bytes=32 tiempo=265ms TTL=64

Estadísticas de ping para 10.50.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 265ms, Máximo = 266ms, Media = 265ms

C:\Users\User>ping 10.50.0.3

Haciendo ping a 10.50.0.3 con 32 bytes de datos:
Respuesta desde 10.50.0.3: bytes=32 tiempo=461ms TTL=63
Respuesta desde 10.50.0.3: bytes=32 tiempo=485ms TTL=63
Respuesta desde 10.50.0.3: bytes=32 tiempo=460ms TTL=63
Respuesta desde 10.50.0.3: bytes=32 tiempo=460ms TTL=63

Estadísticas de ping para 10.50.0.3:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 460ms, Máximo = 485ms, Media = 466ms

C:\Users\User>ping 192.168.50.1

Haciendo ping a 192.168.50.1 con 32 bytes de datos:
Respuesta desde 192.168.50.1: bytes=32 tiempo=463ms TTL=63
Respuesta desde 192.168.50.1: bytes=32 tiempo=461ms TTL=63
Respuesta desde 192.168.50.1: bytes=32 tiempo=460ms TTL=63
Respuesta desde 192.168.50.1: bytes=32 tiempo=460ms TTL=63

Estadísticas de ping para 192.168.50.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 460ms, Máximo = 463ms, Media = 461ms

C:\Users\User>ping 192.168.50.191

Haciendo ping a 192.168.50.191 con 32 bytes de datos:
Respuesta desde 192.168.50.191: bytes=32 tiempo=460ms TTL=62
Respuesta desde 192.168.50.191: bytes=32 tiempo=460ms TTL=62
Respuesta desde 192.168.50.191: bytes=32 tiempo=460ms TTL=62
Respuesta desde 192.168.50.191: bytes=32 tiempo=465ms TTL=62

Estadísticas de ping para 192.168.50.191:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 460ms, Máximo = 465ms, Media = 461ms

C:\Users\User>
  
```

Figura F1 Pruebas de conectividad mediante ping. Fuente. Elaboración propia.

Se muestran las pruebas de conectividad realizadas desde la estación de monitoreo en la sede de Independencia hacia los distintos nodos de la red VPN y la red local del establecimiento, evidenciando respuestas exitosas y ausencia de pérdida de paquetes.

Anexo G: Capturas de monitoreo en Zabbix

Se presentan capturas del sistema Zabbix que evidencian el monitoreo del router MikroTik del establecimiento dentro de la red VPN.

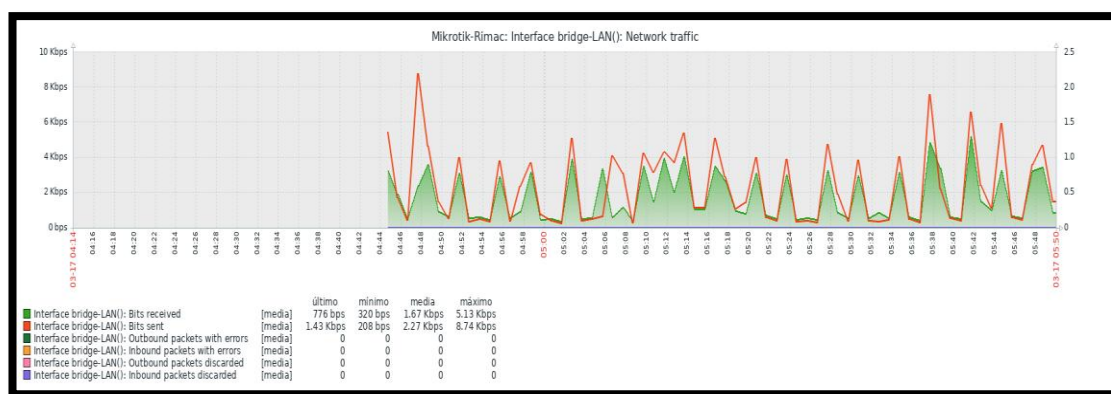


Figura G1 Tráfico de red en la interfaz LAN del router MikroTik. Fuente. Elaboración propia.

Se presenta el tráfico de red en la interfaz bridge-LAN del router MikroTik, correspondiente a la red interna del establecimiento, mostrando el intercambio de datos entre los dispositivos conectados.

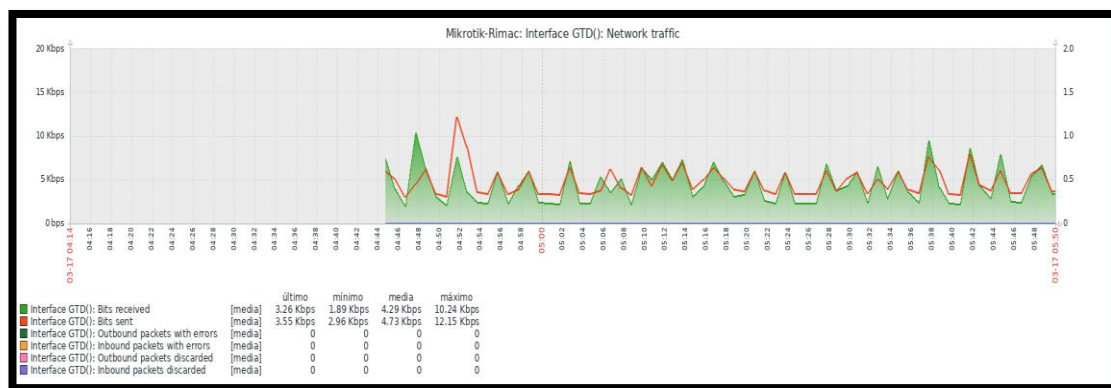


Figura G2 Tráfico de red en la interfaz GTD del router MikroTik. Fuente. Elaboración propia.

Se muestra el tráfico de red en la interfaz GTD del router MikroTik, correspondiente al enlace principal de Internet, evidenciando el comportamiento del flujo de datos entrante y saliente.

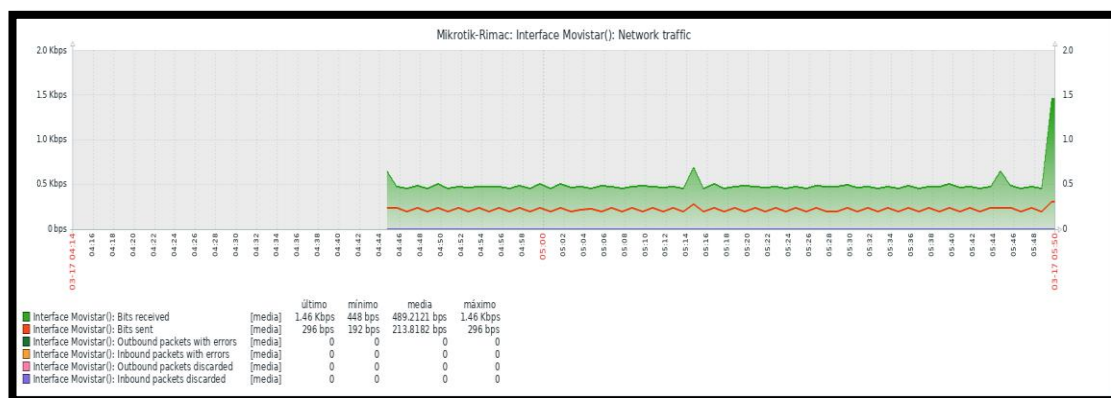


Figura G3 Tráfico de red en la interfaz Movistar del router MikroTik.
Fuente. Elaboración propia.

Se observa el tráfico de red en la interfaz Movistar del router MikroTik, correspondiente al enlace secundario de conectividad, evidenciando el flujo de datos en dicha interfaz.

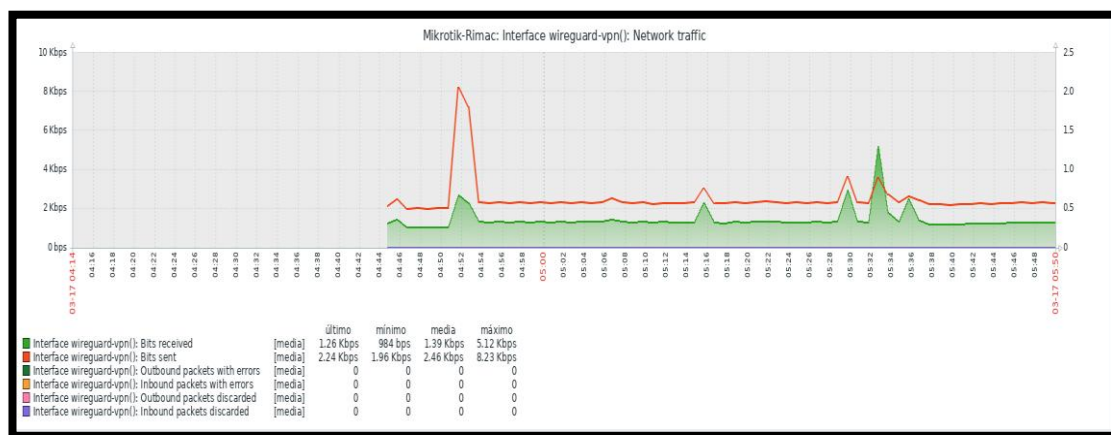


Figura G4 Tráfico de red en la interfaz WireGuard del router MikroTik.
Fuente. Elaboración propia.

Se muestra el tráfico de red en la interfaz WireGuard del router MikroTik, evidenciando el intercambio de datos a través del túnel VPN establecido con el servidor central, lo que confirma el funcionamiento de la comunicación cifrada.

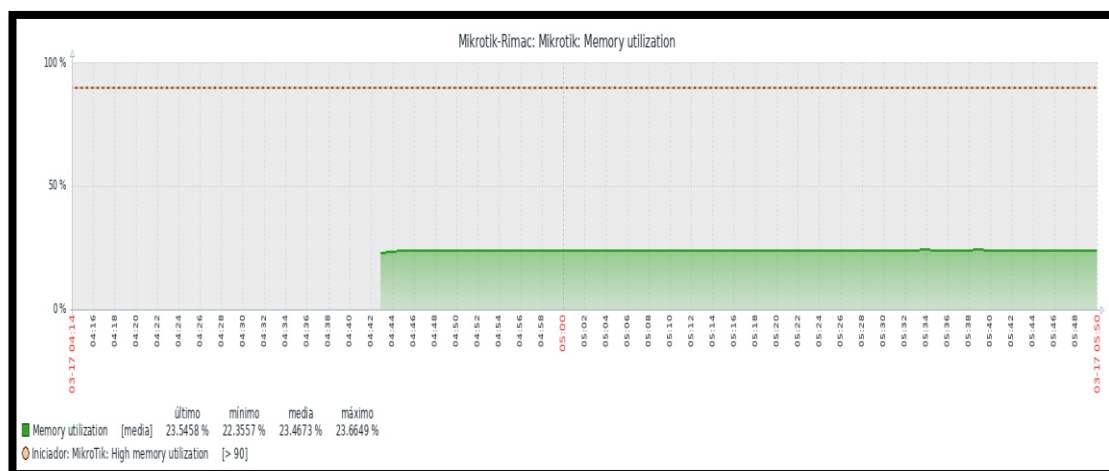


Figura G5 Uso de memoria del router MikroTik en Zabbix. Fuente. Elaboración propia.

Se muestra el monitoreo del uso de memoria del router MikroTik mediante Zabbix, permitiendo evaluar el consumo de recursos y el rendimiento del dispositivo dentro de la red.

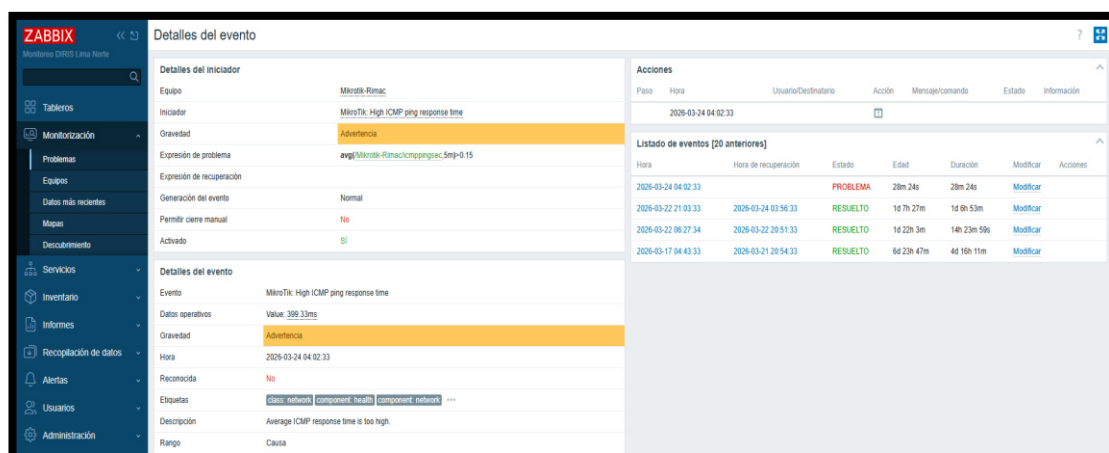


Figura G6 Panel de alertas en Zabbix. Fuente. Elaboración propia.

Se muestra el panel de alertas del sistema Zabbix, donde se visualizan los eventos detectados en la infraestructura monitoreada, permitiendo identificar incidentes, estados críticos o la ausencia de fallas dentro de la red.

En la captura se observan alertas generadas por el sistema, permitiendo identificar eventos y tomar acciones correctivas oportunas.

Anexo H: Costos de implementación

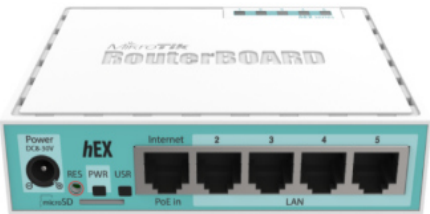
Se detallan los costos asociados a la implementación de la solución de red basada en VPN, considerando los recursos utilizados tanto en hardware como en servicios en la nube y software de monitoreo.

Cuadro H1 Costos de implementación.

Recurso	Costo
MikroTik RB750Gr3	S/ 340
VPS Hetzner	€ 6.49 (~S/ 26.00) mensual
Zabbix	Gratuito

Fuente. Elaboración propia.

La implementación se caracteriza por ser de bajo costo, aprovechando software libre como Zabbix y servicios de infraestructura en la nube con tarifas accesibles, lo que la convierte en una solución viable para entornos con limitaciones presupuestarias.



MikroTik

Mikrotik RB750GR3 Router de 5 Puertos Gigabit 256MB RAM

S/340.00

Router RB750GR3 Mikrotik 5 Puertos

- Producto: Router Board
- Marca: Mikrotik
- Modelo: RB750GR3

Figura H1 Precio referencial del router MikroTik RB750Gr3. Fuente. Página web del proveedor.

Se muestra el costo referencial del router MikroTik utilizado en la implementación, obtenido de una fuente comercial.

The screenshot displays the Hetzner VPS configuration page. The configuration options are as follows:

- ☒ CPX 22 (Type)
- ☒ Helsinki (Location)
- ☒ Ubuntu 24.04 (Image)
- ☒ IPv4, IPv6 (Networking)
- ☒ SSH keys
- ☒ Volumes
- ☐ Firewalls
- ☐ Backups
- ☐ Placement groups
- ☐ Labels

Below the configuration options, the quantity is set to 1 Server. The pricing table is as follows:

Configuration	Price
1 SERVER	€5.99 /mo
1 IPV4	€0.50 /mo
TOTAL	€6.49 /mo

A red button labeled "Create & Buy now" is located at the bottom of the configuration panel.

Figura H2 Plan de servidor VPS utilizado en la implementación. Fuente. Información obtenida de la página web de Hetzner.

Se muestra el costo del servidor VPS contratado en la plataforma Hetzner, utilizado como nodo central para la implementación de la VPN, evidenciando el precio mensual del servicio.

Anexo I: Configuración de firewall en MikroTik

Se presenta la regla de firewall implementada en el router MikroTik del establecimiento, la cual permite el tráfico proveniente de la red VPN hacia la red local interna.

```
/ip firewall filter add chain=forward src-address=10.50.0.0/24 dst-  
address=192.168.50.0/24 action=accept
```

Esta regla permite habilitar la comunicación desde la red VPN (10.50.0.0/24) hacia la red local del establecimiento (192.168.50.0/24), asegurando que los dispositivos conectados a la VPN puedan acceder a los recursos internos de la red LAN.

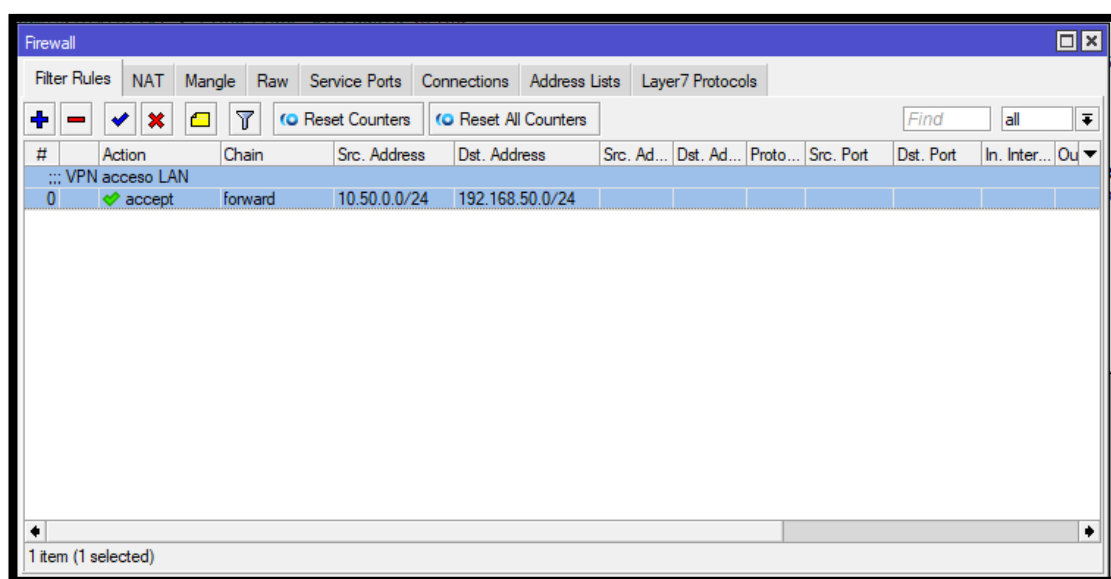


Figura 11 Reglas de firewall implementadas en MikroTik. Fuente. Elaboración propia.

Se muestra la configuración de reglas de firewall en el router MikroTik, donde se permite el tráfico desde la red VPN hacia la red interna del establecimiento, garantizando el acceso remoto seguro.

Anexo J: Diagramas de flujo de monitoreo remoto en Zabbix

Se presenta el flujo de monitoreo implementado desde la sede de Independencia, donde el servidor Zabbix realiza la supervisión de los dispositivos ubicados en la red interna del establecimiento de salud a través de la red privada virtual (VPN) basada en WireGuard.

El proceso inicia con el envío de solicitudes de monitoreo desde el servidor Zabbix, utilizando protocolos como ICMP (ping) y SNMP, las cuales son encapsuladas y transmitidas de forma cifrada a través del túnel VPN hacia el servidor central.

Posteriormente, el tráfico es dirigido hacia el router MikroTik del establecimiento, el cual permite el acceso a la red local (192.168.50.0/24), donde se encuentran los dispositivos monitoreados.

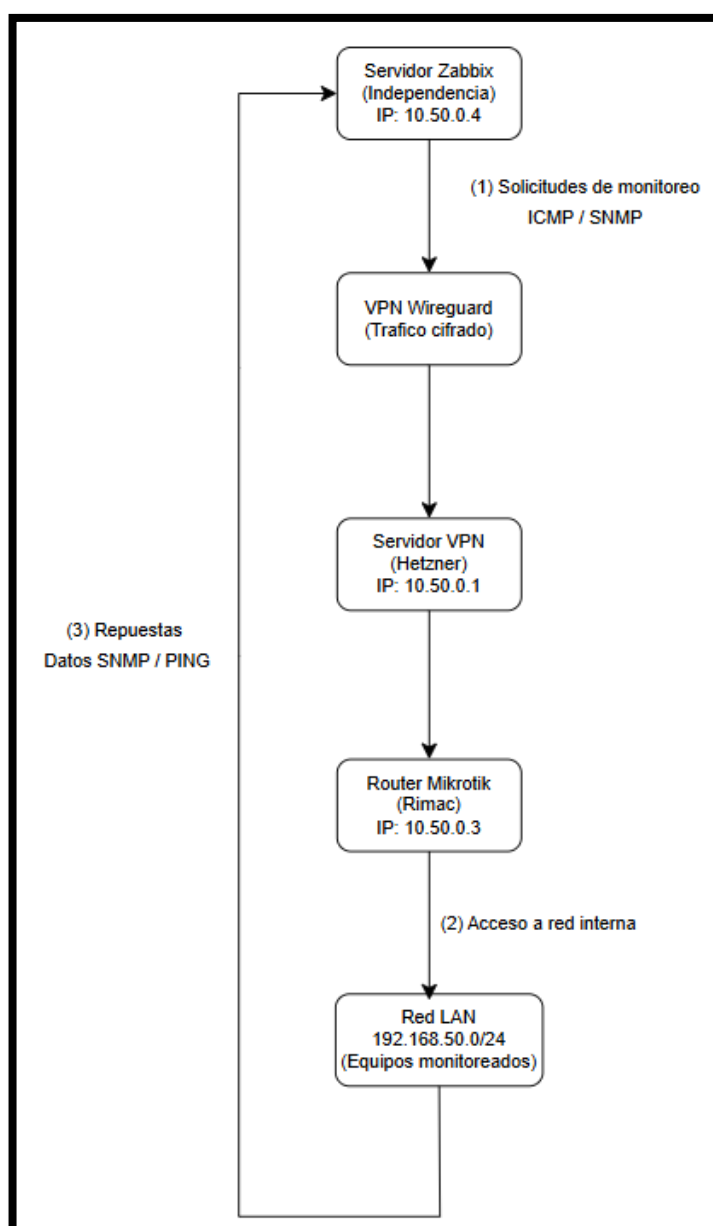


Figura J1 Flujo de monitoreo mediante VPN. Fuente. Elaboración propia.

Finalmente, los equipos responden a las solicitudes generadas, enviando la información de retorno mediante el mismo túnel VPN hacia el servidor Zabbix, permitiendo así la visualización del estado de la red en tiempo real.

Este flujo garantiza una supervisión remota segura, eficiente y sin necesidad de exponer los servicios de la red interna a Internet.

Se muestra el flujo de monitoreo desde el servidor Zabbix hacia los dispositivos de la red local del establecimiento a través de la VPN, incluyendo el envío de solicitudes mediante protocolos ICMP y SNMP, así como la recepción de respuestas desde los equipos monitoreados.

Este modelo permite una gestión centralizada de la infraestructura, facilitando la detección oportuna de fallas y la toma de decisiones.

Anexo K: Capturas de sistemas usados en el Centro de Salud Samay

Se presentan capturas de los principales sistemas informáticos utilizados en el Centro de Salud Mental Comunitario Samay, los cuales operan dentro de la red local del establecimiento.

Estos sistemas son fundamentales para la atención de pacientes y la gestión administrativa, incluyendo módulos de farmacia, admisión, estadística y seguros.

Las capturas permiten evidenciar la operatividad de los sistemas dentro de la red interna, los cuales son accesibles de manera remota a través de la VPN implementada.

Con el fin de proteger la confidencialidad de la información, se han omitido o anonimizado datos sensibles en las imágenes presentadas.

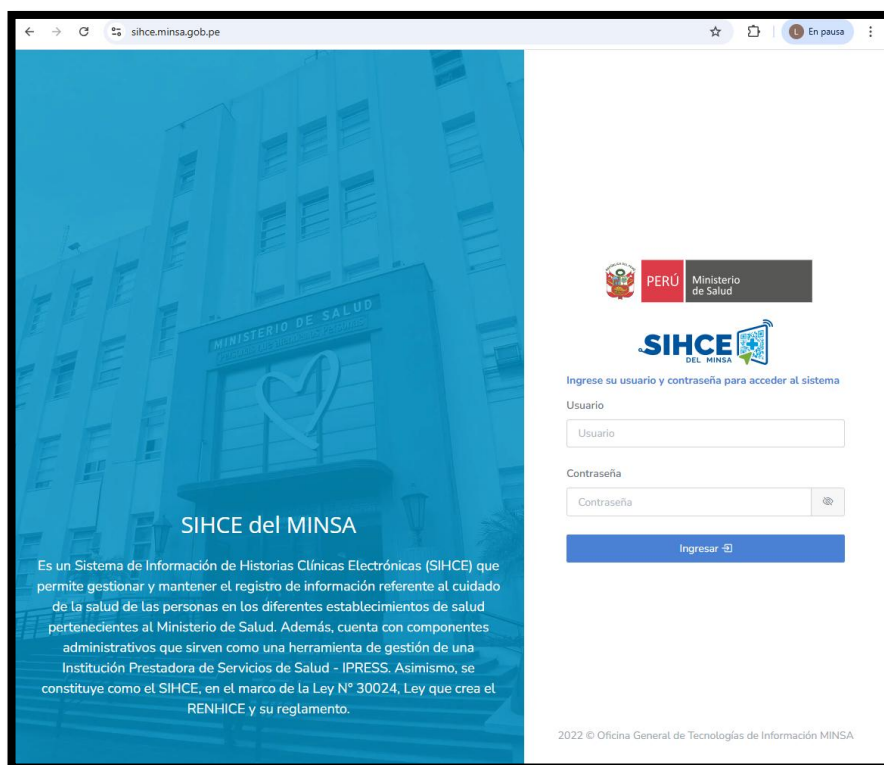


Figura K1 Sistema SIHCE – Registro de pacientes. Fuente. Plataforma SIHCE del Ministerio de Salud (MINSA).

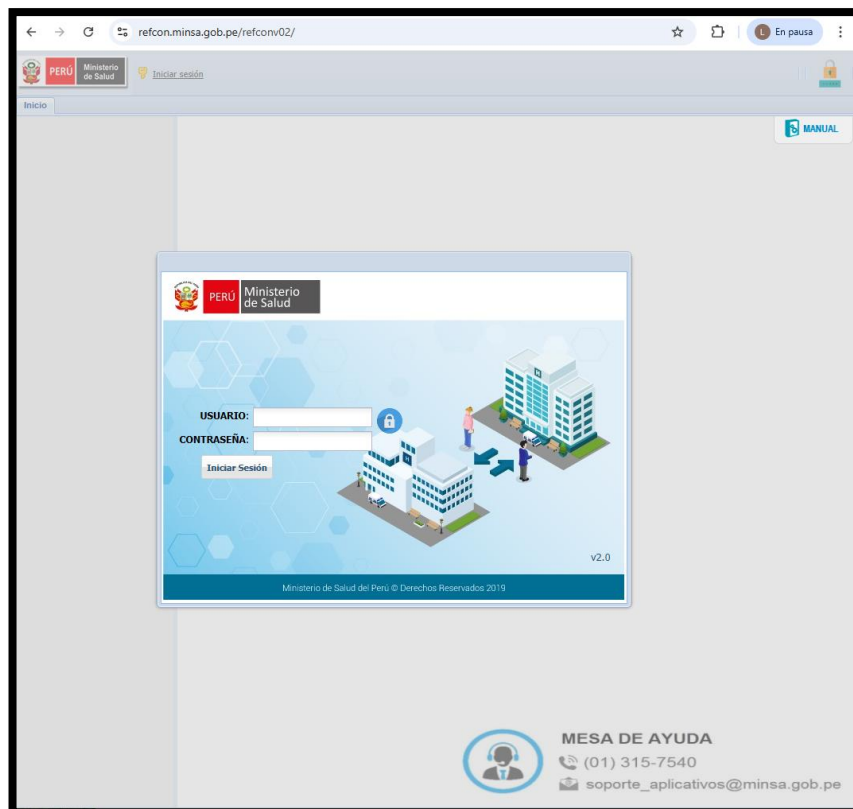


Figura K2 Sistema de referencias médicas. Fuente. Plataforma REFCON del Ministerio de Salud (MINSA).

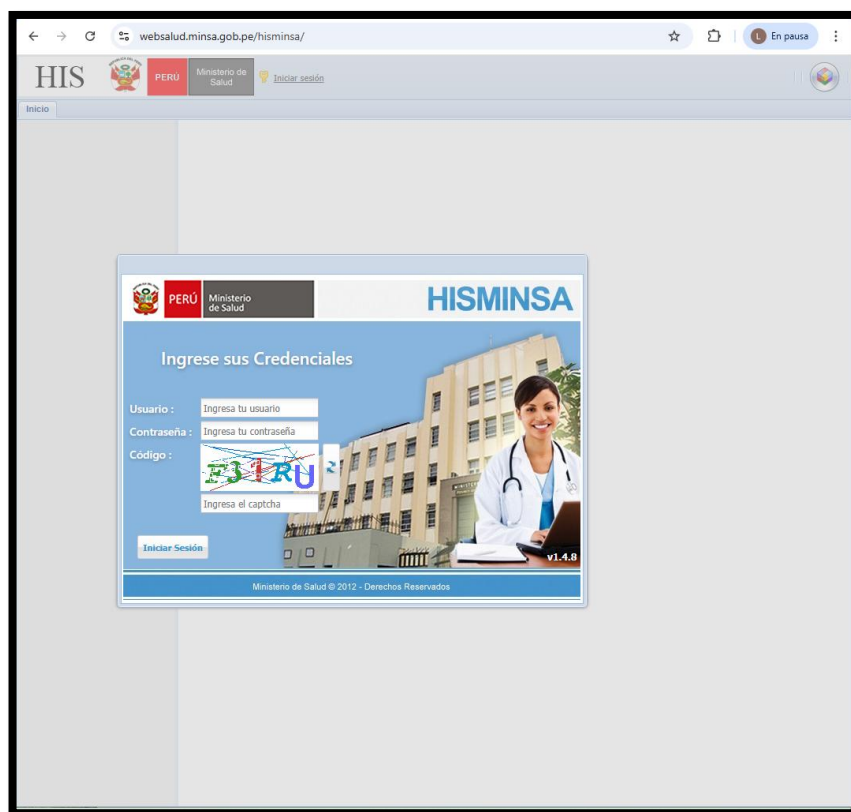


Figura K3 Sistema HISMINSA – Registro estadístico. Fuente. Plataforma HISMINSA del Ministerio de Salud (MINSA).

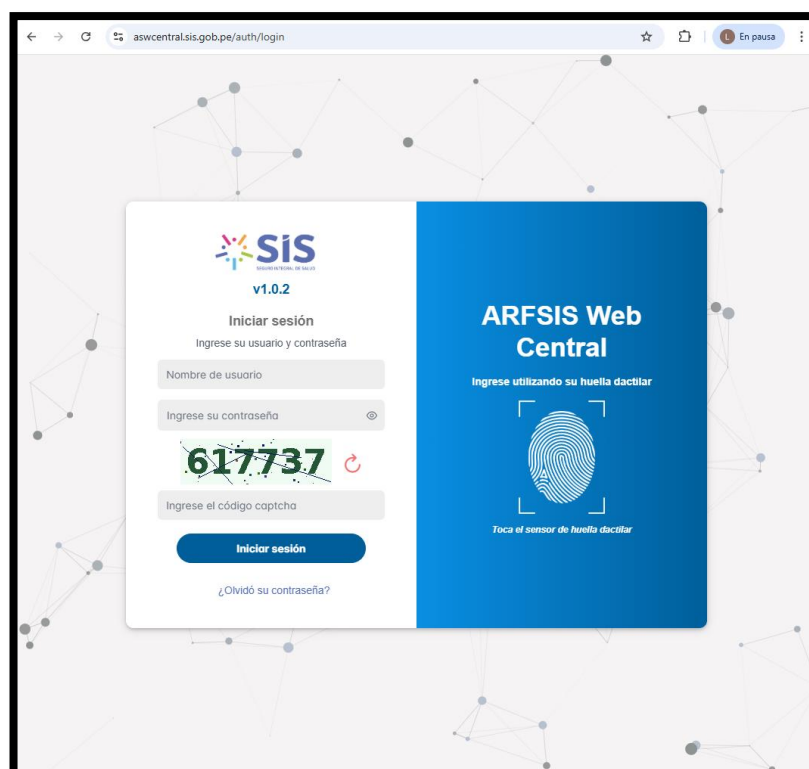


Figura K4 Sistema ARFSIS Web – Validación de seguros. Fuente. Plataforma ARFSIS Web del Seguro Integral de Salud (SIS).



sgd.dirisln.gob.pe/sgd/login.do

Sistema de Gestión Documental

Usuario

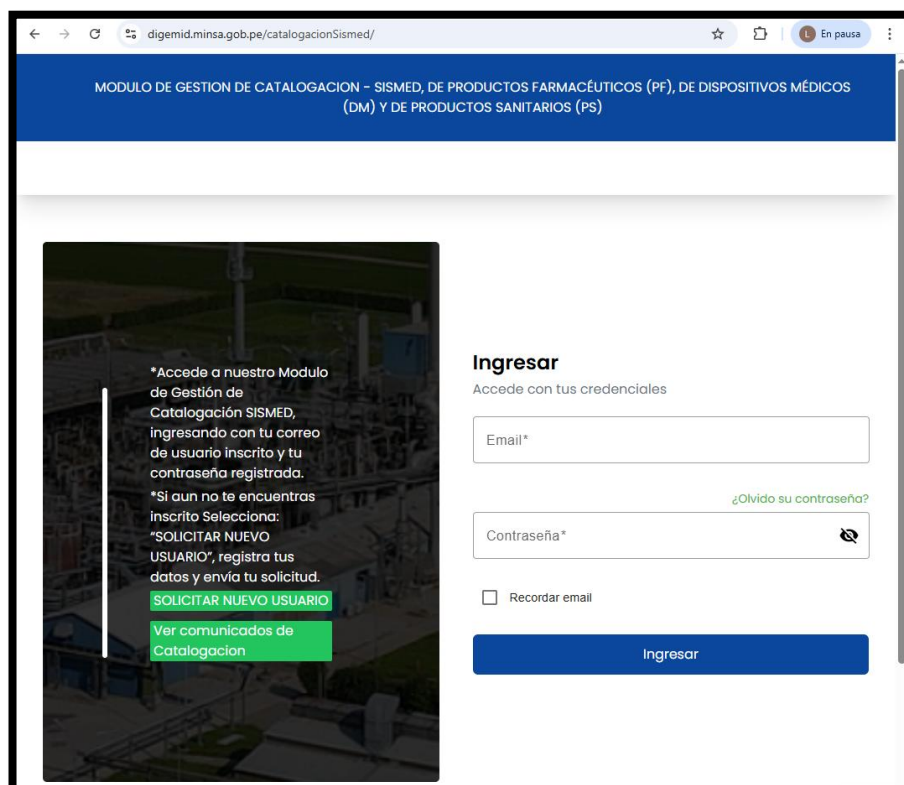
Contraseña

Dependencia

[Ingresar](#)

[Requisitos de sistema](#) [Instructivos](#) [Cambiar contraseña](#)

Figura K5 Sistema de Gestión Documentario. Fuente. Plataforma SGD de la Dirección de Redes Integradas de Salud Lima Norte (DIRIS LN).



digemid.minsa.gob.pe/catalogacionSismed/

MODULO DE GESTION DE CATALOGACION - SISMED, DE PRODUCTOS FARMACÉUTICOS (PF), DE DISPOSITIVOS MÉDICOS (DM) Y DE PRODUCTOS SANITARIOS (PS)

Ingresar
Accede con tus credenciales

Email*

Contraseña*

[¿Olvido su contraseña?](#)

☐ Recordar email

[Ingresar](#)

*Accede a nuestro Modulo de Gestión de Catalogación SISMED, ingresando con tu correo de usuario inscrito y tu contraseña registrada.

*Si aun no te encuentras inscrito selecciona: "SOLICITAR NUEVO USUARIO", registra tus datos y envía tu solicitud.

[SOLICITAR NUEVO USUARIO](#)

[Ver comunicados de Catalogacion](#)

Figura K6 Sistema DIGEMID – Módulo de farmacia. Fuente. Plataforma de catalogación SISMED de DIGEMID (MINSA).

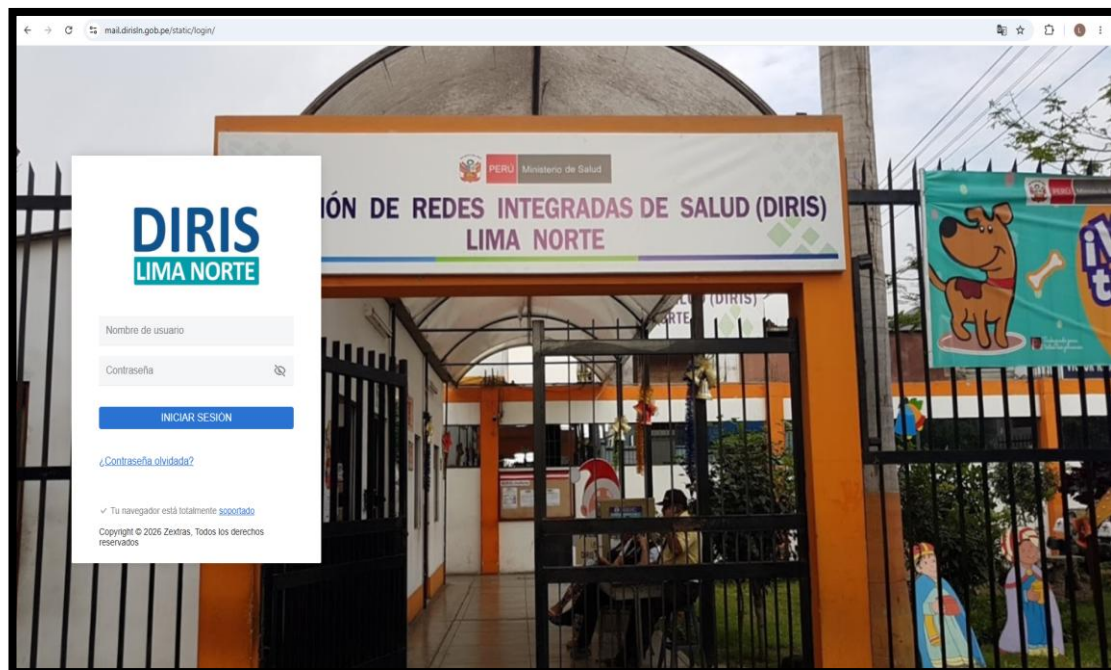


Figura K7 Correo institucional Zimbra. Fuente. Sistema de correo institucional Zimbra de la DIRIS Lima Norte.

Estos sistemas son accesibles a través de la red VPN, permitiendo su supervisión y validación remota desde la sede de Independencia.

Anexo L: Plan de contingencia de conectividad

Se establece el presente plan de contingencia con el objetivo de definir las acciones a seguir ante eventos de interrupción en la conectividad de red, tales como la caída del servicio de internet o la desconexión del túnel VPN.

Este procedimiento permite garantizar la continuidad operativa de los sistemas informáticos del establecimiento, así como una respuesta rápida ante incidencias que afecten la comunicación entre la sede de Independencia y el Centro de Salud Mental Comunitario Samay.

1. Verificación de conectividad a Internet

Se realizan pruebas básicas de conectividad con el fin de validar el acceso a Internet:

a) Ejecución del comando:

ping 8.8.8.8

b) Verificación del estado del servicio con el proveedor de Internet

c) Revisión de la conexión física (cableado, ONT y router)

2. Verificación del túnel VPN

Se valida el estado de la conexión VPN mediante:

a) Ejecución del comando:

wg

b) Revisión de los siguientes parámetros:

Último handshake

Transferencia de datos

En caso de detectar fallas, se procede a reiniciar el servicio:

wg-quick down wg0

wg-quick up wg0

3. Verificación del router MikroTik

Se accede al router del establecimiento para validar:

a) Estado de la interfaz WireGuard

b) Reglas de firewall configuradas

c) Rutas de red establecidas

4. Acciones correctivas

En caso de persistir la incidencia, se ejecutan las siguientes acciones:

- a) Reinicio del router MikroTik
- b) Reinicio del servidor VPN
- c) Coordinación con el proveedor de Internet
- d) Escalamiento al área de soporte técnico

5. Registro de la incidencia

Finalmente, se documenta la incidencia considerando:

- a) Fecha y hora del evento
- b) Tipo de falla detectada
- c) Acciones realizadas
- d) Tiempo de solución

```

root@wireguard-vpn: ~
root@wireguard-vpn:~# wg
interface: wg0
  public key: Jhq8iQK/a7XsYYt/vw8tgQq5eTJAmeYoOv6X5YIe/3c=
  private key: (hidden)
  listening port: 51820

peer: AUCXPLUdnVNS1+IwW9CPh/QsibKRFZVOYJCMqToHcwU=
  endpoint: 181.66.139.26:2049
  allowed ips: 10.50.0.2/32
  latest handshake: 48 seconds ago
  transfer: 3.96 MiB received, 9.19 MiB sent

peer: xweH5AyRHZfk0oxavzwXmgQVb5P+RPi03xPAP25Ijc=
  endpoint: 161.132.159.128:51820
  allowed ips: 10.50.0.3/32, 192.168.50.0/24
  latest handshake: 1 minute, 39 seconds ago
  transfer: 27.57 MiB received, 12.53 MiB sent

peer: 7+6VmGbGfU8XXR4yJ0gc0XU060zoRp+kvkzD1QjmxSs=
  endpoint: 181.66.139.26:2048
  allowed ips: 10.50.0.4/32
  latest handshake: 1 minute, 45 seconds ago
  transfer: 8.99 MiB received, 17.99 MiB sent
root@wireguard-vpn:~# wg-quick down wg0
root@wireguard-vpn:~# wg-quick up wg0
[#] ip link delete dev wg0
[#] ip link add wg0 type wireguard
[#] wg setconf wg0 /dev/fd/63
[#] ip -4 address add 10.50.0.1/24 dev wg0
[#] ip link set mtu 1420 up dev wg0
[#] ip -4 route add 192.168.50.0/24 dev wg0
root@wireguard-vpn:~# wg
interface: wg0
  public key: Jhq8iQK/a7XsYYt/vw8tgQq5eTJAmeYoOv6X5YIe/3c=
  private key: (hidden)
  listening port: 51820

peer: AUCXPLUdnVNS1+IwW9CPh/QsibKRFZVOYJCMqToHcwU=
  allowed ips: 10.50.0.2/32

peer: xweH5AyRHZfk0oxavzwXmgQVb5P+RPi03xPAP25Ijc=
  allowed ips: 10.50.0.3/32, 192.168.50.0/24

peer: 7+6VmGbGfU8XXR4yJ0gc0XU060zoRp+kvkzD1QjmxSs=
  allowed ips: 10.50.0.4/32

```

Figura L1 Verificación del estado de la VPN mediante comando wg.
Fuente. Elaboración propia.

Se muestra la verificación del estado de la VPN en el servidor, donde se observan los peers conectados, el último handshake y la transferencia de datos, permitiendo validar el funcionamiento del túnel.

Cuadro L1 Acciones de contingencia.

Evento	Acción
Sin acceso a internet	Verificar proveedor y cableado
VPN caída	Reiniciar servicio WireGuard
Sin acceso a red LAN	Revisar MikroTik y firewall
Falla persistente	Escalar a soporte técnico

Fuente. Elaboración propia.

Anexo M: Logs de WireGuard (servidor)

Se presenta la salida del comando wg ejecutado en el servidor VPN, la cual permite visualizar el estado de los peers configurados, incluyendo información relevante como el último handshake y la cantidad de datos transmitidos.

Esta información es fundamental para verificar el correcto funcionamiento de la VPN y la conectividad entre los diferentes nodos de la red.

```

root@wireguard-vpn: ~
rtt min/avg/max/mdev = 0.029/0.039/0.049/0.010 ms
root@wireguard-vpn:~# wg
interface: wg0
  public key: Jhq8iQK/a7XsYYt/vw8tgQq5eTJAmeYoOv6X5YIe/3c=
  private key: (hidden)
  listening port: 51820

peer: 7+6VmGbGFU8XXR4yJOgc0XU060zoRp+kvkzD1QjmxSs=
  endpoint: 181.66.139.26:2048
  allowed ips: 10.50.0.4/32
  latest handshake: 2 seconds ago
  transfer: 17.23 KiB received, 25.54 KiB sent

peer: xweH5AyRHZfk0oxavwzWxMgQVb5P+RPi03xPAP25Ijc=
  endpoint: 161.132.159.128:51820
  allowed ips: 10.50.0.3/32, 192.168.50.0/24
  latest handshake: 1 minute, 17 seconds ago
  transfer: 15.52 KiB received, 8.06 KiB sent

peer: AUCXPLUdnVNS1+IwW9CPh/QsibKRFZVOYJCMqToHcwU=
  endpoint: 181.66.139.26:2049
  allowed ips: 10.50.0.2/32
  latest handshake: 1 minute, 32 seconds ago
  transfer: 2.09 KiB received, 1.65 KiB sent
root@wireguard-vpn:~#

```

Figura M1 Estado de peers y handshake en el servidor WireGuard. Fuente. Elaboración propia.

Se muestra la salida del comando wg ejecutado en el servidor VPN, donde se visualizan los peers configurados, el último handshake y la transferencia de datos. Esta información confirma la conectividad activa y el correcto funcionamiento del túnel VPN entre los nodos de la red.

Anexo N: Esquema de direccionamiento IP

Se presenta el esquema de direccionamiento IP utilizado en la red privada virtual (VPN), el cual permite identificar los dispositivos que forman parte de la infraestructura implementada.

Este esquema facilita la gestión de la conectividad, así como la identificación de los nodos dentro de la red, garantizando una correcta comunicación entre la sede de Independencia, el servidor VPN y el establecimiento de salud.

Cuadro N1 Esquema de direccionamiento IP.

Dispositivo	Dirección IP
Servidor VPN (Hetzner)	10.50.0.1
PC Independencia	10.50.0.2
Router MikroTik Rímac	10.50.0.3
Servidor Zabbix	10.50.0.4

Fuente. Elaboración propia.

Todas las direcciones IP pertenecen a la red privada 10.50.0.0/24 definida para la VPN.

Cuadro N2 Redes utilizadas.

Red	Descripción
10.50.0.0/24	Red VPN
192.168.50.0/24	Red LAN del establecimiento

Fuente. Elaboración propia.

Anexo O: Cronograma de implementación

Se presenta el cronograma de actividades correspondiente a la implementación de la red privada virtual (VPN), en el cual se detallan las principales etapas desarrolladas durante el periodo de ejecución del proyecto.

Este cronograma permite evidenciar la secuencia de trabajo realizada, desde la fase de análisis hasta la validación de la solución implementada.

Cuadro O1 Cronograma de implementación.

Actividad	Descripción	Fecha
Análisis de la situación inicial	Evaluación de la infraestructura de red del establecimiento	Agosto 2025
Diseño de la solución	Definición de la arquitectura de red y selección de tecnologías	Agosto 2025
Instalación del servidor VPN	Configuración del servidor WireGuard en el VPS	8/9/2025
Configuración de clientes VPN	Generación de claves y parámetros de conexión	8/9/2025
Configuración del router MikroTik	Integración del router a la red VPN	9/9/2025
Implementación de failover	Configuración de conmutación entre enlaces GTD y Movistar	9/9/2025
Pruebas de conectividad	Validación de comunicación entre sede y establecimiento	9/9/2025
Integración con Zabbix	Configuración del monitoreo remoto	Septiembre 2025
Evaluación y validación	Análisis del funcionamiento y resultados obtenidos	Septiembre 2025

Fuente. Elaboración propia.

Anexo P: Evidencia de conexión activa (handshake)

Se presenta la evidencia de conexión activa en la red privada virtual (VPN) mediante la verificación del parámetro latest handshake, el cual indica la

última comunicación establecida entre los peers configurados en el servidor WireGuard.

Este parámetro permite validar que los nodos de la red se encuentran conectados y transmitiendo datos de manera continua. Un handshake reciente (expresado en segundos o minutos) confirma el correcto funcionamiento del túnel VPN y la estabilidad de la conexión entre la sede de Independencia, el servidor VPN y los dispositivos del establecimiento de salud.

```
peer: 7+6VmGbGfU8XXR4yJ0gc0XU060zoRp+kvkzD1QjmxSs=
  endpoint: 181.66.139.26:2048
  allowed ips: 10.50.0.4/32
  latest handshake: 30 seconds ago
  transfer: 465.88 KiB received, 920.09 KiB sent

peer: AUCXPLUdnVNS1+IwW9CPH/QsibKRFZVOYJCMqToHcwJ=
  endpoint: 181.66.139.26:2049
  allowed ips: 10.50.0.2/32
  latest handshake: 56 seconds ago
  transfer: 13.25 KiB received, 4.44 KiB sent

peer: xweH5AyRHZfk0oxavwzWxmgQVb5P+RPi03xPAP25Ijc=
  endpoint: 161.132.159.128:51820
  allowed ips: 10.50.0.3/32, 192.168.50.0/24
  latest handshake: 1 minute, 30 seconds ago
  transfer: 912.65 KiB received, 454.13 KiB sent
```

Figura P1 Evidencia de conexión activa mediante handshake en WireGuard. Fuente. Elaboración propia

Se muestra la salida del comando wg, donde se observa el parámetro latest handshake con tiempos recientes, evidenciando la comunicación activa entre los peers y el correcto funcionamiento de la VPN.

Anexo Q: Alertas generadas en Zabbix

Se presentan las alertas generadas por el sistema de monitoreo Zabbix, las cuales permiten identificar eventos relacionados con la disponibilidad de los dispositivos de red y la conectividad del establecimiento.

Estas alertas son fundamentales para la gestión proactiva de la infraestructura, ya que permiten detectar fallas en tiempo real, como caídas de enlace, pérdida de conectividad o problemas en el rendimiento de los dispositivos monitoreados.

Gracias a la integración del servidor Zabbix dentro de la red VPN, es posible supervisar de manera remota el estado del router MikroTik del establecimiento, generando notificaciones oportunas ante cualquier incidencia.

The screenshot displays the Zabbix alert interface. On the left, the 'Detalles del evento' (Event Details) section shows information for the 'MikroTik: High ICMP ping response time' event. The event is categorized as 'Advertencia' (Warning) with a severity of 'Normal'. The expression of the problem is 'avg(Mikrotik-Rimacicmpingsec.5m)>0.15'. The event was generated on 2026-03-24 at 19:14:33, and the manual close is set to 'No'. The event is activated ('Sí').

Below the event details, the 'Detalles del evento' section shows the event name, data (Value: 492ms), severity (Advertencia), time (2026-03-24 19:14:33), recognition status (No), tags (class: network, component: health, component: network), description (Average ICMP response time is too high), and range (Causa).

On the right, the 'Acciones' (Actions) section shows a table of actions. Below it, the 'Listado de eventos [20 anteriores]' (List of events [20 previous]) table displays a list of recent events with columns for Hora, Hora de recuperación, Estado, Edad, Duración, and Acciones.

Hora	Hora de recuperación	Estado	Edad	Duración	Acciones
2026-03-24 19:14:33		PROBLEMA	8h 15m 19s	8h 15m 19s	Modificar
2026-03-24 19:05:33	2026-03-24 19:12:33	RESUELTO	8h 24m 19s	7m	Modificar
2026-03-24 04:02:33	2026-03-24 19:58:33	RESUELTO	23h 27m 19s	14h 56m	Modificar
2026-03-22 21:03:33	2026-03-24 03:56:33	RESUELTO	2d 6h 26m	1d 6h 53m	Modificar
2026-03-22 06:27:34	2026-03-22 20:51:33	RESUELTO	2d 21h 2m	14h 23m 59s	Modificar
2026-03-17 04:43:33	2026-03-21 20:54:33	RESUELTO	7d 22h 49m	4d 16h 11m	Modificar

Figura Q1 Panel de alertas en Zabbix. Fuente. Elaboración propia.

Se muestra el panel de alertas del sistema Zabbix, donde se visualizan eventos relacionados con el estado del router MikroTik y la conectividad de red, permitiendo una supervisión centralizada y en tiempo real.

Anexo R: Diagrama de red interna del establecimiento

Se presenta el diagrama de la red interna del Centro de Salud Mental Comunitario Samay, correspondiente a la red LAN 192.168.50.0/24, donde se encuentran conectados los distintos equipos y sistemas utilizados en el establecimiento.

Este diagrama permite visualizar la estructura de la red local, incluyendo el router MikroTik como gateway principal, los equipos de usuario, servidores locales y los sistemas informáticos utilizados en las áreas de atención.

La representación de la red interna facilita la comprensión del flujo de datos dentro del establecimiento y su integración con la red VPN implementada.

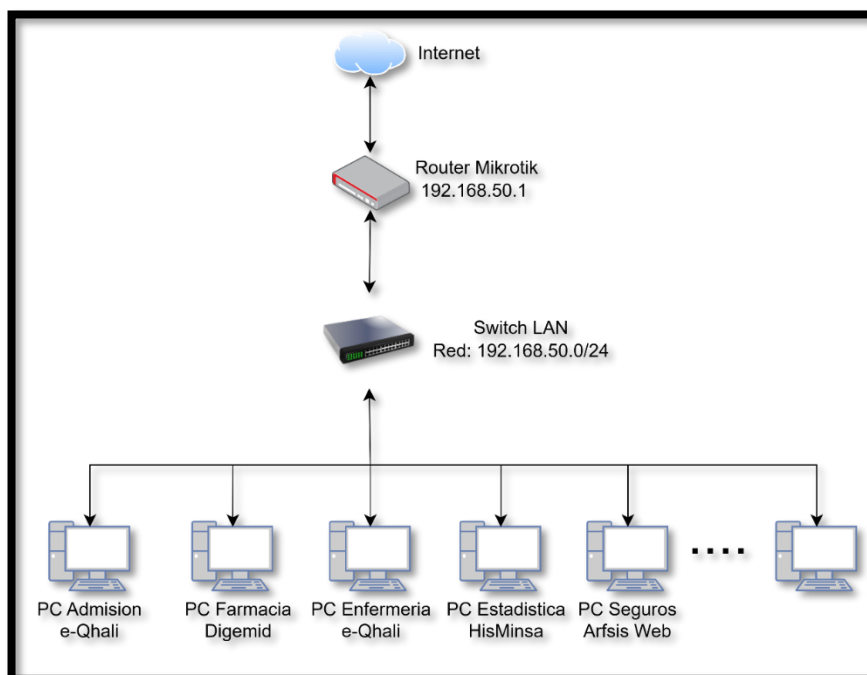


Figura R1 Diagrama de la red LAN del establecimiento (192.168.50.0/24).
Fuente. Elaboración propia.

Se muestra la estructura de la red interna del establecimiento, donde el router MikroTik actúa como gateway y el switch distribuye la conectividad hacia los equipos de las distintas áreas.

Anexo S: Manual básico de operación de la VPN

El presente manual describe los procedimientos básicos para la operación de la red privada virtual (VPN) implementada mediante WireGuard, permitiendo a los usuarios y personal técnico realizar acciones de activación, verificación y reinicio del servicio.

Este documento tiene como finalidad facilitar la gestión operativa de la VPN, asegurando la continuidad del servicio y la rápida atención ante posibles incidencias.

1. Activación de la VPN

En el servidor (Linux)

Ejecutar el siguiente comando:

```
sudo wg-quick up wg0
```

Este comando permite levantar la interfaz de red WireGuard y establecer el túnel VPN.

En la PC (cliente WireGuard)

- a) Abrir la aplicación de WireGuard
- b) Seleccionar el perfil configurado
- c) Hacer clic en "Activate"

2. Verificación de la conexión

2.1 Verificar estado de la VPN

Ejecutar:

```
wg
```

Se debe validar:

Último handshake

Transferencia de datos

2.2 Prueba de conectividad

Ejecutar:

```
ping 10.50.0.1
```

Resultado esperado:

✓ Respuesta exitosa desde el servidor VPN

3. Reinicio del servicio VPN

En caso de fallas en la conexión, reiniciar el servicio:

```
sudo wg-quick down wg0  
sudo wg-quick up wg0
```

Esto permite restablecer la interfaz y reconectar el túnel VPN.

4. Recomendaciones

- a) Verificar la conectividad a Internet antes de activar la VPN
- b) Confirmar que el handshake sea reciente
- c) Revisar la configuración en caso de fallas persistentes

Anexo T: Configuración del servidor Zabbix en la VPN

Se presenta la configuración del servidor Zabbix dentro de la red privada virtual (VPN), mediante el archivo `wg0.conf`, el cual permite su integración a la red segura y la comunicación con los demás nodos.

Esta configuración habilita al servidor Zabbix para realizar monitoreo remoto de los dispositivos ubicados en la red interna del establecimiento.

[Interface]

PrivateKey = <CLAVE_PRIVADA_ZABBIX>

Address = 10.50.0.4/24

DNS = 8.8.8.8

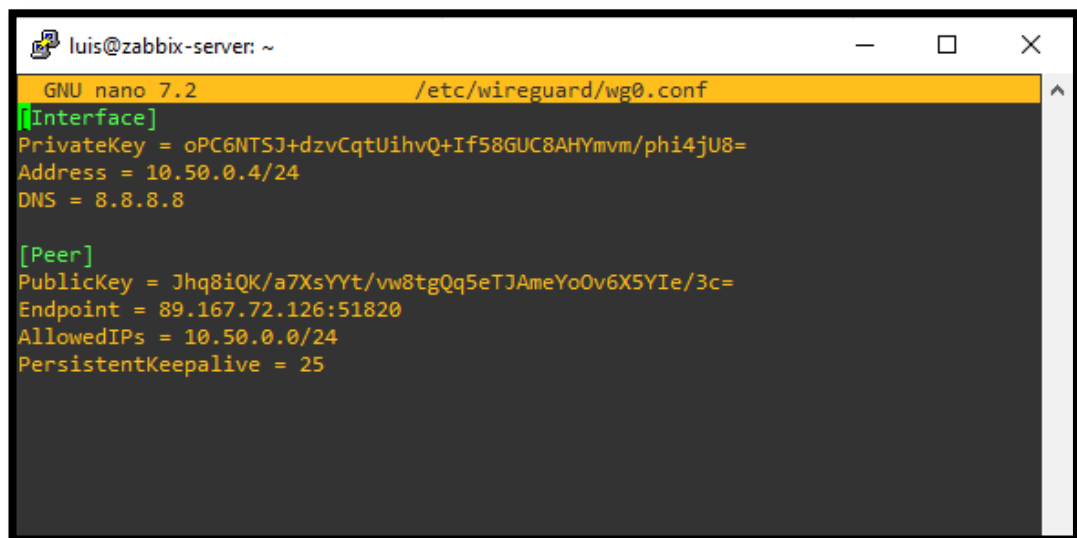
[Peer]

PublicKey = <CLAVE_PUBLICA_SERVIDOR>

Endpoint = 89.167.72.126:51820

AllowedIPs = 10.50.0.0/24

PersistentKeepalive = 25



```

GNU nano 7.2 /etc/wireguard/wg0.conf
[Interface]
PrivateKey = oPC6NTSJ+dzvCqtUihvQ+If58GUC8AHYmvm/phi4jU8=
Address = 10.50.0.4/24
DNS = 8.8.8.8

[Peer]
PublicKey = Jhq8iQK/a7XsYYt/vw8tgQq5eTJAmeYoOv6X5YIe/3c=
Endpoint = 89.167.72.126:51820
AllowedIPs = 10.50.0.0/24
PersistentKeepalive = 25

```

Figura T1 Archivo de configuración wg0.conf del servidor Zabbix. Fuente. Elaboración propia.

Se muestra la configuración del archivo wg0.conf del servidor Zabbix, mediante la cual se establece la conexión con el servidor VPN y se habilita la comunicación dentro de la red privada virtual.

Anexo U: Validación de acceso remoto al router MikroTik

Se presenta la validación del acceso remoto al router MikroTik del establecimiento mediante la red privada virtual (VPN), utilizando la herramienta Winbox.

Gracias a la implementación de la VPN, se logró acceder al dispositivo a través de su dirección IP privada (10.50.0.3), sin necesidad de exponer servicios a Internet mediante direcciones IP públicas.

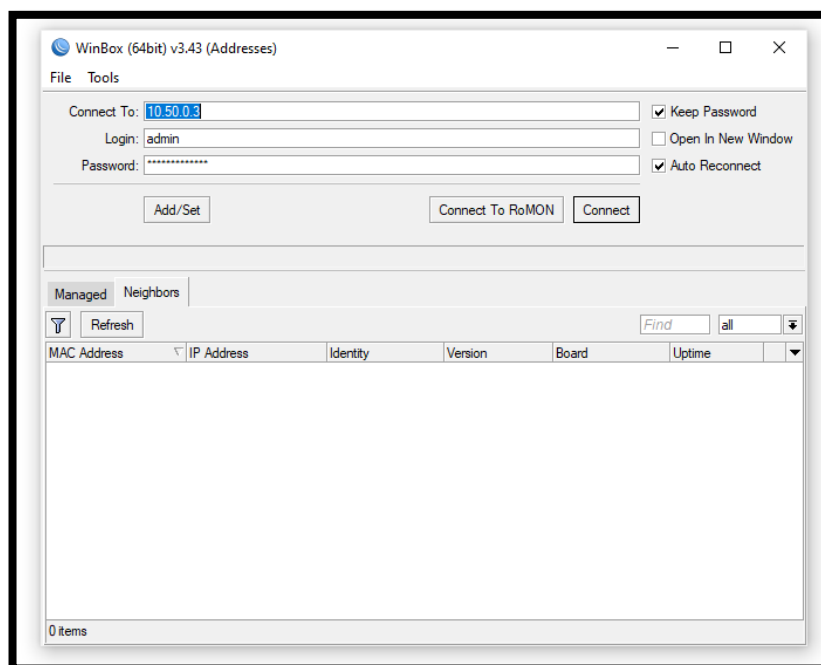


Figura U1 Conexión remota al router MikroTik mediante Winbox a través de la VPN. Fuente. Elaboración propia

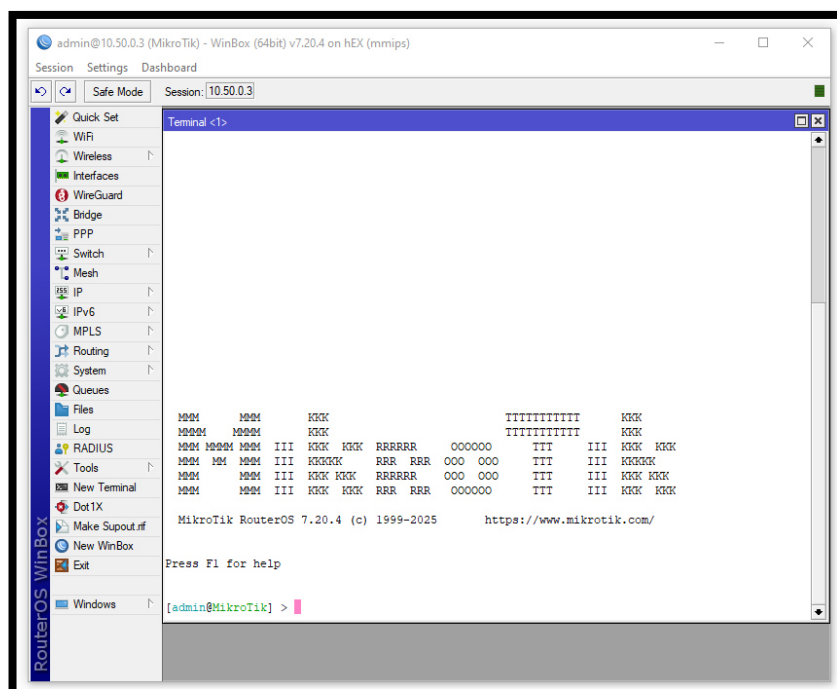


Figura U2 Acceso al entorno de administración del router MikroTik del Rímac. Fuente. Elaboración propia.

Se muestra la conexión remota al router MikroTik utilizando la herramienta Winbox mediante la dirección IP privada 10.50.0.3, evidenciando el acceso a través de la VPN.

Se visualiza la interfaz de administración del router MikroTik, confirmando el acceso remoto exitoso desde la sede de Independencia mediante la red privada virtual.