UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE SQUID-MONITOR PARA LA GESTIÓN DE LA RED DE DATOS DE LA COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA EIRL

Tesis para optar el título profesional

INGENIERO DE SISTEMAS

LINDON ALI CASTILLO FLOREZ

Pucallpa, Perú

2026

UNIVERSIDAD NACIONAL DE UCAYALI
FACULTAD DE INGENIERIA DE SISTEMAS E INGENIERIA CIVIL
ESCUELA PROFESIONAL DE INGENIERA DE SISTEMAS
COMISIÓN DE GRADOS Y TÍTULOS

ACTA DE EVALUACIÓN DE SUSTENTACIÓN DE TESIS N° 029-2026

GRADUANDO : **Bach. CASTILLO FLOREZ LINDON ALI,**

TEMA : **"IMPLEMENTACIÓN DE SQUID-MONITOR PARA LA GESTIÓN DE LA RED DE DATOS DE LA COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA EIRL".**

ASESOR : **Mg.FERRARI FERNANDEZ FREDDY ELAR**

CRITERIOS	PUNTAJE			
	3	2	1	0
I- PRESENTACION				
* MOTIVACION		X		
* TONO DE VOZ		X		
* CALIDAD DE MATERIAL AUDIOVISUAL		X		
II- DESARROLLO DE CONTENIDO				
* SECUENCIA		X		
* DOMINIO DE VOZ		X		
* USO ADECUADO DEL MATERIAL		X		
* VALIDEZ DE LOS HALLAZGOS		X		
III- ABSOLUCION DE PREGUNTAS				
* RESPONDE A LAS PREGUNTAS FORMULADAS POR EL JURADO	X			
IV- APORTE CIENTIFICO Y TECNOLOGICO				
* AL DESARROLLO DE LA COMUNIDAD		X		
* A LA PROFESION		X		

EVALUACION

EXCELENCIA 26 A 30 PUNTOS
UNANIMIDAD 21 A 25 PUNTOS
MAYORIA 16 A 20 PUNTOS
DESAPROBADO 15 A MENOS

CALIFICACION FINAL :
PUNTAJE : 21 / 30

CONCLUSIONES:
APROBADO POR : UNANIMIDAD
DESAPROBADO POR :

JURADO EVALUADOR

Mg.YUPANQUI VILLANUEVA, ARTURO
PRESIDENTE

Mg.AGURTO CHERRE, CESAR AUGUSTO
PRIMER MIEMBRO

M.Sc.BARDALES LINARES, RICHARD PIERO
SEGUNDO MIEMBRO

Dra. RIOS HIDALGO DE CERNA, CLOTILDE
SECRETARIA ACADEMICA

PUCALLPA, 10 DE AGOSTO DEL 2026

ACTA DE APROBACIÓN DE INFORME FINAL DE TESIS

En la Ciudad Universitaria, a los 28 días del mes de MARZO del 2026 siendo horas 10:44:26. Los miembros del Jurado declaran APROBADO POR UNA UNANIMIDAD el PROYECTO DE INVESTIGACIÓN DE TESIS titulado:

"IMPLEMENTACIÓN DE SQUID-MONITOR PARA LA GESTIÓN DE LA RED DE DATOS DE LA COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA EIRL"

Presentado por el Bachiller:

LINDON ALI CASTILLO FLOREZ

De la Escuela Profesional de:

INGENIERÍA DE SISTEMAS

Siendo el Jurado Dictaminador, conformado por:

Presidente	: MG. ARTURO YUPANQUI VILLANUEVA
Primer Miembro	: MG. CESAR AUGUSTO AUGURTO CHERRE
Segundo Miembro	: MG. RICHARD PIERO BARDALES LINARES
Asesor	: MG. FREDDY ELAR FERRARI FERNANDEZ

Para dar fe de este proceso, se le asigna la presente acta y a partir de la presente fecha queda expedito para continuar con los trámites de sustentación de la TESIS.

Pucallpa, 28 de Marzo del 2026.

Mg. ARTURO YUPANQUI VILLANUEVA
PRESIDENTE

Mg. CESAR AUGUSTO AUGURTO CHERRE
MIEMBRO

Mg. RICHARD PIERO BARDALES LINARES
MIEMBRO

UNIVERSIDAD NACIONAL DE UCAYALI

DIRECCIÓN DE PRODUCCIÓN INTELECTUAL

CONSTANCIA

ORIGINALIDAD DE TRABAJO DE INVESTIGACIÓN

Nº **V/739-2025**.

La Dirección de Producción Intelectual de la Universidad Nacional de Ucayali, hace constar por la presente, que el trabajo académico de investigación, titulado:

"**IMPLEMENTACIÓN DE SQUID-MONITOR PARA LA GESTIÓN DE LA RED DE DATOS DE LA COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA EIRL**"

Autor(es)	:	**CASTILLO FLOREZ, LINDON ALI**
Facultad	:	**INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL**
Escuela	:	**ING. DE SISTEMAS**
Asesor(a)	:	**Mg. FERRARI FERNANDEZ FREDDY ELAR**

Presenta un **porcentaje de similitud de 7%,** verificado en el Sistema Antiplagio COMPILATIO,

De acuerdo a los criterios de porcentaje establecidos en el artículo 9 de la DIRECTIVA DE USO DEL SISTEMA ANTIPLAGIO, el cual indica que todo trabajo de investigación no debe superar el 10%. **En tal sentido, se declara, que el presente trabajo de investigación presenta un porcentaje aceptable de similitud,** procediéndose a emitir la presente Constancia de Originalidad de Trabajo de Investigación (COTI) a solicitud del asesor.

En señal de conformidad se firma y sella el presente documento.

Fecha: 04/12/2025

Dr. JOSÉ MANUEL CÁRDENAS BERNAOLA
Director de Producción Intelectual

UNIVERSIDAD NACIONAL DE UCAYALI

DIRECCIÓN DE PRODUCCIÓN INTELECTUAL

AUTORIZACIÓN DE PUBLICACIÓN

Repositorio de la Universidad Nacional de Ucayali

Yo, LINDON ALI CASTILLO FLOREZ

Autor de la tesis titulada : IMPLEMENTACION DE SQUID - MONITOR PARA LA GESTION DE LA RED DE DATOS DE LA COMPAÑIA DE SERVICIOS EN TECNOLOGIA E INFORMATICA EIRL

Sustentada el año 2026

Asesor(a): MG. FREDDY ELAR FERRARI FERNANDEZ

Facultad: INGENIERIA DE SISTEMAS Y DE INGENIERIA CIVIL

Escuela Profesional: INGENIERIA DE SISTEMAS

Autorizo la publicación:

PARCIAL [ ] TOTAL [X]

De mi trabajo de investigación en el Repositorio Institucional de la Universidad Nacional de Ucayali (www.repositorio.unu.edu.pe), bajo los siguientes términos:

Primero: Otorgo a la Universidad Nacional de Ucayali licencia no exclusiva para reproducir, distribuir, comunicar, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público en general mi tesis (incluido el resumen) a través del Repositorio Institucional de la UNU, en formato digital sin modificar su contenido, en el Perú y en el extranjero; por el tiempo y las veces que considere necesario y libre de remuneraciones.

Segundo: Declaro que la tesis es una creación de mi autoría y exclusiva titularidad, por tanto me encuentro facultado a conceder la presente autorización, garantizando que la tesis no infringe derechos de autor de terceras personas, caso contrario, me hago único(a) responsable de investigaciones y observaciones futuras, de acuerdo a lo establecido en el estatuto de la Universidad Nacional de Ucayali, la Superintendencia Nacional de Educación Superior Universitaria y el Ministerio de Educación.

En señal de conformidad firmo la presente autorización.

Fecha: 24/09/26

Email: LINDONALICASTILLO@GMAIL.COM Firma: _____

Teléfono: 978572224 DNI: 46811633

DEDICATORIA

A dios nuestro padre celestial. Por sobre todas las cosas.

A mis padres. Por su apoyo incondicional, hacia ellos tengo un amor y admiración inmenso, por estar siempre a mi lado y por todos los consejos de vida y enseñanzas que forjaron en mí, haciendo que logre realizarme profesionalmente y sea siempre un ciudadano de bien.

A mis hermanos. Por compartir alegrías y estar siempre en las dificultades, logrando superarlas unidos como familia.

Lindon A. Castillo Florez

AGRADECIMIENTO

Un agradecimiento especial a mi asesor de tesis Dr. Freddy Elar Ferrari Fernández, por velar por mi realización profesional para que pueda cumplir una meta más en mi vida.

A mis docentes de la escuela profesional de ingeniería de sistemas por las enseñanzas impartidas en las aulas y consejos profesionales, y a mis compañeros de clases por superar juntos los cursos y hacer llevadera la carrera profesional que escogimos.

Además, un agradecimiento especial a los profesionales que nos dieron la oportunidad de realizar nuestras prácticas y entrar en el mundo laboral Dr. Romel Pinedo Ríos, Dr. Clotilde Ríos, Hidalgo de Cerna, Dr. Jorge Luis Hilario Rivas y Mg. María castillo montero.

Expreso mi más sincero aprecio, estima y consideración personal, deseando que la vida los retribuya de manera multiplicada los esfuerzos que pusieron en mí. Gracias a todos.

RESÚMEN

La presente investigación tuvo como objetivo determinar de qué manera la implementación de Squid-Monitor mejoró la gestión de la red de datos de la Compañía de Servicios en Tecnología e Informática E.I.R.L., empresa que presentaba problemas relacionados con la lentitud en el acceso a Internet, ausencia de mecanismos de control del tráfico de red, escasa supervisión de las conexiones y falta de políticas para restringir el acceso a sitios web no autorizados, situación que afectaba el desempeño de los procesos organizacionales y la satisfacción de los usuarios. La investigación fue de tipo aplicada, con enfoque cuantitativo, nivel descriptivo-experimental y diseño preexperimental con pretest y postest aplicado a un solo grupo. La población y muestra estuvieron conformadas por los 13 trabajadores de la empresa, a quienes se aplicó un cuestionario validado y cuya confiabilidad fue determinada mediante el coeficiente Alfa de Cronbach. Los resultados evidenciaron mejoras significativas después de la implementación de Squid-Monitor. En el pretest, la gestión de la red de datos presentó niveles Bajo (53,8 %) y Regular (46,2 %); mientras que en el postest predominó el nivel Muy alto (84,6 %) y Alto (15,4 %). Asimismo, la prueba de hipótesis general obtuvo un valor de significancia bilateral de p = 0,000, rechazándose la hipótesis nula y aceptándose la hipótesis alternativa, concluyéndose que la implementación de Squid-Monitor mejoró significativamente la gestión de la red de datos.

Palabras clave: Squid-Monitor, gestión de redes, servidor proxy, seguridad informática, monitoreo de red.

ABSTRACT

The objective of this research was to determine how the implementation of Squid-Monitor improved data network management at the company "Compañía de Servicios en Tecnología e Informática E.I.R.L." The company had been experiencing issues such as slow Internet access, a lack of network traffic control mechanisms, insufficient supervision of connections, and an absence of policies to restrict access to unauthorized websites—a situation that negatively impacted organizational processes and user satisfaction. This was an applied research study with a quantitative approach, conducted at a descriptive-experimental level using a pre-experimental design (with a pre-test and post-test applied to a single group). The population and sample consisted of the company's 13 employees, who completed a validated questionnaire; the reliability of this instrument was assessed using Cronbach's alpha coefficient. The results showed significant improvements following the implementation of Squid-Monitor. In the pre-test, data network management was rated as "Low" (53.8%) or "Fair" (46.2%), whereas in the post-test, the ratings were predominantly "Very High" (84.6%) and "High" (15.4%). Furthermore, the general hypothesis test yielded a two-tailed significance value of $p = 0.000$, leading to the rejection of the null hypothesis and the acceptance of the alternative hypothesis. It is concluded that the implementation of Squid-Monitor significantly improved data network management.

Keywords: Squid-Monitor, network management, proxy server, IT security, network monitoring.

ÍNDICE GENERAL

DEDICATORIA.....vi

AGRADECIMIENTO vii

RESÚMEN viii

ABSTRACT.....ix

ÍNDICE GENERAL..... x

ÍNDICE DE TABLAS xiii

ÍNDICE DE FIGURAS xiv

INTRODUCCIÓN xv

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA 17

1.1. ANTECEDENTES DEL PROBLEMA 17

1.2. FORMULACIÓN DEL PROBLEMA..... 18

1.2.1. Problema general. 18

1.2.2. Problemas específicos. 18

1.3. OBJETIVOS DE LA INVESTIGACION..... 19

1.3.1. Objetivo general. 19

1.3.2. Objetivos específicos..... 19

1.4. JUSTIFICACIÓN E IMPORTANCIA..... 20

1.4.1. Justificación..... 20

1.4.2. Importancia..... 21

1.5. HIPÓTESIS..... 21

1.5.1. Hipótesis general. 21

1.5.2. Hipótesis secundarias. 21

1.6. DELIMITACIONES DE LA INVESTIGACIÓN 22

1.6.1. Delimitación espacial 22

1.6.2. Delimitación social 22

1.6.3. Delimitación temporal 22

1.6.4. Delimitación conceptual 23

1.7. VARIABLES 23

1.7.1. Definición conceptual 23

1.7.2. Definición operacional 23

CAPÍTULO II: MARCO TEÓRICO 25

2.1. ANTECEDENTES DE LA INVESTIGACIÓN. 25

2.1.1. Antecedentes internacionales 25

2.1.2. Antecedentes nacionales. 26

2.2. BASES TEÓRICAS 29

2.3. DEFINICIÓN DE TÉRMINOS BÁSICOS 37

CAPÍTULO III: METODOLOGÍA 39

3.1. METODO DE INVESTIGACIÓN 39

3.1.1. Tipo de investigación. 39

3.1.2. Nivel de investigación. 39

3.1.3. Diseño de investigación. 40

3.2. POBLACIÓN Y MUESTRA 40

3.2.1. Población 40

3.2.2. Muestra. 40

3.3. TÉCNICAS E INSTRUMENTOS PARA RECOLECCION DE DATOS 41

3.3.1. Técnicas 41

3.3.2. Instrumentos 41

3.4. TRATAMIENTO DE DATOS. 41

CAPÍTULO IV: PRESENTACIÓN DE RESULTADOS 42

4.1. ANALISIS DE RESULTADOS 42

4.2. DISCUSIÓN DE RESULTADOS 53

CONCLUSIONES 55

RECOMENDACIONES O SUGERENCIAS 57

REFERENCIAS BIBLIOGRÁFICAS 59

ANEXOS 62

Anexo 1: Matriz de consistencia 63

Anexo 2: Cuestionario de preguntas. 64

Anexo 3: Validación de Fiabilidad Alpha Cronbach 68

Anexo 4: "IMPLEMENTACIÓN DE SQUID-MONITOR PARA 70

ÍNDICE DE TABLAS

Tabla 1: *Operacionalización Variable Independiente: Squid-monitor* 23

Tabla 2: *Operacionalización Variable dependiente: Gestión de la red de datos.* *24*

Tabla 3: *Análisis de frecuencia SQUID-MONITOR* 42

Tabla 4: *Análisis de frecuencia SQUID-MONITOR* 43

Tabla 5: *Análisis de frecuencia GESTIÓN DE LA RED DE DATOS*..... 44

Tabla 6: *Análisis de Frecuencia POSTEST GESTIÓN DE LA RED DE DATOS* 45

Tabla 7: *Prueba de Normalidad.* 46

Tabla 8: *Prueba de muestras relacionadas, Hipótesis General.* 47

Tabla 9: *Prueba de muestras relacionadas - Hipótesis Especifica 1* 48

Tabla 10: *Prueba de muestras relacionadas - Hipótesis Especifica 2* 49

Tabla 11: *Prueba de muestras relacionadas - Hipótesis Especifica 3* 51

Tabla 12: *Prueba de muestras relacionadas - Hipótesis Especifica 4* 52

Tabla 13: *Escala de Alfa de Cronbach* 68

Tabla 14: *Análisis de Fiabilidad – Pretest*..... 69

Tabla 15: *Análisis de Fiabilidad – Postest* 69

Tabla 16: *Plan de seguridad y respaldo.* 76

Tabla 17: *Análisis de Fiabilidad – Post test* 84

ÍNDICE DE FIGURAS

Figura 1: *Componentes de la Gestión de Red*. 35

Figura 2: *Gráfica del análisis de frecuencia SQUID-MONITOR* 42

Figura 3: *Gráfica del análisis de frecuencia SQUID-MONITOR* 43

Figura 4: *Análisis de frecuencia GESTIÓN DE LA RED DE DATOS* 44

Figura 5: *Grafica del análisis de frecuencia GESTIÓN DE LA RED DE DATOS* 45

Figura 6: *Arquitectura Squid-Monitor*. 75

INTRODUCCIÓN

Las redes de datos constituyen uno de los principales activos tecnológicos de las organizaciones, debido a que permiten el intercambio de información, el acceso a servicios digitales y la continuidad de los procesos operativos. Sin embargo, el incremento del tráfico de información y la ausencia de mecanismos adecuados de monitoreo y control generan problemas relacionados con el uso ineficiente del ancho de banda, accesos no autorizados, disminución del rendimiento y vulnerabilidades que afectan la disponibilidad y seguridad de los servicios informáticos.

En la Compañía de Servicios en Tecnología e Informática E.I.R.L. se identificó una problemática asociada a la gestión de su red de datos, caracterizada por la lentitud en el acceso a Internet, interrupciones frecuentes del servicio, inexistencia de herramientas para el monitoreo del tráfico, ausencia de políticas de acceso y deficiencias en el control de la navegación web. Estas condiciones repercutían negativamente en la productividad de los trabajadores y en la calidad de atención brindada a los clientes, haciendo necesaria la implementación de una solución tecnológica que permitiera mejorar la administración de la infraestructura de red.

Frente a esta situación, la investigación tuvo como objetivo determinar de qué manera la implementación de Squid-Monitor mejoró la gestión de la red de datos de la empresa, considerando como dimensiones de evaluación la seguridad, la utilización de recursos, el tratamiento de incidentes y la satisfacción de los usuarios. Para ello se desarrolló una investigación aplicada con diseño preexperimental de pretest y postest, utilizando técnicas estadísticas que

permitieron evaluar objetivamente el impacto de la implementación sobre la variable de estudio.

La estructura del trabajo está organizada en cuatro capítulos principales. El primer capítulo presenta el planteamiento del problema, los objetivos, la justificación, las hipótesis y la operacionalización de las variables. El segundo capítulo desarrolla los antecedentes y las bases teóricas relacionadas con la administración de redes y el funcionamiento de Squid-Monitor. El tercer capítulo describe la metodología empleada, incluyendo el diseño de investigación, la población, la muestra, los instrumentos y el procedimiento para el análisis de datos. Finalmente, el cuarto capítulo expone los resultados obtenidos, la prueba de hipótesis, la discusión de los hallazgos y las conclusiones derivadas de la investigación.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. ANTECEDENTES DEL PROBLEMA

La tecnología simplificó las comunicaciones internas y externas, permitiendo que los empleados recibieran información instantánea sobre el estado de la empresa sin interrumpir sus actividades diarias, gracias al acceso a una plataforma que centralizaba todas las comunicaciones corporativas, facilitando así la interacción sin invadir el espacio personal. La tecnología se convirtió en una herramienta de comunicación fundamental para las organizaciones, transformando la forma en que estas gestionaban sus relaciones públicas y marketing, incluyendo sus interacciones con los medios de comunicación y las partes interesadas. Sin embargo, así como existieron grandes aportes de las tecnologías de comunicación, también se presentaron vulnerabilidades cuando su implementación fue parcial.

La COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L. poseía una red LAN para su comunicación interna y una conexión a internet para la comunicación externa, las cuales eran elementos importantes para sus procesos diarios; no obstante, en aquel momento se venían presentando situaciones problemáticas, tales como lentitud en el acceso al servicio de internet, caídas intermitentes del servicio, malestar en los empleados e incomodidad en los clientes debido a la lentitud en la atención.

Por lo mencionado, se realizó una evaluación para determinar las causas, lográndose evidenciar las siguientes: carencia de un sistema de control sobre las peticiones de acceso a través de la red; carencia de una

herramienta de gestión de red y políticas; carencia de un mecanismo de control de tráfico entrante y saliente; y carencia de un sistema de bloqueo de sitios web no permitidos o que no estuvieran relacionados con el desarrollo de las actividades diarias. Como se evidenció, la empresa se encontraba en una situación problemática que, de continuar, habría afectado negativamente la confidencialidad e integridad de la información. En tal sentido, se desarrolló la presente investigación con el propósito de aplicar un tratamiento adecuado que permitiera superar dicha situación problemática.

1.2. FORMULACIÓN DEL PROBLEMA

1.2.1. Problema general.

- ¿De qué manera la implementación de Squid-monitor mejora la gestión de la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.?

1.2.2. Problemas específicos.

- ¿De qué manera la implementación de Squid-monitor mejora la seguridad en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.?
- ¿De qué manera la implementación de Squid-monitor mejora la utilización de recursos en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.?
- ¿De qué manera la implementación de Squid-monitor mejora el tratamiento de incidentes en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.?

- ¿De qué manera la implementación de Squid-monitor mejora la satisfacción de los usuarios que utilizaron la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.?

1.3. OBJETIVOS DE LA INVESTIGACION

1.3.1. Objetivo general.

- Implementar Squid-monitor para la mejora de la gestión de la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.

1.3.2. Objetivos específicos.

- Evaluar de qué manera la implementación de Squid-monitor mejora la seguridad en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.
- Analizar cómo la implementación de Squid-monitor mejora la utilización de recursos en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.
- Determinar en qué medida la implementación de Squid-monitor mejora el tratamiento de incidentes en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.
- Valorar cómo la implementación de Squid-monitor mejora la satisfacción de los usuarios que utilizaron la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.

1.4. JUSTIFICACIÓN E IMPORTANCIA.

1.4.1. Justificación.

- **Justificación teórica.**

  Debido a que los propósitos implícitos de esta investigación estuvieron orientados a la gestión de la red de datos a partir de los componentes de Privacidad, Rendimiento, Control y Gestión, se tomaron en cuenta los fundamentos tecnológicos y teóricos necesarios para un enfoque investigativo apropiado de estas variables de estudio.

- **Justificación práctica.**

  Debido a que mediante esta investigación se pretendió implementar una solución para la gestión de la red de datos basada en la Privacidad, Rendimiento, Control y Gestión, la propuesta permitió salvaguardar la seguridad en la red de datos, optimizar la utilización de recursos, mejorar el tratamiento de incidentes y elevar la satisfacción de los usuarios de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.

- **Justificación metodológica.**

  La metodología y los procedimientos empleados en este estudio ofrecieron una alternativa frente a investigaciones similares, constituyéndose en una guía de referencia para futuros estudios que abordaran las mismas variables de análisis. Asimismo, el instrumento de recopilación de datos pudo ser reutilizado en contextos de investigación semejantes, garantizando validez y confiabilidad en los resultados obtenidos.

1.4.2. Importancia.

La investigación tuvo relevancia porque permitió determinar los objetivos, procesos y procedimientos para el establecimiento de mecanismos de Filtrado, Restricciones, Caching, Balanceo de carga, Acceso y Supervisión, los cuales contribuyeron a gestionar eficazmente el sistema Squid-monitor, considerando la gestión integral de la red de datos en la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.

Limitaciones.

El estudio presentó limitaciones relacionadas con el tamaño reducido de la población, la disponibilidad de tiempo del personal participante y los recursos tecnológicos limitados de la empresa. Además, la subjetividad inherente a los cuestionarios aplicados pudo influir parcialmente en las percepciones, aunque se mitigó mediante la comparación de datos antes y después de la implementación de Squid-monitor.

1.5. HIPÓTESIS

1.5.1. Hipótesis general.

- La implementación de Squid-monitor mejora la gestión de la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.

1.5.2. Hipótesis secundarias.

- La implementación de Squid-monitor mejora la seguridad en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.

- La implementación de Squid-monitor mejora la utilización de recursos en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.
- La implementación de Squid-monitor mejora el tratamiento de incidentes en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.
- La implementación de Squid-monitor mejora la satisfacción de los usuarios que utilizaron la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.

1.6. DELIMITACIONES DE LA INVESTIGACIÓN

1.6.1. Delimitación espacial

La investigación se desarrolló en la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L., ubicada en la ciudad de Pucallpa, región Ucayali, donde se implementó y evaluó el sistema Squid-Monitor en la red de datos de la empresa.

1.6.2. Delimitación social

El estudio involucró a los 13 empleados de la empresa que participaron directa o indirectamente en la gestión, uso y supervisión de la red de datos, incluyendo personal técnico, administrativo y de soporte.

1.6.3. Delimitación temporal

La investigación se llevó a cabo durante el periodo 2024 - 2025, comprendiendo las fases de diagnóstico, implementación de Squid-Monitor, aplicación de instrumentos de evaluación y análisis de resultados.

1.6.4. Delimitación conceptual

El estudio se centró en los conceptos relacionados con la gestión de redes de datos y la implementación de herramientas de monitoreo, específicamente Squid-Monitor, abordando dimensiones como privacidad, rendimiento, control, gestión, seguridad, recursos, incidentes y satisfacción de los usuarios, que fueron medidas mediante indicadores cuantitativos expresados en porcentajes.

1.7. VARIABLES

1.7.1. Definición conceptual

a) Variable independiente

- Squid-monitor

b) Variable dependiente

- Gestión de la red de datos.

1.7.2. Definición operacional

a) Variable Independiente: Squid-monitor

Tabla 1:

Operacionalización Variable Independiente: Squid-monitor

Variable	Dimensiones	Indicadores
Squid-monitor	Privacidad	% de Filtrado Restricciones
	Rendimiento	% de Caching Balanceo de carga
	Control y Gestión	% de Acceso Supervisión

Fuente: Elaboración Propia

b) Variable dependiente**:** Gestión de la red de datos.

Operacionalización Variable dependiente: Gestión de la red de datos.

Tabla 2:

Operacionalización Variable dependiente: Gestión de la red de datos.

Variable	**Dimensiones**	**Indicadores**
Gestión de la red de datos.	Seguridad	% de mejora de Controles
	Recursos	% de optimización de hardware/software
	Incidentes	% de reducción de incidentes
	Satisfacción	% de Satisfacción Conformidad

Fuente: Elaboración Propia

CAPÍTULO II: MARCO TEÓRICO

2.1. ANTECEDENTES DE LA INVESTIGACIÓN.

2.1.1. Antecedentes internacionales.

Según investigación de Benavides Maldonado, (2020), que tiene como meta controlar y distribuir el espectro del ancho de banda haciendo uso de métodos heurísticos para el acceso a internet, logrando al finalizar la conclusión que: La evaluación de los scripts heurísticos de aplicación, extensión de archivo y dominio debería tomar al menos una semana para crear una base de datos robusta a partir de la cual generar informes. Al diseñar heurísticas de fusión, es importante guiarse no solo por los resultados numéricos, sino también por la implementación de la heurística. Las heurísticas de fusión de extensión de archivo y dominio monitorearon y distribuyeron correctamente el ancho de banda para Trovinsa S.A., superando el rendimiento de tres heurísticas desarrolladas previamente.

Según la investigación de López Larreynaga, (2021), que tuvo como finalidad la elaboración de una propuesta de configuraciones que apoyen en la mejora de la seguridad física y lógica a la red; y al finalizar concluyo que: Con base en las deficiencias identificadas en el control del contenido al que se accede a través de Internet, realizamos un estudio del software necesario para abordar este problema. Creamos un cuadro comparativo de diferentes sistemas operativos de red para determinar las mejores opciones y formular recomendaciones para mejorar el proyecto de seguridad informática. ClearOS resultó ser el software adecuado que cumplía con los requisitos, por lo que se implementó para

brindar mejores servicios y, por consiguiente, aumentar la seguridad de la red. Diseñar e implementar mejoras no es tarea fácil, ya que existen muchas limitaciones. El aspecto más desafiante es que, debido a nuestro presupuesto, solo contamos con los recursos de red, el equipo informático y los servicios de Internet que la agencia tiene actualmente. Por lo tanto, las mejoras y configuraciones deben adaptarse al equipo existente para mejorar el rendimiento, la eficiencia y la seguridad de la red sin aumentar los costos de la agencia.

Según investigación de Litardo ordoñez, (2021), que se planteó realizar una restructuración y optimización de los servicios de la red cableada e inalámbrica, así como la implementación de un servidor tipo proxy en Linux; y al finalizar concluyo que: El mismo hardware utilizado para alojar los servidores de archivos de la unidad educativa América del Sur se empleó para implementar el servidor proxy. Esto permite establecer políticas de seguridad que filtran el contenido que utilizan los usuarios en la red, controlando así el acceso no autorizado. Esto facilita a los administradores de red el control de la navegación web de los estudiantes. Tras definir todas las pruebas e instalaciones, la inspección in situ confirmó el cumplimiento de todos los requisitos definidos al inicio del proyecto, lo cual beneficia a la unidad educativa y garantiza un desarrollo óptimo.

2.1.2. Antecedentes nacionales.

Según la investigación de De la curz Bernilla, (2021), que se planteó como finalidad, mejorar la gestión de la intranet a través de uso de una VPN Open Source en la Universidad: al finalizar su investigación

concluyo que: Las topologías físicas y lógicas se diseñaron considerando criterios de seguridad y acceso rápido. Se elaboró un presupuesto para el equipo necesario y se describieron los pasos a seguir para una implementación exitosa. Se evaluó el retorno de la inversión (ROI) del presupuesto utilizando los indicadores VAN, TIR y PR, lo que permitió concluir que el proyecto era viable. La implementación de la VPN se demostró mediante simulación para optimizar la gestión de aplicaciones en la red interna de la UNPRG, con resultados positivos. Se demostró la seguridad e integridad de los datos transmitidos a través de la VPN para garantizar la confidencialidad y la disponibilidad.

Según la investigación de Senteno, (2021), que se planteó como finalidad elaborar un diseño de interceptor proxy usando squit, para la mejorar la seguridad informática; al finalizar concluyo que: Los servidores proxy son esenciales para las empresas que desean mantener seguros sus sistemas, servidores, conexiones a internet, navegación web, usuarios, etc. La seguridad informática, también conocida como seguridad de red, se centra en proteger la infraestructura informática y todo lo conectado a ella, especialmente la información contenida en los ordenadores o transmitida a través de redes informáticas. Con base en los datos recopilados mediante encuestas, los empleados identifican sitios web y contenido seguros a través de publicidad y motores de búsqueda. El informe CIE-2016 muestra que las contraseñas rara vez son pirateadas. Los empleados consideran recomendable cambiar las contraseñas periódicamente para evitar

amenazas. El nivel de seguridad informática de la alianza es bajo. Los antivirus y el software externo brindan protección. Asimismo, el informe CIE-2016 no restringe la navegación, sino que ofrece recomendaciones. Finalmente, los encuestados consideraron que los interceptores de proxy son necesarios para mejorar la seguridad dentro de la federación.

Según la investigación de Tabra Ochoa, (2021), que se propuso determinar el rol de un servidor proxy advisor en el Gobierno de la empresa, breve análisis de la realidad peruana; al finalizar concluyó que: Los asesores de voto trabajan para reducir los problemas de transparencia en la gobernanza de los inversores institucionales que podrían perjudicar los intereses de sus clientes y otros mercados. Su contribución obliga a los inversores a justificar mejor sus propuestas de voto sobre la gobernanza de las empresas emisoras, aumentando así la cuota de mercado de ambas partes (inversores institucionales y empresas emisoras), reduciendo el riesgo de pérdidas o quiebra, y protegiendo los intereses de las partes interesadas. El respaldo de organizaciones como la Autoridad Europea de Mercados Financieros, la Comisión de Bolsa y Valores (SEC) y la Comisión Europea respalda las afirmaciones realizadas en este estudio. La situación actual del mercado peruano justifica la existencia de asesores de voto, que demuestran que los inversores institucionales utilizan los fondos de sus clientes de forma transparente y responsable, sin conflictos de intereses y teniendo en cuenta el interés común. De esta forma, los inversores pueden demostrar que los fondos de sus clientes se dirigen a empresas rentables, eficientes y eficaces. Un estudio conjunto de la OCDE, el

Banco Mundial y el FMI destaca los desafíos que enfrentan las empresas de inversión en la región, en particular las administradoras de fondos de pensiones, de las cuales son responsables asesores fiduciarios como ISS, Glass Lewis, PIRC, Proxinvest y otras. La regulación de los asesores fiduciarios en el mercado peruano debe ser autorregulada. A través del gobierno corporativo, los inversionistas institucionales (como las administradoras de fondos de pensiones) deben desarrollar códigos de conducta para demostrar que sus órganos de gobierno cumplen con sus deberes fiduciarios, operan con transparencia y sin conflictos de interés, y operan en un ambiente de confianza en beneficio de los clientes, accionistas minoritarios y otras partes interesadas. Además, es importante que los fiduciarios e inversionistas institucionales implementen códigos de conducta para prevenir la aparición de presiones cuando alguna de las partes forma parte de un conglomerado. Un estudio de las normas internas de los asesores fiduciarios de Glass Lewis e ISS confirma esta afirmación.

2.2. BASES TEÓRICAS

- **Administración de red**

  Según Cisco, (2025), la gestión de red implica dos conceptos interrelacionados. El primero es el proceso de configuración, monitorización y gestión del rendimiento de la red. El segundo es la plataforma que utilizan los equipos de TI y operaciones de red para realizar estas tareas continuas.

  Los sistemas de gestión de red están evolucionando para ayudar a los departamentos de TI a operar con mayor agilidad

mediante la implementación de análisis avanzados, aprendizaje automático y automatización inteligente para optimizar continuamente el rendimiento de la red. A medida que las organizaciones se adaptan a una fuerza laboral más distribuida, estos sistemas de gestión de red se implementan cada vez más en entornos alojados y en la nube.

De acuerdo con Susnjara, (2025), un sistema de gestión de red (SGR) es un sistema de infraestructura de TI que los administradores y los centros de operaciones de red (NOC) utilizan para configurar, gestionar la configuración, gestionar fallos, gestionar el rendimiento, gestionar la seguridad y realizar otras tareas de gestión de red.

Si bien la administración de red se refiere a las tareas que realizan los administradores para mantener y proteger una red, un SGR (también conocido como software de gestión de red) es un conjunto de herramientas que los administradores utilizan para realizar estas tareas. En concreto, los SGR utilizan herramientas de monitorización y vigilancia de red para recopilar datos en tiempo real de los dispositivos de red (p. ej., conmutadores, enrutadores, puntos de acceso, dispositivos de usuario). Proporciona a los administradores un punto de control central para gestionar las políticas de seguridad de red, asignar recursos de red, etc.

Por ejemplo, los administradores de red pueden configurar políticas de conmutación por error para que las aplicaciones críticas cambien automáticamente del almacenamiento de

respaldo a la memoria cuando un fallo de red amenace el acceso a servicios esenciales.

Un SGR puede:

- Identificar proactivamente los problemas de red mediante IA y aprendizaje automático para detectar patrones de comportamiento de red y responder rápidamente a ellos.
- Controlar la asignación de recursos y la seguridad de la red. Agilice la resolución de problemas con un único punto de visibilidad del tráfico de red y la gestión del rendimiento.

La automatización de la red elimina la necesidad de intervención manual en flujos de trabajo repetitivos, como las tareas de gestión de la configuración de red y las actualizaciones.

- **Componentes de la Gestión de Red.**

Según Spiceworks, (2025), la gestión de red aprovecha múltiples componentes conectados para ejecutar operaciones. Estos incluyen:

- **Conectividad de endpoints**

El propósito principal de una infraestructura de red es conectar los endpoints de una empresa. Esto puede incluir estaciones de trabajo locales, quioscos de vestíbulo y sistemas de salas de conferencias. También puede incluir entornos distribuidos que ayudan a conectar a trabajadores remotos y múltiples sucursales. Los tipos de endpoints varían según las necesidades de la empresa. La gestión de red ayuda a garantizar que los endpoints necesarios estén siempre

conectados, y los administradores de red pueden ver el rendimiento de cada nodo en tiempo real. Los departamentos de TI también pueden utilizar herramientas de monitorización de red centralizadas para supervisar las conexiones de los endpoints en ubicaciones distribuidas a una única interfaz.

- **Sistemas de registro**

  Los sistemas de registro son una parte esencial de la gestión de red, ya que ayudan a supervisar el rendimiento de la red en comparación con las métricas de rendimiento estándar del sector y a mantener registros detallados. Un sistema de registro se conecta a los dispositivos de hardware y componentes de software de la red. Mediante estas herramientas de hardware y software, un sistema de registro registrará toda la actividad para futuras consultas.

  Uno de los mecanismos de registro más populares para la gestión de red es el ampliamente utilizado Syslog, un protocolo que permite crear y mantener registros de todos los eventos de red en un formato de datos como JSON. Sin embargo, por sí solo, no es muy útil. Por eso, la gestión de red moderna combina sistemas de registro con análisis de red para visualizar datos, detectar tendencias y recibir alertas sobre anomalías.

- **Automatización de red**

  La automatización de red reduce la cantidad de trabajo manual asociado con la gestión de cinco tipos diferentes de

redes. Ayuda a solucionar automáticamente problemas comunes basándose en protocolos predefinidos de gestión de fallos de red. Para la gestión de la configuración de red, la automatización puede ayudar a otorgar acceso automáticamente a nuevos usuarios. Para la gestión de cuentas de red, puede ayudar a implementar automáticamente medidas de reducción de costes cuando se superan ciertos umbrales.

Configura automáticamente las políticas de las aplicaciones para gestionar el rendimiento de la red y así apoyar el negocio. La automatización permite reconocer diferentes tipos de amenazas y detectarlas con una mínima intervención manual en la gestión de la seguridad de la red. Según Reportlinker, se espera que la automatización de redes crezca de 3400 millones de dólares en 2021 a más de 8300 millones de dólares en 2026.

- **Conectividad de servidores**

El componente de conectividad de servidores de la gestión de red se encarga de gestionar el estado de la conectividad de los dispositivos que no son de usuario final. Por ejemplo, si su empresa utiliza máquinas virtuales o varios servidores privados para dar soporte a los procesos relacionados con las aplicaciones, necesita mantener estos dispositivos en línea.

La gestión de red debe garantizar el máximo tiempo de actividad para los servidores, así como para los endpoints. Esto puede suponer un reto, ya que los problemas en los servidores son más difíciles de detectar y solo se manifiestan después de que se han extendido por toda la empresa. Por ello, la mayoría de los equipos de administración de red utilizan herramientas de monitorización de red dedicadas para mantener y gestionar este componente.

- **Gestión de switches**

  Los switches de red son dispositivos de hardware que ayudan a conectar los endpoints a la red corporativa central, garantizando al mismo tiempo el cumplimiento de los protocolos de TI necesarios. Las empresas pueden utilizar múltiples capas de switches de red, desde switches de nivel de planta hasta switches de agregación y switches de núcleo.

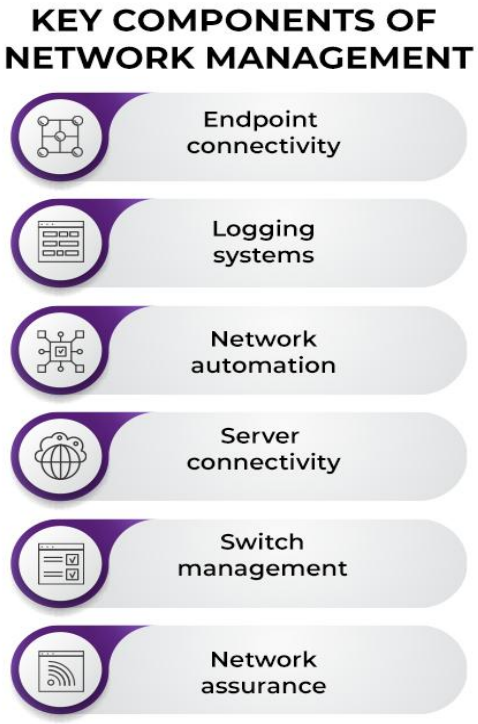
  La gestión de switches proporciona visibilidad del tráfico entrante y saliente, lo que permite diagnosticar problemas de subida, garantizar velocidades constantes y predecir cuellos de botella. Hoy en día, los componentes de la gestión de switches se han vuelto muy complejos. Permite supervisar y coordinar entornos complejos mediante software de gestión de switches. Ayuda a crear un mapa visual de las instalaciones de la empresa y a gestionar los switches conectados a los endpoints.

- **Seguridad de la red**

  El componente de seguridad de la red en la gestión de la red implica la aplicación de políticas para controlar los riesgos, garantizar el cumplimiento interno y prevenir amenazas a la seguridad. El objetivo de la seguridad de la red es garantizar una experiencia segura para todos los usuarios. Por ello, los cinco tipos de gestión de red deben trabajar en conjunto para garantizar el correcto funcionamiento de este componente. Además, la ciberseguridad utiliza la analítica como un componente clave para supervisar los niveles de riesgo dinámicos y alertar a las partes interesadas antes de que surjan problemas graves.

Figura 1:

Componentes de la Gestión de Red.



Fuente: (Spiceworks, 2025)

- **¿Cómo funciona la administración de red?**

Según Kaseya, (2022), la administración de red es el proceso de planificación, diseño y supervisión de las operaciones de red. El Protocolo Simple de Administración de Red (SNMP) es un protocolo estándar de administración de red que permite a los administradores supervisar y gestionar dispositivos de red de forma remota. SNMP es un componente del conjunto de protocolos de Internet definido por el Grupo de Trabajo de Ingeniería de Internet (IETF). Ayuda principalmente a supervisar dispositivos de red como cortafuegos, enrutadores, conmutadores, servidores, impresoras, etc. Además, SNMP facilita el intercambio de información entre los dispositivos de red y los sistemas de administración de red (NMS). Las herramientas NMS utilizan diversos mensajes SNMP para supervisar y gestionar los dispositivos de red (también conocidos como elementos de red).

Las tres fases generales de la administración de red son:

- Planificación: Implica la creación de un diseño de red que satisfaga las necesidades del usuario y de la empresa.
- Diseño: Esta fase implica la selección y el ensamblaje del hardware y el software que mejor se adapten al diseño de red.
- Supervisión: Una vez que la red esté en funcionamiento, es necesario supervisarla y realizarle mantenimiento para garantizar un funcionamiento estable y prevenir fallos y brechas de seguridad.

Las tres tareas principales de la administración de red son:

- **Administración de la configuración:** Garantizar que todos los dispositivos de la red estén configurados correctamente y sean compatibles entre sí.
- **Monitorización del tráfico:** Supervisar el tráfico de la red y los patrones de uso para identificar posibles cuellos de botella o problemas.
- **Administración de la seguridad:** Proteger la red de accesos y ataques no autorizados.

2.3. DEFINICIÓN DE TÉRMINOS BÁSICOS.

- **Implementación.**

  Ya sea software o hardware, la implementación abarca todos los procesos postventa que aseguran el correcto funcionamiento del producto en su entorno. Arimetrics, (2025).

- **Squid proxy.**

  Según Pratama, (2023), Squid Proxy es un servidor proxy web de código abierto que actúa como intermediario entre clientes y servidores en la red. Actúa como puerta de enlace, permitiendo a los clientes acceder a diversos recursos de Internet, como sitios web, archivos y otros contenidos, desde el servidor.

- **Gestión.**

  La gestión es el proceso de coordinar y dirigir recursos para alcanzar objetivos específicos. Incluye actividades como la planificación, la organización, la dirección y el control. Simbiotecs, (2025)

- **Red de datos.**

  Es una infraestructura creada para transmitir información de cualquier naturaleza de un punto a otro mediante el intercambio de datos. Televes, (2025).

CAPÍTULO III: METODOLOGÍA

3.1. METODO DE INVESTIGACIÓN

3.1.1. Tipo de investigación.

El tipo de investigación fue aplicada, ya que buscó resolver un problema práctico relacionado con la gestión de la red de datos en la Compañía de Servicios en Tecnología e Informática E.I.R.L., mediante la implementación de Squid-Monitor. Según el Manual de Frascati (2015), fue específica, porque implicó la aplicación de conocimientos tecnológicos existentes para obtener resultados cuantificables orientados a mejorar la seguridad, el rendimiento y la satisfacción de los usuarios.

3.1.2. Nivel de investigación.

Descriptiva (Se mide las variables relevantes) – Experimental, Según Hernández, Fernández y Baptista, (2010) En la Metodología de la Investigación indica que: “es aquella que obtiene datos a través de la experimentación y los compara con variables constantes, a fin de determinar las causas y/o los efectos de los fenómenos en estudio).

Descriptivas, por cuanto a través de la información obtenida se va a clasificar elementos y estructuras para caracterizar una realidad y, a través del correlacional se miden las relaciones existentes entre dos o más variables (asociaciones, influencias, relaciones, correlaciones).

Método de investigación

Se aplicó el método “Pre test – Post test” en la medición de la variable dependiente ante la aplicación de la variable independiente.

3.1.3. Diseño de investigación.

Se puede representar mediante la siguiente simbología:

Ecuación 1: Método “Pre test – Post test”.

GE: O1 -> X -> O2

Donde:

GE: Grupo Pre Experimental

O1: Datos de la Pre - Prueba para los indicadores de la variable dependiente antes de valorar el Squid-monitor evaluando la Gestión de la red de datos.

X: La propuesta de Squid-monitor evaluando la Gestión de la red de datos = Estimulo o condición experimental.

O2: Datos de la Post- Prueba para los indicadores de la variable dependiente antes de valorar el Squid-monitor evaluando la Gestión de la red de datos.

3.2. POBLACIÓN Y MUESTRA

3.2.1. Población

La población estuvo conformada por el personal de las distintas áreas de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L., integrada por 13 empleados que participaron directa o indirectamente en el uso y gestión de la red de datos.

3.2.2. Muestra.

Debido al tamaño reducido de la población, se aplicó un muestreo no probabilístico por conveniencia, considerando como muestra total a los 13 empleados de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.

Este enfoque permitió obtener información completa y precisa, al incluir a todos los usuarios involucrados en la gestión de la red.

3.3. TÉCNICAS E INSTRUMENTOS PARA RECOLECCION DE DATOS

3.3.1. Técnicas

Para evitar el sesgo estadístico, los empleados que desconocían conceptos técnicos fueron capacitados previamente; por ello, la primera acción consistió en realizar la capacitación, y luego se procedió a aplicar el cuestionario antes y después de implementada la solución a la realidad problemática.

3.3.2. Instrumentos

En esta etapa fue necesario contar con una herramienta que permitiera obtener los datos para demostrar la investigación; en este caso, se hizo uso de un cuestionario de preguntas.

3.4. TRATAMIENTO DE DATOS.

Los datos fueron recolectados y procesados para obtener resultados en formatos estadísticos como gráficos de barras y tablas. Para ello, se utilizó el programa informático SPSS de IBM.

- **Grado de confiabilidad de los datos**

  Para esta evaluación, que tuvo carácter interno del instrumento (cuestionario), y con el fin de fundamentar y asegurar su fiabilidad, se aplicó el coeficiente Alfa de Cronbach.

CAPÍTULO IV: PRESENTACIÓN DE RESULTADOS

4.1. ANALISIS DE RESULTADOS

VARIABLE INDEPENDIENTE: SQUID-MONITOR

PRETEST

Tabla 3:

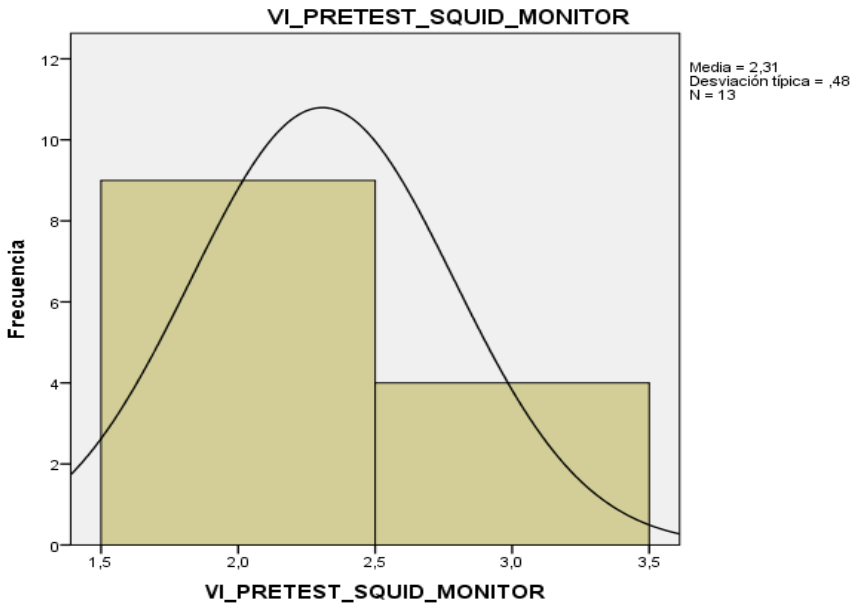
Análisis de frecuencia SQUID-MONITOR

VI_PRETEST_SQUID_MONITOR					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Bajo	9	69,2	69,2	69,2
	Regular	4	30,8	30,8	100,0
	Total	13	100,0	100,0	

Fuente: IBM SPSS

Figura 2:

Gráfica del análisis de frecuencia SQUID-MONITOR



Fuente: IBM SPSS

Interpretación: De acuerdo con la percepción de los encuestados, el 69,2 % se ubica en el nivel Bajo, el 30,8 % en el nivel Regular, considerando que estos datos han sido previamente agrupados en rangos de puntajes.

POSTEST

Tabla 4:

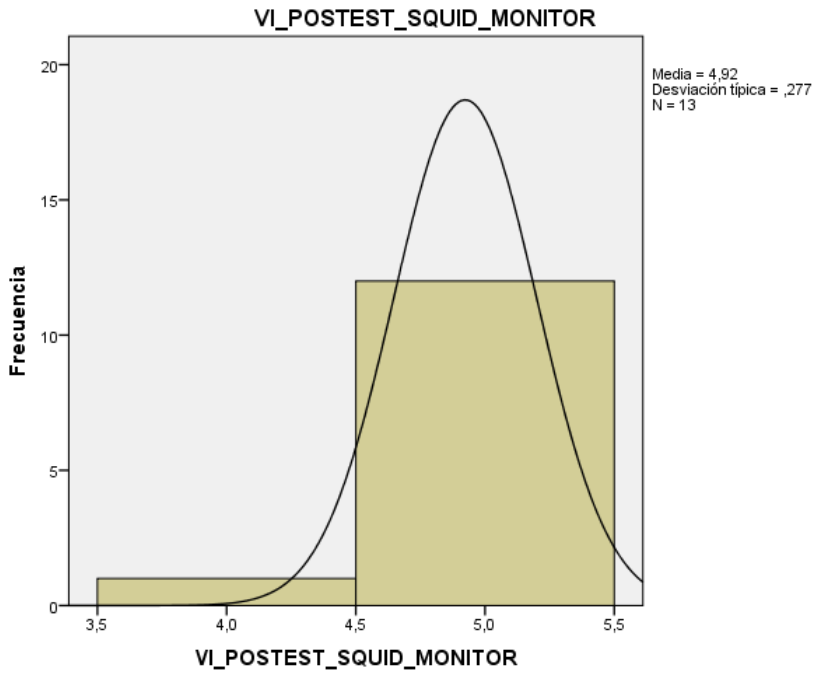
Análisis de frecuencia SQUID-MONITOR

VI_POSTEST_SQUID_MONITOR					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Alto	1	7,7	7,7	7,7
	Muy alto	12	92,3	92,3	100,0
	Total	13	100,0	100,0	

Fuente: IBM SPSS

Figura 3:

Gráfica del análisis de frecuencia SQUID-MONITOR



Fuente: IBM SPSS

Interpretación: De acuerdo con la percepción de los encuestados, el 7,7 % se ubica en el nivel Alto, el 92,3 % en el nivel Muy alto, considerando que estos datos han sido previamente agrupados en rangos de puntajes.

VARIABLE DEPENDIENTE: GESTIÓN DE LA RED DE DATOS

PRETEST

Tabla 5:

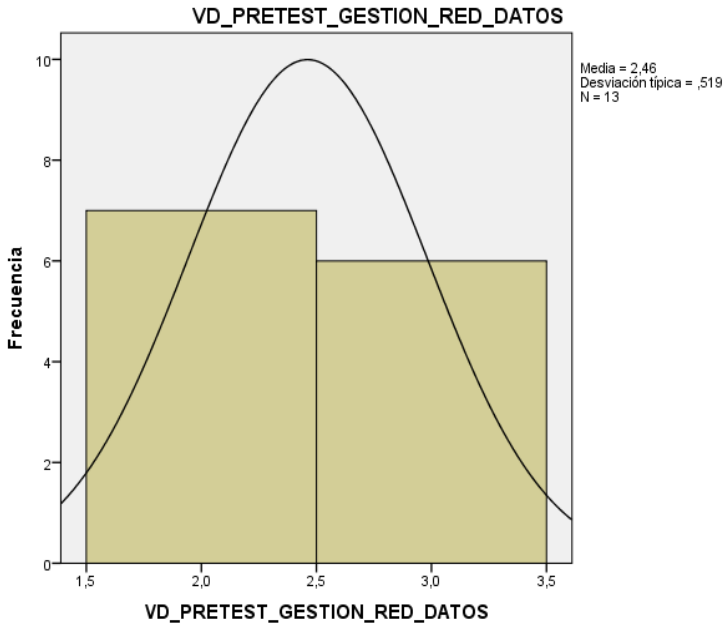
Análisis de frecuencia GESTIÓN DE LA RED DE DATOS

VD_PRETEST_GESTION_RED_DATOS					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Bajo	7	53,8	53,8	53,8
	Regular	6	46,2	46,2	100,0
	Total	13	100,0	100,0	

Fuente: IBM SPSS

Figura 4:

Análisis de frecuencia GESTIÓN DE LA RED DE DATOS



Fuente: IBM SPSS

Interpretación: De acuerdo con la percepción de los encuestados, el 53,8 % se ubica en el nivel Bajo, el 46,2 % en el nivel Regular, considerando que estos datos han sido previamente agrupados en rangos de puntajes.

Tabla 6:

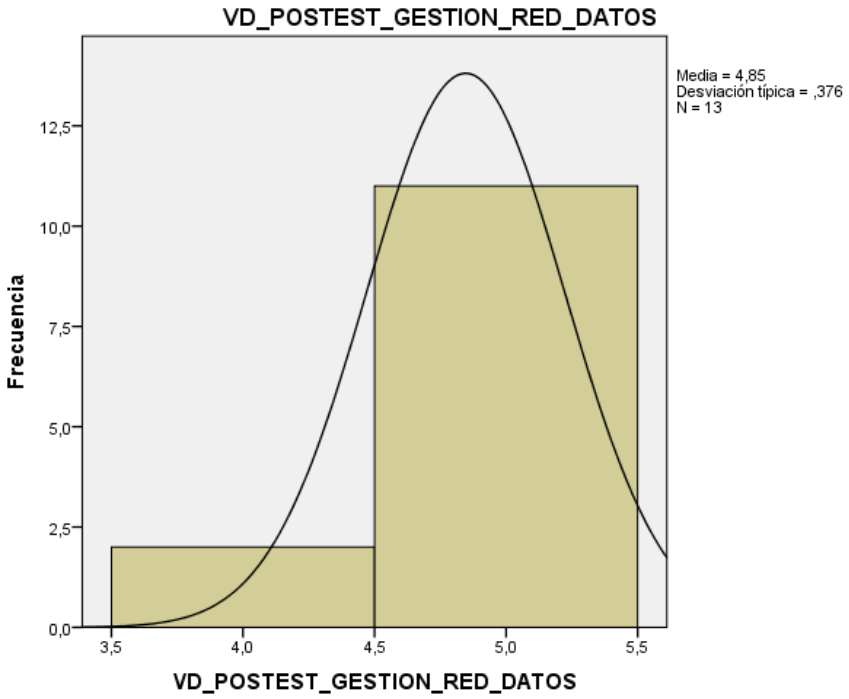
Análisis de Frecuencia POSTEST GESTIÓN DE LA RED DE DATOS

VD_POSTEST_GESTION_RED_DATOS					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Alto	2	15,4	15,4	15,4
	Muy alto	11	84,6	84,6	100,0
	Total	13	100,0	100,0	

Fuente: IBM SPSS

Figura 5:

Grafica del análisis de frecuencia GESTIÓN DE LA RED DE DATOS



Fuente: IBM SPSS

Interpretación: De acuerdo con la percepción de los encuestados, el 15,4 % se ubica en el nivel Alto, el 84,6 % en el nivel Muy alto, considerando que estos datos han sido previamente agrupados en rangos de puntajes.

a) PRUEBA DE HIPÓTESIS GENERAL

Paso 1: Planteamiento, **de la Hipótesis General**

Hipótesis, nula ($\boldsymbol{H0}$) = La implementación de Squid-monitor no mejoró la gestión de la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.

Hipótesis alterna ($\boldsymbol{H1}$) = La implementación de Squid-monitor si mejoró la gestión de la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.

Paso 2: Especificar, **el nivel de significancia y muestra**

Nivel de, significancia (α) = 5% (0.05)

Nivel, de confiabilidad (1-α) = 95% (0.95)

Muestra (n) = 13

Paso 3: Prueba de Normalidad

Tabla 7:

Prueba de Normalidad.

Pruebas de normalidad			
	Shapiro-Wilk, Estadístico,	,gl	,Sig.
PRE_TEST	,977	13,	.958
POS_TEST	,950	13,	.599

Fuente: Elaboración Propia

Interpretación: p(Sig.): De acuerdo a la prueba de normalidad de las variables: SQUID-MONITOR y GESTIÓN DE LA RED DE DATOS con

sus dimensiones se comporta normalmente, en el pre test y post test, de forma explícita presentan distribución normal, según los resultados de la prueba de normalidad (p > 0.05). Debido a que la muestra es menor a 30 casos y se busca establecer un causo - efecto de la intervención, se optó por un análisis paramétrico. En consecuencia, se aplicó la prueba de t-Student para muestras relacionadas, adecuada para contrastar las hipótesis planteadas.

Paso 4: Criterio, de Decisión

Para calcular la función de prueba, se ha empleado el programa SPSS, insertando valores promedios de los resultados del cuestionario aplicado:

Si, p(valor) >= 0.05, procederemos con aceptamos, la hipótesis H0 y rechazamos la H1

Si, p(valor) < 0.05, procederemos con rechazamos, la hipótesis H0 y aceptamos la H1

Paso 05: Toma de decisiones:

Tabla 8:

Prueba de muestras relacionadas, Hipótesis General.

Prueba de muestras relacionadas									
		Diferencias relacionadas					t	gl	Sig. (bilateral)
		Media	Desviación típ.	Error típ. de la media	95% Intervalo de confianza para la diferencia				
					Inferior	Superior			
Par 1	POSTEST - PRETEST	2,60440	,55395	,15364	2,26965	2,93914	16,952	12	,000

Fuente: Elaboración- Propia

Interpretación: Como p(valor) = 0.00 < 0.05, se procede con rechazar la H0 y se acepta la H1, por lo que, luego de aplicar cálculos estadísticos, se determina que: La implementación de Squid-monitor si

mejoró la gestión de la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.

b) PRUEBA DE HIPÓTESIS ESPECIFICA 1

Paso 1: Planteamiento, **de la Hipótesis**

Hipótesis, nula ($\boldsymbol{H0}$) = La implementación de Squid-monitor no mejoró la seguridad en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.

Hipótesis alterna ($\boldsymbol{H1}$) = La implementación de Squid-monitor si mejoró la seguridad en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.

Paso 02: Toma de decisiones:

Tabla 9:

Prueba de muestras relacionadas - Hipótesis Especifica 1

Prueba de muestras relacionadas									
		Diferencias relacionadas					t	gl	Sig. (bilateral)
		Media	Desviación típ.	Error típ. de la media	95% Intervalo de confianza para la diferencia				
					Inferior	Superior			
Par 1	VI__POSTEST_SQUID_MONITOR - VI__PRETEST_SQUID_MONITOR	2,61538	,64777	,17966	2,22394	3,00683	14,558	12	,000
Par 2	DIM_POSTEST_SEGURIDAD - DIM_PRETEST_SEGURIDAD	2,48077	,88070	,24426	1,94856	3,01297	10,156	12	,000

Fuente: Elaboración- Propia

Interpretación: Los resultados obtenidos antes y después de la implementación de Squid-monitor, demostraron un efecto positivo y significativo sobre la dimensión Seguridad de la variable dependiente Gestión de la red de datos en la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L; La prueba t para muestras

relacionadas evidenció un valor de t(12) = 10.156 con una significancia bilateral de p = 0.000 en la dimensión Seguridad, mientras que el valor global correspondiente a la variable independiente Squid-monitor alcanzó t(12) = 14.558 con p = 0.000. Dado que ambos valores de p son menores a 0.05, se confirma la existencia de diferencias estadísticamente significativas entre los resultados del pretest y el postest, lo que indica que la implementación del sistema generó mejoras reales y medibles; Por lo tanto, se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alterna (H_1), concluyéndose que: La implementación de Squid-monitor si mejoró la seguridad en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.

c) PRUEBA DE HIPÓTESIS ESPECIFICA 2

Paso 1: Planteamiento de la Hipótesis

Hipótesis, nula ($\boldsymbol{H0}$) = La implementación de Squid-monitor no mejoró la utilización de recursos en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.

Hipótesis alterna ($\boldsymbol{H1}$) = La implementación de Squid-monitor si mejoró la utilización de recursos en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.

Paso 02: Toma de decisiones:

Tabla 10:

Prueba de muestras relacionadas - Hipótesis Especifica 2

Prueba de muestras relacionadas							
	Diferencias relacionadas				t	gl	Sig.
	Media	Desviación típ.	Error típ. de	95% Intervalo de confianza para la diferencia			(bilateral)

				la media	Inferior	Superior			
Par 1	VI__POSTEST_SQUID_MONITOR - VI__PRETEST_SQUID_MONITOR	2,61538	,64777	,17966	2,22394	3,00683	14,558	12	,000
Par 2	DIM_POSTEST_RECURSOS - DIM_PRETEST_RECURSOS	2,48077	,90979	,25233	1,93099	3,03055	9,831	12	,000

Fuente: Elaboración- Propia

Interpretación: Los resultados obtenidos antes y después de la implementación de Squid-monitor, evidenciaron un efecto positivo y estadísticamente significativo sobre la dimensión Utilización de Recursos de la variable dependiente Gestión de la red de datos en la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L; La prueba t para muestras relacionadas mostró un valor de t(12) = 9.831 con una significancia bilateral de p = 0.000 en la dimensión Utilización de Recursos, mientras que para la variable independiente Squid-monitor se obtuvo t(12) = 14.558 con p = 0.000. En ambos casos, los valores de significancia son inferiores a 0.05, lo que confirma la existencia de diferencias estadísticamente significativas entre las mediciones del pretest y del postest. Por lo tanto, se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alterna (H_1), concluyéndose que: La implementación de Squid-monitor si mejoró la utilización de recursos en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.

d) PRUEBA DE HIPÓTESIS ESPECIFICA 3

Paso 1: Planteamiento de la Hipótesis

Hipótesis, nula ($\boldsymbol{H0}$) = La implementación de Squid-monitor no mejoró el tratamiento de incidentes en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.

Hipótesis alterna ($\boldsymbol{H1}$) = La implementación de Squid-monitor si mejoró el tratamiento de incidentes en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.

Paso 02: Toma de decisiones:

Tabla 11:

Prueba de muestras relacionadas - Hipótesis Especifica 3

Prueba de muestras relacionadas									
		Diferencias relacionadas					t	gl	Sig. (bilateral)
		Media	Desviación típ.	Error típ. de la media	95% Intervalo de confianza para la diferencia Inferior	Superior			
Par 1	VI__POSTEST_SQUID_MONITOR - VI__PRETEST_SQUID_MONITOR	2,61538	,64777	,17966	2,22394	3,00683	14,558	12	,000
Par 2	DIM_POSTEST_INCIDENTES - DIM_PRETEST_INCIDENTES	2,65385	,83876	,23263	2,14699	3,16071	11,408	12	,000

Fuente: Elaboración- Propia

Interpretación: Los resultados obtenidos antes y después de la implementación de Squid-monitor, evidenciaron un efecto positivo y estadísticamente significativo sobre la dimensión Tratamiento de Incidentes de la variable dependiente Gestión de la red de datos en la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L; La prueba t para muestras relacionadas arrojó un valor de t(12) = 11.408 con una significancia bilateral de p = 0.000 para la dimensión Tratamiento de Incidentes, mientras que para el valor global correspondiente a Squid-monitor se obtuvo t(12) = 14.558 con p = 0.000.

En ambos casos, los valores de p son inferiores al nivel de significancia de 0.05, lo que indica la existencia de diferencias estadísticamente significativas entre las mediciones del pretest y el postest.

Por lo tanto, se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alterna (H_1), concluyéndose que: La implementación de Squid-monitor si mejoró el tratamiento de incidentes en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.

e) PRUEBA DE HIPÓTESIS ESPECIFICA 4

Paso 1: Planteamiento de la Hipótesis

Hipótesis, nula ($\boldsymbol{H0}$) = La implementación de Squid-monitor no mejoró la satisfacción de los usuarios que utilizaron la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.

Hipótesis alterna ($\boldsymbol{H1}$) = La implementación de Squid-monitor si mejoró la satisfacción de los usuarios que utilizaron la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.

Paso 02: Toma de decisiones:

Tabla 12:

Prueba de muestras relacionadas - Hipótesis Especifica 4

Prueba de muestras relacionadas									
		Diferencias relacionadas					t	gl	Sig. (bilateral)
		Media	Desviación típ.	Error típ. de la media	95% Intervalo de confianza para la diferencia				
					Inferior	Superior			
Par 1	VI__POSTEST_SQUID_MONITOR - VI__PRETEST_SQUID_MONITOR	2,61538	,64777	,17966	2,22394	3,00683	14,558	12	,000

Par 2	DIM_POSTEST_SATISFACCION - DIM_PRETEST_SATISFACCION	2,76923	,61629	,17093	2,39681	3,14165	16,201	12	,000

Fuente: Elaboración- Propia

Interpretación: Los resultados obtenidos antes y después de la implementación de Squid-monitor, reflejan un impacto estadísticamente significativo y positivo en la dimensión Satisfacción de los Usuarios de la variable dependiente Gestión de la red de datos en la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L; De acuerdo con los datos presentados en la Tabla N.° 10, la prueba t para muestras relacionadas mostró un valor de t(12) = 16.201 con una significancia bilateral de p = 0.000 para la dimensión Satisfacción de los Usuarios. Asimismo, el valor global correspondiente a la variable independiente Squid-monitor obtuvo t(12) = 14.558 con p = 0.000. Dado que ambos valores de p son menores que 0.05, se concluye que existen diferencias estadísticamente significativas entre los resultados del pretest y del postest.

Por lo tanto, se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alterna (H_1), concluyéndose que: La implementación de Squid-monitor si mejoró la satisfacción de los usuarios que utilizaron la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.

4.2. DISCUSIÓN DE RESULTADOS

Los resultados obtenidos confirman que la implementación de Squid-monitor mejoró significativamente la gestión de la red de datos en la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.,

lo que permitió aceptar la hipótesis alterna general. La prueba t de Student para muestras relacionadas evidenció diferencias significativas ($p < 0.001$) entre los valores del pretest y postest en todas las dimensiones analizadas, demostrando que la intervención tuvo un efecto real y positivo.

En la dimensión Seguridad, Squid-monitor fortaleció el control de accesos y la protección de la red, en coherencia con lo reportado por Litardo Ordoñez (2021) y Senteno (2021), quienes destacaron la eficacia de las herramientas de monitoreo para mitigar riesgos informáticos. En cuanto a la Utilización de recursos, se evidenció una optimización del ancho de banda y una administración más eficiente, en línea con lo planteado por Benavides Maldonado (2020).

Respecto al Tratamiento de incidentes, los resultados demuestran mejoras en la detección y resolución de fallas, lo que coincide con los aportes de De la Cruz Bernilla (2021) sobre la importancia de los mecanismos de monitoreo para mantener la estabilidad operativa. Finalmente, la Satisfacción de los usuarios también se incrementó significativamente, corroborando los hallazgos de López Larreynaga (2021) y Ochoa Quezada (2020), quienes señalaron que el uso adecuado de sistemas de control y seguridad incrementa la confianza y percepción positiva de los usuarios.

En conjunto, los hallazgos confirman todas las hipótesis alternas y respaldan la eficacia del sistema Squid-monitor como herramienta de mejora integral en seguridad, eficiencia y experiencia de usuario.

CONCLUSIONES

- Se concluye que la implementación del sistema *Squid-monitor* mejoró significativamente la gestión de la red de datos en la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L. La prueba *t* de Student para muestras relacionadas mostró diferencias estadísticamente significativas ($p < 0.001$) entre el pretest y el postest, evidenciando un impacto real y medible de la intervención.
- La implementación de *Squid-monitor* mejoró la seguridad en la red de datos, fortaleciendo el control de accesos, la protección frente a amenazas y el monitoreo de actividades en línea. Se comprobó la existencia de diferencias significativas ($t = 10.156$; $p < 0.001$) entre los resultados del pretest y postest, lo que confirma que la solución aplicada incrementó la confiabilidad y la integridad de la infraestructura tecnológica.
- *Squid-monitor* optimizó de manera significativa la utilización de los recursos de red, mejorando la eficiencia del uso del ancho de banda y reduciendo el consumo innecesario de tráfico. El contraste estadístico ($t = 9.831$; $p < 0.001$) validó que la herramienta contribuyó a una administración más racional de los recursos disponibles, favoreciendo la continuidad y el rendimiento de los servicios digitales.
- Los resultados confirmaron que *Squid-monitor* fortaleció el tratamiento de incidentes dentro de la red de datos, permitiendo una detección más rápida y una resolución oportuna de fallas. Los valores obtenidos ($t = 11.408$; $p < 0.001$) demuestran un efecto estadísticamente significativo,

evidenciando la capacidad del sistema para mejorar los procesos de respuesta y recuperación ante eventos críticos.

- Se concluye que la implementación de *Squid-monitor* incrementó significativamente la satisfacción de los usuarios de la red de datos ($t = 16.201$; $p < 0.001$). Este resultado refleja una percepción positiva sobre la estabilidad, seguridad y eficiencia del sistema, confirmando que la adopción de tecnologías de monitoreo mejora tanto la experiencia de uso como la confianza de los usuarios en el servicio.

RECOMENDACIONES O SUGERENCIAS

- En primer lugar, se sugiere mantener la implementación activa del sistema *Squid-monitor* como una herramienta permanente de monitoreo y control de la red, dado que su uso ha mostrado una mejora significativa en la gestión global de los recursos informáticos. Además, se recomienda actualizar periódicamente la configuración del sistema para adaptarlo a los cambios en la infraestructura tecnológica y garantizar la continuidad del rendimiento observado.
- Respecto a la seguridad de la red, se propone reforzar las políticas de control de acceso y autenticación de usuarios, integrando las alertas y reportes generados por *Squid-monitor* dentro de un plan de gestión de seguridad basado en las normas ISO/IEC 27001. Esto permitirá mantener la integridad y la confiabilidad de los datos ante nuevas amenazas o vulnerabilidades.
- En cuanto al uso de recursos, se aconseja implementar procedimientos de optimización continua, apoyándose en los informes de tráfico proporcionados por *Squid-monitor*, con el fin de identificar patrones de consumo y reducir el uso ineficiente del ancho de banda. Esta práctica contribuirá a una mayor sostenibilidad operativa y al ahorro de costos en la empresa.
- Sobre el tratamiento de incidentes, se recomienda establecer un protocolo institucional que aproveche las alertas automáticas del sistema para una respuesta más rápida ante fallos o anomalías. La integración de *Squid-monitor* con otros sistemas de gestión de eventos, podría fortalecer aún más la capacidad de detección y recuperación.

- Finalmente, se sugiere continuar evaluando periódicamente la satisfacción de los usuarios de la red, utilizando los indicadores generados por *Squid-monitor* como referencia para mejorar la calidad del servicio. Asimismo, se recomienda extender el uso del sistema a otras áreas de la organización, fomentando una cultura de monitoreo proactivo y gestión basada en evidencia.

REFERENCIAS BIBLIOGRÁFICAS

Arimetrics. (2025). *Implementación*, de https://www.arimetrics.com/glosario-digital/implementacion. Revisado el 20 de 03 de 2025

Benavides Maldonado, D. (2020). *Control del consumo de ancho de banda a travez de médotos heurísticos para el acceso a internet.* Ecuador: UTQ. Revisado el 19 de 03 de 2025

Cisco. (2025). *Administración de red*, de https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-network-management.html. Revisado el 20 de 03 de 2025

De la curz Bernilla, S. (2021). *Implementar una VPN con Open Source para la Gestión de intranet.* Lambayeque: UnPrg. Revisado el 06 de 02 de 2025

Frascati (2015), “Guía para la recopilación y presentación de información sobre la investigación y el desarrollo experimental”, https://www.ovtt.org/wp-content/uploads/2020/05/Manual_Frascati.pdf

Hernández Sampieri, Fernández Collado y Baptista Lucio (2010) – Metodología de la investigación Científica” (p. 115). Revisado el 07 de 02 de 2025

Kaseya. (2022). *Como trabaja la administración de la red*., de https://www.kaseya.com/blog/network-management/. Revisado el 20 de 03 de 2025

Litardo ordoñez, Y. (2021). *Reestructuración de los servicios de la red de datos mediante la implementación de un proxy en Linux.* Mexico: Ups. Revisado el 15 de 03 de 2025

López Larreynaga, J. (2021). *Una propuesta de configuración de seguridad a la red informática de una comunidad educativa.* El salvador: Utes. Revisado el 06 de 02 de 2025

Pratama, D. (2023). *Proxy Squid* de https://www.alibabacloud.com/blog/what-is-squid-proxy_599982. Revisado el 20 de 03 de 2025,

Ruiz Bolívar, C. (2010). “Construcción de Instrumentos de Medición en Ciencias Sociales”. Revisado el 22 de 03 de 2025

Senteno, J. (2021). *Propuesta de un interceptor procy como modelo seguro de acceso a la WEB.* Lima: Ucc. Revisado el 20 de 02 de 2025

Simbiotecs. (2025). *Gestión*, de https://simbiotecs.com/blog/que-es-gestion-ejemplos/. Revisado el 20 de 03 de 2025

Spiceworks. (2025). *Componentes claves de la administración de redes*., de https://www.spiceworks.com/tech/networking/articles/what-is-network-management/. Revisado el 20 de 03 de 2025

Susnjara, S. (2025). *Sistema de administración de red*., de https://www.ibm.com/think/topics/network-management. Revisado el 20 de 03 de 2025

Tabra Ochoa, E. (2021). *El rol del servidor proxy en el gobierno de una empresa.* Lima: Pucp. Revisado el 12 de 03 de 2025

Televes. (2025). *Red de datos*., de https://blogcorporation.televes.com/telecom-tv/que-es-una-red-de-datos. Revisado el 20 de 03 de 2025

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Lawrence Erlbaum Associates. https://www.taylorfrancis.com/books/mono/10.4324/9780203771587/statistical-power-analysis-behavioral-sciences-jacob-cohen

Field, A. (2018). *Discovering statistics using IBM SPSS statistics* (5th ed.). SAGE Publications. https://profandyfield.com/discoverse/dsus/

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la investigación* (6.ª ed.). McGraw-Hill Educación. https://bibliotecadoloresmedina.omeka.net/items/show/176

ANEXOS

Anexo 1: Matriz de consistencia

<table>
<tr><th>Formulación del problema</th><th>Objetivos</th><th>Hipótesis</th><th>Variables/ Dimensiones e indicadores</th><th>Metodología de la investigación</th></tr>
<tr>
<td>¿De qué manera la implementación de Squid-monitor mejora la gestión de la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.?</td>
<td>Implementar Squid-monitor para la mejora de la gestión de la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.</td>
<td>La implementación de Squid-monitor mejora la gestión de la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.</td>
<td rowspan="5">
Variable Independiente: Squid-monitor
<table>
<tr><th>Variable</th><th>Dimensiones</th><th>Indicadores</th></tr>
<tr><td rowspan="3">Squid-monitor</td><td>Privacidad</td><td>% de Filtrado Restricciones</td></tr>
<tr><td>Rendimiento</td><td>% de Caching Balanceo de carga</td></tr>
<tr><td>Control y Gestión</td><td>% de Acceso Supervisión</td></tr>
</table>
Variable dependiente: Gestión de la red de datos.
<table>
<tr><th>Variable</th><th>Dimensiones</th><th>Indicadores</th></tr>
<tr><td rowspan="4">Gestión de la red de datos.</td><td>Seguridad</td><td>% de mejora de Controles</td></tr>
<tr><td>Recursos</td><td>% de optimización de hardware/software</td></tr>
<tr><td>Incidentes</td><td>% de reducción de incidentes</td></tr>
<tr><td>Satisfacción</td><td>% de Satisfacción Conformidad</td></tr>
</table>
</td>
<td rowspan="5">
Tipo de investigación: Aplicada
Nivel de Investigación: El nivel de investigación fue explicativo, porque permitió demostrar cómo la implementación de Squid-monitor mejoró la gestión de la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L., identificando su influencia en la seguridad, utilización de recursos, tratamiento de incidentes y satisfacción de los usuarios.
Población:
La población estuvo conformada por el personal de las distintas áreas de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L., integrada por 13 empleados que participaron directa o indirectamente en el uso y gestión de la red de datos.
Muestra
Debido al tamaño reducido de la población, se aplicó un muestreo no probabilístico por conveniencia, considerando como muestra total a los 13 empleados de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.
Este enfoque permitió obtener información completa y precisa, al incluir a todos los usuarios involucrados en la gestión de la red.

Diseño:
Ecuación 1: Método “Pre test – Post test”.
GE: O1 -> X -> O2
Donde:
GE: Grupo Pre Experimental
O1: Datos de la Pre - Prueba para los indicadores de la variable dependiente antes de valorar el Squid-monitor evaluando la Gestión de la red de datos.
X: La propuesta de Squid-monitor evaluando la Gestión de la red de datos = Estimulo o condición experimental.
O2: Datos de la Post- Prueba para los indicadores de la variable dependiente antes de valorar el Squid-monitor evaluando la Gestión de la red de datos.
</td>
</tr>
<tr>
<td>¿De qué manera la implementación de Squid-monitor mejora la seguridad en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.?</td>
<td>Evaluar de qué manera la implementación de Squid-monitor mejora la seguridad en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.</td>
<td>La implementación de Squid-monitor mejora la seguridad en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.</td>
</tr>
<tr>
<td>¿De qué manera la implementación de Squid-monitor mejora la utilización de recursos en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.?</td>
<td>Analizar cómo la implementación de Squid-monitor mejora la utilización de recursos en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.</td>
<td>La implementación de Squid-monitor mejora la utilización de recursos en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.</td>
</tr>
<tr>
<td>¿De qué manera la implementación de Squid-monitor mejora el tratamiento de incidentes en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.?</td>
<td>Determinar en qué medida la implementación de Squid-monitor mejora el tratamiento de incidentes en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.</td>
<td>La implementación de Squid-monitor mejora el tratamiento de incidentes en la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.</td>
</tr>
<tr>
<td>¿De qué manera la implementación de Squid-monitor mejora la satisfacción de los usuarios que utilizaron la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.?</td>
<td>Valorar cómo la implementación de Squid-monitor mejora la satisfacción de los usuarios que utilizaron la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.</td>
<td>La implementación de Squid-monitor mejora la satisfacción de los usuarios que utilizaron la red de datos de la COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA E.I.R.L.</td>
</tr>
</table>

Anexo 2: Cuestionario de preguntas.

"IMPLEMENTACIÓN DE SQUID-MONITOR PARA LA GESTIÓN DE LA RED DE DATOS DE LA COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA EIRL"

El presente cuestionario tiene como finalidad recopilar información de indicadores correspondientes a las variables principales de la investigación, se le solicita responder las preguntas con mayor seguridad y exactitud, a fin de poder contar con datos relevantes.

INDICACIONES

- Marque con X en el cuadro que considere el valor adecuado como respuesta a las preguntas específicas.

Escala de Likert

Reseña de recolección de datos

Valor numérico	Descripción
1	Muy bajo
2	Bajo
3	Regular
4	Alto
5	Muy alto

Preguntas:
VARIABLE INDEPENDIENTE
Dimensión 1: Privacidad

Nro.	Pregunta	1	2	3	4	5
P01	Según su conocimiento del caso, ¿Cómo calificaría el nivel las operaciones de filtrado de contenido en el acceso a páginas web?					
P02	Según su conocimiento del caso, ¿Cómo calificaría la precisión de filtrado de contenido en el acceso a páginas web?					

Nro.	Pregunta	1	2	3	4	5
P03	Según su conocimiento del caso, ¿Cómo calificaría el nivel de restricciones implementadas para el acceso a contenidos web?					

P04	Según su conocimiento del caso, ¿Cómo calificaría al número de restricciones implementadas para el acceso a contenidos web?					

Dimensión 2: Rendimiento

Nro.	Pregunta	1	2	3	4	5
P05	Según su conocimiento del caso, ¿Cómo calificaría al uso de caching como parte del acceso a páginas web?					
P06	Según su conocimiento del caso, ¿Cómo calificaría la configuración de caching como parte del acceso a páginas web?					

Nro.	Pregunta	1	2	3	4	5
P07	Según su conocimiento del caso, ¿Cómo calificaría la configuración del balance de carga del servicio de internet?					
P08	Según su conocimiento del caso, ¿Cómo calificaría la eficacia del balance de carga del servicio de internet?					

Dimensión 3: Control y Gestión

Nro.	Pregunta	1	2	3	4	5
P09	Según su conocimiento del caso, ¿Cómo calificaría el control de acceso a páginas web?					
P10	Según su conocimiento del caso, ¿Cómo calificaría la practicidad de la gestión de acceso a páginas web?					

Nro.	Pregunta	1	2	3	4	5
P11	Según su conocimiento del caso, ¿Cómo calificaría el nivel de supervisión de las peticiones de acceso web?					
P12	Según su conocimiento del caso, ¿Cómo calificaría la exactitud del proceso de supervisión de las peticiones de acceso web?					

VARIABLE DEPENDIENTE

Dimensión 1: Seguridad

Nro	Pregunta	1	2	3	4	5
P13	Según su conocimiento del caso, ¿Cómo calificaría al nivel seguridad propuesto como parte de la Gestión de red de datos?					
P14	Según su conocimiento del caso, ¿Cómo calificaría al nivel seguridad implementado como parte de la Gestión de red de datos?					

Nro	Pregunta	1	2	3	4	5
P15	Según su conocimiento del caso, ¿Cómo calificaría al número de controles propuesto como parte de la Gestión de red de datos?					
P16	Según su conocimiento del caso, ¿Cómo calificaría al número de controles implementados como parte de la Gestión de red de datos?					

Dimensión 2: Recursos

Nro	Pregunta	1	2	3	4	5
P17	Según su conocimiento del caso, ¿Cómo calificaría al número de componentes de tipo hardware propuesto como parte de la Gestión de red de datos?					
P18	Según su conocimiento del caso, ¿Cómo calificaría al número de componentes de tipo hardware implementados como parte de la Gestión de red de datos?					

Nro	Pregunta	1	2	3	4	5
P19	Según su conocimiento del caso, ¿Cómo calificaría al número de componentes de tipo software propuesto como parte de la Gestión de red de datos?					
P20	Según su conocimiento del caso, ¿Cómo calificaría al número de componentes de tipo software implementados como parte de la Gestión de red de datos?					

Dimensión 3: Incidentes

Nro	Pregunta	1	2	3	4	5
P21	Según su conocimiento del caso, ¿Cómo calificaría la frecuencia de incidentes detectados como parte de la Gestión de red de datos? ?					
P22	Según su conocimiento del caso, ¿Cómo calificaría la frecuencia de incidentes tratados como parte de la Gestión de red de datos? ?					

Nro	Pregunta	1	2	3	4	5
P23	Según su conocimiento del caso, ¿Cómo calificaría el tiempo de impacto de negativo sobre el servicio de acceso a través de la red de datos?					

P24	Según su conocimiento del caso, ¿Cómo calificaría el tiempo de respuesta para el tratamiento de incidentes presentados en el servicio de acceso a través de la red de datos?					

Dimensión 4: Satisfacción

Nro.	Pregunta	1	2	3	4	5
P25	Según su conocimiento del caso, ¿Cómo calificaría el nivel de satisfacción del uso de los servicios de acceso a la red de datos?					
P26	Según su conocimiento del caso, ¿Cómo calificaría el nivel de satisfacción respecto de la seguridad de acceso a servicio de la red de datos?					

Nro.	Pregunta	1	2	3	4	5
P27	Según su conocimiento del caso, ¿Cómo calificaría el nivel de conformidad del uso de los servicios de acceso a la red de datos?					
P28	Según su conocimiento del caso, ¿Cómo calificaría el nivel de conformidad respecto de la seguridad de acceso a servicio de la red de datos?					

Anexo 3: Validación de Fiabilidad Alpha Cronbach

a) INSTRUMENTOS

La validez del instrumento se realizará mediante el análisis de Alfa de Cronbach[1], dicho coeficiente determina, la consistencia interna de una prueba, analizando la correlación, media de una variable con todas las demás que la integran. Por lo general, toma valores dentro del intervalo [0,1], donde un valor próximo al límite inferior indica una consistencia escasa, es decir, con una gran variabilidad de los temas tratados, y, por el contrario, un valor próximo a la unidad conllevaría a un alto de grado de consistencia. No obstante, pudiera tomar valores negativos, lo que indicaría que en el cuestionario hay preguntas que recogen temas opuestos al resto.

Como criterio general, Ruiz Bolívar[2] (2010, p.39) sugieren, las recomendaciones siguientes, para evaluar los coeficientes de alfa de Cronbach:

Tabla 13:

Escala de Alfa de Cronbach

Escala	Descripción - Nivel
0.01 α 0.20	Muy Baja
0.21 α 0.40	Baja
0.41 α 0.60	Moderada
0.61 α 0,80	Alta
0.81 α 1	Muy Alta

Fuente: Construcción de Instrumentos de Medición en Ciencias Sociales.

[1] Hernández Sampieri, Fernández Collado y Baptista Lucio (2010)– Metodología de la investigación Científica 5ta Edición "Instrumentos de Medición" (p. 200)

[2] Ruiz Bolívar, C. (2010). "Construcción de Instrumentos de Medición en Ciencias Sociales"

Tabla 14:

Análisis de Fiabilidad – Pretest

Estadísticos de fiabilidad	
Alfa de Cronbach	N de elementos
,877	28

Fuente: Elaboración Propia

Tasa Porcentual: 87.7% de Fiabilidad, con etiqueta de valor <Muy Alta>

Tabla 15:

Análisis de Fiabilidad – Postest

Estadísticos de fiabilidad	
Alfa de Cronbach-	N de elementos
,908	28

Fuente: Elaboración- Propia

Tasa Porcentual: 90.8% en Fiabilidad, con etiqueta de valor <Muy Alta>

Anexo 4: "IMPLEMENTACIÓN DE SQUID-MONITOR PARA LA GESTIÓN DE LA RED DE DATOS DE LA COMPAÑÍA DE SERVICIOS EN TECNOLOGÍA E INFORMÁTICA EIRL"

1. DISEÑO DE LA SOLUCIÓN

1.1. Diagnóstico de la situación actual de la red de datos

1.1.1. Infraestructura tecnológica existente

En este punto, se procederá a describir el entorno tecnológico actual de la compañía de Servicios en Tecnología e Informática E.I.R.L, para poder identificar los recursos disponibles que se relacionan con el squit-monitor.

Estructura de red

La estructura de la red está organizada a través de un modelo cliente – servidor.

La topología de red es del tipo estrella.

Se posee un router principal para el acceso a internet a través del operador Telefónica.

Como parte de los equipos de red se encuentran switch no administrables y punto de acceso inalámbricos.

El tráfico wed sale directamente hacia internet sin contar con un filtro, esto dificulta el control y el proceso de auditoría de recursos de red.

Equipamiento existente:

Tipo de equipo	Cantidad	Función principal
Servidor principal Windows Server	1	Alojamiento archivos y recursos compartidos
Estaciones de trabajo entre PCs y laptops	14	Operaciones administrativas
Equipos de red (routers, switches, APs)	3	Conectividad y segmentación de red

Fuente: elaboración propia

Servicios actuales

- **Servidores**: un servidor de archivos y servicios de red.
- **Conectividad**: Red LAN interna con salida a internet a través de NAT
- **Gestión**: No disponible, se carece de herramientas de monitoreo de tráfico.
- **Seguridad**: Sin filtrado de contenidos.

1.1.2. Políticas de seguridad vigentes

Actualmente, la empresa no cuenta con normas claras y escritas para mantener la seguridad de su red informática. En cambio, dependen de la configuración de los dispositivos y de las decisiones de los técnicos. Por ello, es más difícil controlar lo que ocurre en la red y responder con rapidez si algo falla. Por eso quieren empezar a usar una herramienta llamada Squid-Monitor. Esta les ayudará a crear normas sobre quién puede acceder a qué, ver qué hacen los usuarios en línea y registrar la actividad web para mayor seguridad.

1.1.3. Uso actual del ancho de banda

Actualmente, todo el tráfico de internet, ya sea laboral o recreativo, pasa por la misma ruta. Por ello, a veces hay mucha congestión, sobre todo cuando se ven vídeos, se juega en redes sociales o se descargan archivos grandes. Esto hace que internet sea lento o esté congestionado en horas punta. La empresa E.I.R.L. cuenta con una conexión a internet especial proporcionada por Telefónica del Perú. Esta conexión es muy rápida, con una velocidad de 400 Mbps, y todos los empleados de la empresa la utilizan para conectarse.

1.1.4. Identificación de incidentes frecuentes

Se han presentado algunos problemas con el servicio de internet en Compañía de Servicios en Tecnología e Informática E.I.R.L. que lo hacen más lento, menos confiable o menos seguro. Estos problemas ocurren a menudo porque no existe un sistema único encargado de supervisar y gestionar todo el tráfico de internet para garantizar un funcionamiento fluido.

Entre los incidentes más frecuentes se destacan los siguientes:

La empresa no cuenta con un sistema específico para detectar automáticamente la causa de estos problemas de internet. Por lo tanto, los técnicos o trabajadores deben detectar los problemas e informar a alguien. Esto puede llevar mucho tiempo y es difícil saber exactamente qué causó el problema o cómo solucionarlo. Mediante

una nueva herramienta llamada Squid-Monitor, la empresa podrá ver cómo todos usan internet en tiempo real. Esto ayudará a detectar problemas con anticipación, determinar su origen y evitar que se repitan. Esto hará que internet sea más rápido, seguro y mejor para todos. Si internet no funciona bien, es difícil que las personas en el trabajo realicen sus tareas.

A veces, las personas visitan sitios web que no deberían o que podrían ser peligrosos. También pueden descargar archivos que podrían causar problemas o virus.

1.2. Requerimientos técnicos y funcionales del Sistema

1.2.1. Requerimientos de hardware

Dado que Squid es como un intermediario que le ayuda a navegar por Internet más rápido al guardar algunos sitios web, y Squid-Monitor es una herramienta que observa y muestra lo que sucede con esas solicitudes de sitios web, el equipo informático que elija debe ser lo suficientemente.

Tomando en cuenta de la cantidad de usuarios y del ancho de banda de 400 Mbps, se plantean los siguientes requerimientos mínimos:

Componente	Requerimiento mínimo	Justificación
Procesador	Intel Core i5	Gestiona eficientemente múltiples solicitudes HTTP simultáneas. Mejora la velocidad de respuesta del proxy al mantener en memoria los objetos a los que se accede con más frecuencia. Almacena registros, archivos de caché e
Memoria RAM	8 GB	
Almacenamiento (Disco duro / SSD)	500 GB HDD	
Tarjeta de red (NIC)	1 Gbps	

		informes generados por Squid-Monitor. Aumenta el rendimiento y separa el tráfico interno del externo. Garantiza la continuidad del servicio incluso durante cortes de energía.
Fuente de poder / UPS	500 W + UPS de respaldo	

Fuente: elaboración propia

1.2.2. Requerimientos de software

Para usar Squid-Monitor correctamente, su computadora debe estar configurada de forma segura y segura para que funcione correctamente con el internet de la empresa. Esta configuración le permitirá instalar el proxy Squid (que ayuda a controlar el uso de internet), controlar los sitios web que visitan los usuarios y generar informes que muestren cuánto usan internet y qué hacen en línea.

A continuación, se detallan los principales requerimientos de software:

Componente	Descripción	Función
Sistema operativo	Linux Ubuntu Server 22.04 LTS	Este es un sistema informático especial que ayuda a gestionar el uso de internet. Interactúa entre las personas de una escuela o empresa y el internet externo. Comprueba qué sitios web se visitan, registra esa información y puede bloquear o permitir el acceso a ciertos sitios. También crea imágenes y gráficos para mostrar los sitios web más utilizados. Los informes se pueden ver en un sitio web para que la persona responsable pueda comprender qué está
Proxy Server	Squid versión 5.x o superior	
Herramienta de monitoreo	Squid-Monitor	
Servidor web	Apache2	
Base de datos (opcional)	MariaDB	
Paquetes complementarios	Perl, PHP, Python	
Navegador web	Mozilla Firefox / Google Chrome	

	sucediendo. Todos los registros e informes se guardan de forma segura para que se puedan consultar más tarde. Además, funciona con herramientas que realizan tareas automáticamente y ayudan a analizar el uso de internet fácilmente.

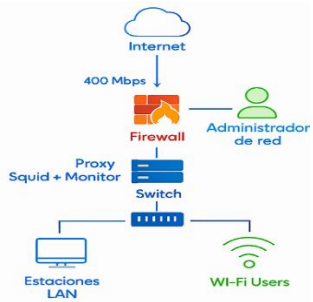
Fuente: elaboración propia

1.3. Diseño de la arquitectura de red con Squid-Monitor

Esta la siguiente imagen muestra cómo se configura una red informática para garantizar su seguridad y correcto funcionamiento. La conexión a internet es muy rápida y, antes de que las computadoras puedan usarla, pasa por un control de seguridad llamado firewall para evitar el acceso de elementos no deseados. Luego, pasa por un servidor especial llamado proxy, que ayuda a supervisar y controlar la entrada y salida de datos. A continuación, la conexión se conecta a un conmutador, que actúa como un director de tráfico y divide la red en dos partes: una para computadoras de escritorio (LAN) y otra para usuarios de red inalámbrica (wi-fi).

Figura 6:

Arquitectura Squid-Monitor.



Fuente: Elaboración propia.

1.4. Plan de seguridad y respaldo

A continuación, se detalla el plan de seguridad y respaldo:

Tabla 16:
Plan de seguridad y respaldo.

Aspecto	Medida principal	Objetivo	Responsable
Control de acceso	Autenticación segura y deshabilitar acceso remoto por root	Evitar accesos no autorizados	Administrador de red
Actualizaciones del sistema	Activar actualizaciones automáticas de seguridad	Proteger contra vulnerabilidades	Administrador de red
Firewall y puertos	Configurar firewall (ufw/iptables) con puertos limitados	Bloquear accesos externos no deseados	Administrador de red
Copia de configuración	Respaldos semanales de archivos clave	Restauración rápida ante fallos	Administrador de red
Respaldo de logs	Copias diarias automáticas de logs por 30 días	Trazabilidad y análisis histórico	Administrador de red
Ubicación de respaldos	Almacenamiento en NAS interno y unidad externa cifrada	Disponibilidad y redundancia	Administrador de sistemas
Cifrado de datos sensibles	Uso de SSL/TLS en administración web	Proteger la confidencialidad	Administrador de red
Política de retención	Mantener respaldos semanales (3 meses) y mensuales (1 año)	Buenas prácticas de conservación	Gerencia de TI
Monitoreo y auditoría	Revisión periódica de logs y reportes del proxy	Detectar anomalías o intrusiones	Administrador de red
Pruebas de restauración	Verificación trimestral de restauración de respaldos	Validar efectividad del plan de recuperación	Administrador de red

Fuente: elaboración propia

2. IMPLEMENTACIÓN DE SQUID-MONITOR

2.1. Preparación del entorno de instalación

Es fundamental tener todo listo antes de instalar Squid y Squid-Monitor. Esto ayuda a garantizar su correcto funcionamiento y seguridad. Durante este

paso, configuramos el hardware y los programas del ordenador para que todo esté en su lugar. De esta manera, el sistema puede supervisar y controlar la red correctamente y funcionar sin problemas.

Aspecto	Acción principal	Objetivo
Tipo de servidor	Mencionado en el 1	Garantizar rendimiento óptimo para Squid y gestión de logs.
Sistema operativo	Instalar Ubuntu Server 22.04 LTS	Asegurar estabilidad, soporte y compatibilidad del entorno.
Red y conectividad	Asignar IP estática (ej. 192.168.1.10), configurar DNS corporativo y gateway con ancho de banda de 400 Mbps.	Mantener conectividad constante y direccionamiento fijo.
Zona horaria / NTP	Establecer zona horaria *America/Lima* y sincronizar reloj mediante NTP.	Garantizar precisión en registros y auditorías.
Dependencias	Instalar servicios base: Apache2/Nginx, PHP, Squid, y herramientas de monitoreo como SARG o SquidAnalyzer.	Habilitar funcionalidades esenciales y análisis de tráfico.
Pruebas básicas	Verificar conectividad (ping, DNS) y estado de servicios (Squid, Apache) antes de configuración final.	Validar correcto funcionamiento previo a implementación.
Seguridad inicial	Actualizar sistema, configurar firewall (puertos 22, 80, 443, 3128), crear usuario seguro y desactivar acceso SSH por root.	Reforzar la seguridad del servidor desde el inicio.
Validación final	Comprobar acceso web, operación de Squid y generación de reportes de monitoreo.	Confirmar que el entorno está listo para producción.

Fuente: elaboración propia

2.2. Instalación y configuración de Squid

Instalar y configurar el servidor proxy Squid es la parte principal de cómo observamos y administramos el flujo de tráfico de Internet, a continuación, se detallan los pasos:

Instalación del servicio Squid

- Actualización del sistema

```
sudo apt update && sudo apt upgrade -y
```

- Instalación de Squid

```
sudo apt install squid -y
```

- Verificar instalación

```
squid -v
```

- Iniciar y habilitar servicio

```
sudo systemctl enable squid
sudo systemctl start squid
```

Configuración del archivo

El archivo principal de configuración de Squid se encuentra en:

/etc/squid/squid.conf

```
# ==============================
# CONFIGURACIÓN BÁSICA DE SQUID
# Compañía de Servicios en Tecnología e Informática E.I.R.L.
# ==============================
```

```
# Puerto en el que escuchará el proxy
http_port 3128
# Nombre visible del servidor proxy
visible_hostname proxy-empresa
# ============================
# DEFINICIÓN DE RED LOCAL
# ============================
# Permitir acceso solo a la red interna (LAN)
acl localnet src 192.168.1.0/24
acl localhost src 127.0.0.1/32
# ============================
# POLÍTICAS DE ACCESO
# ============================
# Permitir acceso desde la red local y localhost
http_access allow localnet
http_access allow localhost
# Denegar todo lo demás (por seguridad)
http_access deny all
# ============================
# CONFIGURACIÓN DE CACHÉ
# ============================
# Tamaño de la memoria caché (RAM)
cache_mem 512 MB
```

```
# Tamaño máximo de objetos que se almacenan en caché
maximum_object_size 50 MB
# Directorio en disco para caché
cache_dir ufs /var/spool/squid 2000 16 256
# ============================
# REGISTROS (LOGS)
# ============================
# Ruta del archivo de accesos
access_log /var/log/squid/access.log
# Log de errores y eventos
cache_log /var/log/squid/cache.log
# ============================
# PARÁMETROS DE RENDIMIENTO
# ============================
# Tiempo de vida (TTL) del contenido almacenado en caché
refresh_pattern ^ftp:          1440    20%     10080
refresh_pattern ^gopher:       1440    0%      1440
refresh_pattern -i (/cgi-bin/|\?) 0     0%      0
refresh_pattern .              1440    20%     4320
# ============================
```

2.3. Integración e instalación de Squid-Monitor

Se procederá con integrar una herramienta de monitoreo (SARG) para analizar los registros del proxy Squid y generar reportes.

Pasos para la instalación y configuración

Instalar SARG (Squid Analysis Report Generator):

```
sudo apt install sarg -y
```

Verificar instalación correcta:

```
sarg -v
```

Crear el directorio para los reportes:

```
sudo mkdir -p /var/www/html/squid-reports
```

Editar el archivo de configuración principal de SARG:

```
access_log /var/log/squid/access.log

output_dir /var/www/html/squid-reports

title "Reportes de uso de Internet – CSTI EIRL"

date_format e
```

2.4. Configuración de políticas de seguridad

2.4.1. Control de acceso y filtrado de contenido

A continuación de describen los pasos a seguir:

1. **Definir listas de control de acceso (ACL):**
   - Crear grupos de IP o usuarios con permisos diferenciados.
   - Ejemplo: permitir acceso completo a administración y restringido a otras áreas.
2. **Configurar políticas de filtrado:**
   - Bloquear sitios con contenido no laboral (redes sociales, streaming, juegos).
   - Establecer horarios de acceso o límites por tipo de contenido.

3. **Activar el filtrado por palabras clave o dominios:**
    - Ingresar en la GUI de Squid-Monitor la lista de términos prohibidos.
    - Ejemplo: “facebook”, “youtube”, “torrent”.
4. **Registrar y monitorear accesos:**
    - Revisar reportes automáticos generados por Squid-Monitor.
    - Detectar intentos de acceso a sitios restringidos.
5. **Actualizar las políticas periódicamente:**
    - Mantener listas de control y dominios actualizadas según las necesidades de seguridad de la empresa.

2.4.2. Bloqueo de sitios y control de descargas

A continuación, se detallan los pasos:

Definir listas de sitios bloqueados:

Crear un archivo de texto con dominios no permitidos

```
/etc/squid/denied_sites.txt
```

Con el siguiente contenido:

```
facebook.com
youtube.com
netflix.com
```

En el archivo squid.conf agregar:

```
acl sitios_bloqueados dstdomain "/etc/squid/denied_sites.txt"
http_access deny sitios_bloqueados
```

Configurar control de descargas por tipo de archivo:

Bloquear extensiones peligrosas o no laborales

```
acl archivos_prohibidos url_regex -i \.mp3$ \.mp4$ \.exe$ \.zip$
http_access deny archivos_prohibidos
```

2.5. Configuración de alertas y reportes de incidentes

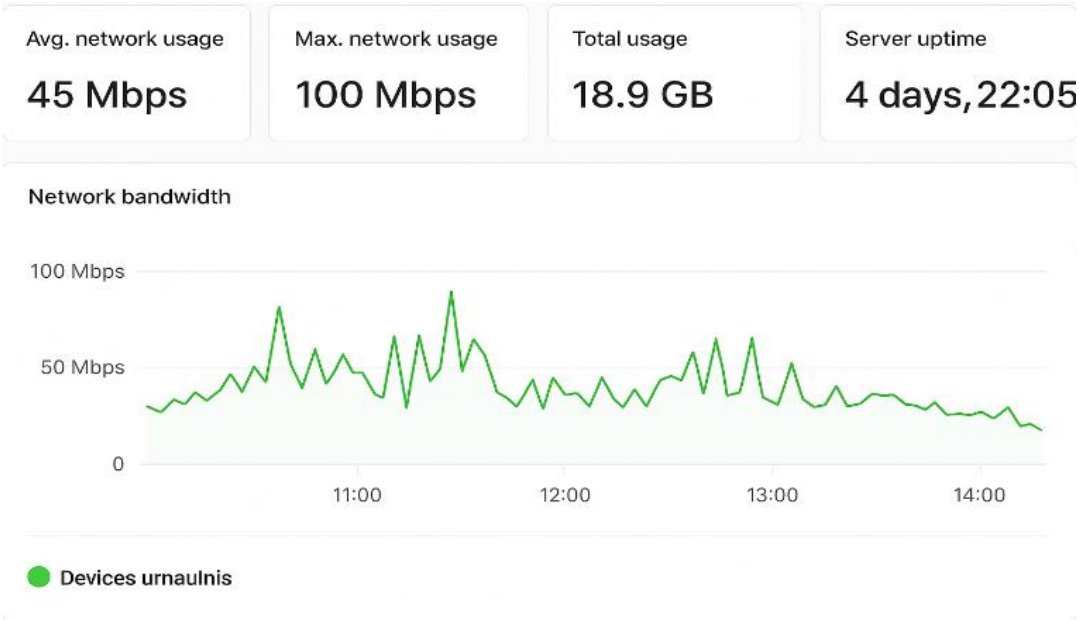
Activar el registro de incidentes en Squid: Verificar que el archivo de logs esté activo:

```
access_log /var/log/squid/access.log
cache_log /var/log/squid/cache.log
```

Integrar los logs con Squid-Monitor (SARG o SquidAnalyzer): Configurar en /etc/sarg/sarg.conf la ruta de los logs:

```
access_log /var/log/squid/access.log
```

2.6. Monitoreo y análisis de desempeño de red



Fuente: Elaboración propia

Tabla 17:

Análisis de Fiabilidad – Post test

Resultados y Cálculo de la Mejora tras la Implementación de Squid-monitor

Hipótesis	Dimensión / Variable	Media Pretest	Media Postest	Diferencia (Post–Pre)	Cálculo (fórmula aplicada)	Mejora (%)
General	(Squid-monitor)	2.38	5.00	2.62	(5.00−2.38) ÷ 5 × 100 = 52.3%	52.3%
Específica 1	Seguridad	2.38	4.92	2.54	(4.92−2.38) ÷ 5 × 100 = 50.8%	50.8%
Específica 2	Utilización de recursos	2.38	4.86	2.48	(4.86−2.38) ÷ 5 × 100 = 49.6%	49.6%
Específica 3	Tratamiento de incidentes	2.38	5.03	2.65	(5.03−2.38) ÷ 5 × 100 = 53.0%	53.0%
Específica 4	Satisfacción de usuarios	2.38	5.15	2.77	(5.15−2.38) ÷ 5 × 100 = 55.4%	55.4%

Fuente: Elaboración Propia

3. JUSTIFICACIÓN CIENTÍFICA Y ESTADÍSTICA DEL CÁLCULO DEL PORCENTAJE DE MEJORA

El cálculo del porcentaje de mejora se fundamenta en el diseño metodológico pre experimental con medición pretest y post test, aplicado a un solo grupo. Este diseño permite comparar los valores obtenidos antes y después de la intervención (implementación de *Squid-monitor*), con el fin de determinar cuantitativamente el impacto en la gestión de la red de datos. Según Hernández, Fernández y Baptista (2022), este enfoque es adecuado para medir la influencia directa de una variable independiente sobre una dependiente en condiciones controladas.

Desde el punto de vista estadístico, se utilizó la prueba t de Student para muestras relacionadas, la cual permitió identificar diferencias significativas entre

las medias del pretest y post test. Sin embargo, para complementar el análisis inferencial y expresar los resultados en términos prácticos, se calculó un porcentaje de mejora, aplicando la siguiente fórmula:

$$Mejora\ (\%) = \frac{(Media_{Postest} - Media_{Pretest}}{Valor\ máximo\ de\ la\ escala}\ x\ 100$$

En este estudio, el valor máximo de la escala fue 5, correspondiente al nivel más alto de desempeño medido en cada dimensión. Esta expresión cuantifica el grado de avance respecto al potencial total de mejora, permitiendo evidenciar de manera porcentual la efectividad de la implementación del sistema.

El uso de indicadores que expresen la magnitud del cambio tras una intervención tiene respaldo metodológico y científico. Cohen (1988) enfatiza la importancia de complementar los resultados de significancia estadística con medidas del tamaño del efecto, ya que estas permiten valorar la relevancia práctica de los hallazgos más allá del valor p. De forma coincidente, Field (2018) sostiene que la inclusión de medidas de tamaño del efecto y proporciones de cambio contribuye a una interpretación más comprensible y aplicada de los resultados experimentales, al reflejar la magnitud real de la diferencia entre condiciones.

En este contexto, el cálculo porcentual de mejora empleado en esta investigación se justifica como una medida descriptiva válida, que permite representar cuantitativamente el impacto de la implementación del sistema Squid-monitor sobre la gestión de la red de datos, complementando el análisis estadístico inferencial.