Universidad Continental

FACULTAD DE INGENIERÍA

Escuela Académico Profesional de Ingeniería de Sistemas e Informática

Tesis

Diseño e Implementación de un servidor de registros Syslog para gestionar los eventos de red en la infraestructura tecnológica de Telecable

Geanpool Matias Canchari Flores
Antoni Maycol Navarro Roman

Para optar el Título Profesional de
Ingeniero de Sistemas e Informática

Huancayo, 2025

INFORME DE CONFORMIDAD DE ORIGINALIDAD DE TRABAJO DE INVESTIGACIÓN

A	**:**	Decano de la Facultad de Ingeniería
DE	**:**	Giancarlo Condori Torres Asesor de trabajo de investigación
ASUNTO	**:**	Remito resultado de evaluación de originalidad de trabajo de investigación
FECHA	**:**	26 de Agosto de 2025

Con sumo agrado me dirijo a vuestro despacho para informar que, en mi condición de asesor del trabajo de investigación:

Título:
Diseño e Implementación de un servidor de registros Syslog para gestionar los eventos de red en la infraestructura tecnológica de Telecable

Autores:
1. Geanpool Matias Canchari Flores – EAP. Ingeniería de Sistemas e Informática
2. Antoni Maycol Navarro Roman – EAP. Ingeniería de Sistemas e Informática

Se procedió con la carga del documento a la plataforma "Turnitin" y se realizó la verificación completa de las coincidencias resaltadas por el software dando por resultado 13 % de similitud sin encontrarse hallazgos relacionados a plagio. Se utilizaron los siguientes filtros:

- Filtro de exclusión de bibliografía — SI [X] NO [ ]
- Filtro de exclusión de grupos de palabras menores — SI [X] NO [ ]
  N° de palabras excluidas **(40)**:
- Exclusión de fuente por trabajo anterior del mismo estudiante — SI [ ] NO [X]

En consecuencia, se determina que el trabajo de investigación constituye un documento original al presentar similitud de otros autores (citas) por debajo del porcentaje establecido por la Universidad Continental.

Recae toda responsabilidad del contenido del trabajo de investigación sobre el autor y asesor, en concordancia a los principios expresados en el Reglamento del Registro Nacional de Trabajos conducentes a Grados y Títulos – RENATI y en la normativa de la Universidad Continental.

Atentamente,

La firma del asesor obra en el archivo original
(No se muestra en este documento por estar expuesto a publicación)

AGRADECIMIENTO

A nuestras familias, por ser el principal motor de nuestros sueños, gracias a ellos porque cada día depositaron su confianza en cada uno de nosotros.

A la Universidad Continental por darnos la oportunidad de estudiar y prepararnos en el campo que más interés tenemos y apoyar en nuestra formación profesional. A nuestros docentes, quienes con su experiencia, dedicación y motivación han sido de mucha ayuda para lograr este gran objetivo y así dar por culminada esta investigación con éxito.

Para ellos:

Muchas gracias.

Los Investigadores

DEDICATORIA

Esta investigación está dedicada a todos, y cada uno de los profesionales que nos apoyaron en este extenso camino que recorrimos, desde nuestros amigos, colegas y compañeros de estudio. A nuestras familias por ser el principal punto de apoyo en nuestra educación, tanto académica como personal, y por su incondicional apoyo a través del tiempo.

Los investigadores

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La problemática de esta investigación se enfoca en abordar los desafíos de seguridad y eficiencia operativa en la red de TELECABLE, cuando surgen problemas, los registros de eventos pueden proporcionar información valiosa para diagnosticar y resolver el problema. Un servidor syslog facilita el acceso a estos registros, lo que agiliza el proceso de resolución de problemas y minimiza el tiempo de inactividad. Dentro de esta investigación se pueden observar conceptos teóricos para comprender lo que es un servidor syslog y el protocolo Rsyslog.

La metodología PPDIOO de Cisco, aplicada a nuestra investigación fue de tipo tecnológico, teniendo como alcance llegar hasta la fase de implementación; en la etapa de preparación se realizó el análisis del presupuesto total para el proyecto, así como también para la etapa del diseño e implementación, por otro lado, también se evaluó el modelo de red existente con el que trabaja actualmente Telecable.

Se ha demostrado que el tiempo de diagnóstico de incidencias se redujo de 45 a 15 minutos, el número de incidentes sin resolver a falta de datos se redujo hasta en un 80%, en cuanto a incidentes críticos a causa de la sobreescritura de registros se redujo de 5 incidentes a 1.

Se concluye que desde el aspecto tecnológico y económico este diseño e implementación es muy viable, ya que mejora la manera tradicional en la que se usan los servidores syslog, generando así un impacto positivo en los trabajadores de Telecable.

Palabras claves: Implementación, Diseño, Syslog, WAN, Redes, Seguridad, Encriptación, Disponibilidad, Continuidad. Eficiencia.

ABSTRACT

The objective of this research focuses on addressing security and operational efficiency challenges in TELECABLE's network. When problems arise, event logs can provide valuable information for diagnosing and resolving the issue. A syslog server facilitates access to these logs, streamlining the troubleshooting process and minimizing downtime. This research explores theoretical concepts to understand what a syslog server and the Rsyslog protocol are.

The Cisco PPDIOO methodology applied to our research was technological, extending to the implementation phase. The total project budget was analyzed during the preparation phase, as well as the design and implementation phases. The existing network model currently used by Telecable was also evaluated.

It has been demonstrated that incident diagnosis time was reduced from 45 to 15 minutes, the number of unresolved incidents due to missing data was reduced by up to 80%, and critical incidents due to log overwriting were reduced from 5 incidents to 1.

It is concluded that from a technological and economic perspective, this design and implementation is highly viable, as it improves the traditional way in which syslog servers are used, thus generating a positive impact on Telecable employees.

Keywords: Implementation, Design, Syslog, WAN, Networks, Security, Encryption, Availability, Continuity, Efficiency.

INTRODUCCIÓN

Una red, se interpreta como la interconexión de dos o más dispositivos a través de un medio físico, tales como son la fibra óptica, cable coaxial, cable utp, de tal manera que puedan compartir información entre ellas.

Uno de los objetivos de las redes de comunicación es compartir información y permitir que los datos estén siempre disponibles para todos los usuarios que lo soliciten, sin importar el medio físico o el estado donde se encuentren. Cabe resaltar que en la actualidad es imprescindible la velocidad con la que estos datos puedan estar siempre disponibles.

Nuestra investigación se ha dirigido a cómo centralizar y gestionar los eventos de red de Telecable, para eso, en esta investigación se han desarrollado cinco capítulos.

En el capítulo uno, se identifica y analiza la problemática de Telecable, para formular los problemas generales y específicos, así como también para definir los objetivos, además de brindar la justificación teórica, práctica e importancia de nuestra investigación.

En el capítulo dos, se detallan y analizan los antecedentes del problema para identificar la coincidencia con nuestro tema de investigación, también se definen las bases teóricas y las herramientas utilizadas.

En el capítulo tres, se desarrolla la ejecución de la metodología elegida para este proyecto PPDIOO de Cisco, el cual otorga 6 etapas para una correcta implementación del servidor syslog.

En el capítulo cuatro, se presentan los resultados y discusión de resultados del proyecto.

En el quinto capítulo, presentamos las conclusiones, recomendaciones y anexos.

CAPÍTULO I: PLANTEAMIENTO DEL ESTUDIO

1.1 Planteamiento y formulación del problema

1.1.1 Planteamiento del Problema

Durante los últimos años los sistemas informáticos se han convertido en un aliado fundamental para las empresas, ya que permiten gestionar y manejar su información de manera más rápida y sencilla.

En el entorno empresarial, la correcta gestión de un activo de red o infraestructura tecnológica es esencial para poder garantizar la continuidad de servicio y la seguridad de los sistemas de información, en ese aspecto la empresa Telecable, dentro de su infraestructura tecnológica se enfrenta cada vez más al desafío de administrar y mantener en monitoreo constante una red más avanzada y robusta, compuesta por diferentes dispositivos.

Además, la falta de un servidor robusto y centralizado para soportar toda la información y gestionar los eventos de red dificulta la capacidad de Telecable para poder identificar y responder de manera rápida ante incidentes, así como también para realizar el seguimiento adecuado y el análisis de las actividades de la red.

Actualmente, la empresa no dispone de un servidor de registros para poder soportar todos sus procesos, perdiendo registros de eventos generados por los dispositivos de red, ya que los mismos equipos almacenan sus registros de manera local, por lo que ello limita su capacidad para detectar y mitigar amenazas de seguridad, identificar inconvenientes de rendimiento y cumplir con los requisitos de auditoría y el cumplimiento normativo.

Durante el periodo 2024, Telecable ha tenido varios incidentes relacionados a la pérdida de registros, afectando la capacidad de diagnóstico de fallas. Un echo particular sucedió en febrero, cuando la repentina caída del enlace principal no pudo ser diagnosticada rápidamente debido a la falta de registros históricos, Además, se ha reportado la perdida de información importante por fallas en equipos locales sin mecanismos centralizados de respaldo, lo que dificultó la trazabilidad de los eventos.

Estos inconvenientes presentados con anterioridad evidencian la necesidad urgente de un servidor Syslog que permita la centralización y análisis efectivo de eventos de red, mejorando así la respuesta y mitigación de problemas.

Caso 1: Avería del Router Principal en marzo de 2024

En marzo de 2024, el router del enlace principal tuvo una caída de servicio, por lo que el tiempo de diagnóstico y solución fue extendida debido a la falta de logs históricos. Dicha avería tuvo impacto en más de 1500 clientes hogar, teniendo como resultado una pérdida de dinero por más de 15,000 mil soles por horas de inactividad, sin un servidor de registros, se tardó 2 horas en identificar la causa: una actualización de firmware no programada.

Caso 2: Pérdida de Registros por Sobreescritura en febrero de 2024

En febrero de 2024, el switch core tuvo un reinicio inesperado, lo cual causó la pérdida de sus logs almacenados en su propia memoria, dicho evento eliminó datos importantes sobre posibles intentos de acceso a la red. La falta de un servidor de registros centralizado no permitió que el equipo de seguridad determinara si se produjo o no la vulneración de nuestra red.

Caso 3: Falta de seguimiento en Cambios de Configuración en febrero de 2024

En febrero de 2024, por un cambio de configuración que no fue autorizado en un equipo de red "mikrotik" se dejó expuesta la IP pública de varios clientes corporativos. Como no se contaba con un servidor de logs centralizado, se desconocía el usuario que había realizado este cambio, por lo que la reconfiguración del equipo tomó un tiempo considerable por lo que se hizo vulnerable temporalmente la seguridad de datos de los clientes.

Desde el punto de vista tecnológico, se debe implementar un servidor de registros syslog centralizado, el cual permitirá a Telecable almacenar y analizar los registros de eventos de red de todos los equipos dentro de la infraestructura tecnológica, facilitando la detección de problemas, así como también responder de manera rápida a incidentes y generar reportes detallados sobre las actividades de la red. En consecuencia, la implementación de un servidor syslog requiere un enfoque metodológico que tenga en cuenta las facilidades técnicas de la empresa, la

compatibilidad con la red actual y las mejores prácticas de la seguridad de la información.

1.1.2 Formulación del Problema

Problema General

¿Es posible diseñar e implementar un servidor de registros syslog para mejorar la gestión de eventos de red en la infraestructura tecnológica de Telecable?

Problemas Específicos

¿Cómo documentar y recopilar datos sobre el diseño e implementación de un servidor de registros syslog?

¿Cómo seleccionar los criterios clave para la plataforma del servidor syslog?

¿Cómo evaluar el entorno de red existente?

¿Cómo elaborar un plan de presupuesto económico para la implementación del servidor syslog?

¿Cómo analizar los datos de registro para diagnosticar y resolver los problemas de red?

1.2 Objetivos

Objetivo General

Diseñar e implementar un servidor de registros syslog para mejorar la gestión de eventos de red en la infraestructura tecnológica de Telecable.

Objetivos Específicos

Documentar y recopilar datos sobre el diseño e implementación de un servidor de registros syslog.

Seleccionar los criterios clave para la plataforma del servidor syslog.

Evaluar el entorno de red existente.

Elaborar un plan de presupuesto económico para la implementación del servidor syslog.

Analizar los datos de registro para diagnosticar y resolver los problemas de red.

1.3 Justificación e importancia

Justificación Teórica

Esta investigación tiene como propósito emplear las buenas prácticas de la seguridad de la información con relación a la tecnología, el cual nace debido a la gran cantidad de información y datos que se necesitan registrar para tener un control de los eventos que hace cada usuario al ingresar a la red, que pueda garantizar el correcto funcionamiento de los activos tecnológicos y, también garanticen la disponibilidad de datos en la red de Telecable.

Dentro del campo laboral se dan modificaciones en el servidor, es por ello que malos usuarios pueden modificar los datos para fines personales, los cuales pueden llevar a la empresa a tener pérdidas económicas y también desprestigiar el nombre de la compañía.

Por ello, se debe realizar un análisis de la infraestructura de Telecable para poder determinar los procedimientos que se requieren y poder asegurar un buen funcionamiento del servidor y así garantizar el buen uso de la información.

Justificación Práctica.

Nuestro tema de investigación fue elegido a partir de las labores desempeñadas como profesionales en el área de tecnología y redes, también al uso de herramientas de diseño de red tales como: (a) Microsoft Visio, para luego aplicarlas en un entorno real dentro de Telecable. Nuestra principal motivación es, el compromiso de aplicar las buenas prácticas de la seguridad de la información, además de contar con ardua experiencia en el área de

diseño, implementación y configuración de equipos de red como: (a) Routers, (b) Módems, (c) Servidores, (d) Switches y (e) Firewall.

Importancia

La implementación del servidor syslog, garantiza la eficiencia operativa, ya que los datos quedarán registrados dentro de la base de datos del servidor.

En la actualidad se cuenta con muchos recursos tecnológicos con los que se puede trabajar en esta área. Cabe mencionar que muchas de ellas tienen detalles bastante importantes, pero desde nuestra perspectiva consideramos que, para el tema de registro de eventos, es mejor utilizar el protocolo rsyslog para que pueda almacenar la información enviada desde el equipo de red hacia el servidor, por lo tanto, necesitamos registrar todos los eventos para poder brindar los respaldos a la empresa y así poder identificar las manipulaciones que se hicieron en nuestra red.

CAPÍTULO II: MARCO TEÓRICO

2.1 Antecedentes del Problema

2.1.1 Antecedentes Nacionales

a) La metodología de investigación aplicada por Ramírez (1), en la tesis titulada Alternativas de configuración con el uso de los protocolos syslog y snmp para la gestión de red de redes avanzadas, en la Universidad Nacional Agraria de la Selva "se basa en la evaluación de los protocolos para aprovechar así sus capacidades. Este estudio identifica a dos protocolos comúnmente utilizados para la gestión de red, con amplia difusión y disponibilidad en los dispositivos propios de una red avanzada […]" (1), como primera fase de la investigación realizaron la propuesta de una topología para reinsertarla en la red académica peruana, ya que esta misma se encontraba inactiva, como segunda fase los investigadores realizaron la emulación de los protocolos snmp y syslog cada uno configurado en la misma topología (1). Esta investigación concluye que "las pruebas realizadas demostraron que Syslog y SNMPv3 poseen capacidades propias, pero que pueden complementarse configurándose de forma paralela; SNMPv3 se cataloga como una configuración "compleja" frente a SNMPv2c y Syslog que se considera entre regular y simple" (1).

   De acuerdo con el estudio se proporcionó un análisis sobre la configuración de protocolos SNMP y Syslog. Por lo que el enfoque no se basa en una evaluación técnica, el cual no se puede profundizar como en la seguridad y escalabilidad de estas configuraciones. Si bien es cierto los autores indican que SNMPv3 presenta una configuración compleja, no hace un gran impacto en grandes infraestructuras o en redes que requieren un monitoreo personalizado. Conforme a la investigación presentada, el estudio resulta relevante, ya que si permite identificar estrategias para la gestión de registros.

2.1.2 Antecedentes Internacionales

b) En la investigación de Hernández (2) titulada Evaluación de los mecanismos de seguridad en los sistemas de notificación y registro de eventos para la gestión de redes, en la Universidad Central de Venezuela, los autores indican que "los sistemas de gestión de redes proveen facilidades para alentar condiciones críticas como

congestión, fallas o ataques de intrusos". En el presente trabajo se estudian y evalúan los sistemas de notificación y registro de eventos basados en Syslog y SNMP con el fin de buscar posibles mejoras de seguridad que sean fáciles de implementar. Además, se describen las pruebas llevadas a cabo con diferentes protocolos, los cuales establecen un canal seguro para las notificaciones (2). Esta investigación concluye que "entre las diferentes tecnologías de túneles estudiadas y probadas, la que representa la mejor alternativa para la mejora de la seguridad en los mensajes de notificación y registros de eventos es el Protocolo de Túnel de Punto a Punto (PPTP) […]" (2). Aunque esta investigación aporta un análisis sobre la mejora de la seguridad en los sistemas de notificación y registro de eventos, su principal restricción reside en la elección del protocolo PPTP como la mejor alternativa para la protección de los mensajes.

En el presente, PPTP es un protocolo antiguo ya que tiene muchos fallos de seguridad, existía mecanismos de cifrado y encriptaciones, pero vulnerables para la seguridad. En ese sentido, la investigación se enfoca en soluciones más robustas, tales como las VPNs, IPSec o TLS, que nos dan una mayor protección en la transmisión de datos.

Por lo que se pudo ver en la investigación, se llegó a la conclusión que es significativo porque destaca la importancia de crear seguridad para la administración de eventos en la red. Sin embargo, se trabajará en este asunto de otro punto de vista más moderno y seguro, por lo que nuestro estudio examinará la incorporación de procedimientos en un ambiente empresarial, dando la garantía para situaciones reales de negocios.

c) En la investigación de Becerra y Paramo (3) titulada Implementación de un sistema de correlación de eventos basado en software libre para la empresa sistemas integrales de informática SISA S.A enfocado al área del SOC SISAMAX, en la universidad Piloto de Colombia, se buscó implementar una herramienta que facilite la búsqueda y control de aquellos eventos anómalos o vulnerabilidades existentes, con un monitoreo apropiado de la mano con el proceso de gestión de incidentes, lo cual brindará una mejor visibilidad en tiempo real para la toma de decisiones. Esta investigación concluye que "el desarrollo del proyecto se expondrá a la empresa Sistemas Integrales De Informática SISA, la correlación de eventos basado en software libre, el cual tomará las acciones adecuadas sobre aquellos eventos que impacten en los activos críticos de la compañía" (3). Esta investigación tiene un aporte al ver la importancia de la correlación de eventos en las vulneraciones de la seguridad, dando importancia a los sofwares como una opción adecuada y que se

adapte a la empresa. Las restricciones también son importantes ya que se pueden infiltrar usuarios falsos y afectar la organización en las operaciones. Además, a pesar de que la investigación destaca la visibilidad en tiempo real, no se especifica de forma exhaustiva cómo se evalúa el verdadero impacto de la solución en la seguridad de la compañía ni qué indicadores concretos se emplearon para medir su eficacia. Este estudio es relevante porque tiene mucha importancia en el control de la seguridad con el monitoreo de los sistemas, nuestra investigación también evaluara soluciones que puedan ser integradas con mecanismos de autenticación como TACACS, el cual puede mejorar la protección de datos y la gestión de accesos.

d) La metodología de investigación aplicada por Carrión (4), en la tesis titulada Diseño e Implementación de una solución de gestión centralizada de los de aplicaciones, sistemas y dispositivos basada en Logstash que permita la creación de cuadros de mando para explotar, analizar y monitorear eventos de seguridad, de la Universidad Oberta de Catalunya, "Pretende diseñar e implementar una solución de gestión centralizada de logs de aplicaciones, sistemas y dispositivos basados en logtash que permita crear cuadros para explorar y monitorear todos los eventos de seguridad." Durante el desarrollo de este proyecto se realizó una investigación aplicada que se enfoca en evaluar la pertinencia del proyecto de código abierto basado en Logstash para procesar datos y análisis de logs, teniendo como resultados una vasta gestión de logs de seguridad generados por diferentes fuentes de la empresa (4). El proyecto concluye que "gran parte del éxito o fracaso de la implantación de un sistema de gestión de logs depende fundamentalmente de su alineamiento a los objetivos de seguridad de la empresa." (4). Esta investigación aporta una visión relevante sobre la implementación de soluciones de gestión centralizada de logs mediante herramientas de código abierto, lo que representa una alternativa flexible y accesible para las organizaciones. Sin embargo, una de sus principales limitaciones radica en que no aborda en profundidad los desafíos operativos y técnicos asociados con la gestión de grandes volúmenes de datos en entornos de producción, como la escalabilidad, la conservación de logs y el desempeño del procesamiento en tiempo real. Además, si bien se menciona la importancia del alineamiento con los objetivos de seguridad de la empresa, la investigación no proporciona un marco metodológico claro para evaluar dicho alineamiento ni estrategias para garantizar su cumplimiento a largo plazo.

   Desde el punto de vista de nuestra investigación, este trabajo es significativo ya que resalta la importancia de una administración eficaz de los registros como un elemento crucial en la protección de la información. Sin embargo, nuestra

investigación no solo se enfocará en la administración centralizada de registros, sino que también examinará su integración con sistemas de autenticación centralizada, como TACACS, con el objetivo de optimizar la trazabilidad y el control de accesos en la infraestructura de red. De igual manera, se evaluará la eficacia de la solución propuesta en la detección temprana de incidentes y su impacto en la resistencia de la seguridad de la empresa.

e) Las empresas cuentan con servidores, base de datos, aplicaciones web y correos corporativos, por ello la importancia de monitoreo, para prevenir problemas y conocer el mantenimiento de los servidores.

   En la investigación de Velasco y Cagua (5) titulada Implementación de un sistema de monitoreo de redes utilizando herramientas open source y proveer servicios de directorio a través de active directory en la facultad de filosofía, letras y ciencias de la educación de la universidad de guayaquil, de la Universidad Politécnica Salesiana, se indica que "En la facultad de Filosofía de la universidad de Guayaquil, no se sabe el estado de los servidores, ni el consumo de ancho de banda y se ve alteraciones en las configuraciones de las máquinas de los usuarios […]" (5). Es por eso que se necesita una herramienta que monitoree los servidores, también el ancho de banda que provee. Por lo que se planteó la implementación de Nagios como herramienta de monitoreo de redes y para la administración de los equipos. Se implementó el software y se vieron cambios positivos para la administración y tiempo. Como resultado en el uso de las herramientas de monitoreo se obtuvo la información de estadística del estado de los servidores, alertas por el correo corporativo y el consumo del ancho de banda, por lo que la implementación fue satisfactoria para la facultad. (5).

   La investigación nos mostró la importancia de las herramientas que monitorean la gestión de los recursos tecnológicos de una red. Por lo cual una de las principales limitantes son las configuraciones y personalización de Nagios. Además, esta investigación se enfocó en soluciones específicas sin tener en cuenta las alternativas modernas que nos podrían ayudar a automatizar la administración de la red, como Zabbix, que cuenta con capacidad avanzada de recolección de datos y análisis predictivo.

f) Actualmente, los sistemas informáticos se ejecutan en muchos programas, la mayoría de los servidores tienen alojamiento para los servicios según la necesidad de cada empresa. Todos los programas notifican acciones que realizan los usuarios, en las fichas de registro de actividad. En la investigación de Mellouk (6) titulada Diseño e Implementación de un sistema para la recogida de los en sistemas distribuidos, de la Universidad Autónoma de Madrid, se propone "Una herramienta que usa una aplicación en Android para la visualización de resultados y usa un servidor Flask en Python que es el encargado los logs, almacenarlos en un formato XML […]" (6). Dicha herramienta propone recoger toda la información relevante de los logs para un análisis, creando resultados en un dispositivo móvil, se pudo lograr una interfaz gráfica, usando un aplicativo móvil, para mostrar los resultados. Por otro lado, la correlación entre logs mejora la precisión de resultados y la detección de anomalías en el sistema, ya que ahora la herramienta permite análisis de logs histogramas y clustering. (6)

   En la investigación se ve la aportación innovadora para poder integrar los logs en una app móvil, el cual ayuda a ver los datos con flexibilidad, no obstante, presenta limitaciones, como la utilización de XML como almacenamiento, que no es la mejor opción para rendimiento y escalabilidad, aunque la correlación de eventos es relevante, la investigación no detalla cómo gestionar los análisis de logs en la detección de anomalías.

   Desde nuestra investigación, se puede ver que el análisis es relevante y es importante para la correlación de eventos lo cual sirve para la seguridad y la prevención de las anomalías que pueden infiltrarse en nuestra red. Además, se evaluará el impacto del análisis de logs en la mejora de la seguridad organizacional y su potencial para optimizar la reacción frente a incidentes de seguridad.

g) Este proyecto trata sobre un repositorio logs para varios servidores, el cual trata de la instalación y configuración de sistema de control. Anteriormente los logs no se revisaban porque eran tediosos de analizar cada log, el proyecto se realizó para solucionar los problemas que tenían los departamentos. En la investigación de Salazar (7) titulada Sistemas de información para el repositorio de logs, control de versiones de las aplicaciones internas y actualización de Aranda en la empresa UNE – TELEFÓNICA de Pereira, de la Universidad Católica de Pereira, indica que "la herramienta implementada es eficiente para revisar lo que sucede en los servidores en cuanto a ingresos a la máquina, errores que produce, debido a que soporta grandes volúmenes de logs por minuto y no se ve afectado el rendimiento […]" (7). La elección de las herramientas Syslog y Loganalyzer, fue la mejor ya que el

funcionamiento no es difícil de manejar y permite que el usuario pueda observar de manera más sencilla las búsquedas. Se llegó a la conclusión que la instalación fue exitosa ya que fue acertada porque permite que varios desarrolladores trabajen y se realizan modificaciones de la herramienta. Los análisis se hicieron sencillos para adaptarse y manejar la herramienta, pues simplificara el uso de la administración de las solicitudes. (7)

Esta investigación es relevante porque aborda la problemática del almacenamiento y análisis de grandes volúmenes de registros logs, destacando la importancia de contar con herramientas eficientes para su gestión. Sin embargo, lo que restringe es que no tiene un buen mecanismo de seguridad que protejan los logs y no garantiza los controles de acceso la integridad y confidencialidad de la información que se almacena. Además, la investigación se baza solo en syslog y loganalyzer sin ver alternativas más avanzadas, que nos ofrecen capacidades más robustas.

Desde el punto de vista de nuestra investigación, este estudio es un poco relevante ya que demuestra la necesidad de tener un repositorio de logs para optimizar la administración del servidor. Sin embargo, nuestro estudio se hará con una implementación del sistema centralizado con Graylog, con el cual el acceso al registro de eventos sea controlado y auditado.

h) La investigación de Nebrera (8) titulada Desarrollo de un sistema de gestión syslog en cloud, de la Universidad de Sevilla, se centra en desarrollar un sistema de gestión de logs para una plataforma de red en tiempo real y ciberseguridad, en la cual se hace una investigación sobre el protocolo Syslog y logs para poder definir una estructura que pueda gestionar los logs antes mencionados, nos indican que "Para la implementación del sistema, se desarrolló inicialmente una configuración que los diferentes servicios trabajen en CentOS. Para el sistema usaremos framework de automatización de infraestructuras que facilitan la configuración y herramientas […]" (8). La integración en la empresa se hizo con un framework el cual nos facilitó la tarea de instalación y configuración. Se concluye que se ha configurado e integrado en la plataforma de la empresa las herramientas necesarias, para poder ver los logs recolectar de las diferentes fuentes, para hacerlos llegar al administrador, se cumplieron los objetivos propuestos. (8)

   Esta investigación tiene un aporte favorable en el tema de gestión de logs en entornos cloud, ya que nos ayuda a automatizar la configuración e implementación de sistemas de monitoreo. No obstante, tiene limitaciones una de ellas y la más principal es que no profundiza aspectos de seguridad relacionado a la protección de

registros almacenados en la nube, aunque se demuestra la viabilidad de centralizar logs en la nube, no garantiza la disponibilidad de los datos.
Desde la perspectiva de nuestra investigación, esta investigación es relevante ya que demuestra cómo puede automatizar los logs en la nube, pero como sabemos nuestro estudio no solo analizara la recopilación de logs, sino que se enfoca en la integración de los registros de eventos. Se evaluará también la integración de logs con mecanismos de autenticaciones, para asegurar que solo personal autorizado pueda tener acceso a la información y sean auditables en tiempo real.

2.2 Bases teóricas

2.2.1 Servidor Syslog

a) Registro de eventos

Un log "es un registro de eventos que pasa en un rango de tiempo en particular. Las aplicaciones o dispositivos que lo utilizan para registrar datos o información sobre quién, qué, cuándo, dónde y por qué ocurre algún evento." (9)

En la presente investigación, nuestro servidor graylog se implementó como una solución para centralizar la gestión de los logs, lo que facilita el almacenamiento y análisis de eventos provenientes de diferentes dispositivos de red, dicha implementación mejora la capacidad de organización para detectar problemas, analizar incidentes y tomar decisiones basadas en datos más precisos.

b) Protocolo syslog

"Es una forma en que los dispositivos de red pueden usar un formato de mensaje estándar para comunicarse con un servidor de registro. Fue diseñado específicamente para facilitar el monitoreo de dispositivos de red" (10). Estos mensajes incluyen una clasificación, tales como ID, dirección IP e información específica de un evento para después poder visualizarlos. (10)

Syslog "si se puede instalar en Unix y Linux, así como MacOS. El sistema de Windows no admite Syslog". (10)

Dentro de este proyecto, se instaló y configuró graylog para el servidor central de registros, procesando eventos enviados a través del syslog desde diferentes dispositivos dentro de la red, la compatibilidad del protocolo de syslog con Unix lo hace ideal para integrarse con graylog.

c) Mensajes de syslog

Los mensajes de Syslog pueden tener un formato legible por humanos, aunque no es obligatorio. Cada mensaje contiene un nivel de prioridad en su encabezado, que combina un código para el proceso del dispositivo y un nivel de gravedad. Los códigos de proceso, llamados "instalaciones", provienen de UNIX. Los niveles de gravedad van desde 0 para emergencias y 1 para atención inmediata, hasta 7 para mensajes informativos y 8 para mensajes de depuración. (10)

En la figura 1, podemos observar un cuadro con la criticidad de los mensajes manejados en syslog.

Figura 1. Niveles de gravedad para mensajes syslog

Código numérico	Severidad	Significado
1	Emergencia	El sistema es inutilizable
2	Alerta	Actuar de inmediato
3	Crítico	Condiciones críticas
4	Error	Condiciones de error
5	Advertencia	Condiciones de advertencia
6	Aviso	Condición normal pero significativa
7	Informativo	Mensajes informativos
8	Depuración	Mensajes de nivel de depuración

Fuente [https://blog.invgate.com/es/que-es-syslog]

Graylog facilita la recopilación, clasificación y análisis de los mensajes de syslog, gracias a su capacidad para filtrar eventos por nivel de severidad, graylog permite detectar incidentes críticos en tiempo real y generar alertas basadas en umbrales predefinidos, esta funcionalidad optimiza la seguridad de la red y mejora la capacidad de respuesta ante posibles amenazas o fallos en la red.

d) Diferencia entre syslog y SNMP

"SNMP significa Simple Network Management Protocol, por sus siglas en inglés. Se trata de un protocolo para la gestión de la transferencia de información en redes, especialmente para uso en LAN." (11)

SNMP es otro protocolo para la administración de dispositivos de red ya que funciona de manera diferente, obteniendo la mayor parte de su información mediante dispositivos de sondeo. (10)

"SNMP es mejor para situaciones restringidas con condiciones predecibles, mientras que Syslog es más amplio en escala y menos restringido en formato, y cubre muchos tipos diferentes de eventos." (10)

En la figura 2, podemos observar la comparación entre distintos protocolos.

Figura 2. Diferencias entre SNMP y SYSLOG.

N°	SNMP	SYSLOG
1	SNMP permite el monitoreo remoto de dispositivos permitidos por SNMP en la red	SYSLOG es un protocolo diferente que se puede utilizar para intercambiar mensajes de registro de diferente gravedad con un dispositivo de red capaz de recibir mensajes syslog.
2	SNMP se utiliza para alertar sobre acciones críticas, como los cambios de estado HSRP mencionados.	También se recopila SYSLOG, lo que me permite profundizar más para descubrir por qué ocurrió el cambio de estado de HSRP.
3	SNMP funciona en sondeo: mecanismo de recursos con un servidor SNMP que sondea el dispositivo para obtener respuesta sobre la interfaz/estado/proceso.	SYSLOG funciona con el mecanismo PUSH en el dispositivo final para enviar información de registro.
4	Se hace referencia a SNMP para obtener información en tiempo real.	Generalmente se hace referencia a SYSLOG para adquirir datos históricos.
5	La configuración del dispositivo final se puede realizar a través del conjunto SNMP. Por ejemplo: reiniciar el sistema	La configuración del dispositivo final no se puede realizar a través del conjunto syslog.
6	Las capturas SNMP se comparten en formato binario.	Los eventos de Syslog se comparten en texto sin formato.
7	Seguro	Inseguro
8	Activo	Pasivo
9	Utiliza el puerto número 161 y 162	Utiliza TCP/UDP el puerto número 514

Fuente [https://ipwithease.com/wp-content/uploads/2020/10/SNMP-VS-SYSLOG-TABLE-NEW.jpg]

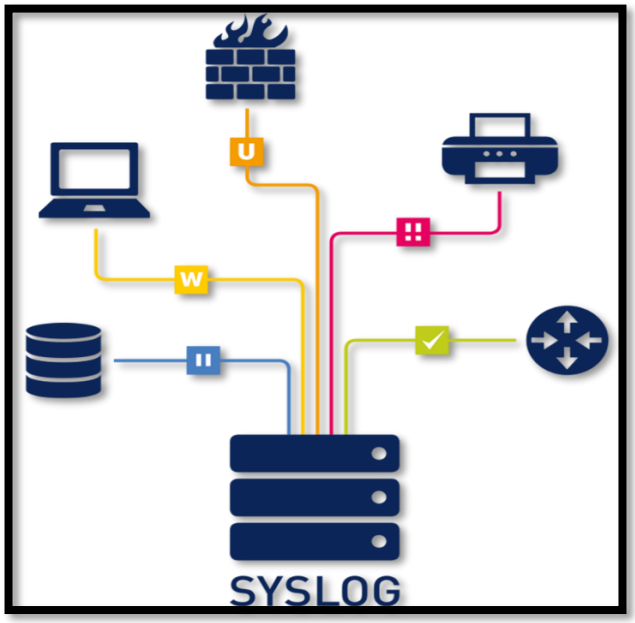
En esta investigación, se prioriza el uso de syslog debido a su capacidad para capturar una mayor variedad de eventos sin requerir solicitudes constantes por parte de nuestro servidor, graylog nos brinda una visión integral del estado de la red y mejora la detección de incidentes de seguridad, a comparación de SNMP que es útil para monitorear parámetros específicos en los dispositivos.

e) Arquitectura de un servidor syslog

La arquitectura de un servidor syslog consta de 2 componentes principales: el servidor syslog propiamente y una base de datos o sistema de almacenamiento para guardar los registros recibidos. El servidor syslog puede ejecutarse en sistemas operativos Linux y Windows. (12)

En la figura 3, Se muestra una arquitectura de syslog integrada con una base de datos y varios dispositivos de red.

Figura 3. Arquitectura de un servidor syslog.



Fuente [https://www.paessler.com/es/it-explained/syslog]

En la presente investigación, Graylog se implementó como un servidor de administración de logs, proporcionando capacidades avanzadas de indexación, almacenamiento y gestión de eventos, a diferencia de los servidores tradicionales, Graylog añade funcionalidades como el filtrado y la correlación de eventos, lo que facilita al operador la detección más eficiente de problemas y mejora la respuesta ante incidentes de seguridad, además, la arquitectura de Graylog es escalable y es compatible con varios formatos de logs, lo que convierte a este proyecto en una solución robusta para la gestión de registros logs.

2.2.2 Infraestructura de red

Toda empresa que desea tener una infraestructura de red debe contar con los siguientes elementos básicos:

a) **Cuarto de Telecomunicaciones:** Es un espacio exclusivo que se utiliza para alojar elementos del cableado estructurado, equipos de red y telecomunicaciones. (13)

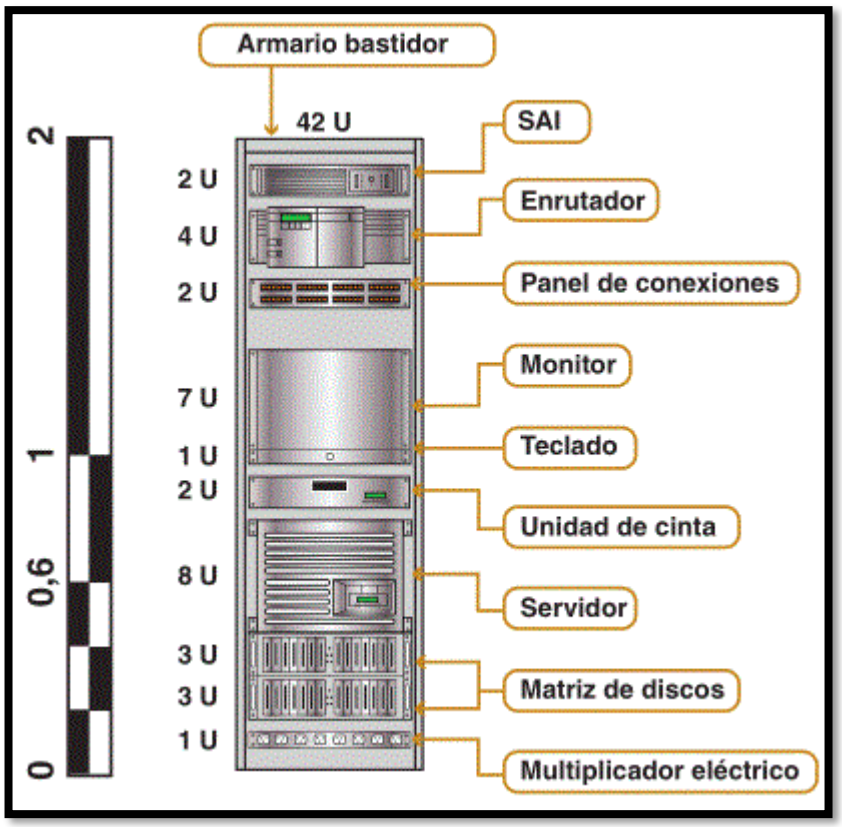
Nuestro servidor Graylog se encuentra implementado dentro de las instalaciones y data center de la empresa Telecable en la ciudad de Jauja, respaldado por un UPS

con autonomía de 6 horas y un firewall de seguridad perimetral, lo cual garantiza la funcionalidad constante del servidor.

b) **Armario de comunicaciones:** "Las medidas para la anchura están normalizadas para que sean compatibles con equipamiento de cualquier fabricante. De esta forma, cualquier electrónica o accesorio fabricado según el estándar de 19 pulgadas podrá ser instalado en el armario y fijado al rack." (13)

En la figura 4, Se muestra un ejemplo para la distribución de dispositivos de red dentro del gabinete de comunicaciones.

Figura 4. Distribución en rack de 2 metros.



Fuente [https://www.adrformacion.com/knowledge/administracion-de-sistemas/el_armario_de_comunicaciones_de_una_red_local.html]

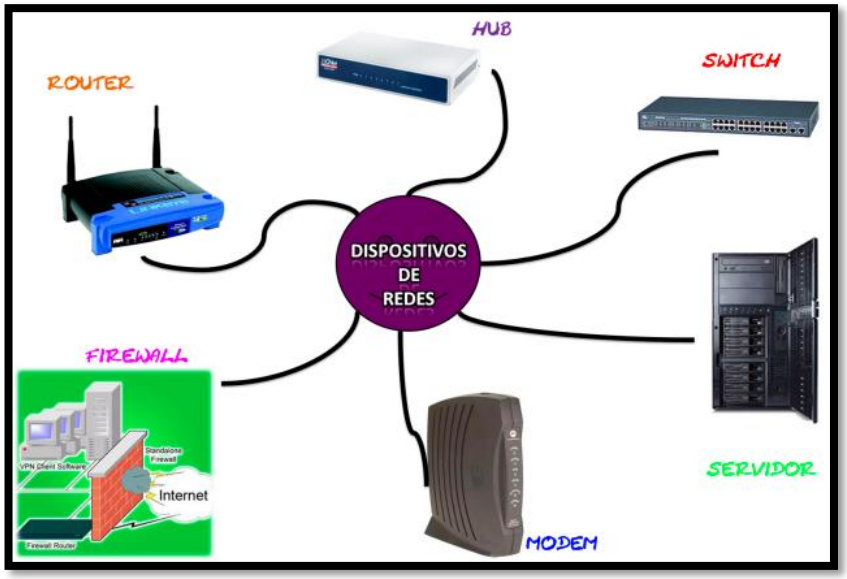
El servidor Graylog se ubica dentro de un rack de piso, ocupando 2 RU de espacio, el cual tiene un fácil acceso para la administración física.

c) **Dispositivos de red:** "Al estructurar una red, se emplean diferentes componentes que permiten que la información se transmita de un sistema a otro,

ya que, como cualquier forma de comunicación, requiere de un emisor, un canal, un mensaje y un receptor.” (14)

Dentro de una infraestructura de red se tienen diferentes equipos como: a) router b) hub c) switch d) firewall e) modem f) servidor, tal como se muestra en la figura 5.

Figura 5. Dispositivos de red.



Fuente [https://dvegar01.wordpress.com/2014/03/07/dispositivos-de-red/]

Dentro del data center de Telecable se ubican los diferentes dispositivos mencionados en la figura 5, lo que garantiza una rápida comunicación entre ellos y también con el servidor.

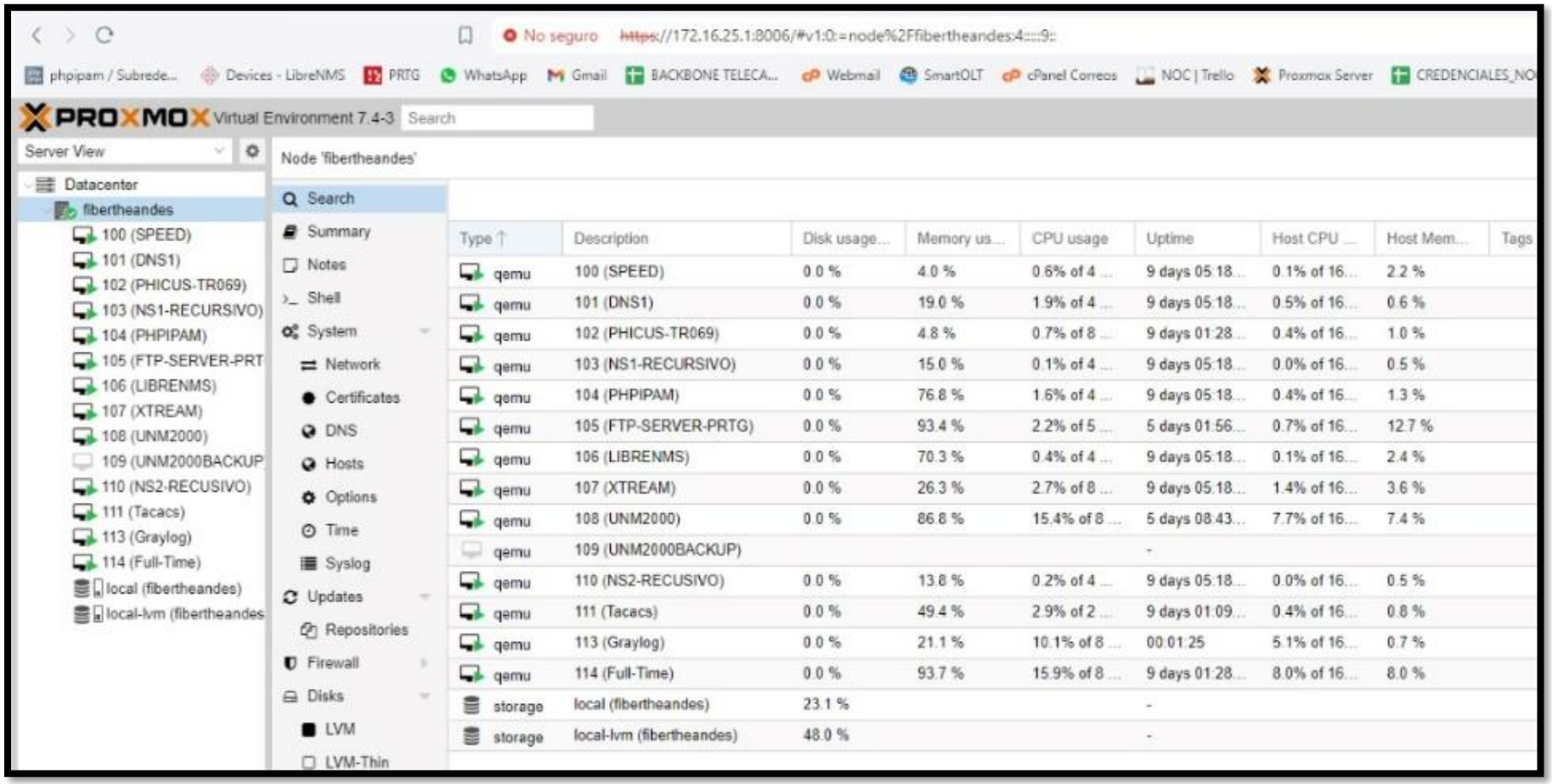
2.2.3 Herramientas para el desarrollo del diseño e implementación

a) PROXMOX VM

Según (15) “Es una solución de código abierto para la virtualización empresarial. Su objetivo es ayudarte a optimizar el uso de los recursos ya existentes, minimizar el costo por hardware y el tiempo empleado.”

En la figura 6, se visualiza la interfaz gráfica de proxmox.

Figura 6. Interfaz de proxmox.



Fuente [Propia]

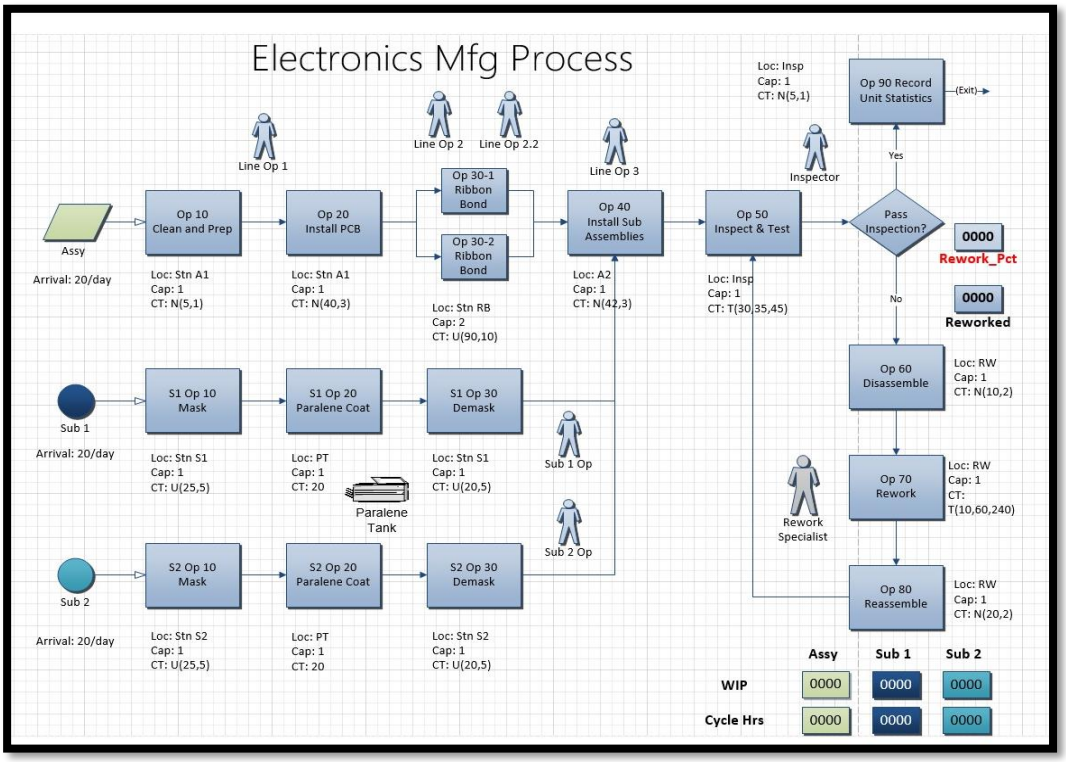
Proxmox VM se empleó para la virtualizar el servidor Graylog, proporcionando un entorno seguro y aislado para su funcionamiento, este procedimiento facilita la asignación dinámica de recursos, asegurando que Graylog opere con el rendimiento adecuado sin afectar a otros servicios.

b) Microsoft Visio

Según, (16) "Es una aplicación de diagramación y gráficos vectoriales que forma parte de la suite ofimática Microsoft Office"

En la figura 7, se muestra la interfaz del programa y un esquema de ejemplo.

Figura 7. Interfaz de usuario de Microsoft Visio.



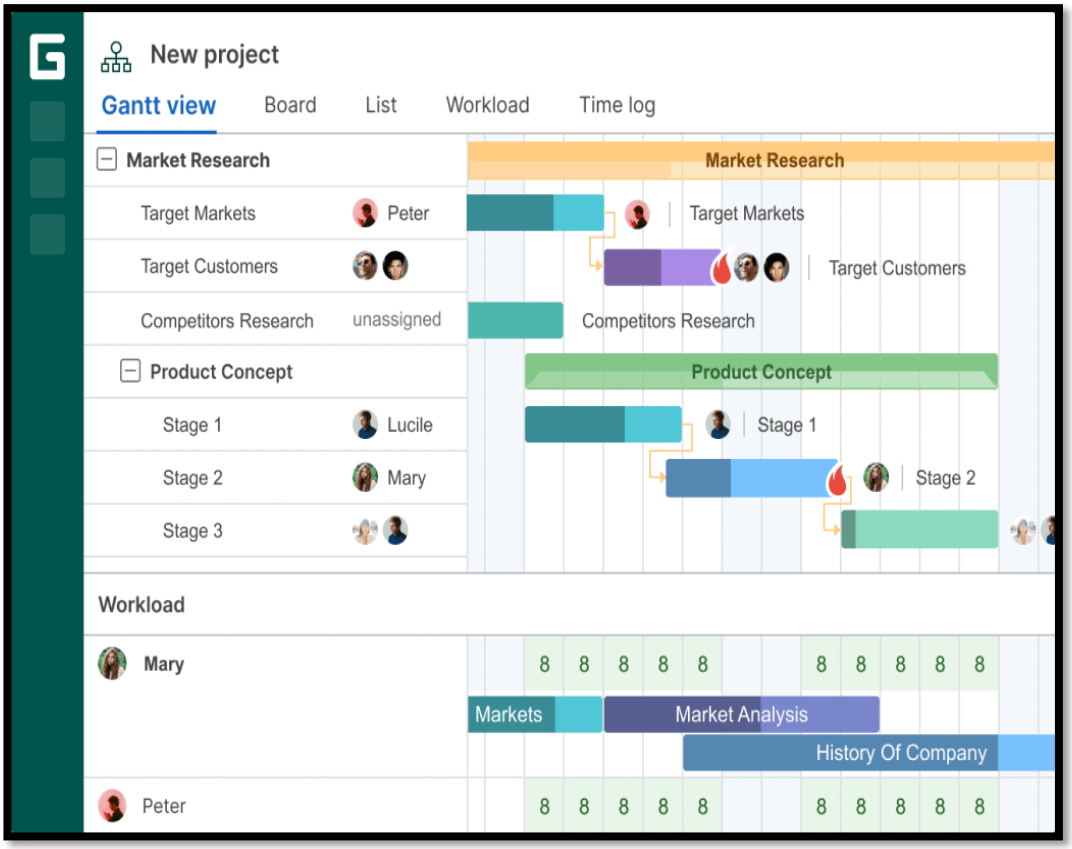
Fuente [https://www.lucidchart.com/pages/es/que-es-microsoft-visio]

En esta investigación, Microsoft Visio se empleó para diseñar la topología antes y después de la implementación del servidor Graylog, además también se utilizó para generar los diagramas de flujo sobre ciertas operaciones.

c) GanttPro

Según (17), "es un software de gestión de proyectos online que facilita la planificación e implementación de proyectos con la ayuda de diagramas de Gantt" En la figura 8, se muestra un ejemplo de cronograma.

Figura 8. Interfaz de usuario de GanttPro.



Fuente [https://projectmanagers.net/the-pros-and-cons-of-using-ganttpro-software/]

Esta herramienta se utilizó para la creación del cronograma de implementación.

2.2.4 Metodología PPDIOO

Según Salcedo y Cubillas (18) la metodología PPDIOO "tiene como enfoque principal definir las actividades mínimas requeridas, por la tecnología y complejidad de la red, que permitan asesorar de la mejor forma posible a nuestros clientes, instalando y operando exitosamente las tecnologías."

a) **Preparar. -** "Esta fase es la evaluación inicial de las necesidades comerciales y la definición de una arquitectura conceptual." (19)

b) **Planear. -** "Hacer plan o proyecto de una acción." (20)

c) **Diseñar. -** "Es un proceso de planificación creativa de objetos, procedimientos o sistemas para satisfacer necesidades estéticas y funcionales." (21)

d) **Implementar. -** "Poner en funcionamiento, aplicar métodos, medidas, para llevar algo a cabo." (22)

e) **Operar. -** "Son las actividades que se realizan de forma periódica o repetitiva, es decir, no poseen fecha fin." (23)

f) **Optimizar. -** "Buscar la mejor manera de realizar una actividad." (24)

En la presente investigación, se siguió la metodología PPDIOO para definir la arquitectura adecuada, se planificó su despliegue, se diseñó la integración con los dispositivos de red, se implementó la solución teniendo en cuenta todos los requerimientos y se pasó a la fase de operación con monitoreo continuo, la fase de optimización se realizará de acuerdo a las mejoras que se requiera en el futuro.

2.3 Definición de términos básicos

a) **Almacenamiento. -** "Son medios magnéticos, ópticos o mecánicos que registran y preservan información digital para operaciones en curso o futuras." (25)

b) **Encriptación. -** "El encriptado es uno de los pilares fundamentales de la ciberseguridad y sirve para proteger los datos y evitar que se roben, cambien o se vulneren." (26)

c) **Enrutador. -** "Un router es un dispositivo que conecta dos o más redes o subredes de conmutación de paquetes. Cumple dos funciones principales: gestionar el tráfico entre estas redes mediante el reenvío de paquetes de datos a sus direcciones IP previstas" (27)

d) **Facilidad. -** "Capacidad o aptitud especial para hacer cierta cosa sin gran esfuerzo." (28)

e) **Instalación. -** "Colocar servicios que en él se hayan de utilizar." (29)

f) **Log. -** "Registro secuencial y cronológico de las operaciones realizadas por un sistema informático, independientemente de si se trata de acciones de usuarios o de procesos automatizados." (30)

g) **Matriz De Discos. -** "Es un sistema de almacenamiento de datos que se utiliza para el almacenamiento basado en bloques, el almacenamiento basado en archivos o el almacenamiento de objetos. " (31)

h) **Máquina Virtual. -** "Es un entorno informático que funciona como un sistema aislado con su propia CPU, memoria, interfaz de red y almacenamiento, el cual se crea a partir de un conjunto de recursos de hardware." (32)

i) **Mensaje. -** "Es aquello que deseamos comunicar, o sea, el contenido que el emisor desea transmitirle al receptor." (33)

j) **Nivel de gravedad. -** "Está asociado con cada alerta generada para ayudarle a priorizar y gestionar alertas en la lista de sucesos" (34)

k) **Panel de Conexiones. -** "Es una pieza de montaje de hardware con varios puertos para conectar y gestionar los cables LAN o los cables de fibra/cobre entrantes y salientes." (35)

l) **Protocolo syslog. -** "Se utiliza para que dispositivos como routers, switches, firewalls, puntos de acceso Wi-Fi y servidores Linux generen sus propios registros." (36)

m) **Red. -** "Es la interconexión física o inalámbrica que vincula varios dispositivos informáticos (servidores, computadoras, teléfonos móviles, periféricos, entre otros) para que se comuniquen entre sí, con la finalidad de compartir datos y ofrecer servicios." (37)

n) **Registro de eventos. -** "Es un estándar para el registro de mensajes de sistema e integra datos de registro de muchos tipos diferentes de sistemas en un repositorio central." (38)

o) **SAI. -** "Un sistema de alimentación ininterrumpida (SAI) es una unidad eléctrica que suministra energía a servidores y equipos de telecomunicaciones, y centros de datos.

No sólo ofrece una reserva de energía de emergencia, sino que también protege los dispositivos o servidores en uso." (39)

p) **Seguridad. -** "Una red segura es aquella que cuenta con las políticas y prácticas necesarias para prevenir y supervisar el acceso no autorizado, así como el uso indebido, en la información de su empresa y sus recursos." (40)

q) **Servidor. -** "Un servidor es un sistema que proporciona recursos, datos, servicios o programas a otros ordenadores, conocidos como clientes, a través de una red." (41)

r) **Switch. -** "Los switches o conmutadores permiten que los dispositivos en su red se comuniquen entre sí, recibiendo paquetes de datos y direccionándolos al destinatario correcto […]" (42)

s) **Tecnología. -** "Tecnología viene del griego τέχνη (se pronuncia "téchnē") y quiere decir arte, oficio o destreza. Por lo tanto, la tecnología no es una cosa sino un proceso, una capacidad de transformar o combinar algo ya existente para construir algo nuevo o bien darle otra función." (43)

t) **Unidad De Cinta. -** "Es un dispositivo de modalidad continua que se utiliza principalmente para: Salvar y restaurar archivos de datos del sistema. Archivar registros importantes. Distribuir ampliaciones de software del sistema operativo. " (44)

u) **WAN. -** "Una red de área extensa (WAN) es un tipo de red que existe en un área geográfica de gran escala. Tu módem envía y recibe información hacia y desde Internet mediante su puerto WAN." (45)

CAPÍTULO III: METODOLOGÍA

3.1 Método, tipo y alcance de la investigación

3.1.1 Tipo de investigación

El tipo de investigación a realizar será el tecnológico, porque producto de la investigación se obtendrá un artefacto tecnológico que consistirá en una infraestructura tecnológica con un servidor de registros syslog, el mismo que centralizará los logs de los equipos de red de la empresa Telecable.

3.1.2 Método de investigación

Método científico; porque se ejecutará una serie de fases que consistirán en: identificar el problema existente en los recursos tecnológicos, revisar incidentes previos y observar el estado actual de la red para documentarlos y de acuerdo a ello llegar a la solución.

3.1.3 Alcance

El alcance de investigación será el explicativo, porque se ha determinado que en la empresa Telecable existe una problemática que dificulta la centralización de logs en un solo lugar y la pérdida de estos registros, frente a lo cual se formula como solución la implementación de un servidor de registros syslog para gestionar los eventos de red y así garantizar la disponibilidad de registros en todo momento.

3.1.4 Metodología Cisco PPDIOO

La metodología elegida en este proyecto, define las tareas necesarias en cada etapa del ciclo de vida real dentro de la red para poder asegurar la eficiencia de sus servicios. PPDIOO de Cisco se enfoca principalmente en definir las actividades requeridas por la tecnología con el objetivo de brindar un mejor servicio a los clientes y optimizar el funcionamiento de la red. (18)

Si bien se sabe, el modelo PPDIOO cuenta con seis fases a trabajar, pero en este proyecto solo se desarrollarán las primeras cinco fases y la última se desarrollará mediante trabajos programados en cuanto sea necesario.

a) Etapas de PPDIOO

- ✓ **Preparar:** En esta etapa se elaborará el presupuesto económico para todo el proyecto.

- ✓ **Planear:** En esta etapa se evaluará el diseño de red actual de Telecable.

- ✓ **Diseñar:** En esta etapa se detalla la propuesta de solución del diseño y validar si esta propuesta de red encajaría con el trabajo de los usuarios de forma eficiente.

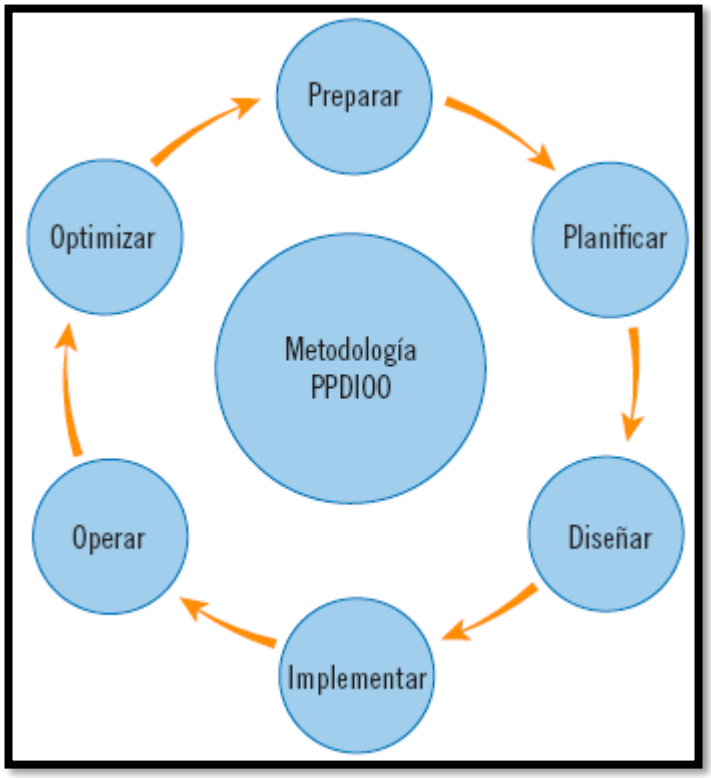
- ✓ **Implementar:** En esta etapa se añadirá una nueva solución evitando crear vulnerabilidades o alterando el funcionamiento de la red.:

- ✓ **Operar:** Se asociarán los equipos a monitorear y a configurar las alertas para los tipos de mensajes enviados desde los equipos de red.

- ✓ **Optimizar:** Para esta etapa se requiere que el servidor se encuentre operando, para poder visualizar los errores y así poder corregirlos.

En la figura 9, se muestran las siglas del modelo PPDIOO que se refiere a las diferentes etapas anteriormente mencionadas.

Figura 9. Etapas del modelo PPDIOO.



Fuente
[https://reader.digitalbooks.pro/content/preview/books/37922/book/OEBPS/Text/chapter1.html]

3.1.5 Criterios para la elección de la Metodología Cisco PPDIOO

En este proyecto, la metodología Cisco PPDIOO fue elegida por su enfoque específico en redes y su aplicabilidad en proyectos tecnológicos complejos, como la implementación de servidores Syslog.

Según Oppenheimer (46), la metodología PPDIOO permite una gestión integral del ciclo de vida de la red, desde su concepción hasta su optimización, lo que la diferencia de otras metodologías más generalistas como ITIL o PMBOK. Mientras que ITIL se enfoca en la gestión de servicios de TI y PMBOK proporciona un marco estructurado para la gestión de proyectos en diversos sectores, PPDIOO está diseñada específicamente para abordar los desafíos inherentes a la infraestructura de redes (47).

Tanenbaum y Wetherall (48) mencionan que, la metodología PPDIOO resulta especialmente ventajosa para proyectos de infraestructura de red debido a su

estructura modular, que permite una planificación detallada y reduce el tiempo de despliegue, asegurando una operación eficiente y una optimización continua del sistema. Esto es crucial en entornos donde la confiabilidad y la seguridad de la red son factores determinantes para la operatividad organizacional.

Asimismo, la aplicación de PPDIOO en este proyecto permite una alineación efectiva con las mejores prácticas de la industria en diseño e implementación de redes. La fase de optimización, en particular, es un valor añadido que garantiza que la infraestructura pueda adaptarse a cambios y mejoras futuras sin comprometer su funcionalidad inicial.

En conclusión, la metodología PPDIOO es la más adecuada para este proyecto debido a su enfoque especializado en redes, su estructura cíclica que promueve la mejora continua y su respaldo por parte de expertos en la industria de redes y telecomunicaciones. Su aplicación garantizará que la implementación del servidor Syslog se realice de manera eficiente, con un diseño sólido y una operación confiable a lo largo del tiempo.

A continuación, en la tabla 1, se muestra un cuadro comparativo entre las diferentes metodologías.

Tabla 1. Cuadro comparativo sobre las metodologías PPDIOO, ITIL y PMBOK

	PPDIOO	**ITIL**	**PMBOK**
Enfoque	Ciclo de vida para proyectos tecnológicos, especialmente infraestructura TI.	Marco unificado para el ciclo de vida de la información en TI.	Estándar integral de gestión de proyectos, aplicable a cualquier industria.
Tipo de proyecto	Proyectos tecnológicos, redes e infraestructuras, con enfoque en optimización constante.	Proyectos de tecnología de la información y gestión de datos a lo largo de su ciclo de vida.	Proyectos de cualquier tipo, con énfasis en la gestión estructurada de tiempo, costos, calidad y recursos.
Enfoque de Gestión	Fase de mejora continua con énfasis en la operación y optimización post implementación.	Su enfoque técnico y de TI.	Su estructura es formal y detallada para todas las fases del proyecto.
Documentación	Requiere documentación continua durante todas las fases, especialmente en la operación y optimización.	La documentación es centrada en la gestión de datos a lo largo de su ciclo de vida.	La documentación es extensa y formalizada, con énfasis en la planificación y control del proyecto.

Fuente [https://maaz.ihmc.us/rid=1NGMTBN5N-T3JLG4-15JJ/Dif_Itil_Pmbok.pdf]

3.2 Materiales y Métodos

Para la implementación del servidor de registros syslog, se aplicó la metodología cisco PPDIOO, el cual consta de 6 etapas: Preparar, Planear, Diseñar, Implementar, Operar y Optimizar. A continuación, se detalla la aplicación de cada una de ellas en el desarrollo del proyecto:

3.2.1 Preparar

Se analizó la infraestructura de Telecable para identificar problemas en la gestión de registros de eventos, detectando incidentes críticos como la pérdida de logs por sobreescritura y la falta de trazabilidad en cambios de configuración. Con base en ello, se definieron los objetivos del proyecto y los beneficios esperados con la implementación del servidor Syslog, además de identificar los recursos de hardware y software necesarios para su desarrollo.

Análisis de la situación actual de la empresa

TELECABLE es una empresa dentro del sector de redes y telecomunicaciones, que brinda servicios de internet y cable a hogares e internet dedicado a medianas y grandes empresas, actualmente tiene 3 sedes de operaciones en Jauja, El Tambo y La Oroya.

Fue creada en el año 1996, en el distrito de Xauxa de la ciudad de Jauja, actualmente realiza trabajos de instalación de internet doméstico, residencial, corporativo e instalación de Cable TV en esa misma ciudad. Telecable brinda el servicio de atención presencial y soporte remoto al cliente, entregándoles equipos de marcas reconocidas en el mercado, además cuenta con una mesa de ayuda disponible los 7 días de la semana, 24 horas al día, para atender cualquier eventualidad dentro de la red.

Para el diseño y análisis de los requerimientos se debe tener en cuenta lo siguiente:

- ✓ Topología
- ✓ Red LAN
- ✓ Servidores
- ✓ Software

3.2.2 Planear

Se analizó la infraestructura de Telecable para identificar problemas en la gestión de registros de eventos, detectando incidentes críticos como la pérdida de logs por sobreescritura y la falta de trazabilidad en cambios de configuración. Con base en

ello, se definieron los objetivos del proyecto y los beneficios esperados con la implementación del servidor Syslog, además de identificar los recursos de hardware y software necesarios para su desarrollo.

Plan de negocios

El costo para cada etapa del proyecto se ha distribuido en porcentajes de la siguiente forma:

a) **Etapa de Planificación:** En esta etapa se usará el 75% del costo total del proyecto, debido a que se usará internet para realizar distintas investigaciones y análisis acerca de las necesidades y requerimientos necesarios para el proyecto, tal como se muestra en el ID 2 de la figura 10.

b) **Etapa de Diseño:** En esta etapa se usará el 25% del costo total del proyecto, debido a que se hará el modelamiento y diseño de la red, tal como se muestra en el ID 10 de la figura 10.

c) **Etapa de Implementación:** Para realizar la instalación que requiere el proyecto no se tiene un presupuesto asignado, ya que se usará la infraestructura de red de Telecable, y al ser una proveedora de servicios cloud, internet y seguridad, cuenta con servidores virtualizados, por lo tanto, no implicará costo adicional en instalación del sistema operativo y alquiler del servidor, tampoco de la mano de obra, ya que son los mismos trabajadores quienes realizarán todos estos cambios, tal como se muestra en el ID 15 de la figura 10.

d) **Etapa de Optimización:** En esta etapa no se tiene presupuesto asignado, ya que es el mismo personal de Telecable quien se encargará de optimizar y corregir errores que pueda presentarse en la red más adelante, tal como se muestra en el ID 29 de la figura 10.

e) **Costos Futuros:** La infraestructura puede escalarse sin necesidad de inversiones adicionales en hardware costoso. En el futuro, si la empresa aumenta su volumen de logs, bastará que el personal técnico de la propia empresa añada almacenamiento y ajuste las configuraciones manteniendo la solución costo-efectiva, asegurando una inversión sostenible a largo plazo. Adicionalmente, se realizó un manual de uso del servidor graylog para futuros operadores que ingresen a laborar en la empresa Telecable. Por lo que se determina que el

mantenimiento anual del servidor Graylog, incluyendo actualizaciones, infraestructura en hardware y gestión de base de datos será de 150 soles. tal como se muestra en el ID 32 de la figura 10.

Figura 10. Se muestra el costo total para las fases de diseño, implementación, optimización y costos futuros del proyecto.

ID	NOMBRE DE TAREA	SUB TOTAL	CANTIDAD	TOTAL	PORCENTAJE
1	PROYECTO DE DISEÑO E IMPLEMENTACIÓN DE UN SERVIDOR DE REGISTROS SYSLOG PARA GESTIONAR LOS EVENTOS DE RED EN LA INFRAESTRUCTURA TECNOLOGICA DE TELECABLE			S/ 568.00	100%
2	Etapa de Planificación			S/ 426.00	75%
3	Investigación y Análisis de Requisitos			S/ -	
4	Análisis de Necesidades	S/ -		S/ -	
5	Identificación de Requisitos	S/ -		S/ -	
6	Listado de Compras y Servicios			S/ 426.00	
7	Internet	S/ 90.00	3	S/ 270.00	
8	Electricidad	S/ 52.00	3	S/ 156.00	
9	Software	S/ -		S/ -	
10	Etapa de Diseño			S/ 142.00	25%
11	Diseño de la Arquitectura del Servidor			S/ -	
12	Crear la Arquitectura del Servidor	S/ 142.00	1	S/ 142.00	
13	Determinar la Configuración Necesaria	S/ -		S/ -	
14	Elección del Sistema Operativo	S/ -		S/ -	
15	Etapa de Implementación			S/ -	
16	Adquisición del Hardware y Software			S/ -	
17	Compra de Servidor	S/ -		S/ -	
18	Comprar de Sistema Operativo	S/ -		S/ -	
19	Licencia del sofware graylog	S/ -		S/ -	
20	Configuración del Hardware y Software			S/ -	
21	Instalación del Sistema Operativo	S/ -		S/ -	
22	Configuración del Sistema Operativo	S/ -		S/ -	
23	Pruebas de Funcionamiento			S/ -	
24	Prueba de recepción de logs	S/ -		S/ -	
25	Prueba de gestión de usuarios	S/ -		S/ -	
26	Documentación			S/ -	
27	Creación de Manuales de usuario	S/ -		S/ -	
28	Documentación Técnica	S/ -		S/ -	
29	Etapa de Optimización			S/ -	
30	Informe de Seguimiento y Control	S/ -		S/ -	
31	Costos Futuros	S/ -		S/ -	
32	Mantenimiento anual del servidor Graylog, incluyendo actualizaciones, infraestructura en hardware y gestión de base de datos	S/ 150.00		S/ 150.00	

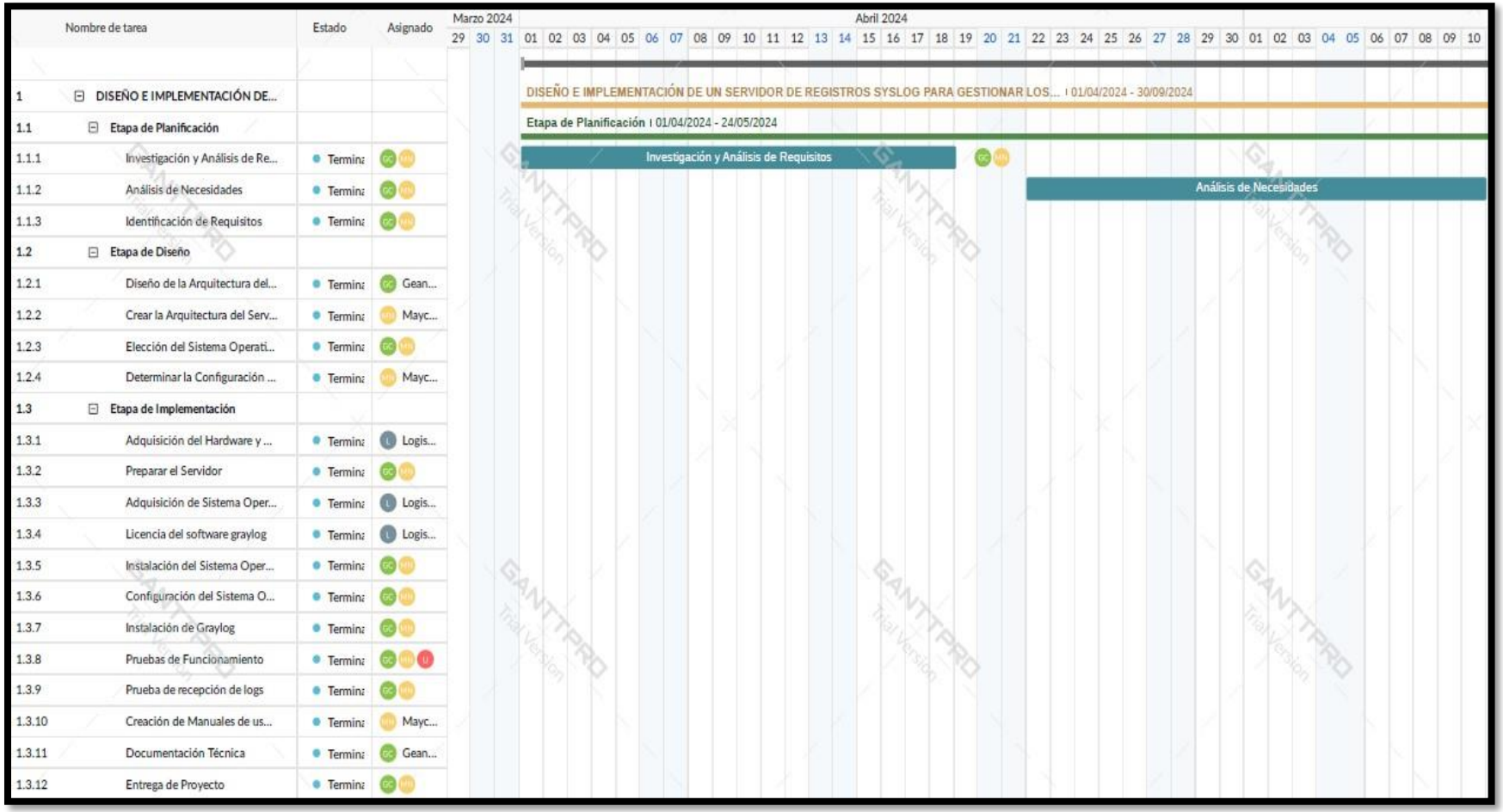
Fuente [Propia]

Cronograma de ejecución

El proyecto se llevó a cabo desde el 01 de abril hasta el 31 de setiembre del 2024. Debido al espacio del documento se mostrará el cronograma en varías imágenes.

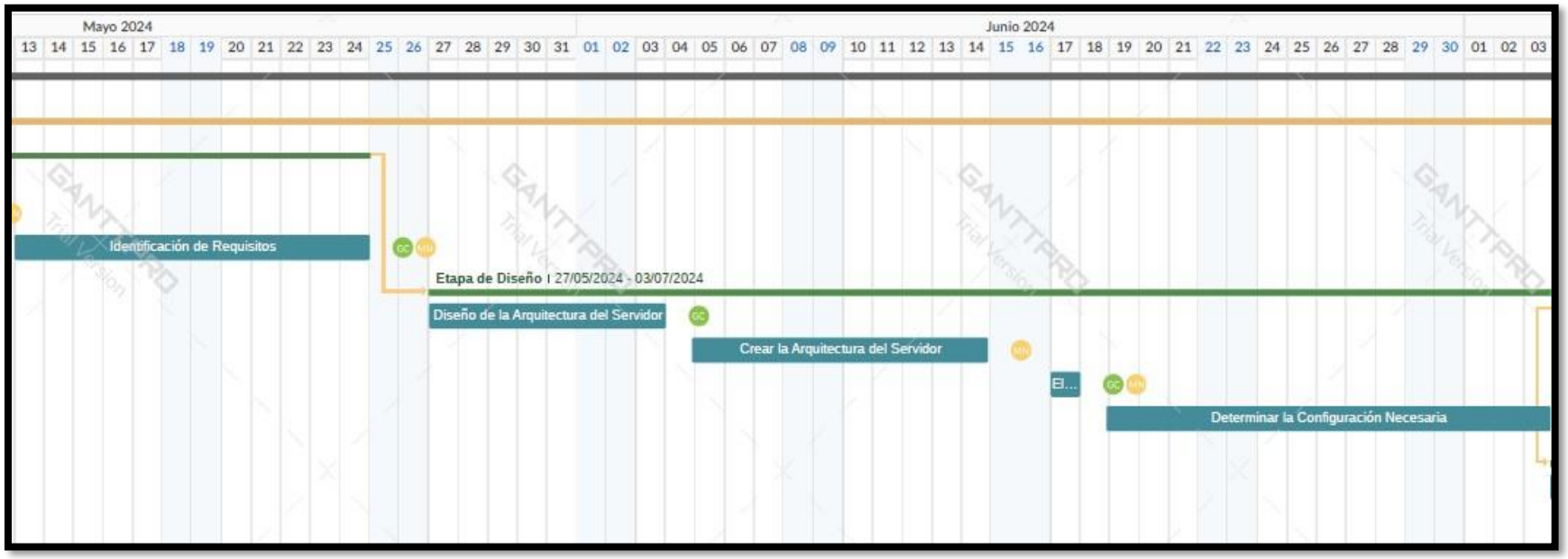
En la figura 11, se muestra el cronograma con las fechas para cada actividad desde el inicio del proyecto el día 01 de abril hasta el día 10 de mayo.

Figura 11. Se muestra cronograma del proyecto.



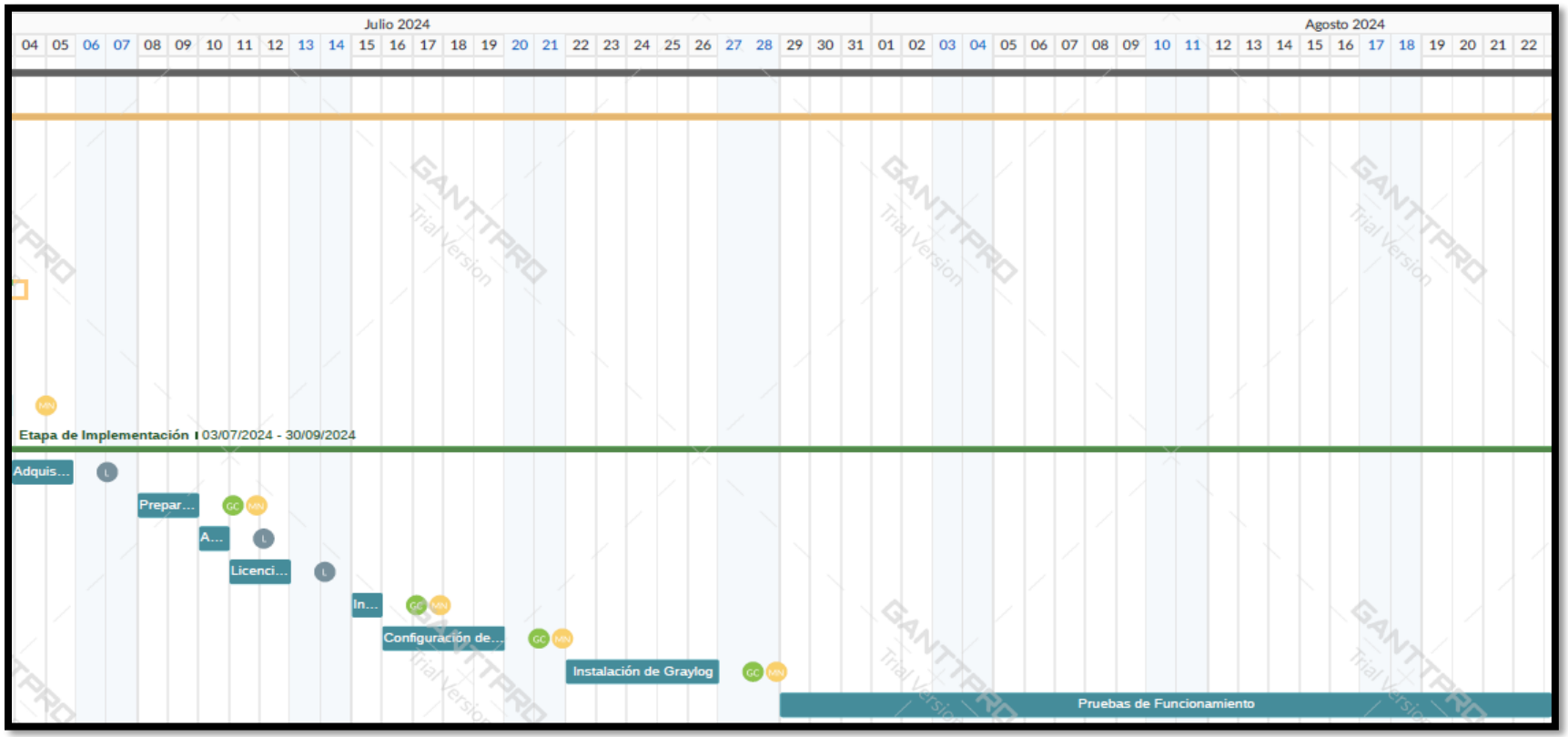
Fuente [Propia]

Figura 12. Se muestra el cronograma con las fechas para cada actividad desde el 13 de mayo hasta el 03 de julio.



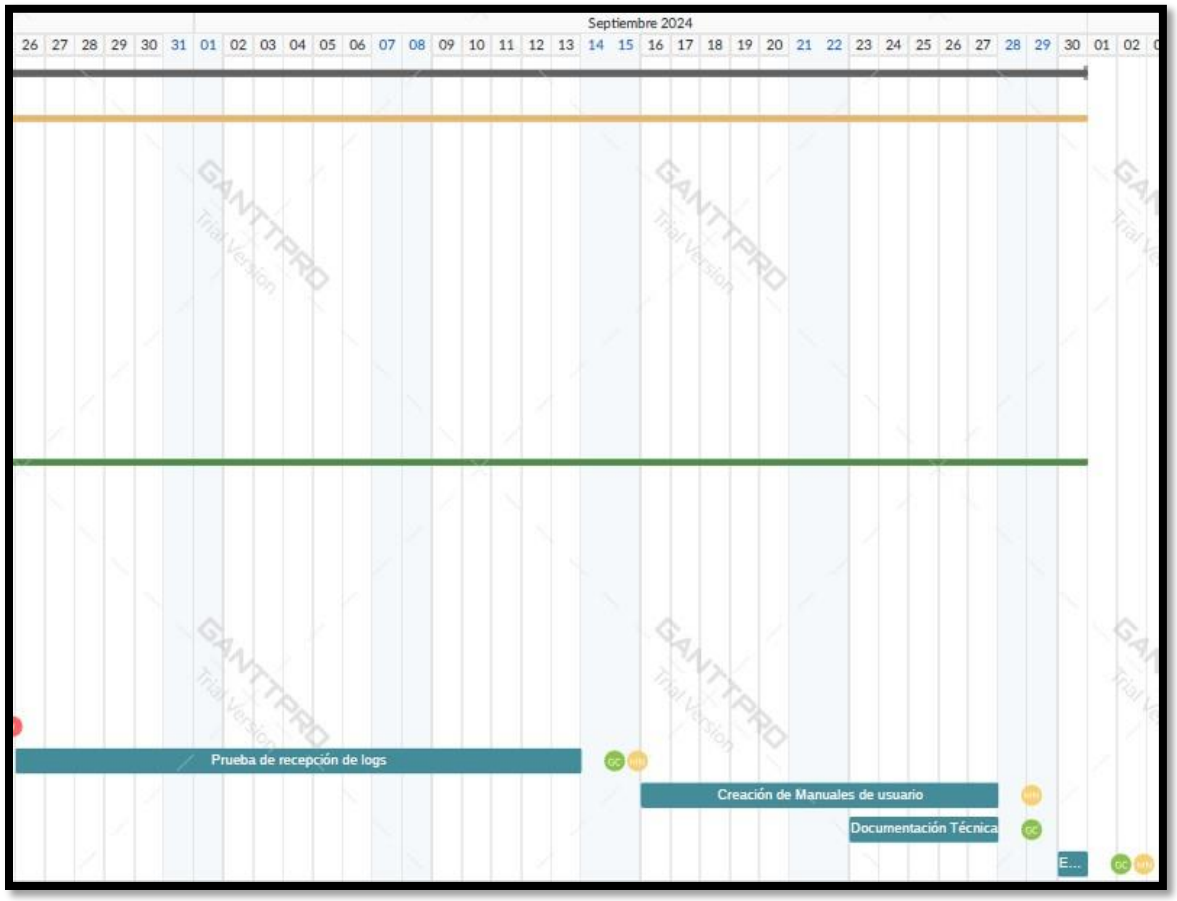
Fuente [Propia]

Figura 13. Se muestra el cronograma con las fechas para cada actividad desde el 04 de julio hasta el 22 de agosto.



Fuente [Propia]

Figura 14. Se muestra el cronograma con las fechas para cada actividad desde el 26 de agosto hasta el 30 de setiembre.



Fuente [Propia]

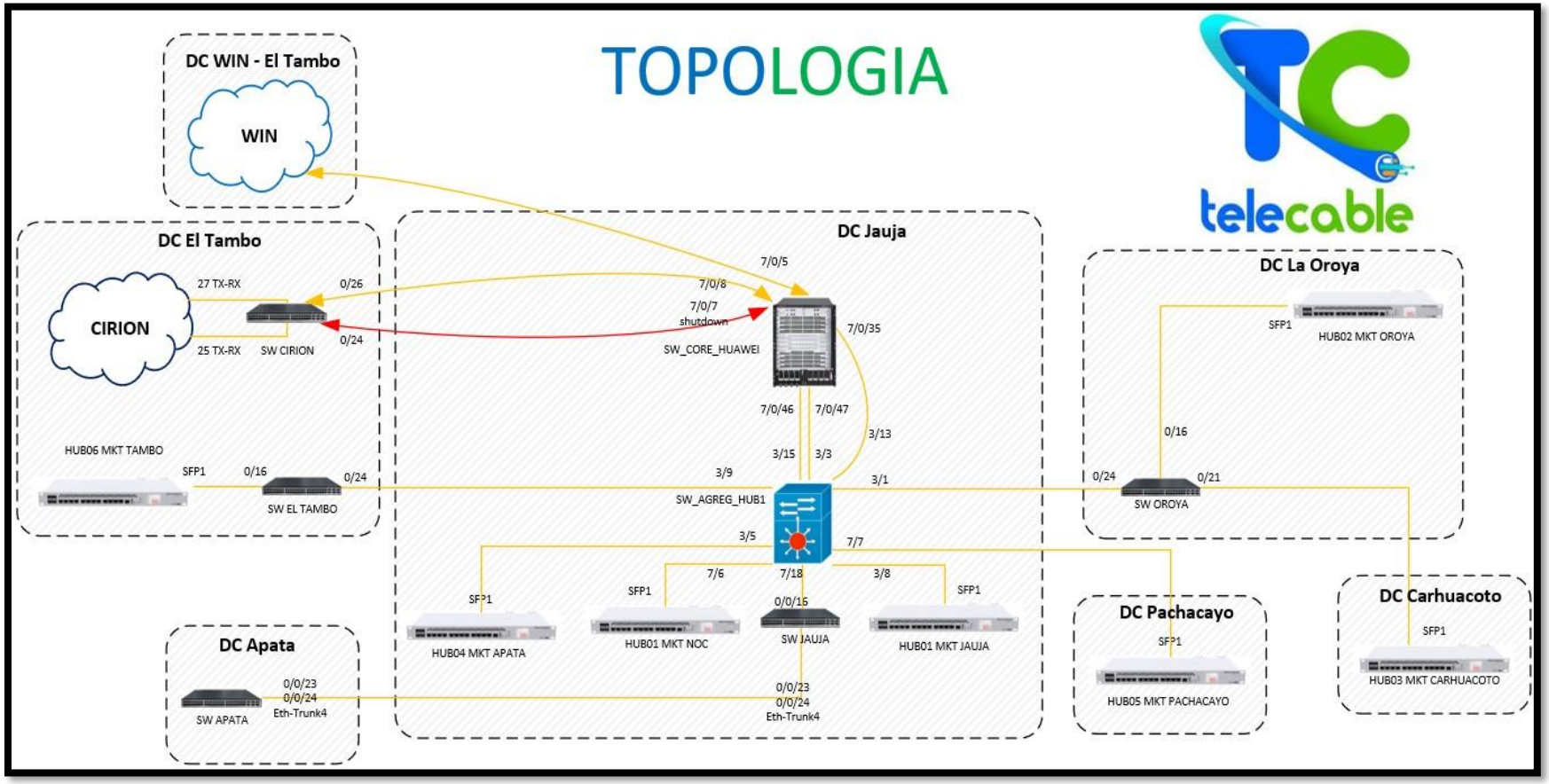
Evaluación de red existente

Telecable actualmente almacena los logs de manera local en cada uno de los equipos, esto conlleva un riesgo de nivel medio, ya que si el equipo se inhibe o se reinicia se pierden todos los datos almacenados y no habría manera de saber la causa del porque el equipo tuvo dicho evento. Además, la gestión descentralizada de logs impide una visión más amplia de la seguridad y el rendimiento de la infraestructura, dificultando la detección de problemas y posibles eventos críticos dentro de la red.

Tener los datos almacenados de esa manera conlleva riesgos como pérdida de datos, falla del hardware, sobreescritura de logs, limitaciones en la recuperación de incidentes, dificultad de diagnóstico y la manipulación de los logs.

En la figura 15, se muestra el diagrama de red actual, y la distribución de los equipos Core en sus diferentes data center ubicados en diferentes zonas geográficas.

Figura 15. Diseño de topología actual.



Fuente: [TELECABLE de Jauja]

Criterios clave para la elección del servidor graylog

a) Capacidad de Manejo de Datos

Volumen de Datos: Se evalúo la cantidad de registros logs que la red genera diariamente.

Calculo total de datos por día, para este análisis se ha tomado la media promedio de logs que se almacenan por día, el cual llega a ser de 10 mil logs con un peso de 334 KB o (342,283 bytes), con esos datos realizaremos la siguiente operación:

$$\frac{342{,}283\ bytes}{10{,}000\ logs} = 34.23\ bytes\ por\ log$$

La capacidad del disco duro es de 500GB, a eso le restamos el peso del sistema operativo y de otras aplicaciones, teniendo un espacio libre de almacenamiento de 400GB, con el cual calcularemos el tiempo en el que este disco se llenará.

Calculamos la capacidad del disco duro de GB a bytes

$$1\ GB = 1{,}073{,}741{,}824\ bytes$$
$$400\ GB = 400 \times 1{,}073{,}741{,}824\ bytes = 429{,}496{,}729{,}600\ bytes$$

Para determinar cuánto tiempo se tardará en llenar el disco duro, dividimos la capacidad total del disco por la cantidad de bytes generados por día:

$$\frac{429{,}496{,}729{,}600\ bytes}{342{,}283\ bytes} = 1{,}254{,}800\ días$$

Convertimos los días en años:

$$\frac{1{,}254{,}800\ días}{365\ días} = 3{,}438\ años$$

Nos brinda el resultado total de almacenamiento de 3 años y 4 meses.
Velocidad de Escritura de datos: La plataforma elegida procesa de manera eficiente los datos de ingreso.

b) Compatibilidad y Flexibilidad

Compatibilidad con Protocolos: El servidor elegido es soportado por los protocolos UDP 514.

Integración con Sistemas Existentes: Nuestro servidor se integró de manera eficiente al sistema de gestión Smart Olt.

c) Características de Gestión de Logs

Almacenamiento y Retención: Para nuestro servidor se tiene asignado las siguientes características de hardware: 8GB de memoria RAM, 500GB de disco duro y un procesador Intel i440fx de 8 núcleos para que pueda procesar la cantidad de datos que ingresa cada minuto.

d) Seguridad y Cumplimiento

Cifrado: Actualmente nuestro servidor de registros tiene activo el control de cuentas de usuario.

Cumplimiento Normativo: El servidor cuenta con el reglamento general de protección de datos y la ISO 27001 para establecer la mejora continua del sistema de gestión de seguridad de la información.

e) Monitoreo y Alertas

Alertas en Tiempo Real: Nuestro servidor tiene la capacidad de generar reportes en tiempo real para todos los eventos.
Dashboards y Visualizaciones: El servidor cuenta con una interfaz web personalizada para la visualización de datos.

f) Análisis y Correlación de Datos

Capacidades de Análisis: Con ayuda de elasticsearch, nuestro servidor cuenta con el análisis de información avanzada para detectar errores, anomalías y generar informes detallados con ayuda de macros.

g) Escalabilidad

Escalabilidad: El servidor implementado es altamente escalable tanto de manera horizontal, es decir que podemos agregar más servidores y vertical para mejorar los componentes de hardware, además, se integra muy bien en muchos clústeres como: elasticsearch, mongobd o aws.

h) Facilidad de Uso y Gestión

Interfaz de Usuario: La interfaz de usuario es muy amigable y sencilla de usar, para gestionar y consultar los logs de manera eficiente.

i) Soporte

Soporte Técnico: El servidor elegido tiene soporte para la versión Enterprise, y se puede ubicar en todos los idiomas disponibles.

Documentación y Comunidad: Actualmente se tiene una comunidad muy activa que ofrece documentación muy útil para resolver problemas y optimizar la plataforma.

j) Costo

Costos de Licencia y Mantenimiento: Para este proyecto no se tuvo un presupuesto asignado, por lo que nos vimos en la necesidad de trabajar con herramientas netamente open source.

A continuación, en la tabla 2, se muestra una comparación entre los diferentes servicios de syslog, para poder elegir la mejor solución a utilizar.

Tabla 2. Cuadro comparativo sobre servidores syslog

Criterio	Syslog-ng	Rsyslog	Graylog
Capacidad de manejo de datos	Buen manejo de grandes volúmenes de datos	Eficiente en el manejo de grandes volúmenes de datos	Optimizado para manejar gran cantidad de datos
Compatibilidad y Flexibilidad	Compatibilidad con protocolos estándares	Alta compatibilidad y flexibilidad	Alta compatibilidad con múltiples fuentes
Gestión de logs	Buena para almacenamiento y retención	Buena para almacenamiento y retención	Buenas opciones para soporte con elasticsearch
Seguridad y Cumplimiento	Buen soporte de cifrado y autenticación	Soporte adaptable a normativas	Buenas capacidades de seguridad, especialmente con elasticsearch
Monitoreo y alertas	Alertas de monitoreo básico	Monitoreo básico	Dashboard de alertas y revisiones personalizadas
Análisis de datos	Análisis básico	Análisis básico	Integración con elasticsearch para análisis
Escalabilidad	Escalabilidad horizontal y vertical	Escalabilidad horizontal y vertical	Escalable en cluster
Facilidad de uso y Gestión	Intuitivo, fácil documentación	Buena documentación	Interfaz web amigables, fácil de usar
Soporte	Buen soporte comercial	Buen soporte comercial	Excelente soporte
Costo	Medio	Medio	Bajo, versiones gratuitas

Fuente [https://serverfault.com/questions/692309/what-is-the-difference-between-syslog-rsyslog-and-syslog-ng]

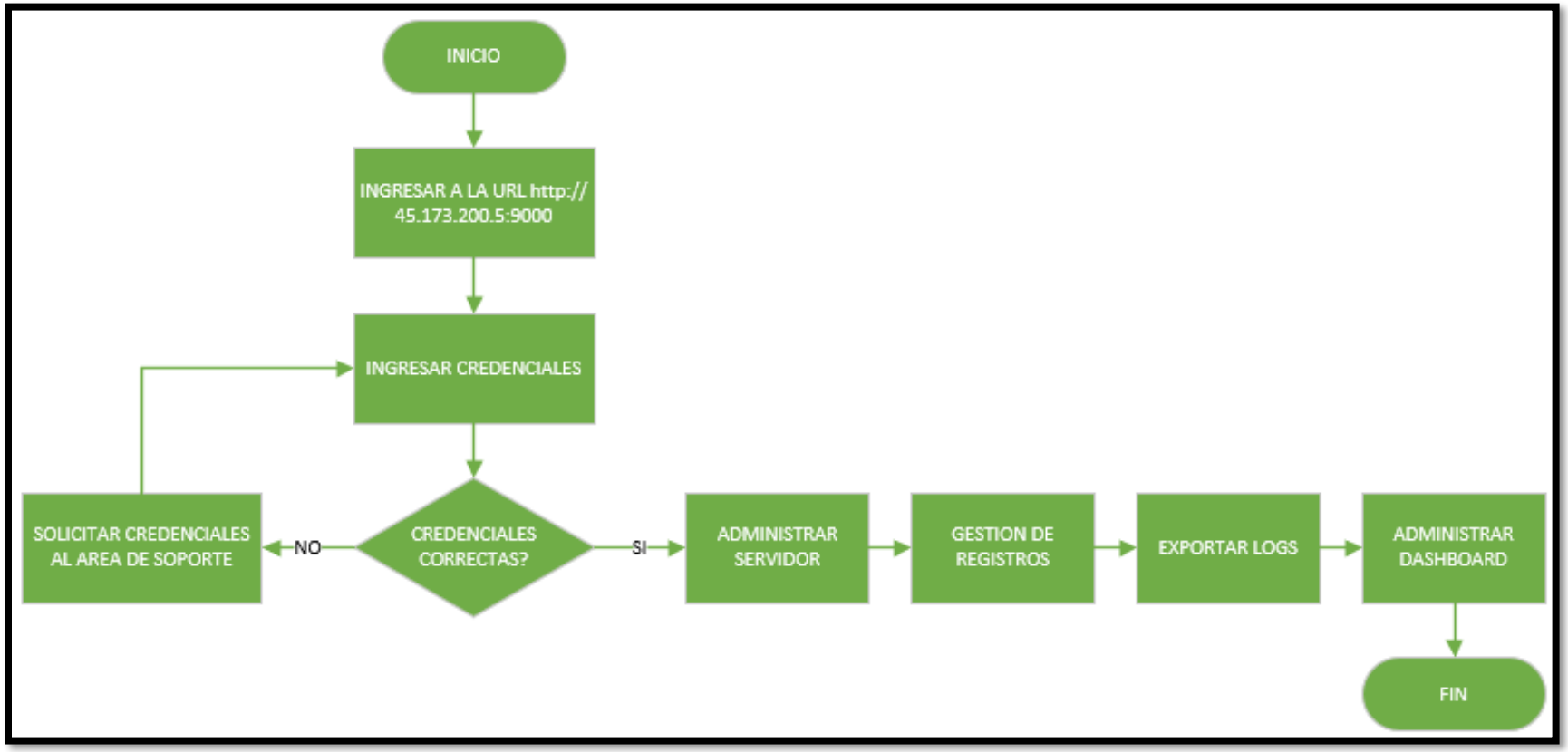
Dentro de este proyectó se eligió el servidor Graylog, ya que de acuerdo al análisis desarrollado y en comparación de otras herramientas, nos brinda mayor escalabilidad, seguridad, gran manejo de datos, una interfaz amigable donde toda persona puede entender el funcionamiento y lo más importante que es de fácil implementación e integración con múltiples herramientas y al ser cero costos es mucho más beneficioso para la empresa.

Graylog fue seleccionado por sus avanzadas capacidades de análisis y búsqueda en tiempo real, que superan a alternativas como Rsyslog y Syslog-ng. Su integración nativa con Elasticsearch permite un manejo eficiente de grandes volúmenes de datos, asegurando la escalabilidad. Además, Graylog ofrece una interfaz intuitiva y amigable, facilitando la adopción por parte del personal técnico sin costos adicionales, ya que es una solución open-source, lo que se traduce en ahorros significativos.

Diagrama de flujo sobre el proceso de inicio de sesión y administración del servidor Graylog

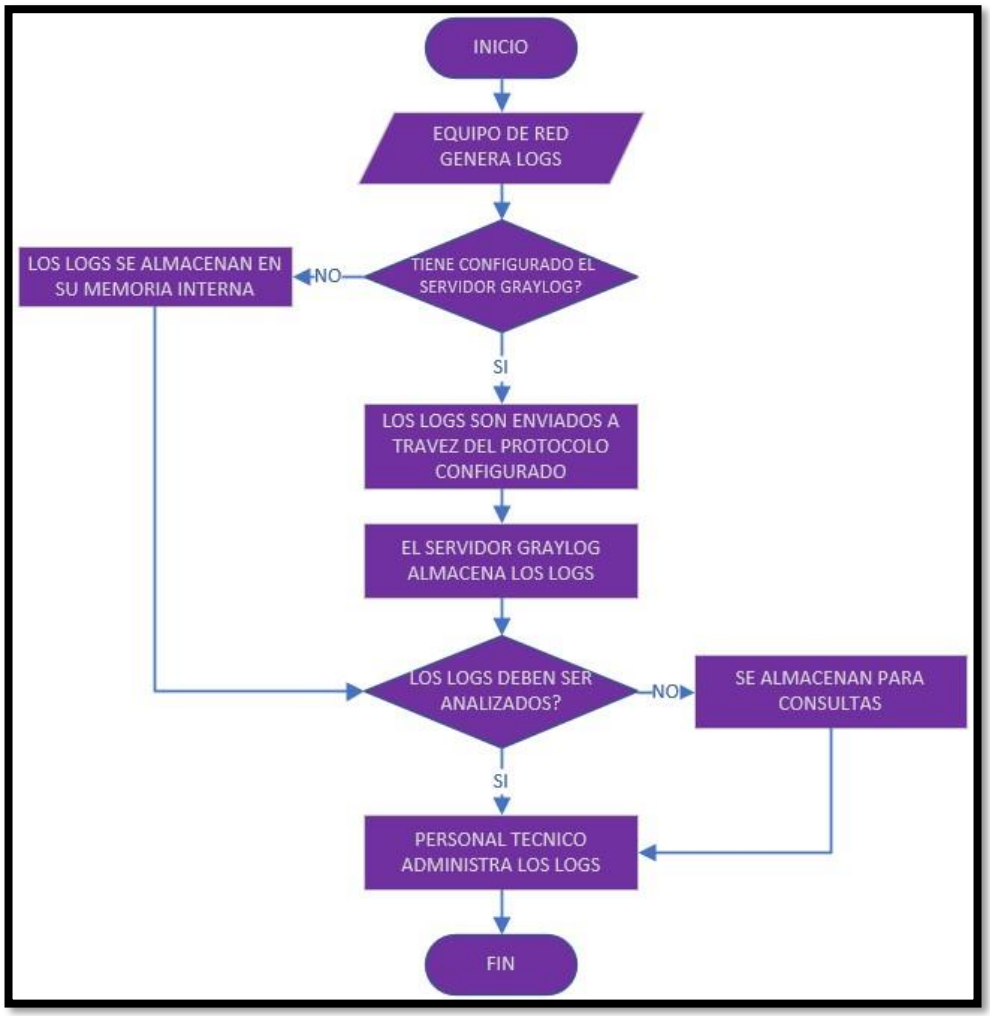
En la figura 16, se muestra el diagrama de flujo del proceso de inicio de sesión para tener acceso a la administración del servidor Graylog a los usuarios permitidos.

Figura 16. Diagrama de flujo del proceso de inicio de sesión.



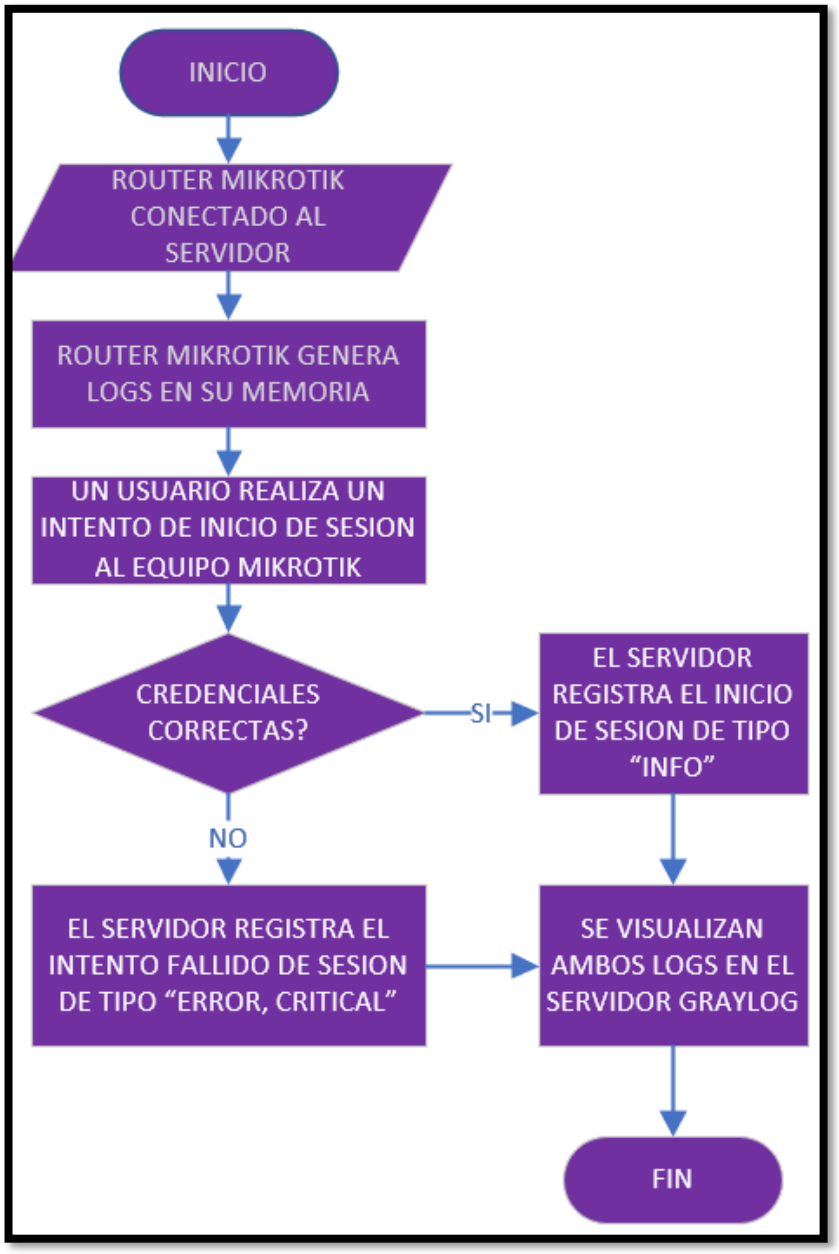
Fuente: [propia]

Figura 17. Se muestra el diagrama de flujo del proceso de envío y recepción del log desde el equipo de comunicación hasta el servidor Graylog.



Fuente: [propia]

Figura 18. Se muestra un ejemplo de intento de inicio de sesión a un router mikrotik, tal como se aprecia en el diagrama el servidor log almacena el evento de intento fallido de sesión y el login exitoso para ser visualizado en el servidor Graylog.



Fuente: [propia]

3.2.3 Diseño

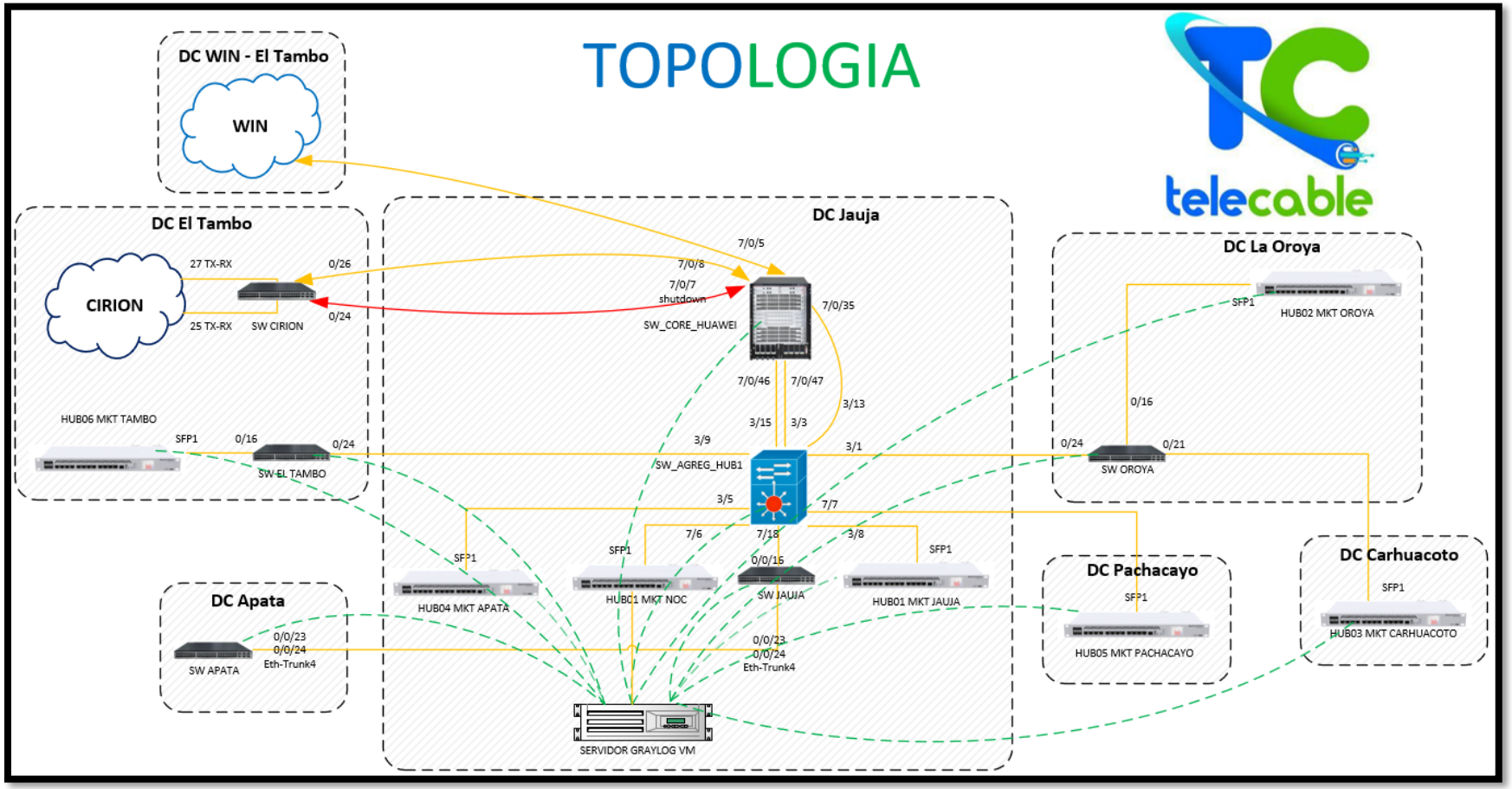
Según el análisis realizado en las instalaciones de Telecable, nos dimos cuenta que a nivel técnico y por un tema de salud administrativa deberíamos contar con un servidor de registros syslog. Este servidor actuará como un repositorio centralizado donde se recopilarán y almacenarán los registros de eventos enviados por nuestros diferentes equipos de red como: Cisco, Mikrotik y Huawei.

Al centralizar los registros en un único servidor, se reducirá significativamente el riesgo de pérdida de información crucial en caso de eventos importantes o incidentes de red. Además, esta solución facilitará la realización de análisis sobre posibles incidencias dentro de la infraestructura de red.

Es preciso detallar que la implementación de este servidor de registros syslog no requiere la adquisición de un servidor dedicado y costoso. Para este proyecto se optó por una solución open source.

La red de Telecable está compuesta por diferentes Data Centers (DC) interconectados a través de switches de agregación y distribución. El diseño propuesto integra un servidor Graylog como repositorio central de registros Syslog, al que se conectan los equipos de red, como routers y switches de marcas Cisco, Mikrotik y Huawei, esta conexión se ve representado por las líneas de color verde, tal como se muestra en la figura 19.

Figura 19. Diseño de topología a implementar.



Fuente: [propia]

Dispositivos en la topología:

Core de Red (SW_CORE_HUAWEI - DC Jauja), es el switch principal de la red y se encarga de distribuir el tráfico entre los diferentes DC. Donde se observan múltiples enlaces de fibra óptica hacia los enlaces principales de internet y al switch de agregación.

SW_AGREG_HUB1, el switch de Agregación que se conecta con el core de la red y distribuye tráfico hacia otros equipos.

SW_JAUJA es el switch de acceso principal de distribución para el DC Jauja.

SW_EL_TAMBO y SW_OROYA son switches de interconexión en sus respectivos DC.

Se observa el uso de router Mikrotik en cada sede:

HUB06 MKT TAMBO
HUB04 MKT APATA
HUB02 MKT OROYA
HUB05 MKT PACHACAYO
HUB03 MKT CARHUACOTO

Todos estos switches conectan clientes y dispositivos de red en sus respectivas zonas.

Líneas amarillas: Representan enlaces de datos entre los Data Centers.

Líneas verdes: Representan la comunicación con el servidor Graylog, lo que confirma que todos los dispositivos están enviando logs hacia este servidor.

El servidor Graylog es un equipo clave en esta infraestructura. Sus funciones principales permitirán la correlación de eventos y análisis de fallos, recopilación y almacenamiento de logs de los equipos de red y generar reportes para administración de la red.

La integración de este servidor en la topología mejora la visibilidad y control de la red, ayudando en la administración y respuesta ante incidentes.

3.2.4 Implementación

Es importante resaltar que el servidor de registros Graylog no funciona por sí solo, esta plataforma necesita de una base de datos no lineal y de un software que permita administrar, buscar y analizar los datos almacenados.

Durante la implementación se trabajó con software netamente open source, como base de datos se utilizó el motor de base de datos mongodb, el cual nos permite almacenar los logs y eventos de los equipos que envían sus registros y para realizar las búsquedas, añadir y analizar los datos registrados dentro del servidor Graylog se utilizó elasticsearch.

Al haber utilizado software libre para la implementación del servidor syslog también tuvimos que usar un sistema operativo que vaya acorde a los fines desarrollados.

Sistema operativo

Un sistema operativo es aquel programa que permite gestionar los dispositivos de hardware de un pc tales como la memoria RAM, la CPU y periféricos, permitiendo la ejecución de aplicaciones dentro de ella. Además; el sistema operativo le brinda una interfaz gráfica al usuario, lo cual la hace fácil de usar.

a) Diferencias entre Linux y Windows para syslog

En la tabla 3, se muestra una comparativa entre los sistemas operativos más usados y las diferencias más notables para determinar cuál es la mejor plataforma para implementar syslog.

Tabla 3. Cuadro comparativo sobre sistema operativo Linux y Windows.

Característica	Linux	Windows Server
Costo	Gratuito (generalmente de código abierto)	Requiere licencia
Estabilidad y Seguridad	Altamente estable y seguro	Mejoras significativas, pero algunos perciben Linux como más seguro
Flexibilidad y Personalización	Altamente personalizable y flexible	Personalizable, pero posiblemente menos flexible que Linux
Herramientas y Aplicaciones	Amplia gama de herramientas de código abierto disponibles, como syslog-ng, rsyslog, etc.	Variedad de herramientas disponibles, pero puede ser menos que Linux
Interoperabilidad y Compatibilidad	Altamente interoperable con una variedad de sistemas y protocolos	Integración más fluida con otros productos de Microsoft
Comunidad de Soporte	Gran comunidad de usuarios y desarrolladores	Soporte robusto de Microsoft y comunidad de usuarios
Experiencia del Administrador	Preferido por usuarios con experiencia en línea de comandos y sistemas basados en Unix	Más familiar para usuarios con experiencia en entornos Windows
Características	Multitarea Multiusuario S.O basado en Unix Alto nivel de seguridad	Multitarea Interfaz de usuario gráfica Muchos desarrolladores crean versiones nuevas para este S.O
Ventajas	Escasez de virus Las actualizaciones de seguridad son automáticas Es gratis y de libre comercio Se modifica a gusto de cada usuario	Existen bastante información para solucionar problemas
Desventajas	Poco soporte para tarjetas aceleradoras de graficas. Existen muchas versiones que crean confusiones.	Gran cantidad de virus diseñados para este S.O Las actualizaciones de seguridad son tardías.

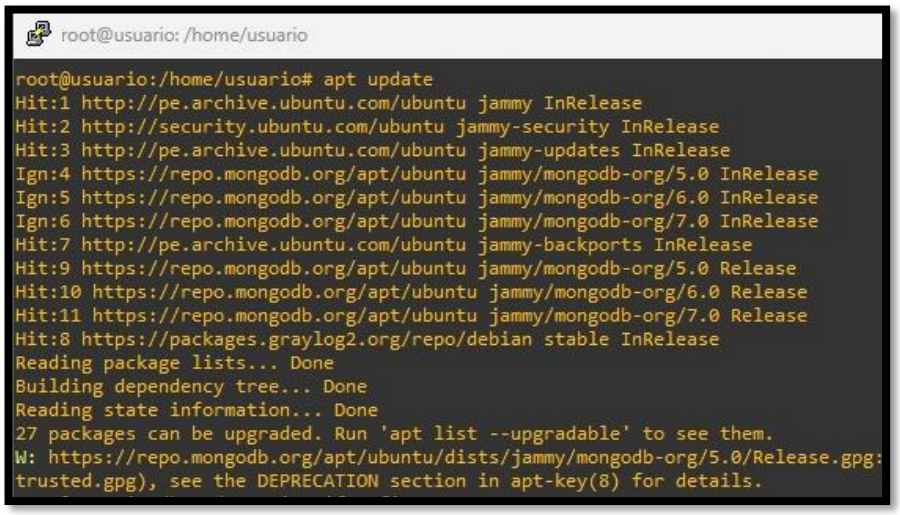
Fuente [https://es.slideshare.net/slideshow/cuadro-comparativo-de-los-sistemas-operativos-windows-y-linux/264513012]

Durante este proyecto se ha seleccionado el sistema operativo basado en Linux con distribución Ubuntu, ya que es el más adecuado para ejecutar servicios nativos de syslog. Para poder realizar una correcta instalación del sistema operativo se deben tomar varios pasos los cuales se encuentran documentados en el anexo número 1.

b) Configuración del sistema operativo

Es necesario tener actualizado el sistema operativo para evitar errores durante el proceso de descarga e instalación de los programas a utilizar, en la figura 20, se muestra el comando para actualizar Ubuntu mediante la consola.

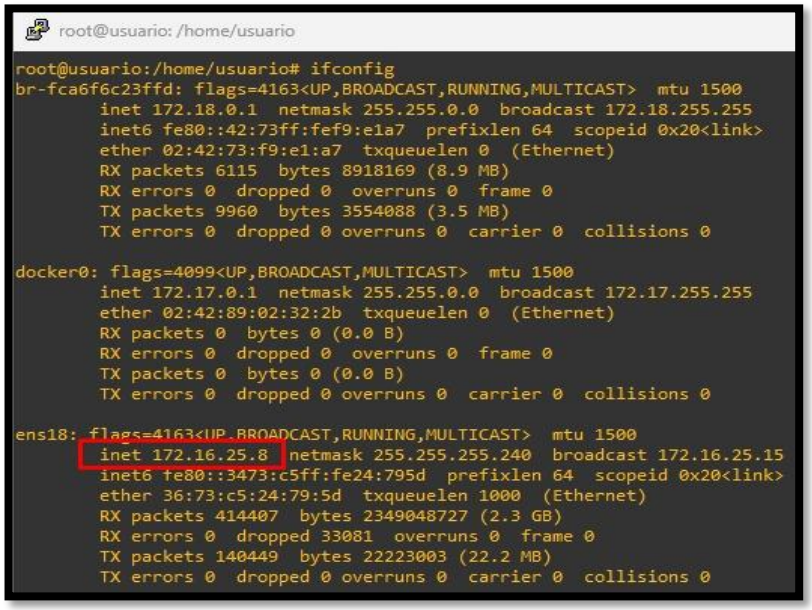
Figura 20. Actualización del sistema operativo.



Fuente: [Propia]

Asignamos una dirección IP estática a nuestro servidor, tal como se muestra en la figura 21.

Figura 21. Configuración de dirección IP.



Fuente: [Propia]

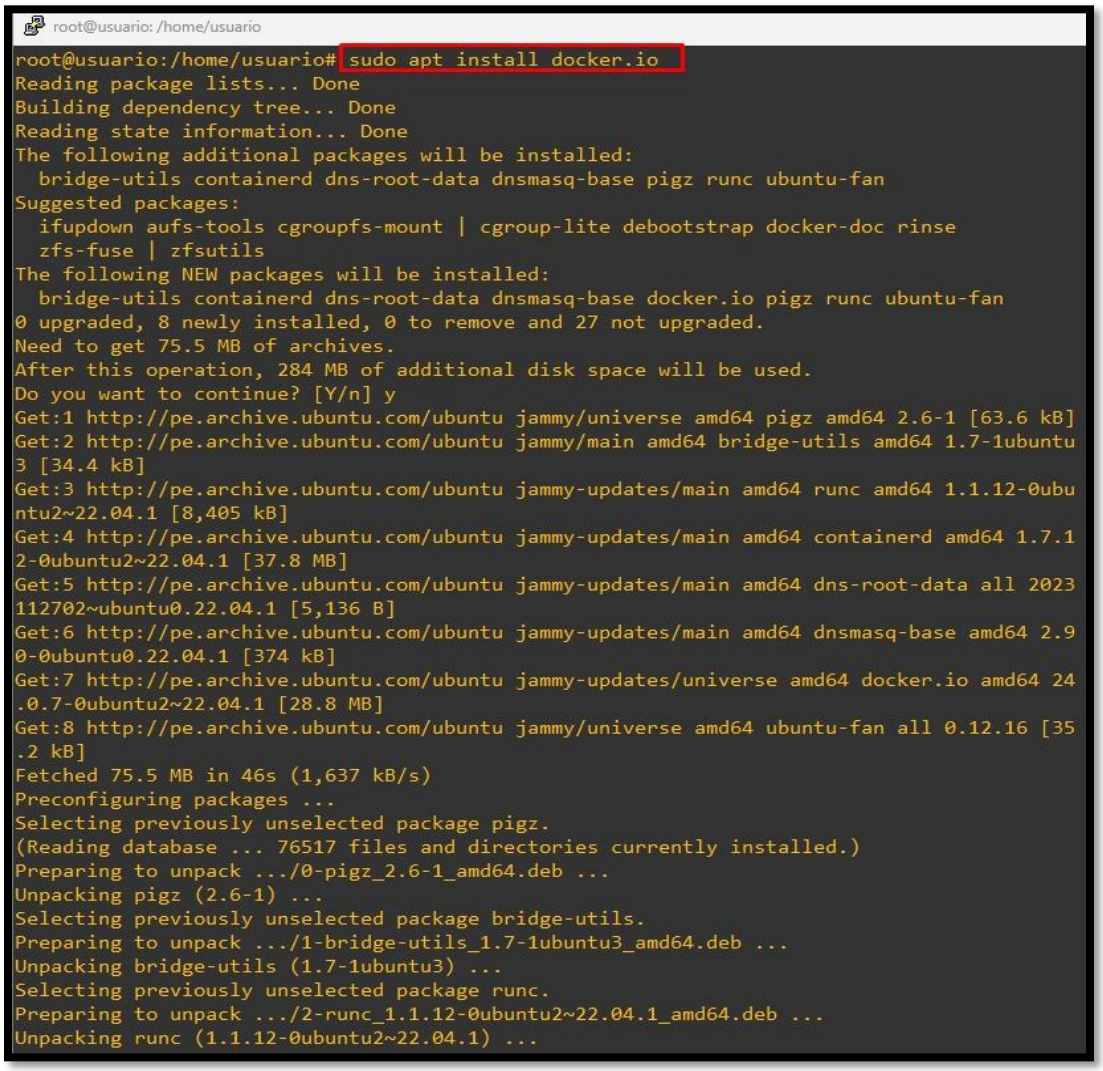
Para poder instalar los programas necesarios haremos uso de un contenedor llamada Docker.

Instalación de DOCKER

Docker es una plataforma de software que permite crear, probar e implementar aplicaciones rápidamente. (49) "Docker empaqueta software en unidades estandarizadas llamadas contenedores que incluyen todo lo necesario para que el software se ejecute, incluidas bibliotecas, herramientas de sistema, código y tiempo de ejecución." (49)

En la figura 22, se muestra el comando para actualizar e instalar el contenedor Docker.

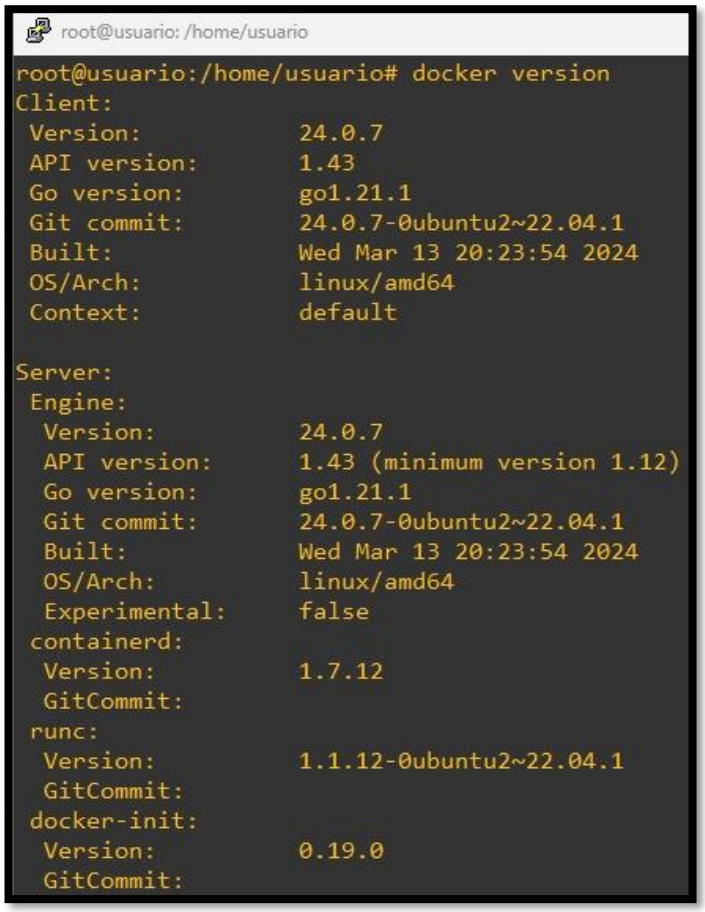
Figura 22. Instalación de Docker.



Fuente: [Propia]

En la figura 23, visualizamos la versión instalada

Figura 23. Versión de Docker.



Fuente: [Propia]

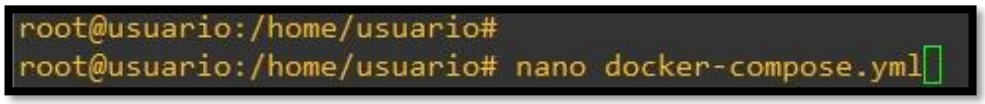
Instalación de MONGODB

MongoDB es un sistema de gestión de bases de datos NoSQL que se ha vuelto muy popular para el análisis de datos. A diferencia de las bases de datos relacionales tradicionales, como MySQL o PostgreSQL, que utilizan un esquema fijo y tablas con filas y columnas, MongoDB utiliza un modelo de documentos JSON flexible, lo que significa que los datos se almacenan en forma de documentos similares a objetos JSON. Este sistema nos da una mayor flexibilidad en la base de datos, porque no requiere un esquema predefinido y los campos varían de un documento a otro dentro de una misma colección.

MongoDB también puede manejar grandes volúmenes de datos y es escalable, también lo conocen por tener la capacidad de distribuir los datos en diferentes servidores.

A continuación, ingresaremos al contenedor Docker para configurar la base de datos mongodb, tal como se muestra en la figura 24.

Figura 24. Comando para acceder al archivo Docker.



Fuente: [Propia]

Figura 25. Se muestra la configuración, la url de donde obtendremos el servicio de mongodb y el volumen para los datos.

Figura 25. Instalación de mongodb.

Fuente: [Propia]

Figura 26. Se muestra el comando para iniciar el contenedor docker con mongo-db.

Figura 26. Servicio mongo-db iniciado.

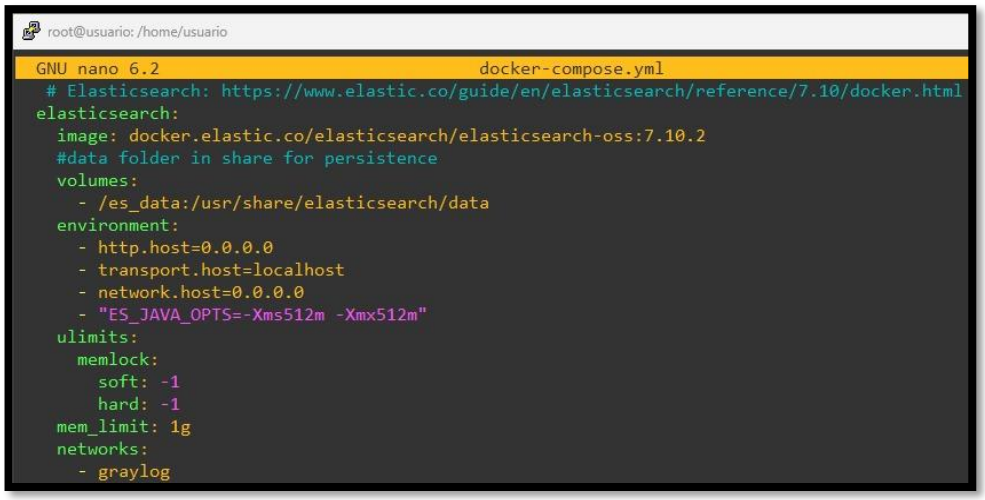
Fuente: [Propia]

Instalación de ELASTICSEARCH

Elasticsearch es un proyecto de código abierto que nos ayuda a dar solución de búsqueda, además que ofrece opciones de búsqueda avanzados, Puede ser utilizado para diferentes casos de uso, dentro de estas la búsqueda de texto en grandes volúmenes de datos, análisis de registros y métricas, monitoreando aplicaciones y sistemas.

Dentro del mismo contenedor Docker se procede a insertar la configuración de elasticseach, tal como se muestra en la figura 27.

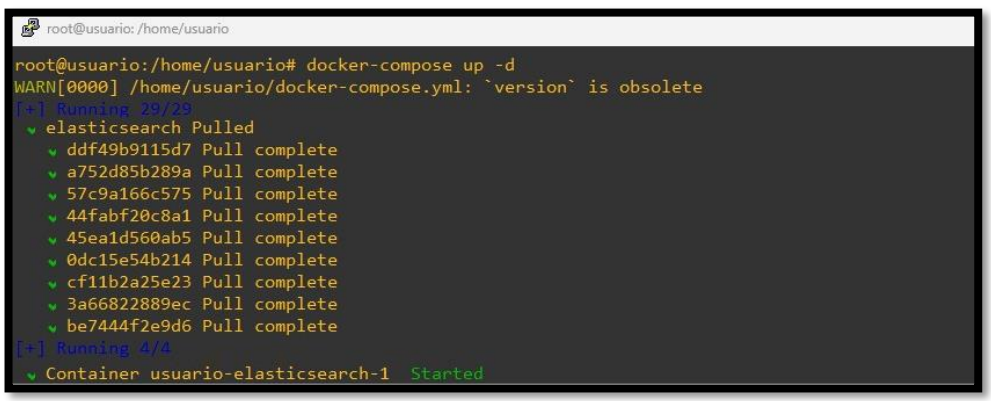
Figura 27. Instalación de elasticsearch.



Fuente: [Propia]

En la figura 28, se muestra el comando para iniciar el contenedor Docker con elasticsearch.

Figura 28. Servicio elasticsearch iniciado.



Fuente: [Propia]

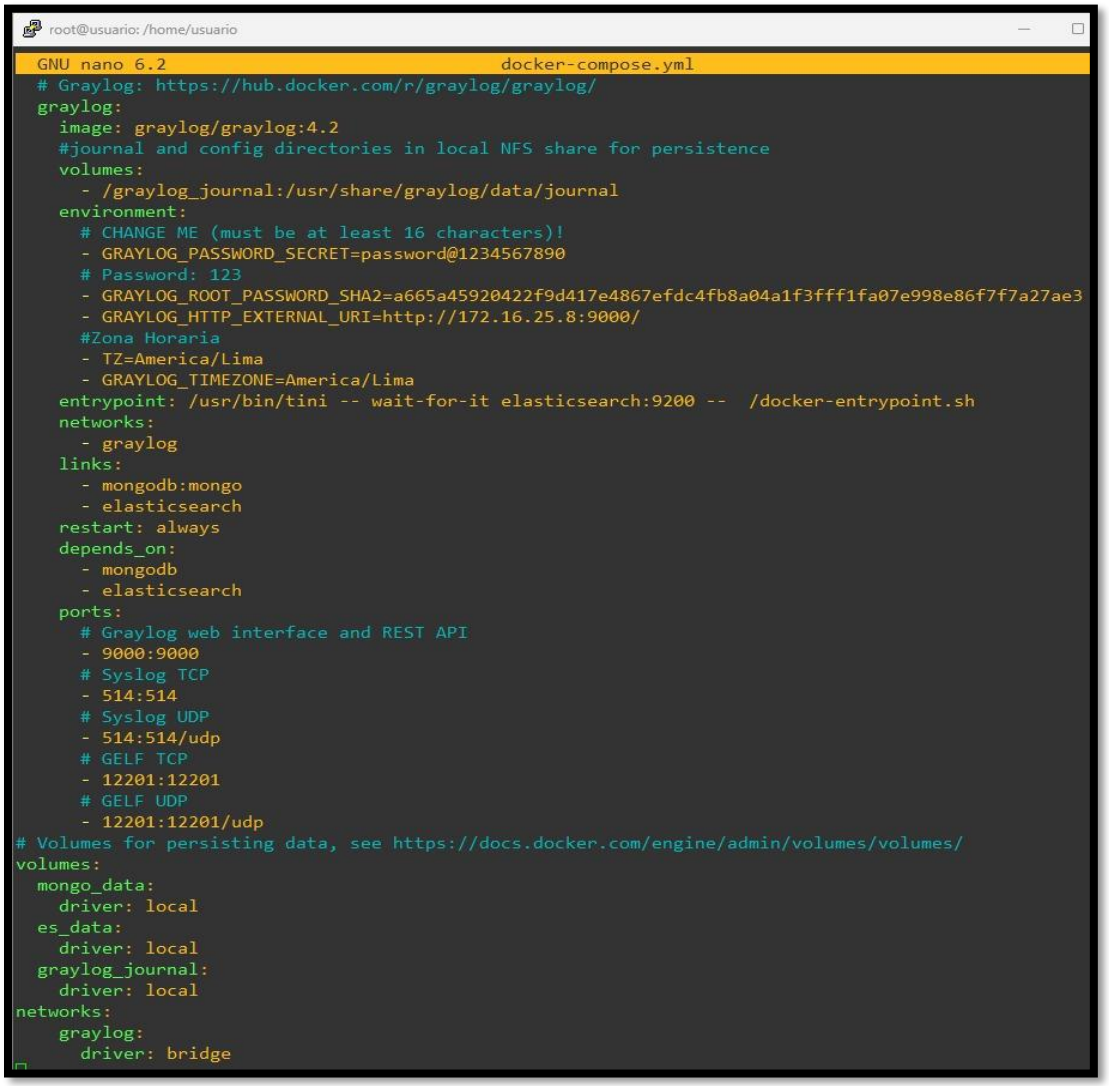
Instalación de GRAYLOG SERVER

Graylog es una plataforma de gestión de registros y análisis de registros de código abierto. Está diseñada para recopilar, indexar y analizar grandes volúmenes de registros de diversos sistemas y aplicaciones en tiempo real.

Algunas de las características principales de Graylog incluyen: recopilación de registros, indexación, almacenamiento, análisis, búsqueda, visualización, tableros, escalabilidad y disponibilidad.

Dentro del mismo contenedor Docker se procede a insertar la configuración de Graylog, se debe cambiar el hash de la contraseña admin para el acceso a la web y adicionar la IP del server, tal como se muestra en la figura 29.

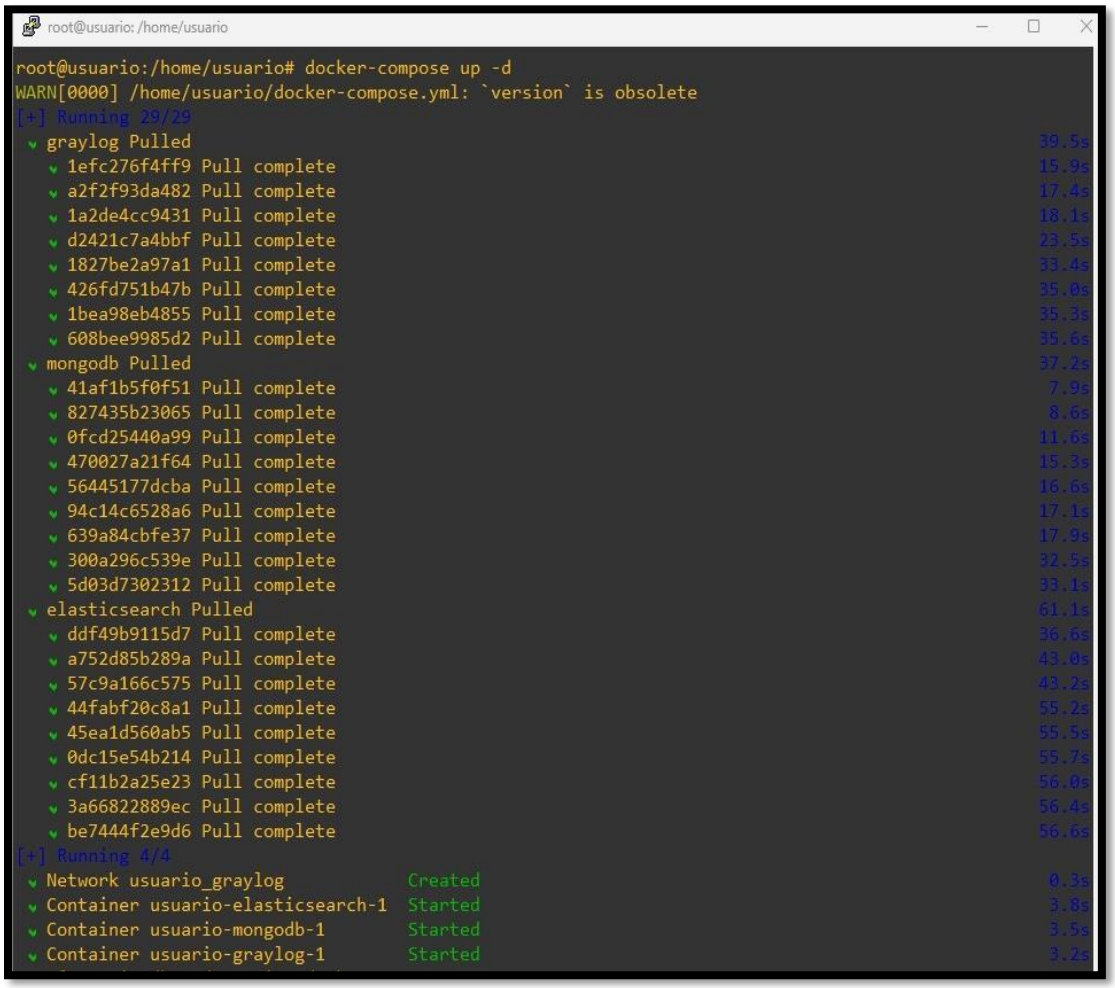
Figura 29. Instalación de Graylog.



Fuente: [Propia]

En la figura 30, se muestra el comando para iniciar el contenedor docker con graylog, en conjunto con mongo-db y elasticsearch.

Figura 30. Servicio graylog iniciado.



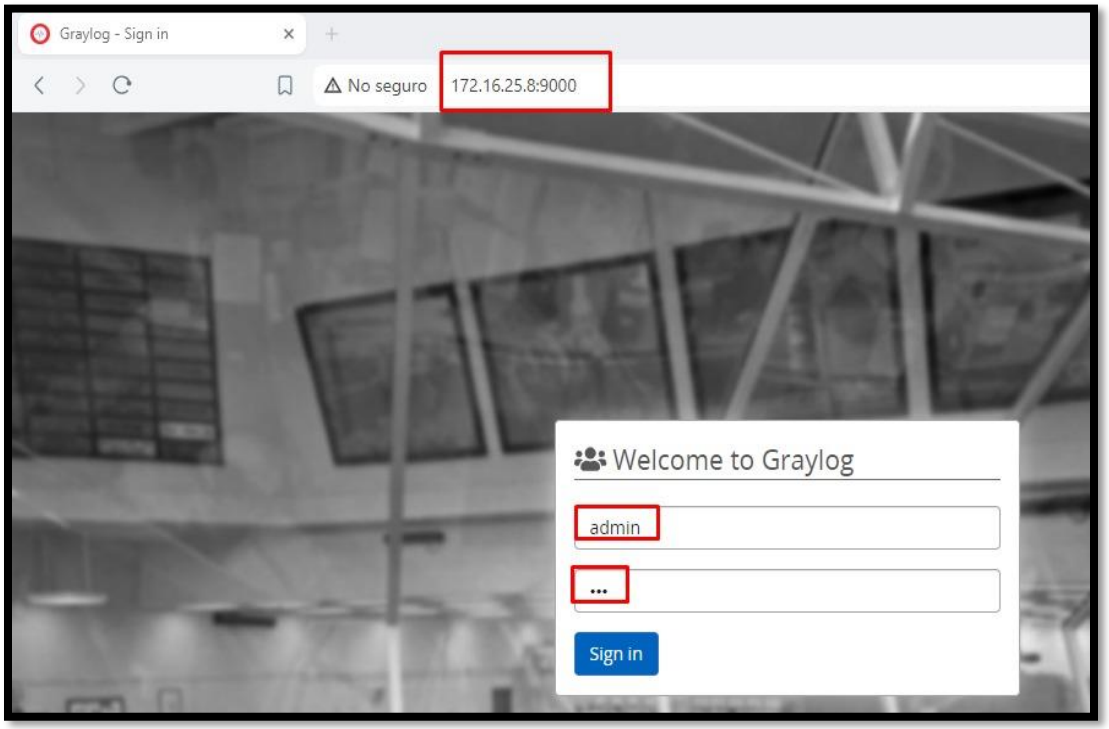
Fuente: [Propia]

Configuración de GRAYLOG SERVER

Posterior a la instalación de los 3 servicios, mongodb, elasticsearch y graylog dentro del contenedor Docker, se procedió a configurar la interfaz gráfica de Graylog para empezar a recibir logs.

Para la configuración de nuestro servidor, accedemos mediante un navegador con la IP 172.16.25.8:9000 y ponemos nuestras credenciales de usuario, tal como se muestra en la figura 31.

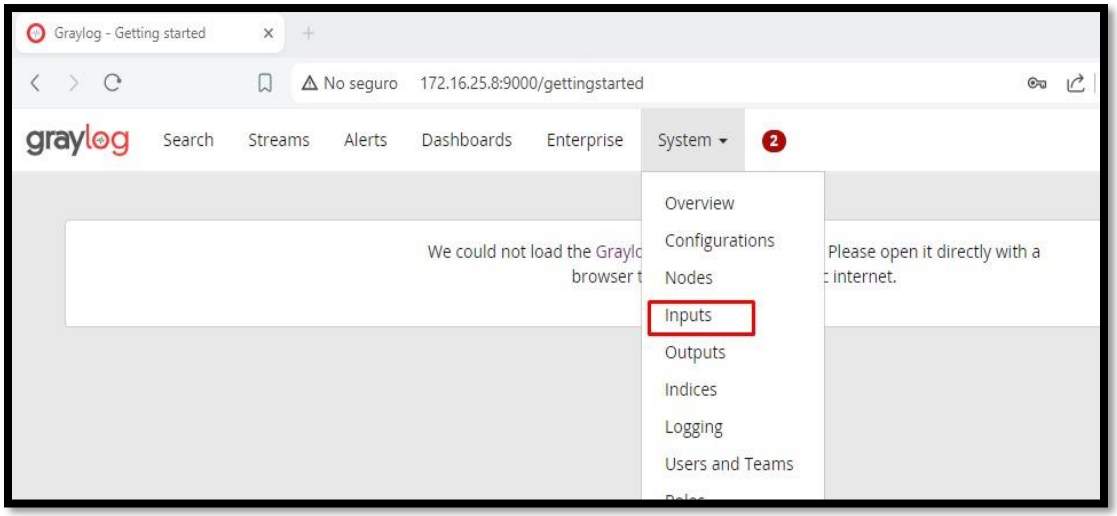
Figura 31. Inicio de sesión en Graylog.



Fuente: [Propia]

Una vez dentro de la plataforma, nos dirigimos a System y seleccionamos Inputs, tal como se muestra en la figura 32.

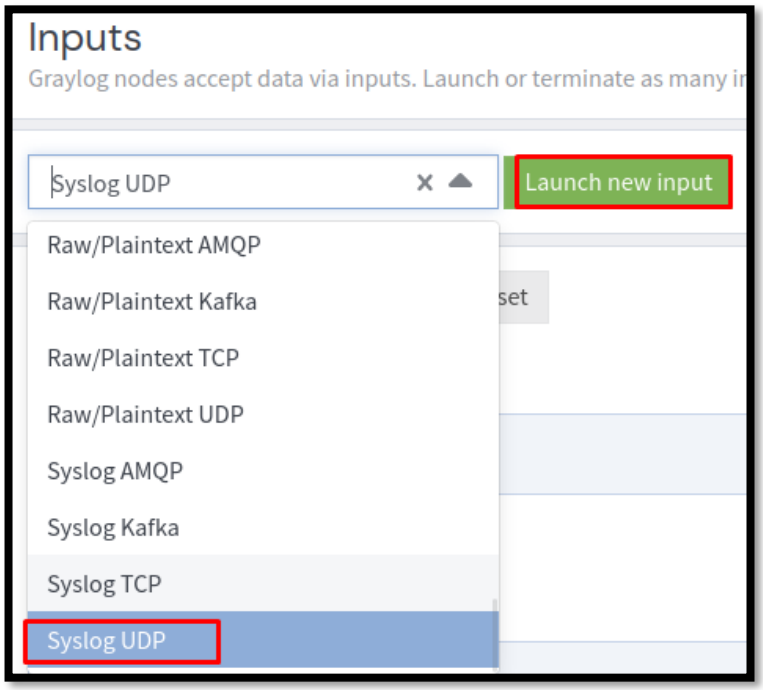
Figura 32. Menú system de Graylog



Fuente: [Propia]

Dentro de Inputs, seleccionamos la opción Syslog UDP y presionamos el botón Launch new input, tal como se muestra en la figura 33.

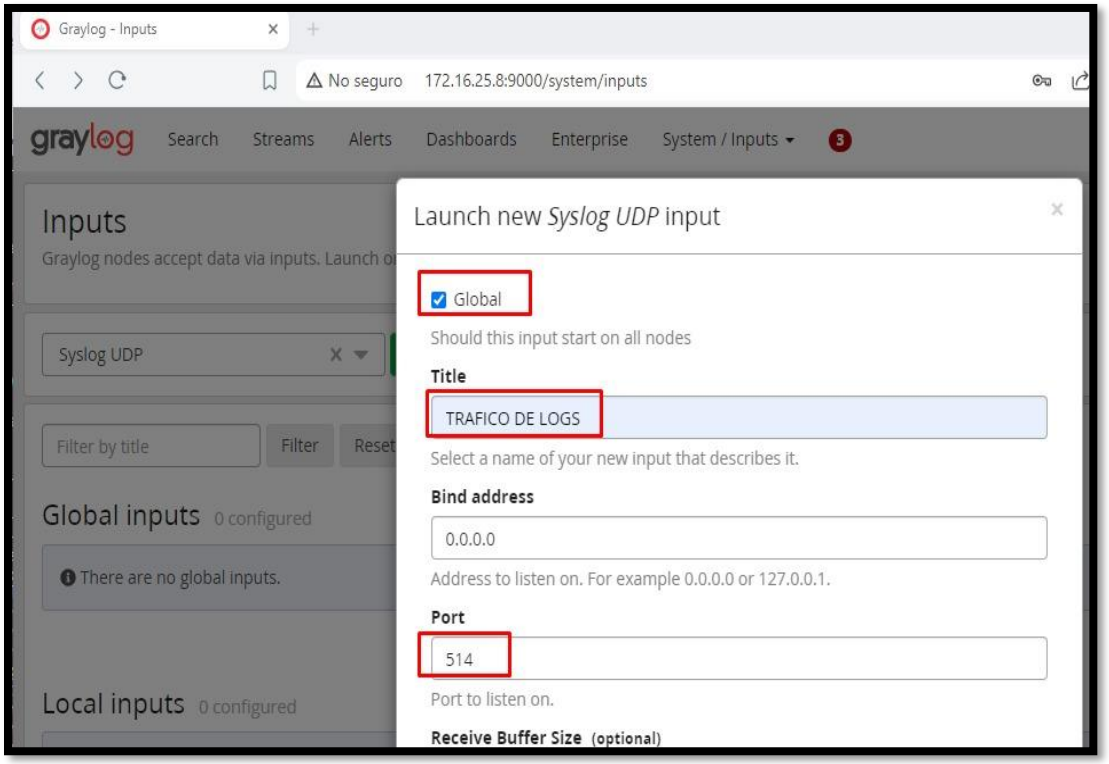
Figura 33. Selección de la opción syslog udp



Fuente: [Propia]

En la figura 34, se muestra los parámetros a configurar: se debe seleccionar el modo global, se asigna un nombre, para esta ocasión se utilizó “TRAFICO DE LOGS”, y se debe elegir el puerto 514 ya que con ese puerto trabaja graylog.

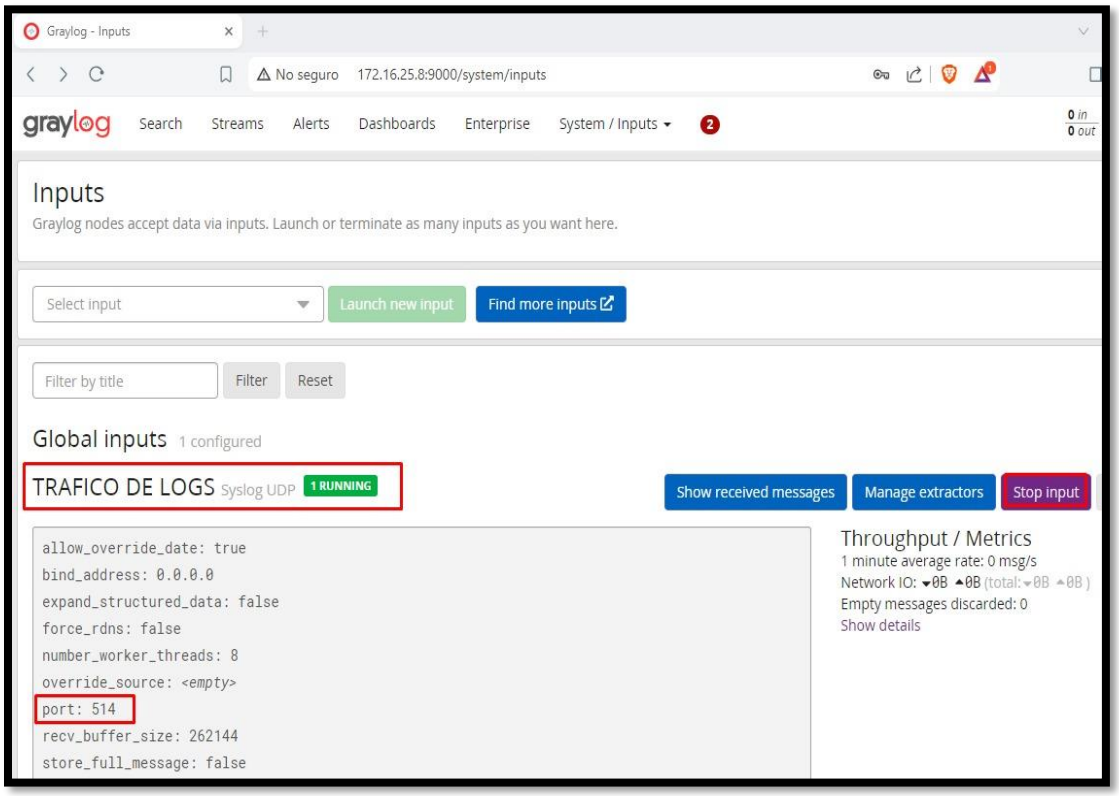
Figura 34. Configuración de parámetros syslog udp.



Fuente: [Propia]

Para finalizar con la configuración de graylog se debe inicializar el servicio, tal como se muestra en la figura 35.

Figura 35. Servicio Graylog activo e iniciado.



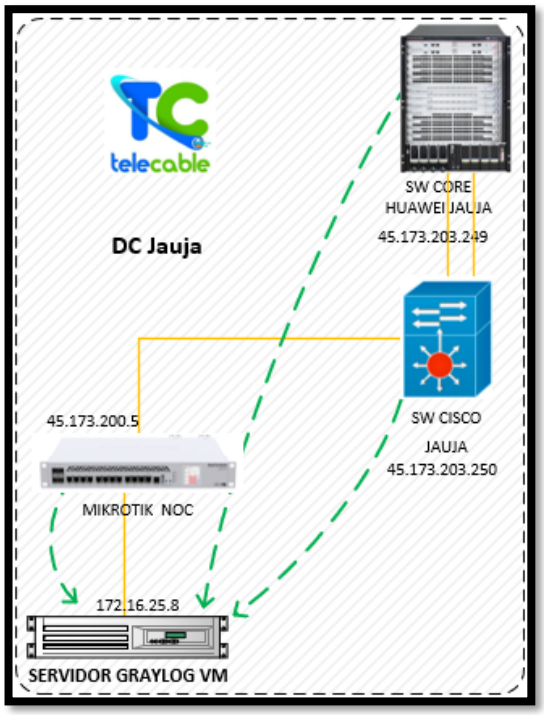
Fuente: [Propia]

3.2.5 Operar

De acuerdo con la topología actual mostrada en el punto 3.2.3, se presenta un pequeño fragmento de ello para realizar las pruebas correspondientes en cada equipo de diferente proveedor que utiliza Telecable como parte de sus operaciones.

En la figura 36, se muestran 3 equipos, los cuales tienen un equipo router de la marca Mikrotik, un switch Cisco y un switch Huawei respectivamente, cabe mencionar que esta topología trata de hacer entender sobre la forma en la cual trabajan y se conectan los equipos de Telecable hacia el servidor GRAYLOG.

Figura 36. Topología con 3 equipos diferentes.



Fuente: [Propia]

Antes de poder comenzar con los escenarios de prueba recordemos que los equipos se encuentran activos y solo realizaremos cambios que no afecten la operatividad del servicio.

Además, se visualiza que el servidor aun no cuenta con tráfico debido a que no se tiene configurado ningún equipo, tal como se muestra en la figura 37.

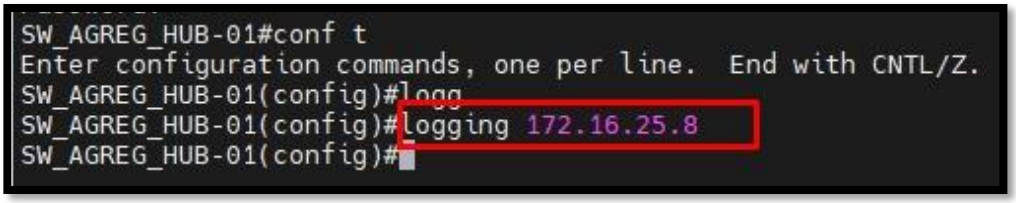
Figura 37. Interfaz de inicio de syslog udp.

Fuente: [Propia]

Escenario 1 – Switch Cisco

Procederemos a configurar el switch cisco para que se asocie a nuestro servidor Graylog, tal como se muestra en la figura 38.

Figura 38. Comando para asociar dispositivos cisco a un servidor Graylog.



Fuente: [Propia]

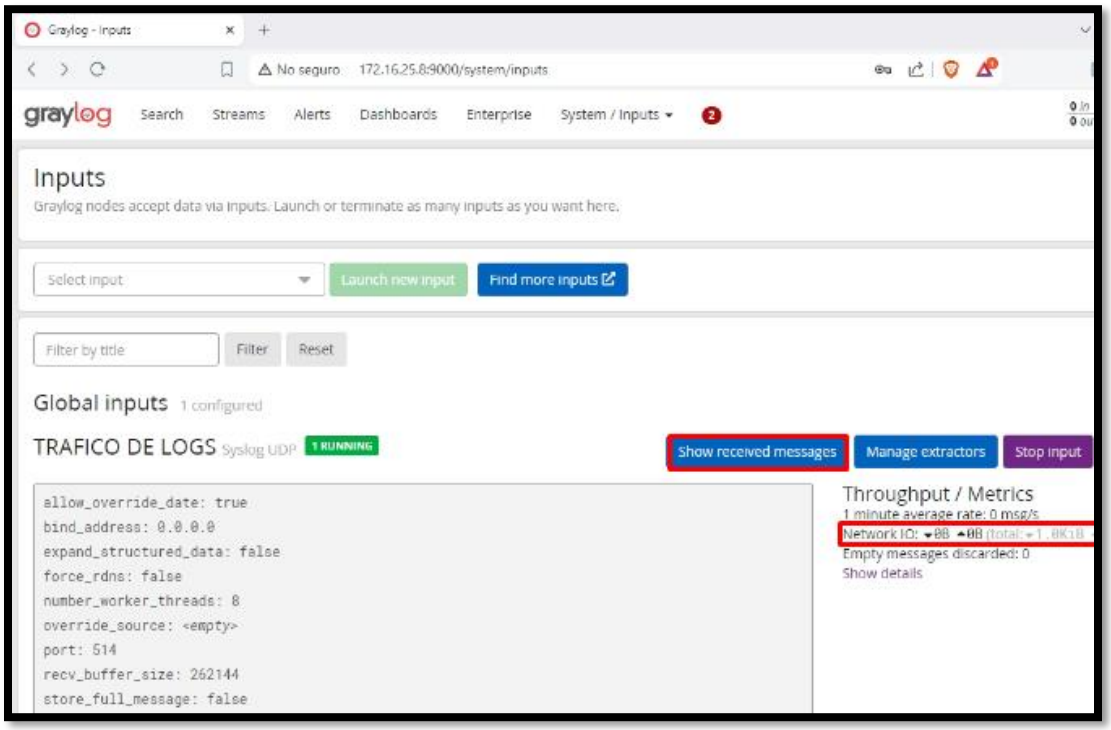
En la figura 39, se visualiza un mensaje donde indica que el equipo se ha conectado de manera satisfactoria al servidor y algunos otros mensajes emitidos por el propio equipo.

Figura 39. Logs internos del switch cisco.

Fuente: [Propia]

Al ingresar al servidor vía web, nos percatamos que el tráfico ya empezó a elevarse debido a que nuestro switch está enviando mensajes de manera constante y para poder visualizarlos presionamos sobre el botón Show received messages, tal como se muestra en la figura 40.

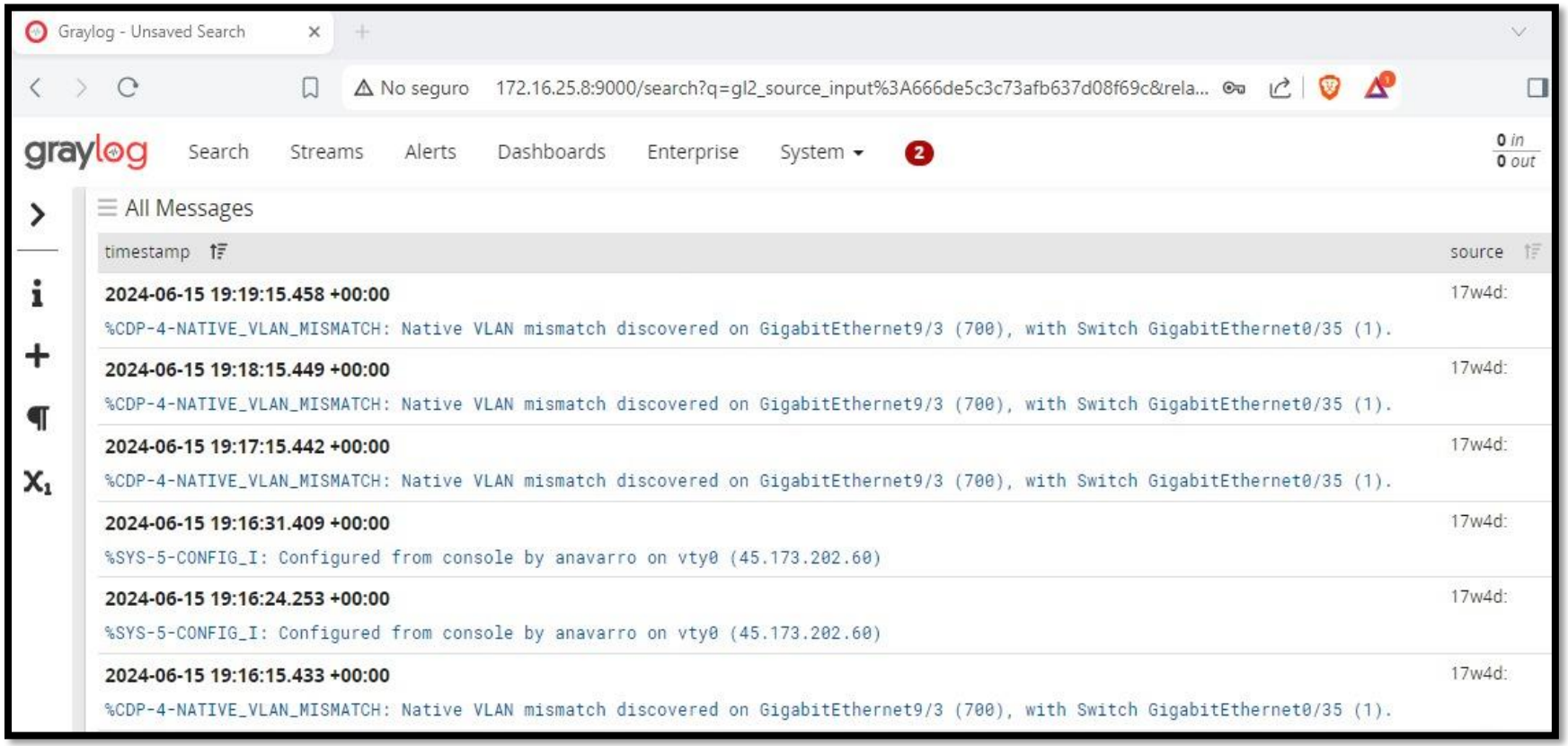
Figura 40. Visualización del tráfico entrante y saliente.



Fuente: [Propia]

En la figura 41, dentro del servidor Graylog, en el apartado de show received messages se visualizan los mismos logs que emitió el switch cisco en la figura 39.

Figura 41. Logs del switch cisco almacenados en el servidor Graylog.

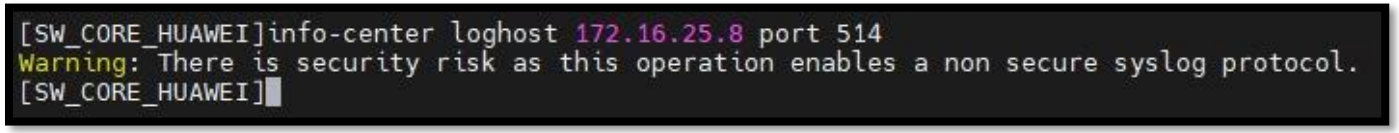


Fuente: [Propia]

Escenario 2 – Switchcore Huawei

Procederemos a configurar el switchcore huawei para que se asocie a nuestro servidor graylog, tal como se muestra en la figura 42.

Figura 42. Comando para asociar dispositivos huawei a un servidor graylog.



Fuente: [Propia]

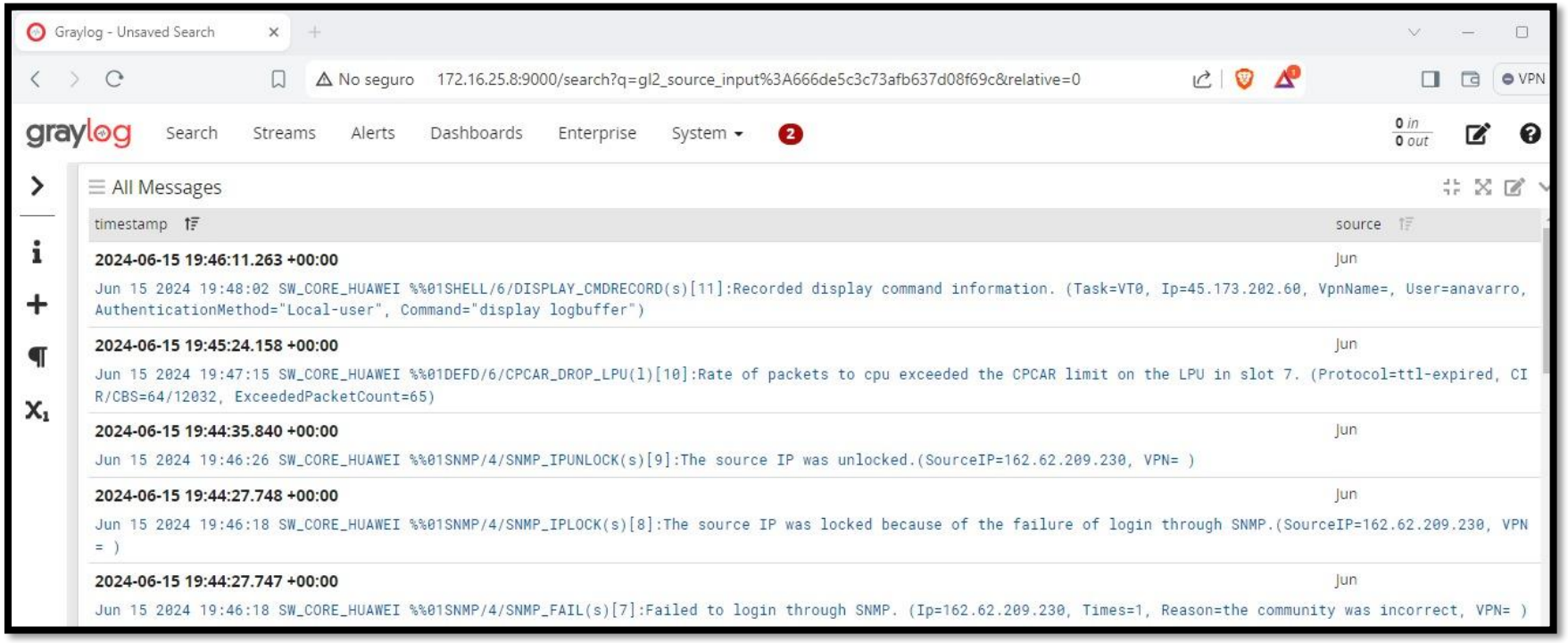
En la figura 43, se visualizan los logs emitidos por el propio equipo Huawei.

Figura 43. Logs internos del switchcore huawei.

Fuente: [Propia]

En la figura 44, dentro del servidor Graylog, en el apartado de show received messages se visualizan los mismos logs que emitió el switchcore Huawei en la figura 43.

Figura 44. Logs del switchcore huawei almacenados en el servidor Graylog.

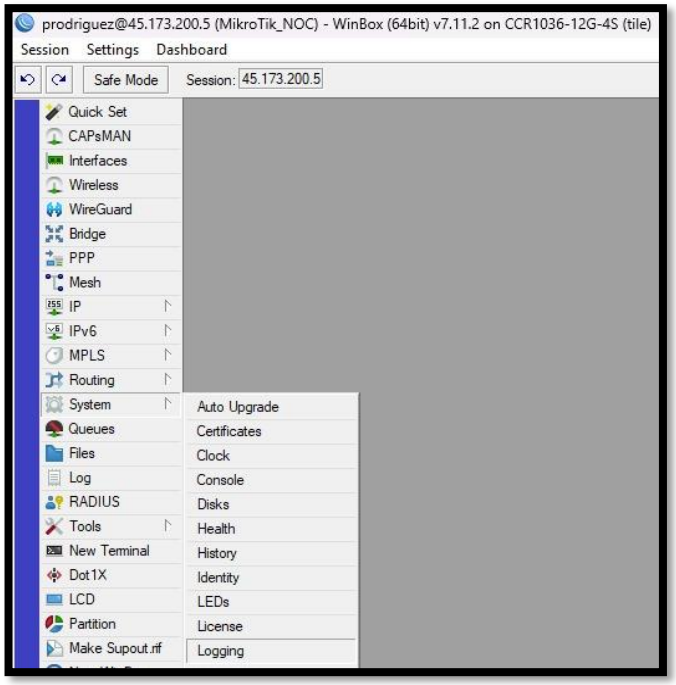


Fuente: [Propia]

Escenario 3

Procederemos a configurar el router mikrotik para que se asocie a nuestro servidor graylog, por lo cual ingresaremos a system/loggin, tal como se muestra en la figura 45.

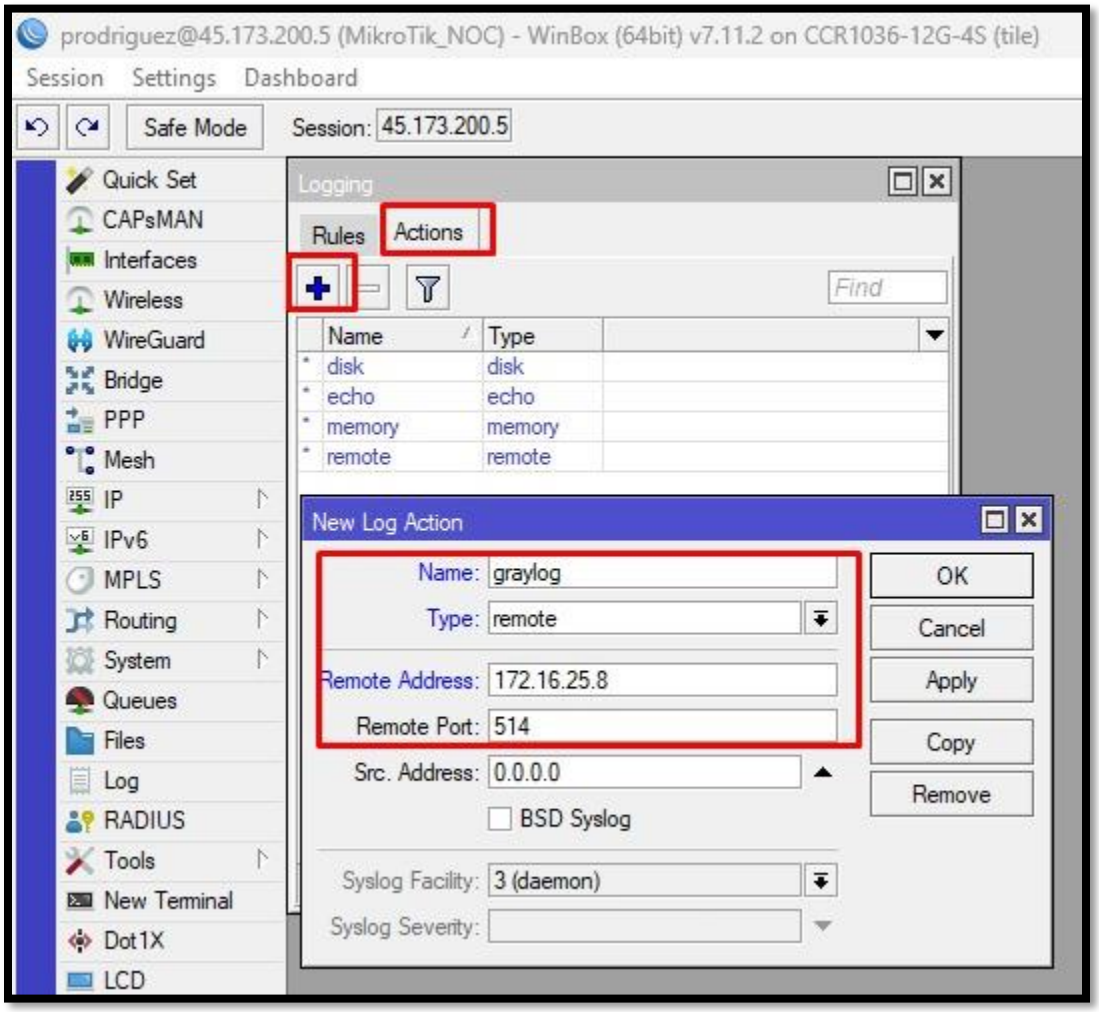
Figura 45. Menú de opciones de mikrotik.



Fuente: [Propia]

En el apartado de actions presionamos el icono de + y configuramos los siguientes parámetros, como nombre, tipo, la ip del servidor y el puerto 514, tal como se muestra en la figura 46.

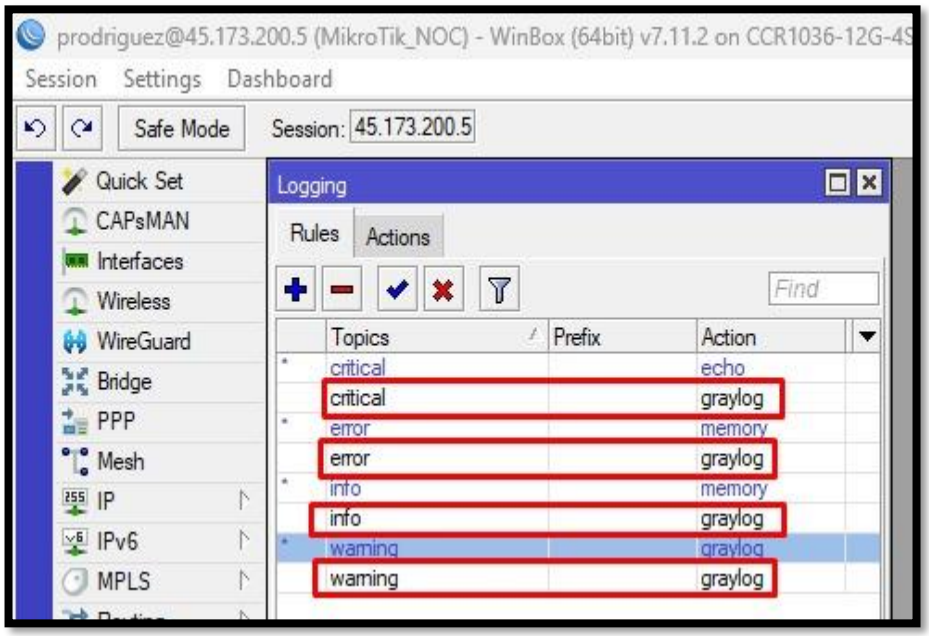
Figura 46. Configuración hacia el servidor Graylog.



Fuente: [Propia]

En el apartado de rules asociamos el tipo de alerta hacia la acción que generamos en el paso anterior llamada Graylog, tal como se muestra en la figura 47.

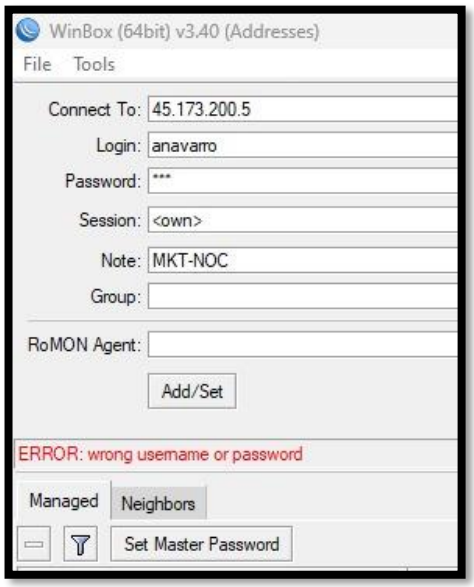
Figura 47. Creación de alertas asociadas a la acción Graylog.



Fuente: [Propia]

En la figura 48, se muestra un intento fallido de acceso al equipo.

Figura 48. Intento fallido de logeo en el router mikrotik

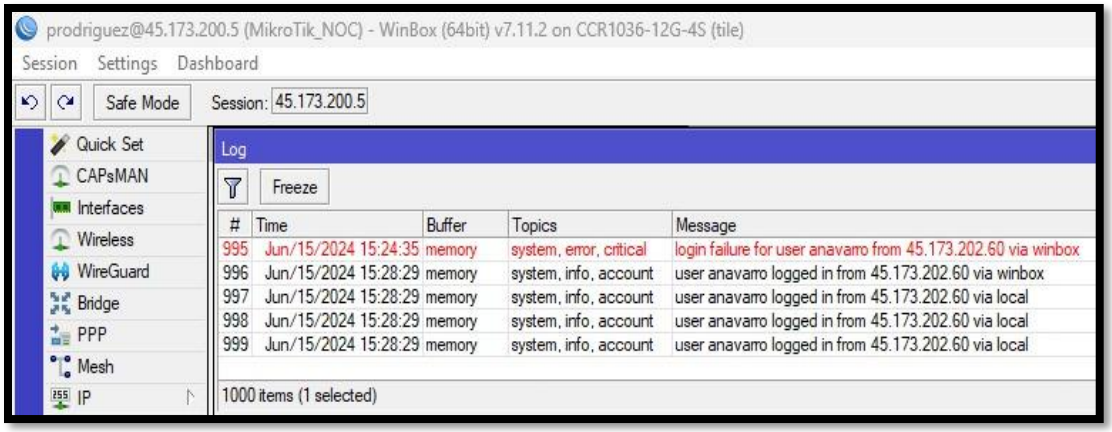


.

Fuente: [Propia]

Como se puede visualizar en la figura 49, se muestra el mensaje de intento fallido de logueo y también 4 mensajes de acceso correcto al equipo, los cuales fueron registrados dentro de la memoria del propio equipo mikrotik.

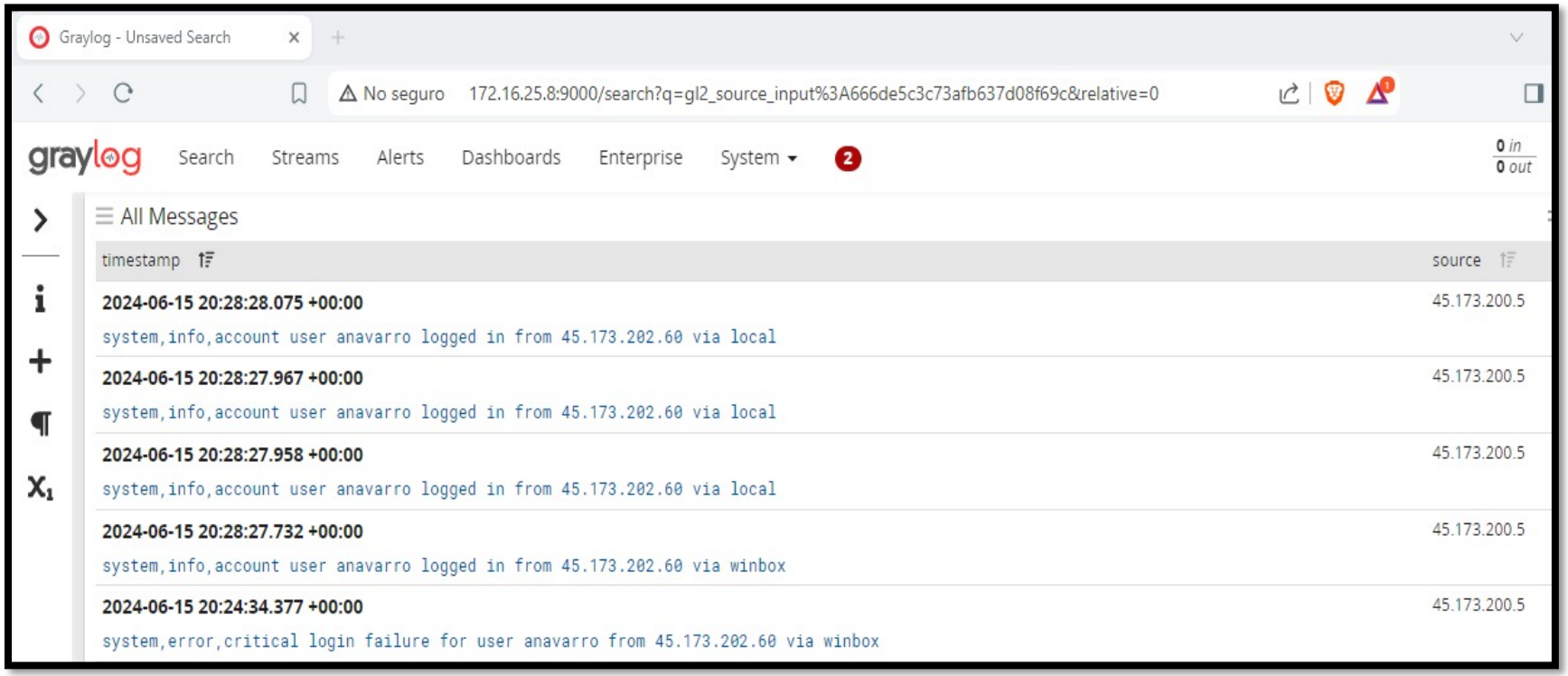
Figura 49. Logs dentro del equipo mikrotik.



Fuente: [Propia]

Dentro del servidor podemos visualizar que los logs del equipo mikrotik se registraron de manera correcta, tal como se muestra en la figura 50.

Figura 50. Logs registrados correctamente.



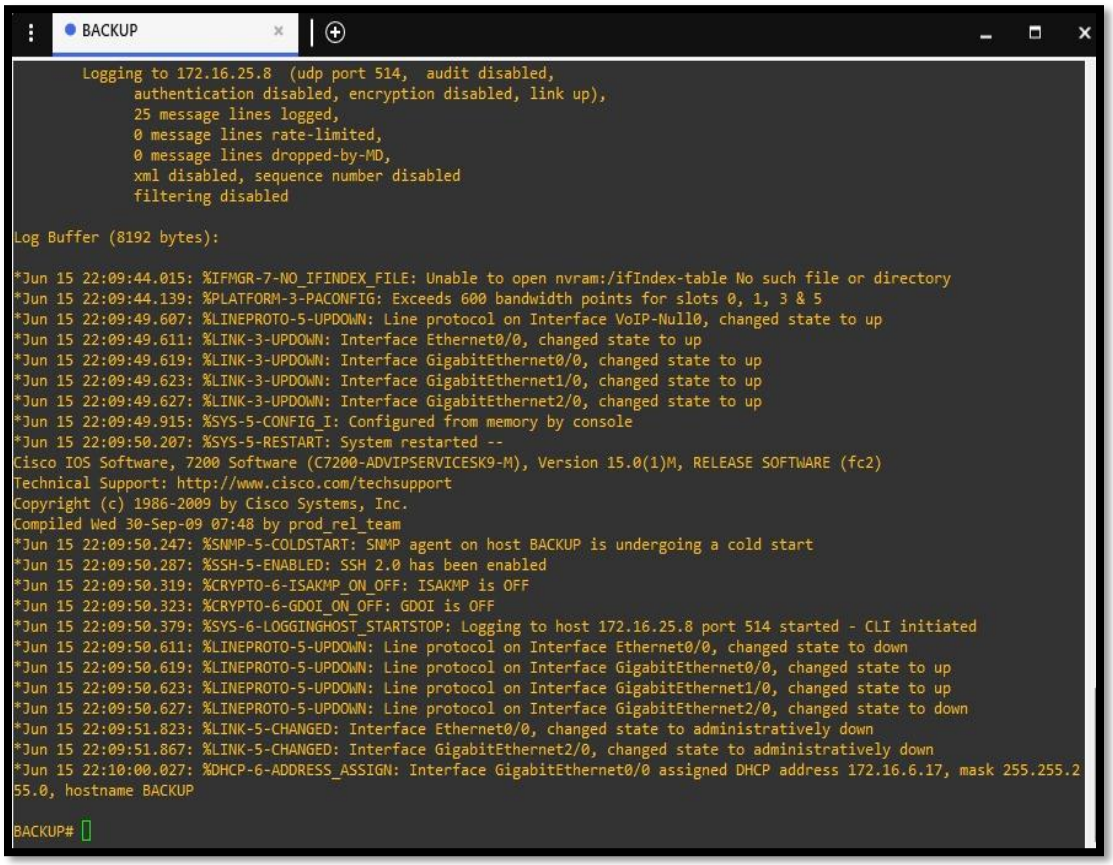
Fuente: [Propia]

Diagnóstico y resolución de problemas de red

Para realizar estas pruebas adicionaremos un equipo cisco dentro de la red, y realizaremos las pruebas sobre el mismo, esto con el fin de no comprometer la disponibilidad de los equipos core, ya que esos equipos se encuentran en producción y un reinicio en ellos afectaría gravemente a nuestros clientes.

En la figura 51, se visualizan los logs del equipo router antes de ser accedido por algún usuario.

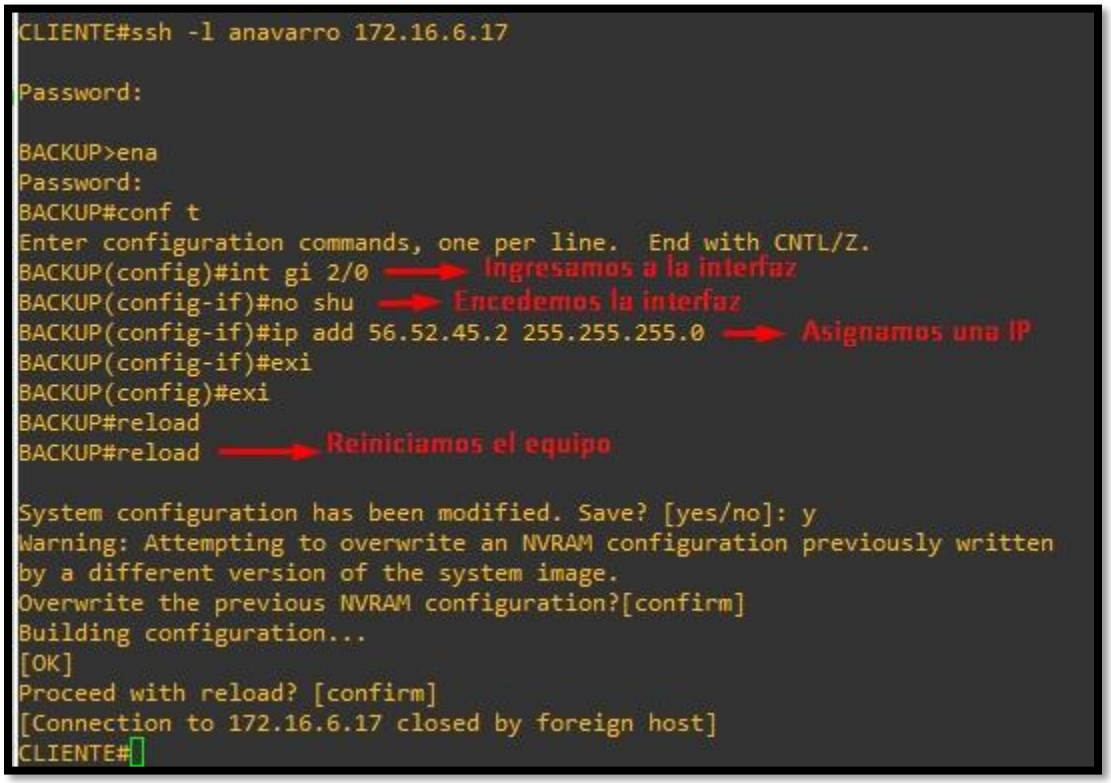
Figura 51. Logs del router cisco.



Fuente: [Propia]

Ingresamos mediante ssh con el usuario “anavarro” desde un cliente hacia el equipo cisco backup para realizar cambios como: encender la interfaz gigaethernet 2/0, configurar una IP y ejecutar un reinicio, con el fin de que se pierda la información almacenada en la memoria interna del equipo, tal como se muestra en la figura 52.

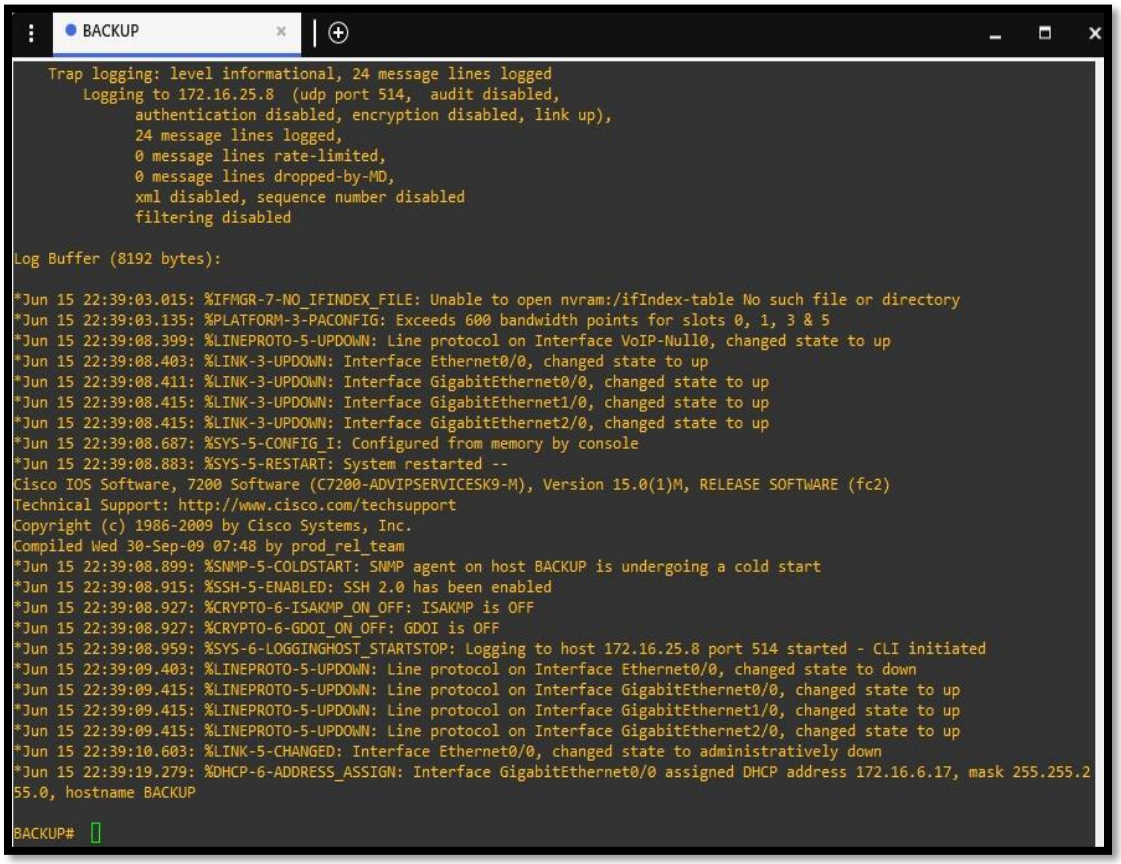
Figura 52. Cambios realizados mediante ssh en el equipo backup



Fuente: [Propia]

Como bien se menciona este es una prueba donde se simula la pérdida de logs dentro de la memoria del equipo cisco, ante esta situación nosotros como administradores de red ingresamos al router para visualizar los logs, pero al haber sido reiniciado se perdió toda la información y no pudimos detectar quien realizó dicha acción, tal como se muestra en la figura 53.

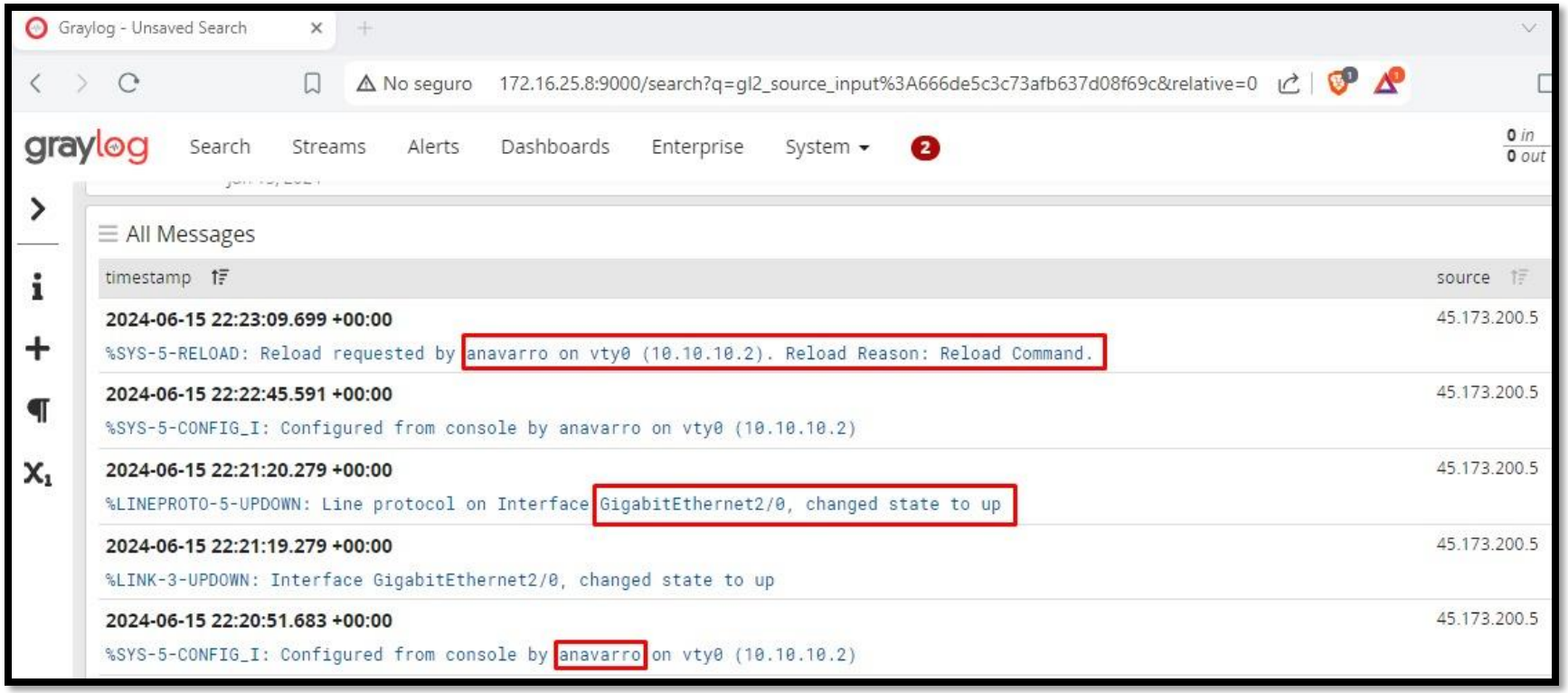
Figura 53. Visualización de logs después del reinicio



Fuente: [Propia]

Debido a que perdimos toda la información de los logs dentro del equipo, nos vimos en la necesidad de ingresar al servidor Graylog para tener más detalle de lo sucedido, y dentro de los registros visualizamos que el usuario "anavarro" realizó el reinicio del equipo, tal como se muestra en la figura 54.

Figura 54. Logs almacenados dentro del servidor Graylog.



Fuente: [Propia]

Al haber implementado nuestro servidor Graylog pudimos tener un respaldo de los logs y logramos detectar al usuario que estuvo involucrado en los cambios realizados dentro del equipo, dato que hubiera sido imposible saber si no tendríamos nuestro servidor de registros syslog.

Como medida de solución se quitaron los permisos de escritura al usuario "anavarro", y a cambio de ello solo se le otorgaron permisos de lectura para prevenir que vuelva a realizar cambios sin autorización.

3.2.6 Optimizar

Esta fase se ejecutará en el futuro, esperando el reporte de los operadores acerca del funcionamiento para realizar las mejoras correspondientes, las cuales incluirán: ajustes en la configuración del servidor, mejorar la escalabilidad del sistema y la capacitación continúa del personal técnico.

CAPÍTULO IV: RESULTADOS Y DISCUSIÓN

4.1 Presentación de resultados

A continuación, se presentan los resultados obtenidos tras la implementación del servidor Graylog, los cuales fueron evaluados conforme a los objetivos planteados:

Objetivo General: Diseñar e implementar un servidor de registros Syslog para mejorar la gestión de eventos de red en la infraestructura tecnológica de Telecable.

- Se logró la implementación del servidor Graylog, el cual centraliza la información del registro de eventos, mejorando así la trazabilidad de la información en la red.

- Se redujo el tiempo de diagnóstico de incidencias de 45 a 15 minutos, optimizando la gestión operativa de la infraestructura tecnológica.

- Se mejoró la seguridad y el cumplimiento normativo mediante una adecuada administración de registros.

Objetivo Específico 1: Documentar y recopilar datos sobre el diseño e implementación de un servidor de registros Syslog.

- Se elaboró una documentación detallada del diseño, implementación y configuración del servidor Syslog, asegurando su operatividad y mantenimiento futuro.

- Se registraron los procedimientos técnicos para la instalación y configuración de Graylog, Docker, MongoDB y Elasticsearch.

Objetivo Específico 2: Seleccionar los criterios clave para la plataforma del servidor Syslog.

- Se realizó una comparativa entre diversas soluciones de servidores syslog, tales como: (Syslog-ng, Rsyslog y Graylog) y seleccionamos a Graylog por su buena escalabilidad, compatibilidad y facilidad de integración.

- Se verificó que mediante el motor de almacenamiento de Elasticsearch los logs se registran de manera rápida y eficiente en el servidor Graylog.

Objetivo Específico 3: Evaluar el entorno de red existente.

- Se identificaron debilidades en la administración descentralizada de logs, lo que dificultaba la detección y resolución de incidencias.

- Se validó la infraestructura actual y su compatibilidad con la solución implementada, asegurando un despliegue sin afectaciones en la operatividad de la red.

Objetivo Específico 4: Elaborar un plan de presupuesto económico para la implementación del servidor Syslog.

- Se estableció un presupuesto basado en software de código abierto, reduciendo costos sin comprometer el rendimiento.

- Se determinó que el mantenimiento anual del sistema requerirá una inversión mínima, garantizando su sostenibilidad a largo plazo.

Objetivo Específico 5: Analizar los datos de registro para diagnosticar y resolver los problemas de red.

- Se logró centralizar y analizar los eventos de red, permitiendo la detección oportuna de fallos y ataques de seguridad.

- Se implementaron alertas en tiempo real que mejoraron la capacidad de respuesta ante incidentes críticos.

Tratamiento y análisis de la encuesta de satisfacción a los trabajadores (tablas y figuras)

A continuación, se presenta los resultados de la encuesta de satisfacción realizada a 12 trabajadores del área del centro de operaciones de red (NOC) de la empresa Telecable sobre la implementación del servidor Graylog, para el tratamiento estadístico de los datos se ha utilizado los programas Google forms y Microsoft Excel, para Windows.

Pregunta 1. ¿Se siente cómodo con la implementación del servidor Graylog?

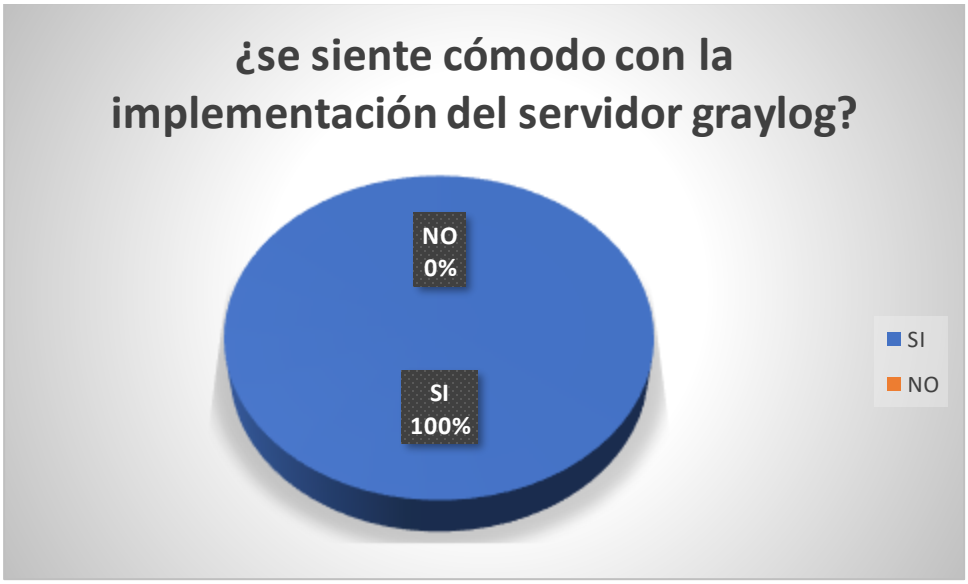
Tabla 4. Pregunta 1 ¿Se siente cómodo con la implementación del servidor Graylog?

	Frecuencia	Porcentaje
Sí	12	100%
No	0	0%
Total	12	100%

Fuente: [Propia]

En la tabla 4, se muestra una frecuencia de 0 trabajadores de la empresa Telecable que no están cómodos con la implementación del servidor.

Figura 55. ¿Se siente cómodo con la implementación del servidor graylog?



Fuente: [Propia]

En la figura 55, podemos observar que el 100% de los trabajadores se encuentran cómodos con la implementación del servidor.

Pregunta 2. ¿El servidor Graylog le parece complejo de usar?

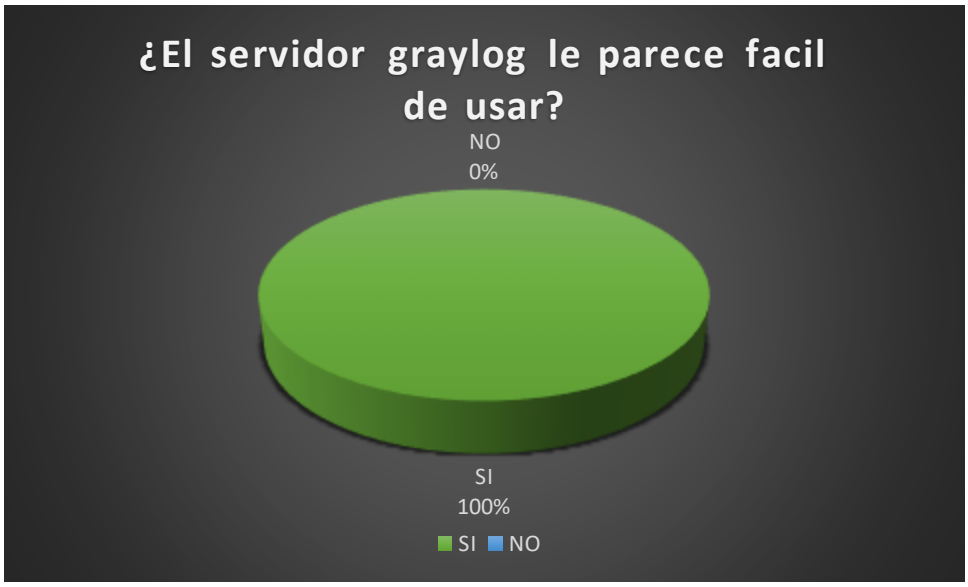
Tabla 5. Pregunta 2 ¿El servidor Graylog le parece complejo de usar?

	Frecuencia	Porcentaje
Sí	12	100%
No	0	0%
Total	12	100%

Fuente: [Propia]

En la tabla 5, se muestra una frecuencia de 0 trabajadores de la empresa Telecable que les parece complejo usar el servidor.

Figura 56. ¿El servidor Graylog le parece complejo de usar?



Fuente: [Propia]

En la figura 56, podemos observar que al 100% de los trabajadores les parece fácil usar el servidor.

Pregunta 3. ¿Cree que el servidor Graylog brinda mejoras al momento de solucionar problemas?

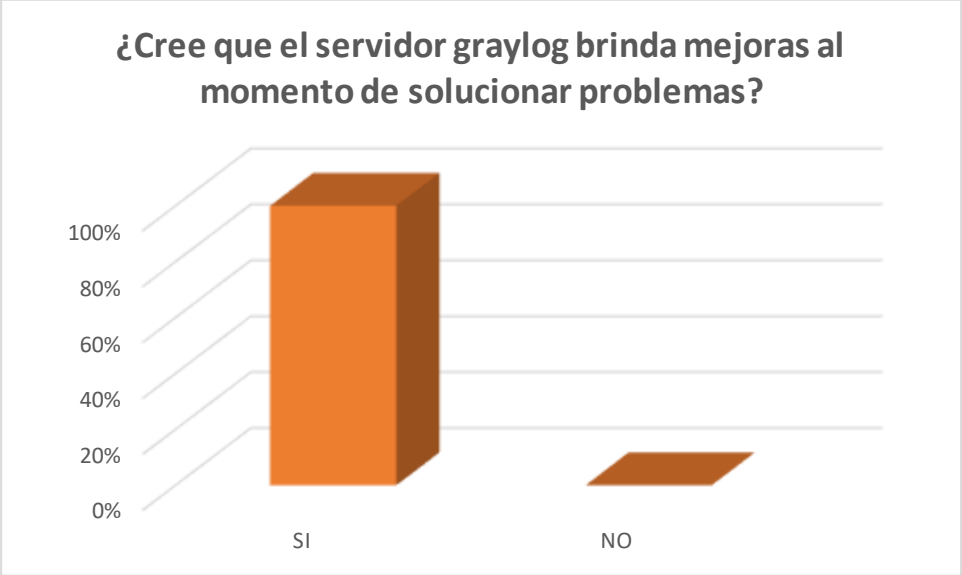
Tabla 6. Pregunta 3 ¿Cree que el servidor Graylog brinda mejoras al momento de solucionar problemas?

	Frecuencia	Porcentaje
Si	12	100%
No	0	0%
Total	12	100%

Fuente: [Propia]

En la tabla 6, se muestra una frecuencia de 0 trabajadores de la empresa Telecable que no creen que el servidor brinda mejoras al momento de solucionar problemas.

Figura 57. ¿Cree que el servidor Graylog brinda mejoras al momento de solucionar problemas?



Fuente: [Propia]

En la figura 57, podemos observar que el 100% de los trabajadores afirma que el servidor brinda mejoras al momento de solucionar problemas.

Pregunta 4. ¿Cómo califica usted la función del servidor Graylog en la empresa?

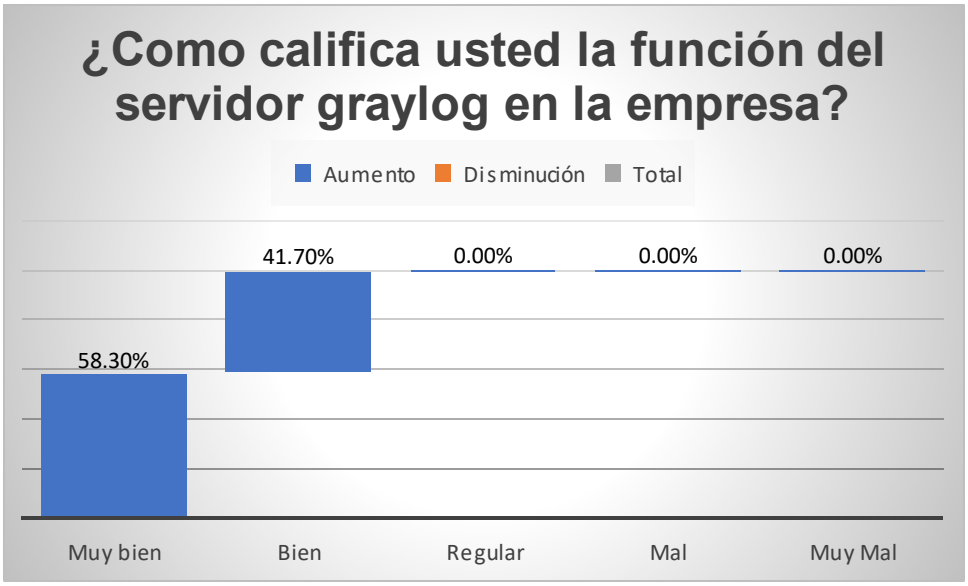
Tabla 7. Pregunta 4 ¿Como califica usted la función del servidor Graylog en la empresa?

	Frecuencia	Porcentaje
Muy bueno	7	58.3%
Bueno	5	41.7%
Regular	0	0%
Mal	0	0%
Muy Mal	0	0%
Total	12	100%

Fuente: [Propia]

En la tabla 7, se visualiza que la mayoría de los trabajadores calificaron como "muy bueno" a la función que desempeña el servidor.

Figura 58. ¿Como califica usted la función del servidor Graylog en la empresa?



Fuente: [Propia]

En la figura 58, podemos observar que el 58.30% de los trabajadores califica "muy bien" a la función que desempeña el servidor.

Pregunta 5. ¿Usted cree que la implementación del servidor Graylog reduce el tiempo de resolución de problemas en la red?

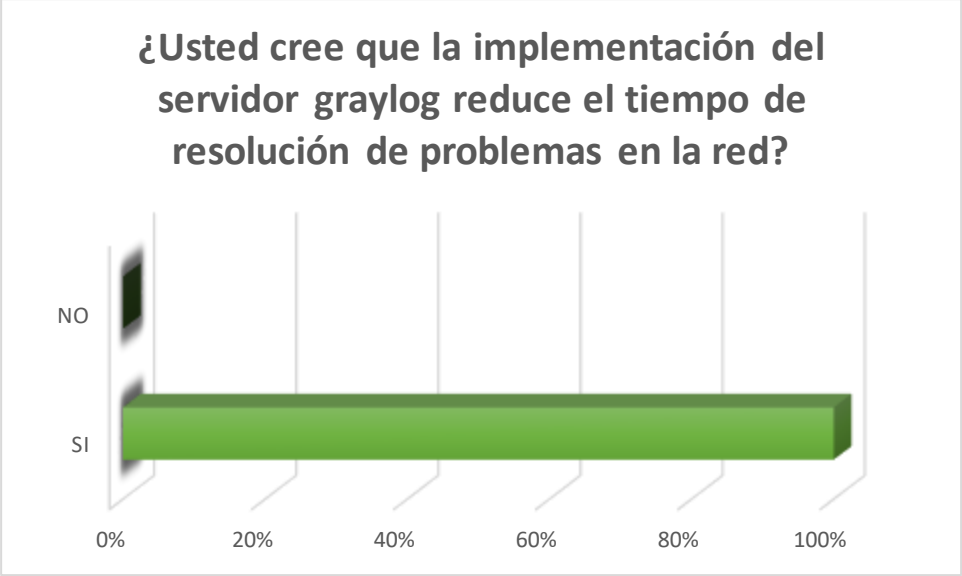
Tabla 8. Pregunta 5 ¿Usted cree que la implementación del servidor Graylog reduce el tiempo de resolución de problemas en la red?

	Frecuencia	Porcentaje
Si	12	100%
No	0	0%
Total	12	100%

Fuente: [Propia]

En la tabla 8, se muestra una frecuencia de 0 trabajadores de la empresa Telecable que no creen que el servidor reduce el tiempo de solución de problemas en la red.

Figura 59. ¿Usted cree que la implementación del servidor Graylog reduce el tiempo de resolución de problemas en la red?



Fuente: [Propia]

En la figura 58, podemos observar que al 100% de los trabajadores afirma que la implementación del servidor reduce el tiempo de resolución de problemas en la red.

Pruebas comparativas antes y después de la implementación

Se realizaron pruebas comparativas antes y después de la implementación de Graylog. Antes, el tiempo promedio de diagnóstico de incidentes era de 45 minutos; después, se redujo a 15 minutos, una mejora del 66%. El número de incidentes sin resolución por falta de datos se redujo en un 80%. Estas métricas destacan la efectividad de la nueva solución en mejorar la eficiencia operativa.

a) Reducción en la Pérdida de Datos Críticos

Antes de Graylog, se perdía un promedio de 5 incidentes críticos por mes debido a la sobreescritura de registros locales. Después de la implementación, la pérdida se redujo a cero, permitiendo un análisis completo y preciso de todos los eventos.

b) Mejora en la Seguridad de la Red

Se detectaron y respondieron intentos de acceso no autorizado 40% más rápido gracias a la correlación de eventos proporcionada por Graylog. La detección de vulnerabilidades críticas, que antes tomaba días, ahora se realiza en cuestión de horas.

c) Satisfacción del Personal Técnico

Una encuesta realizada a los 12 técnicos del NOC mostró que el 100% considera que Graylog ha facilitado sus tareas de monitoreo y gestión de la red, reduciendo el tiempo de resolución de problemas en un 50%.

d) Disminución del Tiempo de Recuperación ante Fallas

Antes de la implementación, el tiempo de recuperación promedio ante incidentes era de 1 hora y 30 minutos. Después, se redujo a 35 minutos, lo que implica una mejora del 61%.

4.2 Discusión de resultados

La investigación de Ramírez (2021) demostró que la consolidación de registros mediante Syslog y SNMP mejora la administración de los eventos en redes empresariales. En nuestra investigación, la implementación de Graylog permitió que la información crítica almacenada dentro de este servidor tenga una mayor trazabilidad y disponibilidad, ayudando así a recudir el tiempo de respuesta ante averías e incidentes.

La investigación de Hernández (2022) demostró que los mecanismos de seguridad, como el acceso por credenciales a servidores de gestión de registros mejora la integridad de datos. En nuestra investigación, la implementación de Graylog con el método de autenticación de usuarios y restricción por niveles fortaleció la protección de los registros logs.

En la investigación de Becerra & Páramo (2021) se implementó las herramientas para los seguimientos de eventos en el cual ayuda a optimizar el tiempo de respuesta ante los diferentes incidentes que se puede encontrar en los registros de eventos. En la investigación realizada, la implementación del Graylog nos ayuda a tener herramientas para poder generar alertas al instante y enviarlas por correo, esto nos ayuda a ver los fallos de manera rápida y segura.

La investigación de Carrión (2023) se basa en los estudios de los logs en Logtash y también en ver lo importante que es el registro de eventos para el mismo. En nuestra investigación, se observa las políticas que tiene nuestro almacenamiento en el Graylog el cual ayuda a gestionar los registros de eventos sin afectar el acceso de los usuarios.

Salazar (2020) nos indica que la implementación del Syslog reduce los costos ya que es gratuita y de código abierto. La elección del Graylog nos permitió minimizar costos de funcionabilidad y escalabilidad del sistema.

Mellouk (2022) resaltó que el análisis de registro con sus herramientas permite reducir tiempos en las incidencias. En nuestra investigación, se disminuyó con el tiempo de solución de problemas de 45 minutos a 15 minutos, lo cual evidencia la efectividad del servidor Syslog.

Velasco y Cagua (2022) se indicó que los monitores de red deben adaptarse a distintas infraestructuras. Es por ello que, en nuestra investigación, el servidor Graylog se integró con equipos de diferentes marcas como: Cisco, Huawei y Mikrotik, ya que nos permite unificar los eventos sin necesidad de configuraciones complejas.

Nebrera (2021) determinó que el servidore Syslog nos facilita el complimiento de las normativas de seguridad. Es por eso que, en nuestra investigación, la generación de reportes de los eventos se fortaleció con la capacidad de cumplir los estándares de seguridad en los registros de eventos.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

1. Se diseñó e implementó un servidor de registros syslog para mejorar la gestión de eventos de red en la infraestructura tecnológica de Telecable.

    - Se logró centralizar y almacenar los registros de eventos en un solo repositorio, mejorando la trazabilidad y disponibilidad de datos.
    - Se determinó que los incidentes que no eran resueltos por falta de datos menoraron de 5 a 1, por lo que se concluye que la reducción de perdidas en logs críticos es del 80%.

2. Se documentó y recopiló información sobre el diseño e implementación del servidor de registros syslog, obteniendo los datos necesarios y las ventajas que nos ofrece este protocolo.

    - Se generó un registro estructurado del proceso de instalación, configuración y pruebas del servidor.
    - Esta documentación permitirá futuras expansiones y mejoras en la infraestructura de Telecable.

3. Se seleccionaron los criterios clave para la plataforma del servidor Graylog.

    - Se realizó un análisis comparativo entre diversas soluciones y se determinó que Graylog era la opción más adecuada.
    - Factores clave: escalabilidad, compatibilidad con protocolos y facilidad de uso.
    - Su implementación sin costos de licencia permitió reducir el presupuesto requerido.

4. Se evaluó el entorno de red existente, dando a conocer cómo trabaja actualmente la red y con ello se pudo realizar el análisis de mejora.

    - Se identificaron problemas en la gestión de logs y seguridad de la información, como:

Registros dispersos: Los logs estaban almacenados en diferentes dispositivos, lo que dificultaba su consulta y análisis.
Sobrecarga en dispositivos: Los equipos de red procesaban grandes volúmenes de logs, afectando su rendimiento.
Falta de alertas automatizadas: No se contaba con un sistema de notificación en tiempo real, lo que retrasaba la detección de incidentes.

- La implementación del servidor Graylog permitió centralizar la gestión de logs, reduciendo la carga en los dispositivos y mejorando la capacidad de monitoreo.

5. Se elaboró un plan de presupuesto económico para la implementación del servidor Graylog.

- Gracias al uso de software open-source y la infraestructura existente de Telecable, se logró la implementación sin gastos elevados.
- Nuestra implementación requiere solo 150 soles anuales para el mantenimiento del servidor, lo que representa un ahorro del 90% en comparación con soluciones comerciales que pueden costar hasta 1500 soles en licencias y suscripciones. Sin Graylog, Telecable tendría que optar por un servicio costoso, pero gracias a esta solución open source, se logra una alternativa eficiente y sostenible con un ahorro significativo.

6. Se analizaron los datos de registro para diagnosticar y resolver los problemas de red disminuyendo el tiempo de solución de problemas.

- Se redujo el tiempo promedio de diagnóstico de fallos de 45 a 15 minutos.
- Se eliminaron incidentes relacionados con la sobreescritura de registros y se mejoró la trazabilidad de accesos y cambios en la configuración de dispositivos.
- La integración de alertas en tiempo real permitió detectar y mitigar amenazas de manera más rápida.

5.2 Recomendaciones

1. Brindar mantenimiento preventivo y correctivo al servidor para un correcto funcionamiento a nivel físico y lógico.

2. Optimizar los recursos para el funcionamiento eficiente del servidor.

3. Asegurar el paso de la información y mantenerla controlada en todo momento, para evitar posibles fallas.

4. Brindar capacitación constante sobre el uso del servidor a los operarios del área correspondiente.

5. Crear una solución de redundancia ante cualquier evento en el servidor principal.

6. Migrar el servidor Graylog a la nube.

REFERENCIAS BIBLIOGRÁFICAS

Ramírez, D. (2019). *Alternativas de configuración con el uso de los protocolos SYSLOG y SNMP para la gestión de red de redes avanzadas* (Tesis de grado, Universidad Nacional Agraria de la Selva, Facultad de Ingeniería de Sistemas, Tingo María).

Hernández, M. (2024). *Evaluación de los Mecanismo de Seguridad en los Sistemas de Notificación y Registro de Eventos* (Tesis de grado, Universidad Central de Venezuela, Facultad de Ingeniería de Sistemas, Caracas).

Becerra, G. y Paramo, C. (2021). *Implementación de un sistema de correlación de eventos basado en software libre para la empresa sistemas integrales de informática SISA S.A enfocado al área del SOC SISAMAX* (Tesis de grado, Universidad Piloto de Colombia, Facultad de Ingeniería de Sistemas, Bogotá).

Carrión, B. (2022). *Diseño e Implementación de una solución de gestion centralizada de logs de aplicaciones, sistemas y dispositivos basada en Logstash que permita la creación de cuadros de mando para explorar, analizar y monitorear eventos de seguridad* (Tesis de maestría, Universidad Oberta de Catalunya, Facultad de Ingeniería de Sistemas, Catalunya).

Velasco, C. y Cagua, G. (2022). *Implementación de un sistema de monitoreo de redes utilizando herramientas open source y proveer servicios de directorio a través de active directory en la facultad de filosofía, letras y ciencias de la educación de la Universidad de Guayaquil* (Tesis de grado, Universidad de Guayaquil, Facultad de Ingeniería de Sistemas, Guayaquil).

Mellouk, M. (2021). *Diseño e implementación de un sistema para la recogida de logs en sistemas distribuidos* (Tesis de maestría, Universidad Autónoma de Madrid, Facultad de Ingeniería Informática y Matemáticas, Madrid).

Salazar, E. (2023). *Sistemas de información para el repositorio de logs, control de versiones de las aplicaciones internas y actualizacion de aranda en la empresa une – telefónica de pereira* (Tesis de grado, Universidad Católica de Pereira, Facultad de Ingeniería de Sistemas y Telecomunicaciones, Pereira).

Nebrera, P. (2019). *Desarrollo de un Sistema de Gestión Syslog en cloud* (Tesis de grado, Universidad de Sevilla, Facultad de Ingeniería de las Tecnologías de Telecomunicación, Sevilla).

Progess, S. (2022). *¿Qué es un servidor Syslog y cómo funciona?* Disponible en: https://www.whatsupgold.com/es/blog/que-es-un-servidor-syslog-y-como-funciona#:~:text=El%20Protocolo%20de%20registro%20del,con%20un%20servidor%20de%20registro. [Consulta: 3 de marzo de 2025].

Morales, R. (2020). *ticARTE. Syslog, Registro de Eventos.* Disponible en: https://www.ticarte.com/contenido/syslog-registro-de-eventos. [Consulta: 3 de marzo de 2025].

Paessler. (2024). *snmp.* Disponible en: https://www.paessler.com/es/it-explained/snmp. [Consulta: 3 de marzo de 2025].

Paessler, A. [s.f.]. *¿Qué es syslog?* Disponible en: https://www.paessler.com/es/it-explained/syslog. [Consulta: 3 de marzo de 2025].

Martínes, R. (2024). *El armario de comunicaciones de una red local.* Disponible en: https://www.adrformacion.com/knowledge/administracion-de-sistemas/el_armario_de_comunicaciones_de_una_red_local.html. [Consulta: 3 de marzo de 2025].

Conzultek. (2022). *Dispositivos de Red: Características.* Disponible en: https://blog.conzultek.com/dispositivos-de-red-caracteristicas. [Consulta: 3 de marzo de 2025].

Genos. (2024). *Proxmox VE.* Disponible en: https://genos.es/proxmox-ve/. [Consulta: 3 de marzo de 2025].

Microsoft. [s.f.]. *MS Visio.* Disponible en: https://support.microsoft.com/es-es/office/v%C3%ADdeo-qu%C3%A9-es-visio-421b0c94-7ecf-4e62-8072-d27e04d24fe6. [Consulta: 3 de marzo de 2025].

Ganttpro. (2023). *¿Qué es GanttPRO?* Disponible en: https://help.ganttpro.com/hc/es/articles/360019585457--Qu%C3%A9-es-GanttPRO. [Consulta: 3 de marzo de 2025].

Salcedo, D. y Cubillas, A. (2015). *Metodología Cisco.* Disponible en: https://prezi.com/obuiwmoo_vbv/metodologia-cisco/. [Consulta: 3 de marzo de 2025].

Accelerates. (2018). *Presentamos Cisco PPDIOO para Diseño de Red.* Disponible en: https://accelerates.it/blog/networking/cisco-ppdioo/. [Consulta: 3 de marzo de 2025].

Diccionario de la Lengua Española. (2024). *Planificar.* Disponible en: https://dle.rae.es/planificar. [Consulta: 3 de marzo de 2025].

Concepto. (2024). *¿Qué es el diseño?* Disponible en: https://concepto.de/diseno/. [Consulta: 3 de marzo de 2025].

Diccionario de la Lengua Española. (2001). *Implementar.* Disponible en: https://www.rae.es/drae2001/implementar. [Consulta: 3 de marzo de 2025].

Mestro de Proyectos. (2023). *¿Qué es un proyecto?* | Diferencia entre Proyecto y Operación. Disponible en: https://www.maestrodeproyectos.com/2022/09/diferencias-entre-proyecto-y-operacion.html. [Consulta: 3 de marzo de 2025].

Word Reference. (2005). *Optimizar.* Disponible en: https://www.wordreference.com/definicion/optimizar. [Consulta: 3 de marzo de 2025].

Porto. (2021). *Almacenamiento.* Disponible en: https://definicion.de/almacenamiento/. [Consulta: 3 de marzo de 2025].

Google. [s.f.]. *Qué es el encriptado.* Disponible en: https://cloud.google.com/learn/what-is-encryption?hl=es. [Consulta: 3 de marzo de 2025].

Cloudfare. (2022). *¿Qué es un enrutador?* Disponible en: https://www.cloudflare.com/es-es/learning/network-layer/what-is-a-router/. [Consulta: 3 de marzo de 2025].

Larousse, E. (2016). *Facilidad.* Disponible en: https://www.diccionarios.com/diccionario/espanol/facilidad. [Consulta: 3 de marzo de 2025].

Porto. (2022). *Instalación.* Disponible en: https://definicion.de/instalacion/. [Consulta: 3 de marzo de 2025].

Keepcoding. (2023). *Qué son los logs y para qué sirven.* Disponible en: https://keepcoding.io/blog/que-son-logs-y-para-que-sirven/. [Consulta: 3 de marzo de 2025].

IBM. (2021). *Matrices de discos.* Disponible en: https://www.ibm.com/docs/es/power7?topic=srcao-disk-arrays. [Consulta: 3 de marzo de 2025].

Ramírez, I. (2020). *Máquinas virtuales: qué son, cómo funcionan y cómo utilizarlas.* Disponible en: https://www.xataka.com/especiales/maquinas-virtuales-que-son-como-funcionan-y-como-utilizarlas. [Consulta: 3 de marzo de 2025].

Editorial, E. (2020). *Mensaje.* Disponible en: https://concepto.de/mensaje/. [Consulta: 3 de marzo de 2025].

IBM. (2024). *Niveles de gravedad de sucesos.* Disponible en: https://www.ibm.com/docs/es/netcoolomnibus/8.1?topic=list-event-severity-levels. [Consulta: 3 de marzo de 2025].

Fs.com. (2021). *¿Qué es un patch panel y por qué lo necesitamos?* Disponible en: https://community.fs.com/es/article/what-is-a-patch-panel-and-why-use-it.html. [Consulta: 3 de marzo de 2025].

Invgate. (2024). *Que es Syslog.* Disponible en: https://blog.invgate.com/es/que-es-syslog. [Consulta: 3 de marzo de 2025].

Cisco. (2024). *Ventajas de las redes.* Disponible en: https://www.cisco.com/c/es_mx/solutions/small-business/networking.html?ccid=cc001535. [Consulta: 3 de marzo de 2025].

IBM. (2014). *Configuración de error del sistema o registro de eventos (syslog).* Disponible en: https://www.ibm.com/docs/es/db2/11.1?topic=logs-configuring-system-error-event-log-syslog. [Consulta: 3 de marzo de 2025].

Digital360. (2023). *Qué es un SAI y cuál es su función en un data center.* Disponible en: https://www.datacentermarket.es/tendencias-ti/los-sai-en-el-data-center-guia-practica/. [Consulta: 3 de marzo de 2025].

Cisco. (2024). *¿Por qué la seguridad de Cisco?* Disponible en: https://www.cisco.com/c/es_mx/solutions/small-business/security.html. [Consulta: 3 de marzo de 2025].

Paessler. [s.f.]. *Qué es un servidor.* Disponible en: https://www.paessler.com/es/it-explained/server. [Consulta: 3 de marzo de 2025].

Cisco. (2024). *Cómo funciona un switch.* Disponible en: https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/network-switch-how.html. [Consulta: 3 de marzo de 2025].

Universidad Nacional del Litoral. (2020). *Qué es la tecnología.* Disponible en: http://www.unl.edu.ar/ingreso/cursos/cac/21ot/. [Consulta: 3 de marzo de 2025].

IBM. (2021). *Unidades de cintas.* Disponible en: https://www.ibm.com/docs/es/power7?topic=drives-tape. [Consulta: 3 de marzo de 2025].

Google. [s.f.]. *Qué es WAN.* Disponible en: https://support.google.com/googlenest/answer/6274166?hl=es-419. [Consulta: 3 de marzo de 2025].

AWS. (2023). *Qué es Docker*. Disponible en: https://aws.amazon.com/es/docker/. [Consulta: 3 de marzo de 2025].

Cisco. (2016). *PPDIOO Lifecycle Approach to Network Design and Implementation*. Disponible en: https://www.ciscopress.com/articles/article.asp?p=1608131&seqNum=3. [Consulta: 3 de marzo de 2025].

Oppenheimer, P. (2011). *Top-Down Network Design*. Disponible en: https://faculty.kfupm.edu.sa/COE/marwan/richfiles/Cisco.Press.Top-Down.Network.Design.3rd.Edition.Aug.2010.pdf. [Consulta: 3 de marzo de 2025].

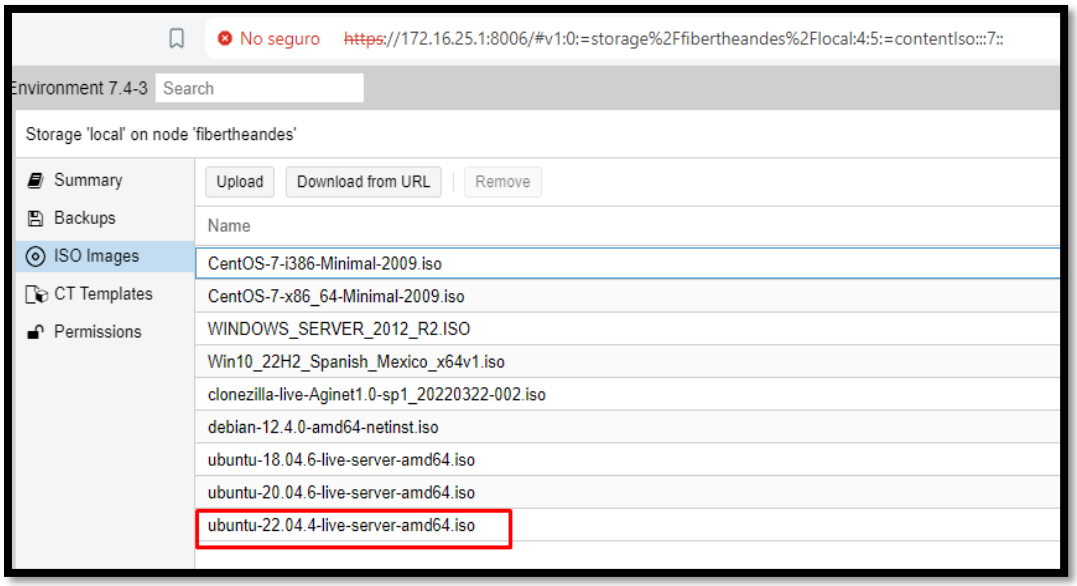
Tanenbaum, A. y Wetherall, D. (2021). *Computer Networks*. Disponible en: https://csc-knu.github.io/sys-prog/books/Andrew%20S.%20Tanenbaum%20-%20Computer%20Networks.pdf. [Consulta: 3 de marzo de 2025].

ANEXOS

ANEXO A: INSTALACIÓN DEL SISTEMA OPERATIVO UBUNTU EN PROXMOX

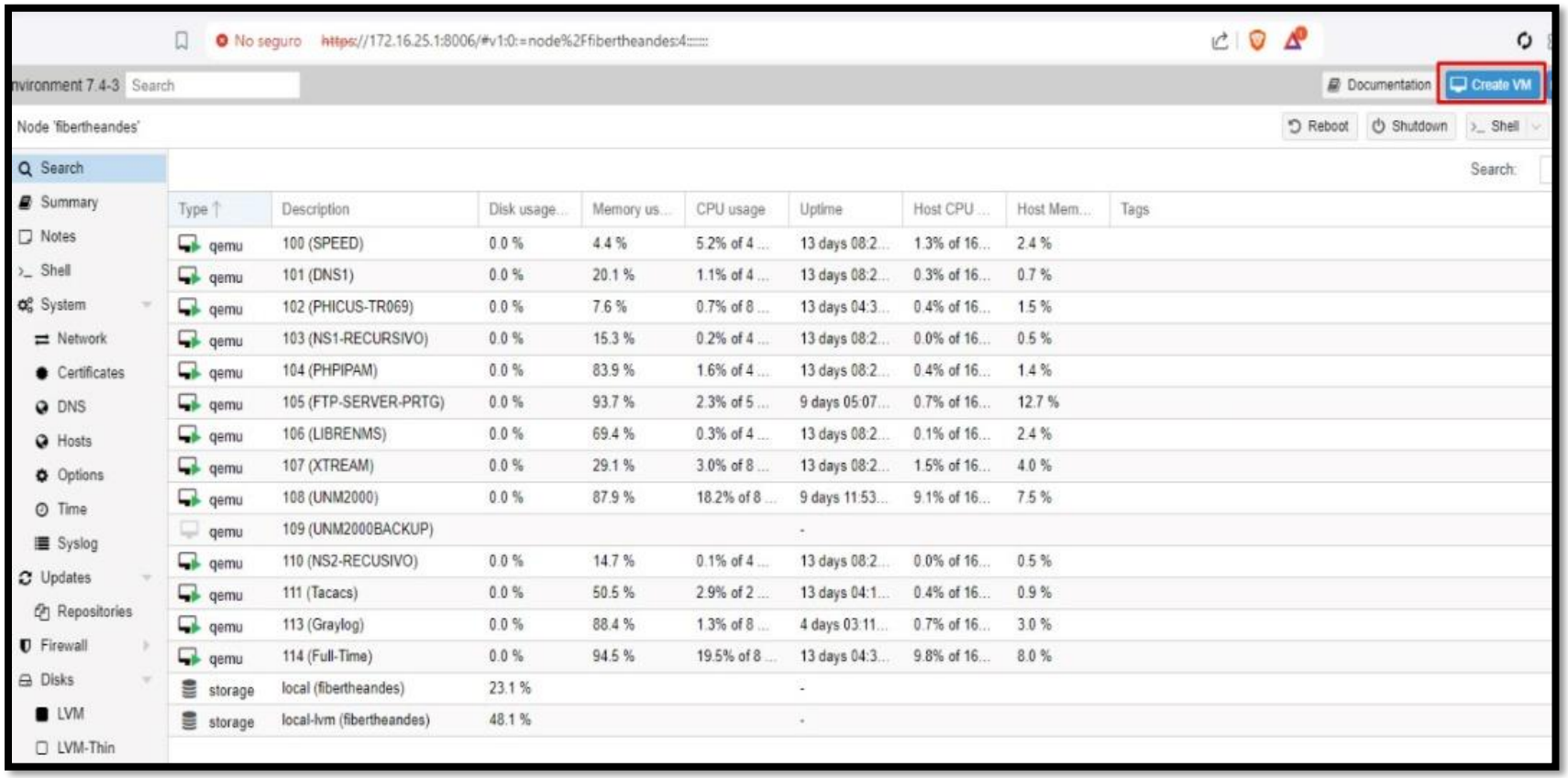
Paso 1

El sistema operativo está alojado en la plataforma proxmox dentro de la nube de Telecable, para ello se necesita el archivo ISO de Ubuntu 22.04.4 y tenerlo cargado en proxmox, tal como se muestra en la figura.



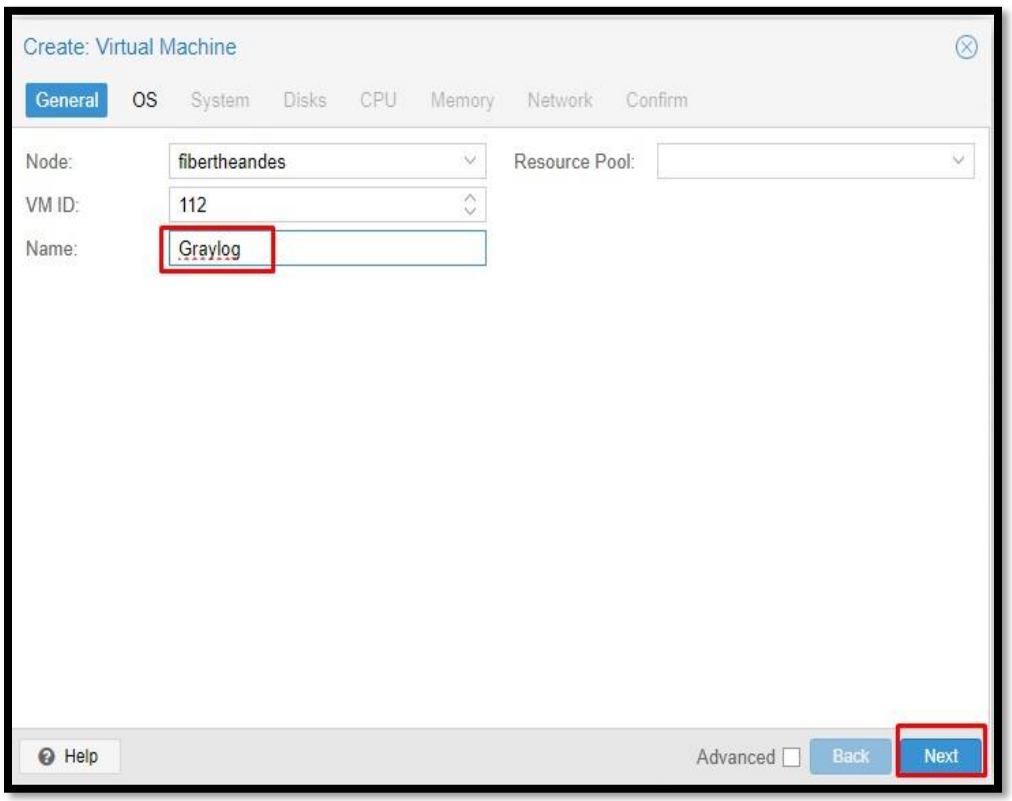
Paso 2

Presionamos el botón que dice “Create VM” para crear una nueva máquina virtual, tal como se muestra en la figura.



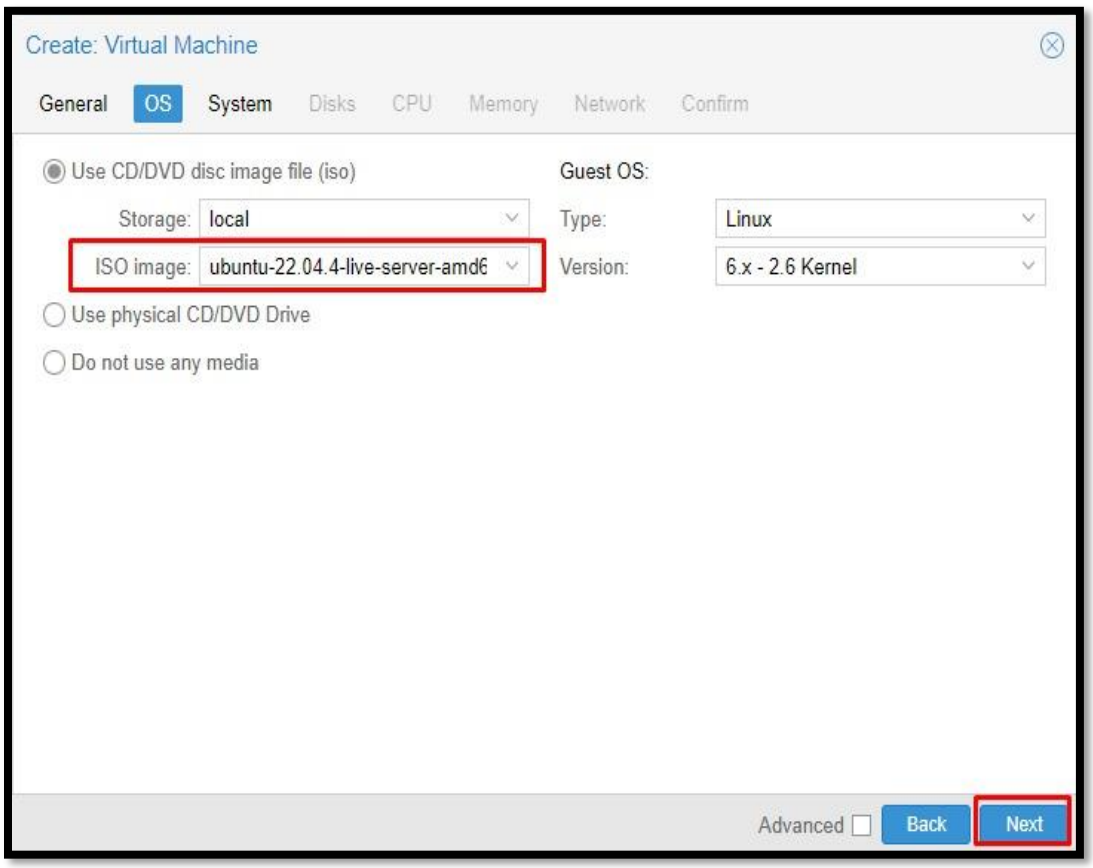
Paso 3

Asignamos un nombre para identificar la máquina virtual, tal como se muestra en la figura.



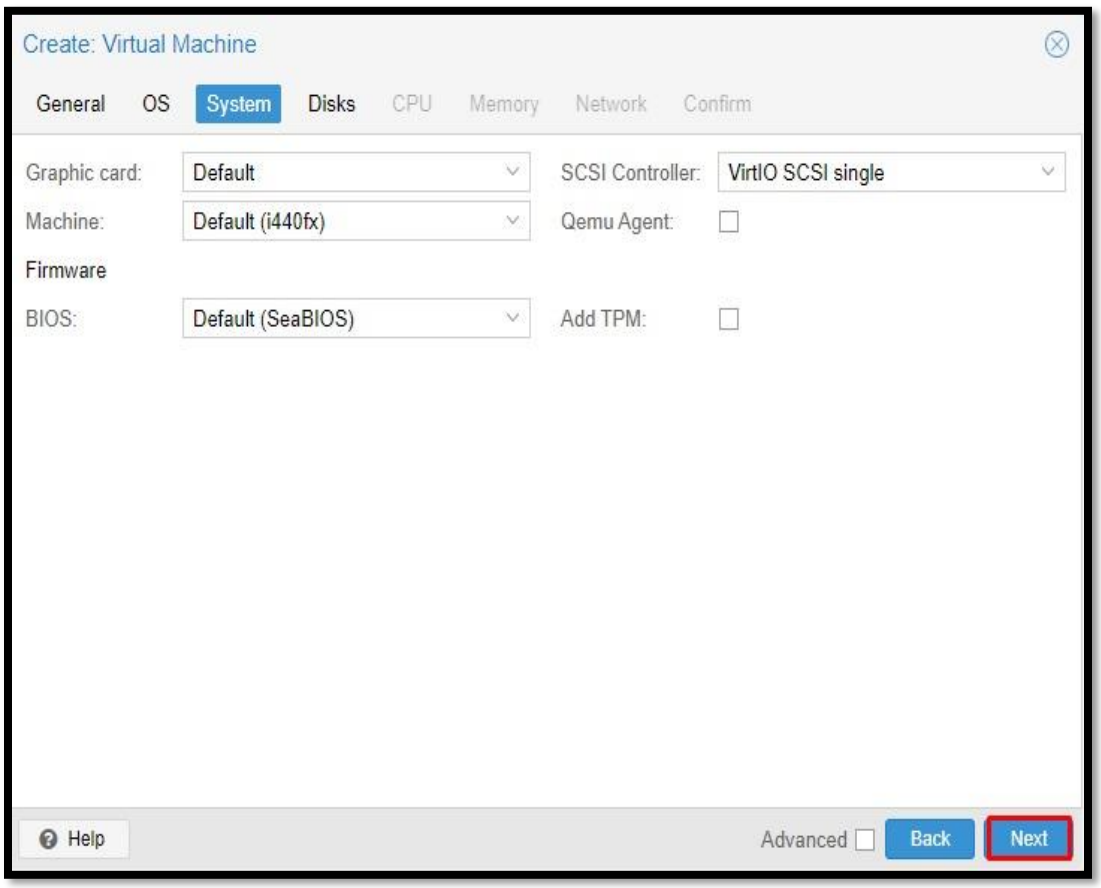
Paso 4

Seleccionamos la ISO del sistema operativo a instalar, tal como se muestra en la figura.



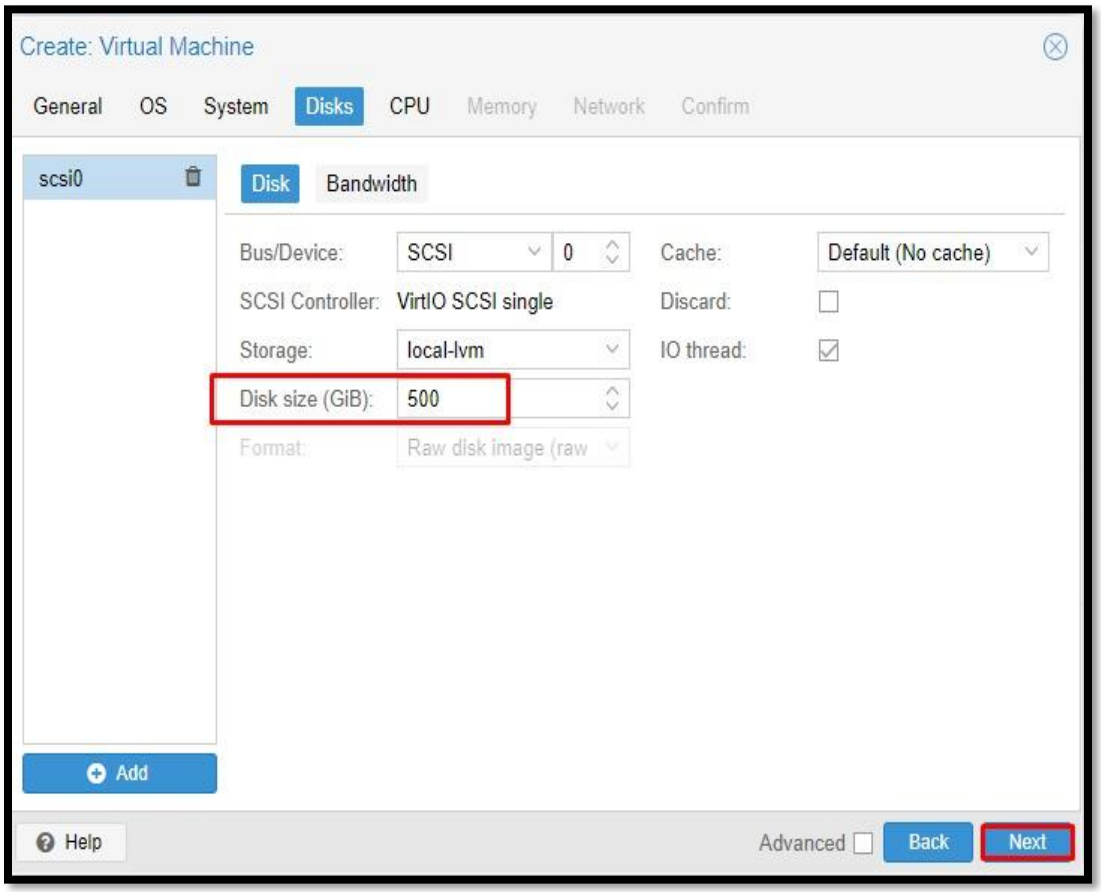
Paso 5

En la ventana Systema dejamos todo por defecto, tal como se muestra en la figura .



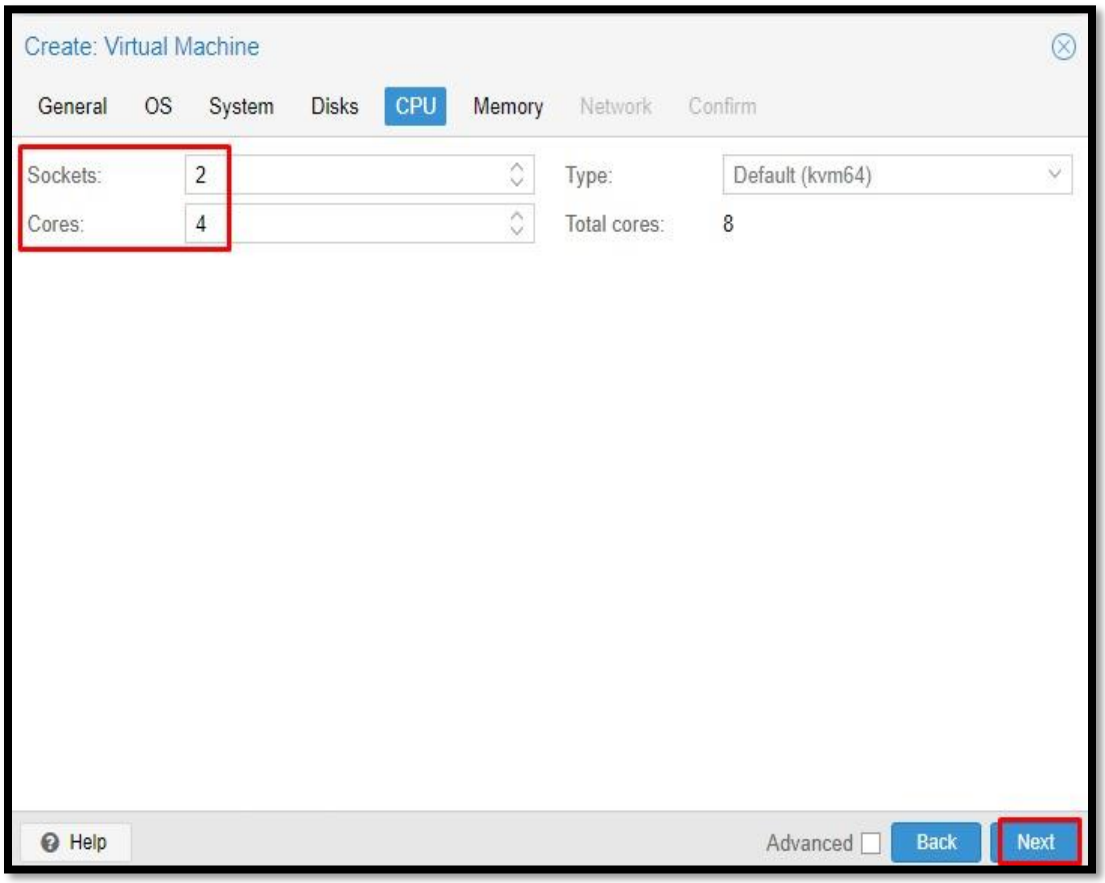
Paso 6

En la figura, se muestra la asignación de capacidad de almacenamiento, este debe tener como mínimo 500GB de espacio, ya que el servidor syslog ocupara muchos datos para los registros.



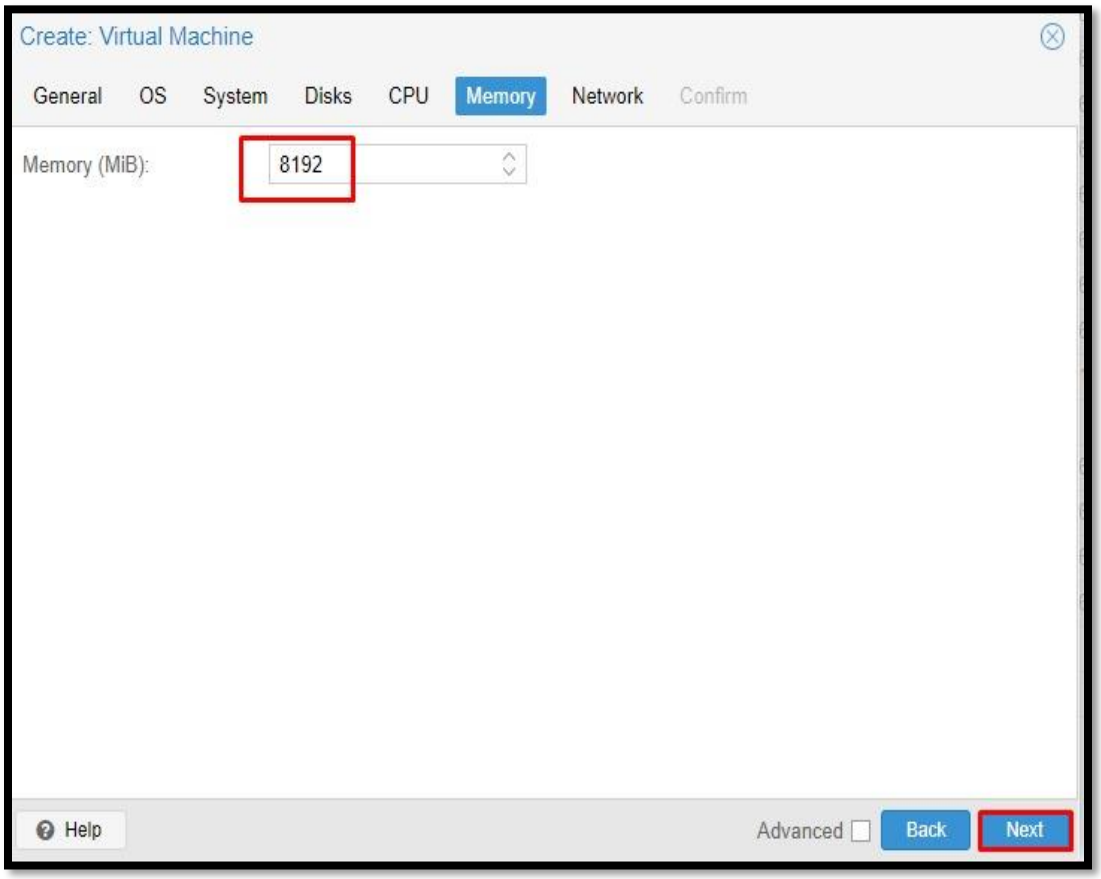
Paso 7

En la figura, se muestra la asignación total de socket y cores para el procesador.



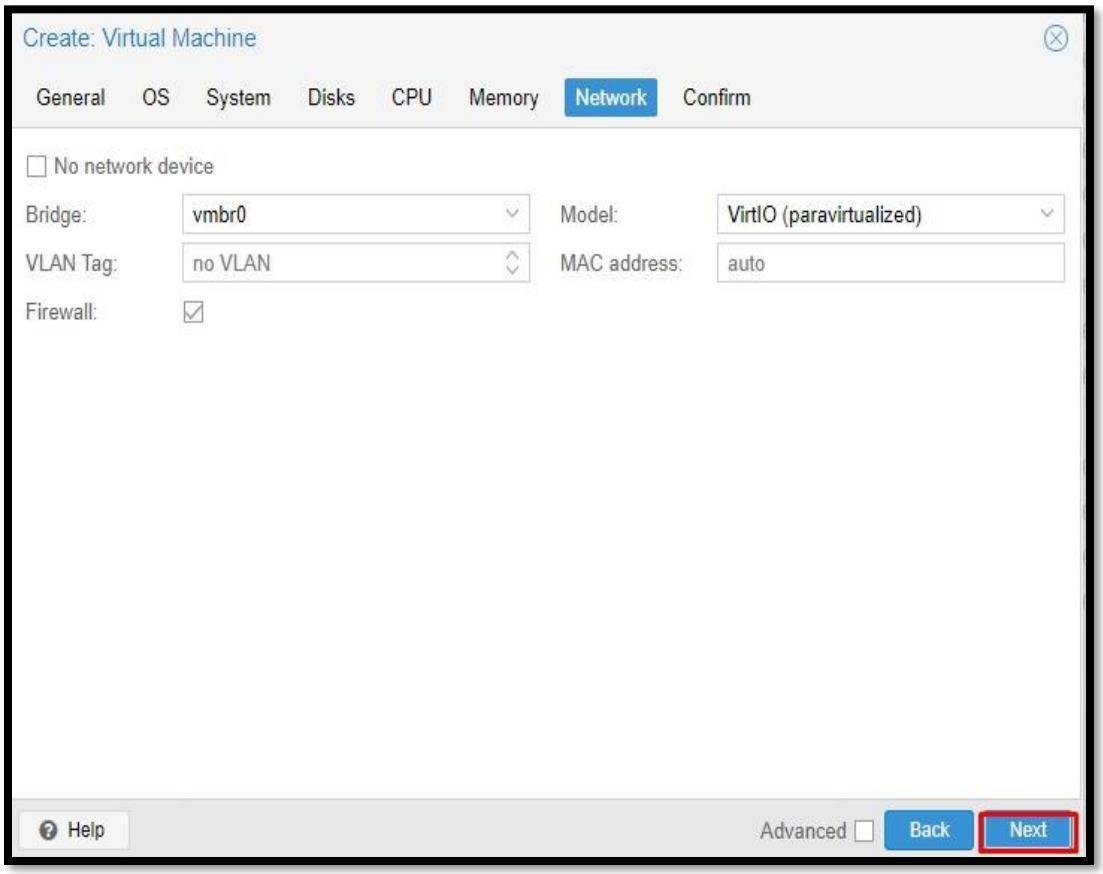
Paso 8

En la figura, se muestra la asignación de memoria ram, en total 8GB.



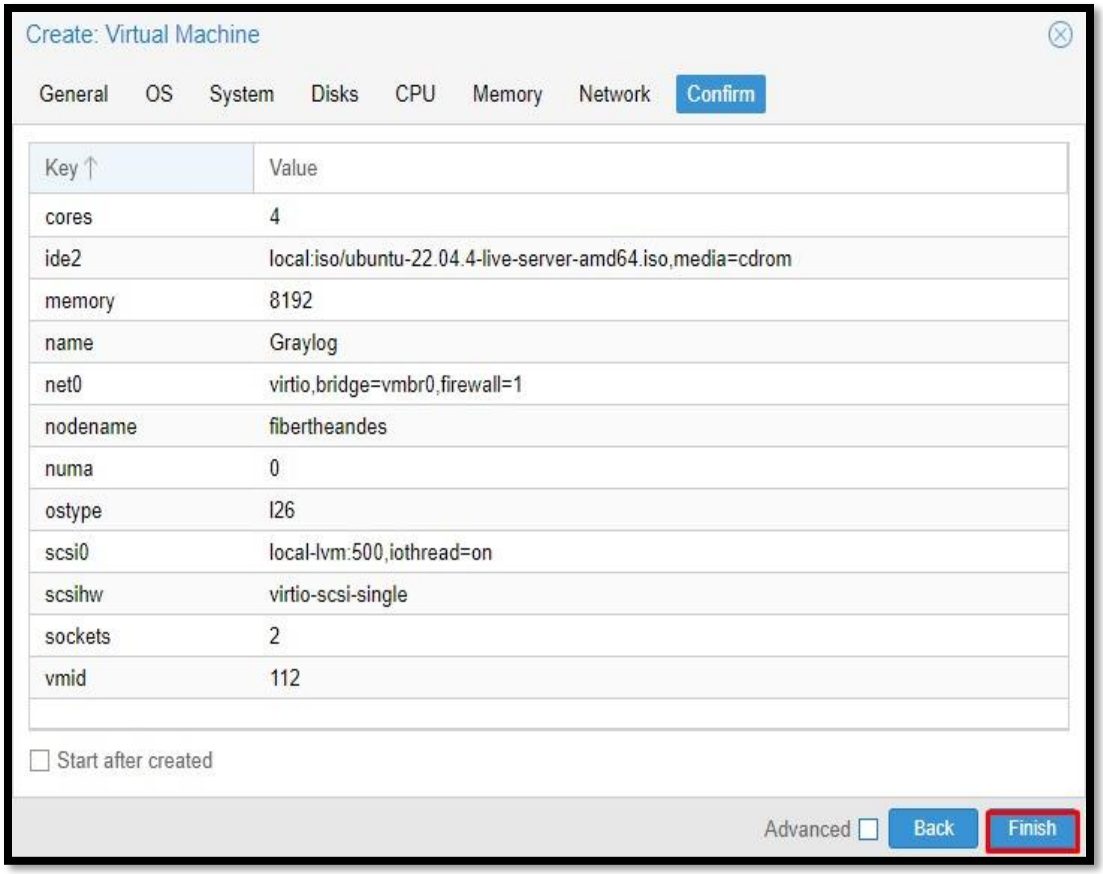
Paso 9

En el apartado de Network, se dejan las opciones por defecto, tal como se muestra en la figura.



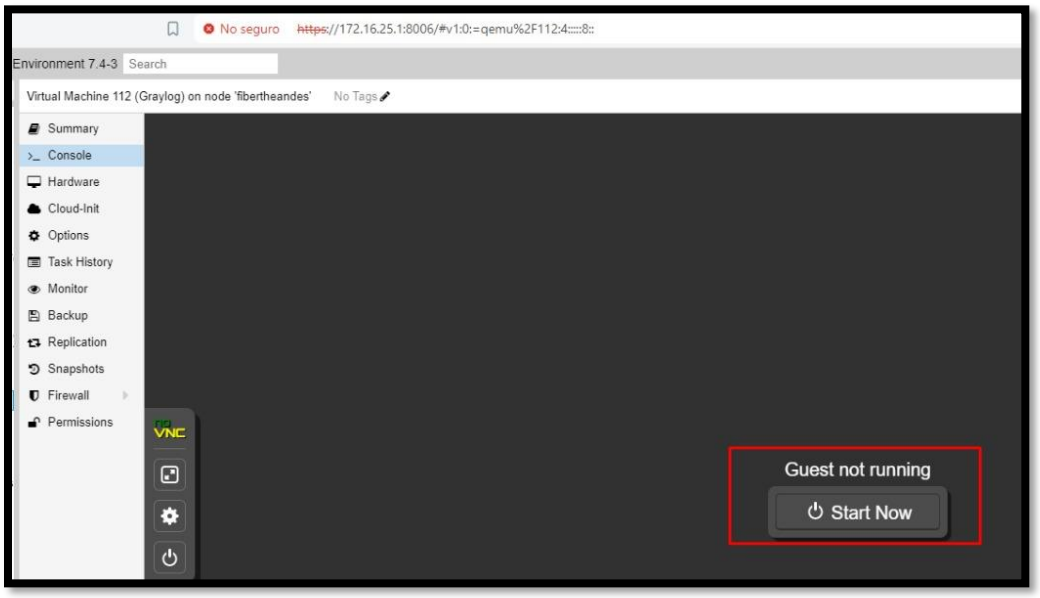
Paso 10

En la figura, se muestra un resumen de las características aplicadas previo a la instalación del sistema operativo.



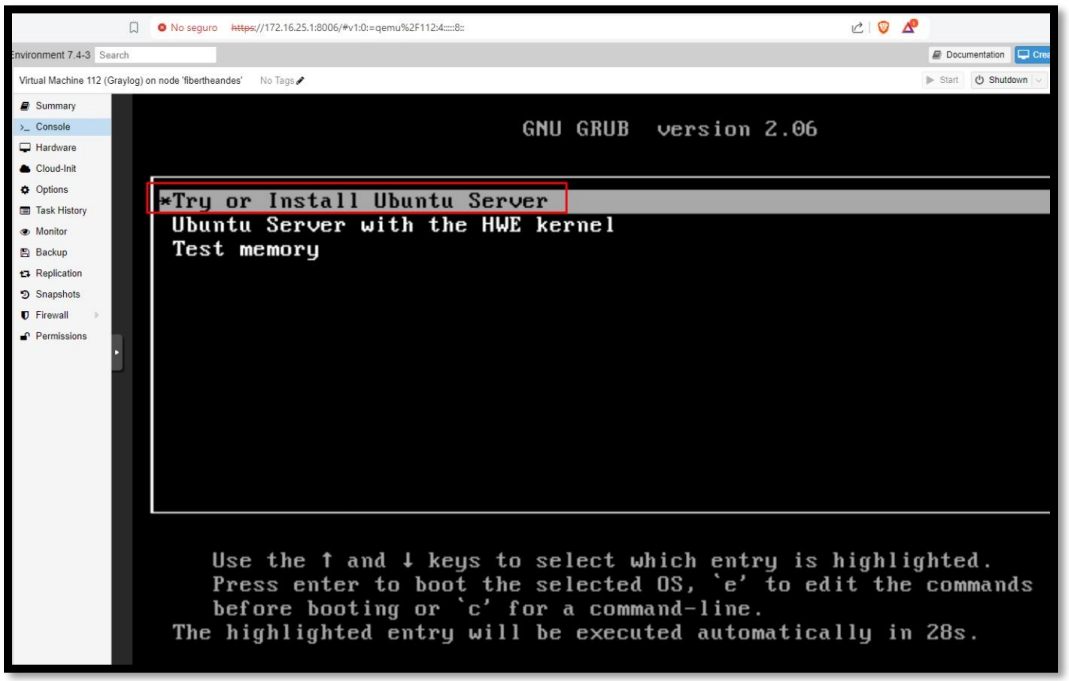
Paso 11

En la figura, se muestra el botón de inicio para empezar con la instalación del sistema operativo.



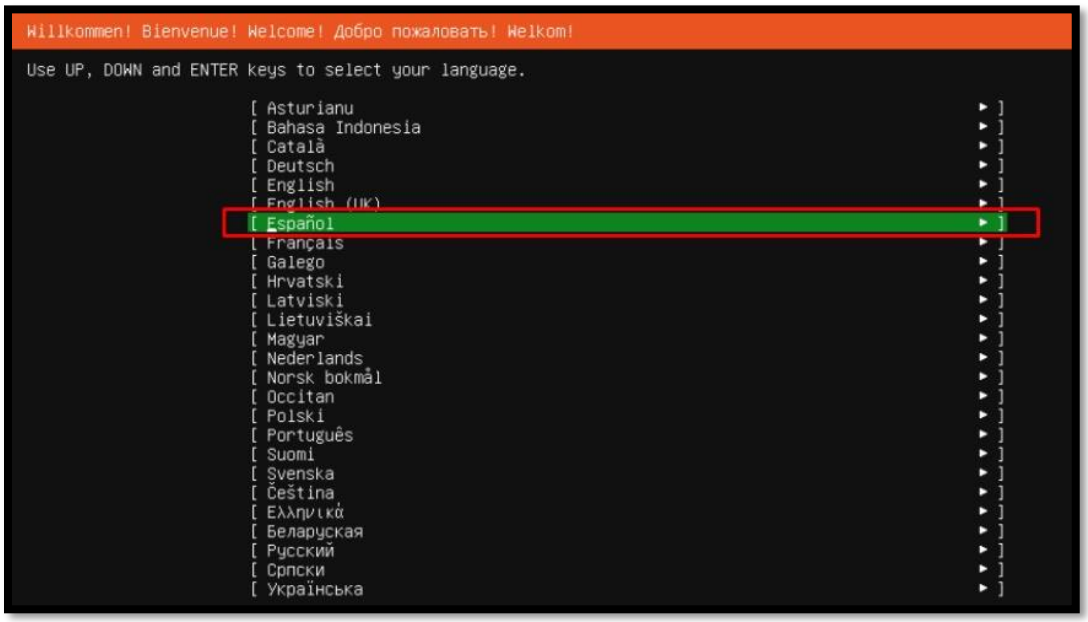
Paso 12

En la figura, se muestra la opción para instalar el sistema operativo Ubuntu server.



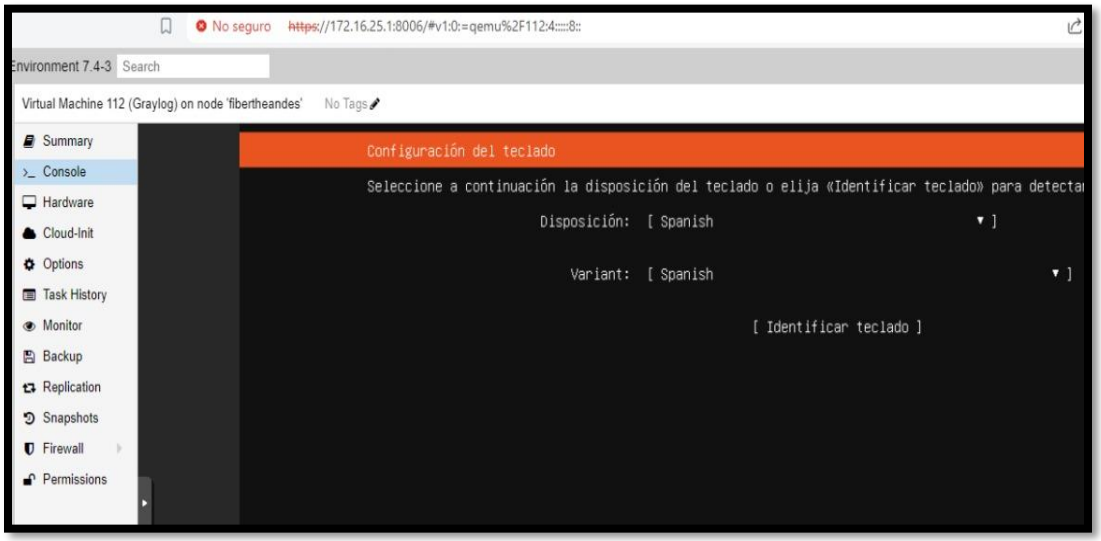
Paso 13

En la figura, se muestra el menú para la selección de idioma.



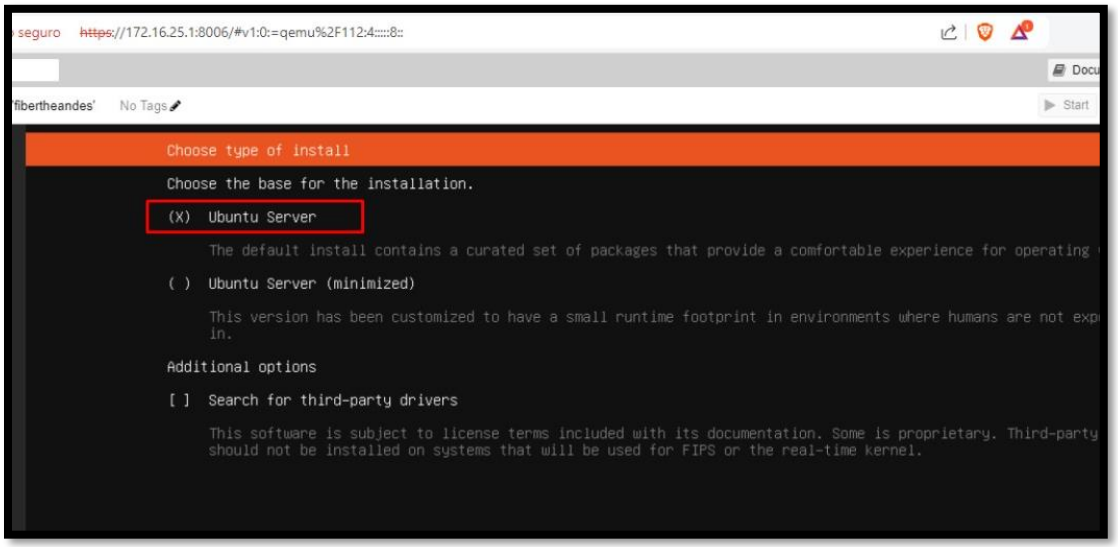
Paso 14

En la figura, se muestra el menú para la identificación del teclado.



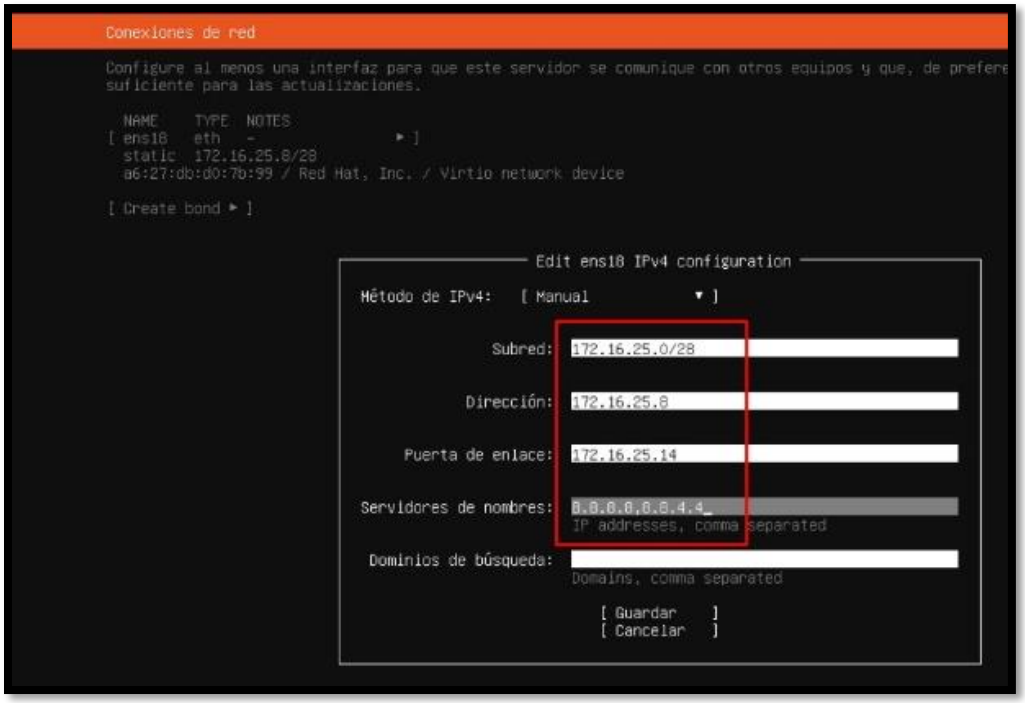
Paso 15

En la figura, seleccionamos el tipo de instalación del servidor.



Paso 16

Se procede a asignar el nombre la dirección ip, mascara de subred, Gateway y dns, tal como se muestra en la figura.

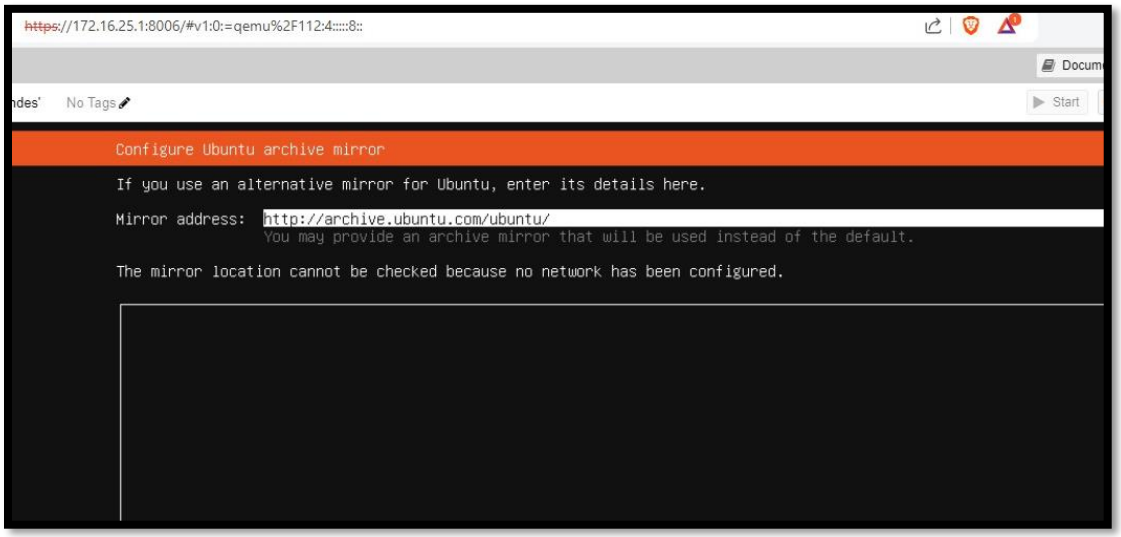


Paso 17

Confirmamos que la dirección IP asignada es la correcta, tal como se muestra en la figura.

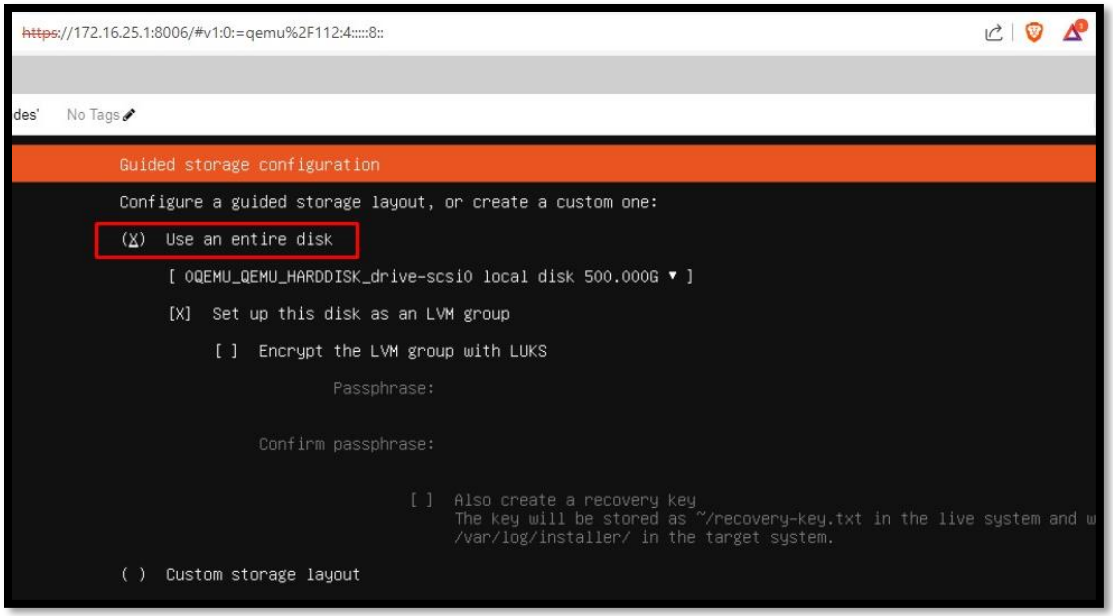
Paso 18

Verificamos la ruta de donde se descargarán las actualizaciones para el servidor, tal como se muestra en la figura.



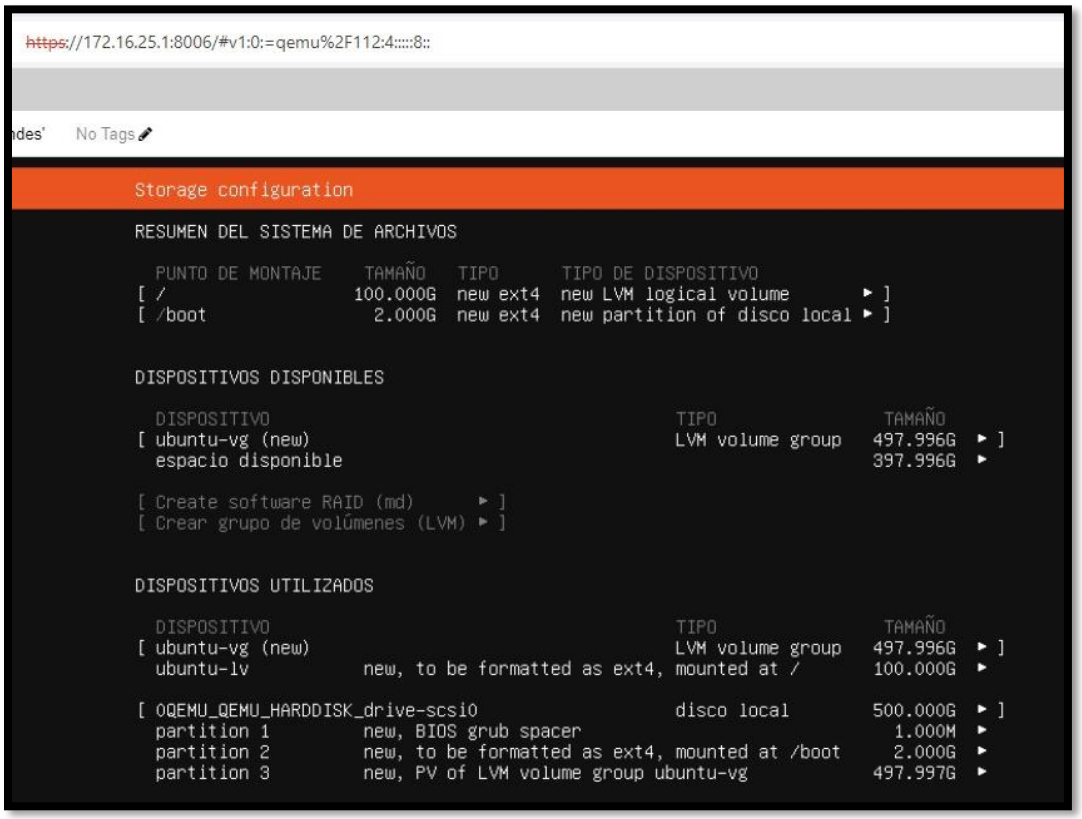
Paso 19

En la figura, se muestra la partición del disco duro, este debe tener como mínimo 500GB de espacio, ya que el servidor syslog ocupara muchos datos para los registros.



Paso 20

En la figura, validamos las particiones que se generan de manera automática en el disco duro.

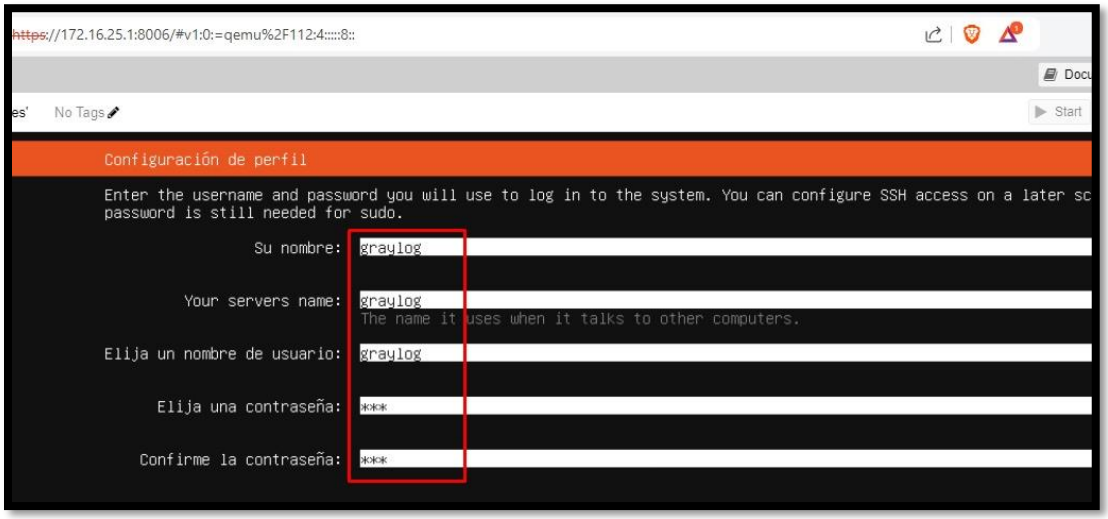


Paso 21

En la figura, confirmamos la acción de formateo.

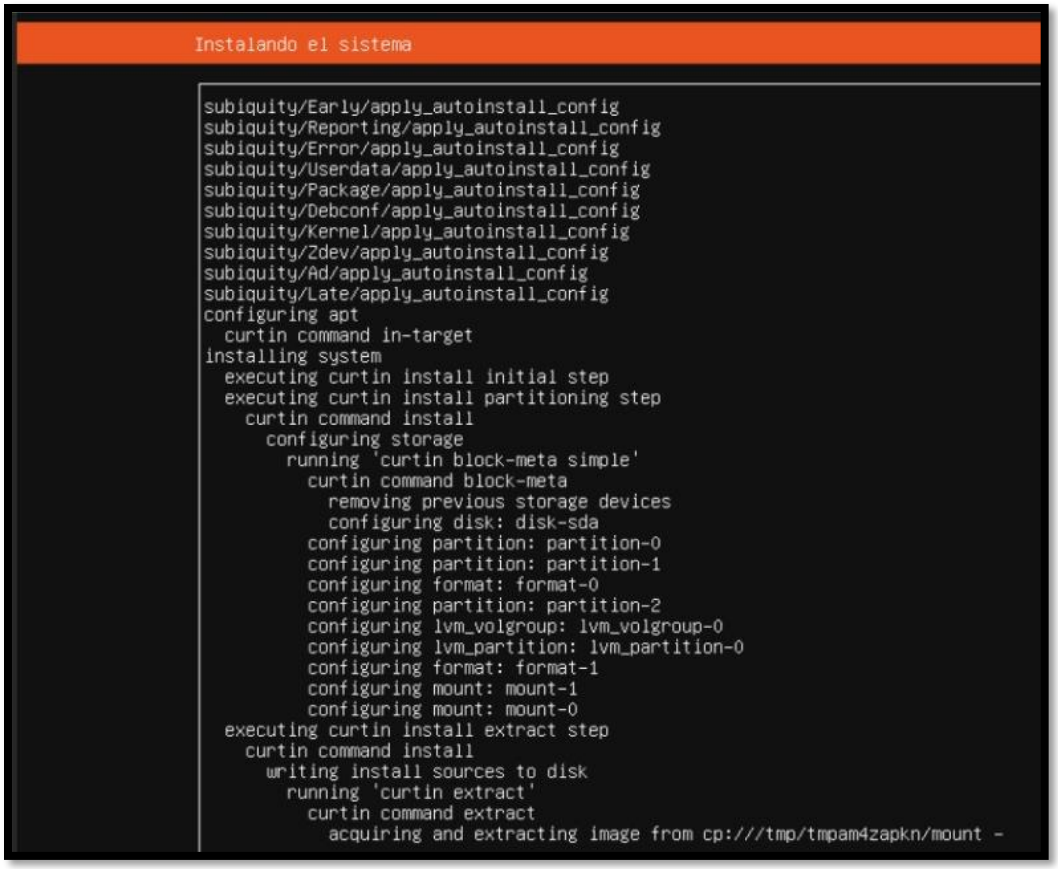
Paso 22

En la figura, asignamos el nombre de usuario y contraseña para el super usuario.



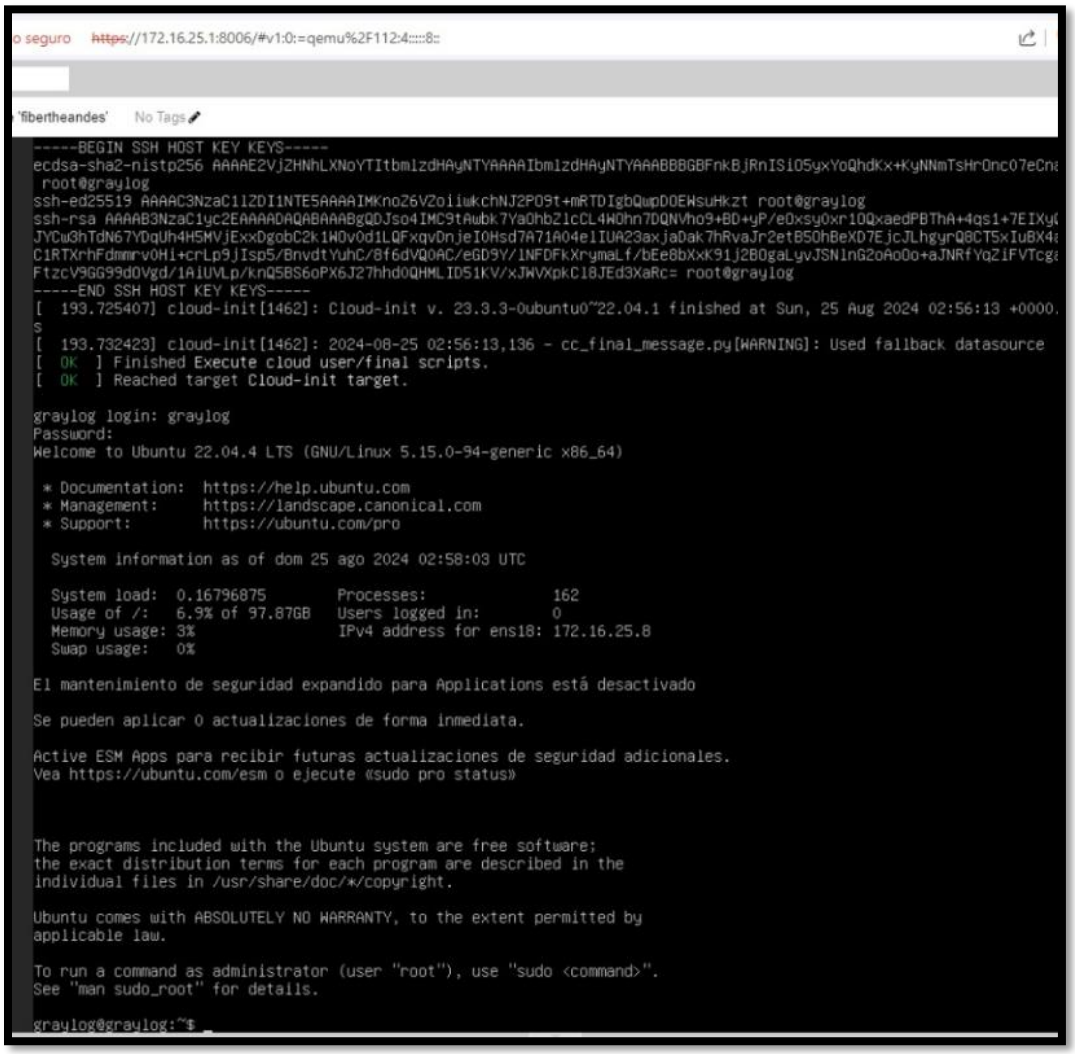
Paso 23

En la figura, el sistema empezará a instalar los archivos necesarios para que levante el Ubuntu server.



Paso 24

En la figura, se visualiza el sistema operativo instalado de manera correcta.



ANEXO B

En la figura, se visualizan los comandos para la instalación del contenedor Docker.

```
sudo apt install docker.io
sudo usermod -aG docker $USER
newgrp docker
docker version
sudo apt install -y curl wget
curl -s https://api.github.com/repos/docker/compose/releases/latest | grep browser_download_url |
grep docker-compose-linux-x86_64 | cut -d '"' -f 4 | wget -qi –
chmod +x docker-compose-linux-x86_64
sudo mv docker-compose-linux-x86_64 /usr/local/bin/docker-compose
docker-compose version
sudo systemctl start docker && sudo systemctl enable docker
```

ANEXO C

En la figura, se visualizan los comandos para la instalación del Mongo-DB dentro del contenedor Docker.

```
nano docker-compose.yml
version: '2'
services:
  # MongoDB: https://hub.docker.com/_/mongo/
  mongodb:
    image: mongo:4.2
    networks:
      - graylog
  #DB in share for persistence
    volumes:
      - /mongo_data:/data/db
```

ANEXO D

En la figura, se visualizan los comandos para la instalación de Elasticsearch dentro del contenedor Docker.

```
# Elasticsearch: https://www.elastic.co/guide/en/elasticsearch/reference/7.10/docker.html
 elasticsearch:
   image: docker.elastic.co/elasticsearch/elasticsearch-oss:7.10.2
   #data folder in share for persistence
   volumes:
     - /es_data:/usr/share/elasticsearch/data
   environment:
     - http.host=0.0.0.0
     - transport.host=localhost
     - network.host=0.0.0.0
     - "ES_JAVA_OPTS=-Xms512m -Xmx512m"
   ulimits:
     memlock:
       soft: -1
       hard: -1
   mem_limit: 1g
   networks:
     - graylog
```

ANEXO E

En la figura, se visualizan los comandos para la instalación de Graylog dentro del contenedor Docker.

```
  # Graylog: https://hub.docker.com/r/graylog/graylog/
  graylog:
    image: graylog/graylog:4.2
    #journal and config directories in local NFS share for
persistence
    volumes:
      - /graylog_journal:/usr/share/graylog/data/journal
    environment:
      # CHANGE ME (must be at least 16 characters)!
      - GRAYLOG_PASSWORD_SECRET=123
      # Password: admin
      - GRAYLOG_ROOT_PASSWORD_SHA2=
a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e
86f7f7a27ae3
      -
GRAYLOG_HTTP_EXTERNAL_URI=http://172.16.25.8:9000/
    entrypoint: /usr/bin/tini -- wait-for-it elasticsearch:9200
--  /docker-entrypoint.sh
    networks:
      - graylog
    links:
      - mongodb:mongo
      - elasticsearch
    restart: always
    depends_on:
      - mongodb
      - elasticsearch
    ports:
      # Graylog web interface and REST API
      - 9000:9000
      # Syslog TCP
      - 514:514
      # Syslog UDP
      - 514:514/udp
      # GELF TCP
      - 12201:12201
      # GELF UDP
      - 12201:12201/udp
# Volumes for persisting data, see
https://docs.docker.com/engine/admin/volumes/volumes/
volumes:
  mongo_data:
    driver: local
  es_data:
    driver: local
  graylog_journal:
    driver: local
networks:
  graylog:
    driver: bridge
```

Presionamos control + o para guardar y control + x para salir

ANEXO F

En la figura, se visualiza la creación de carpetas, asignación de permisos e inicio de los servicios.

Creamos las carpetas	Asignamos permisos	Iniciamos los servicios
sudo mkdir /mongo_data	sudo chmod 777 -R /mongo_data	docker-compose up -d
sudo mkdir /es_data	sudo chmod 777 -R /es_data	docker ps
sudo mkdir /graylog_journal	sudo chmod 777 -R /graylog_journal	sudo ufw allow 9000/tcp

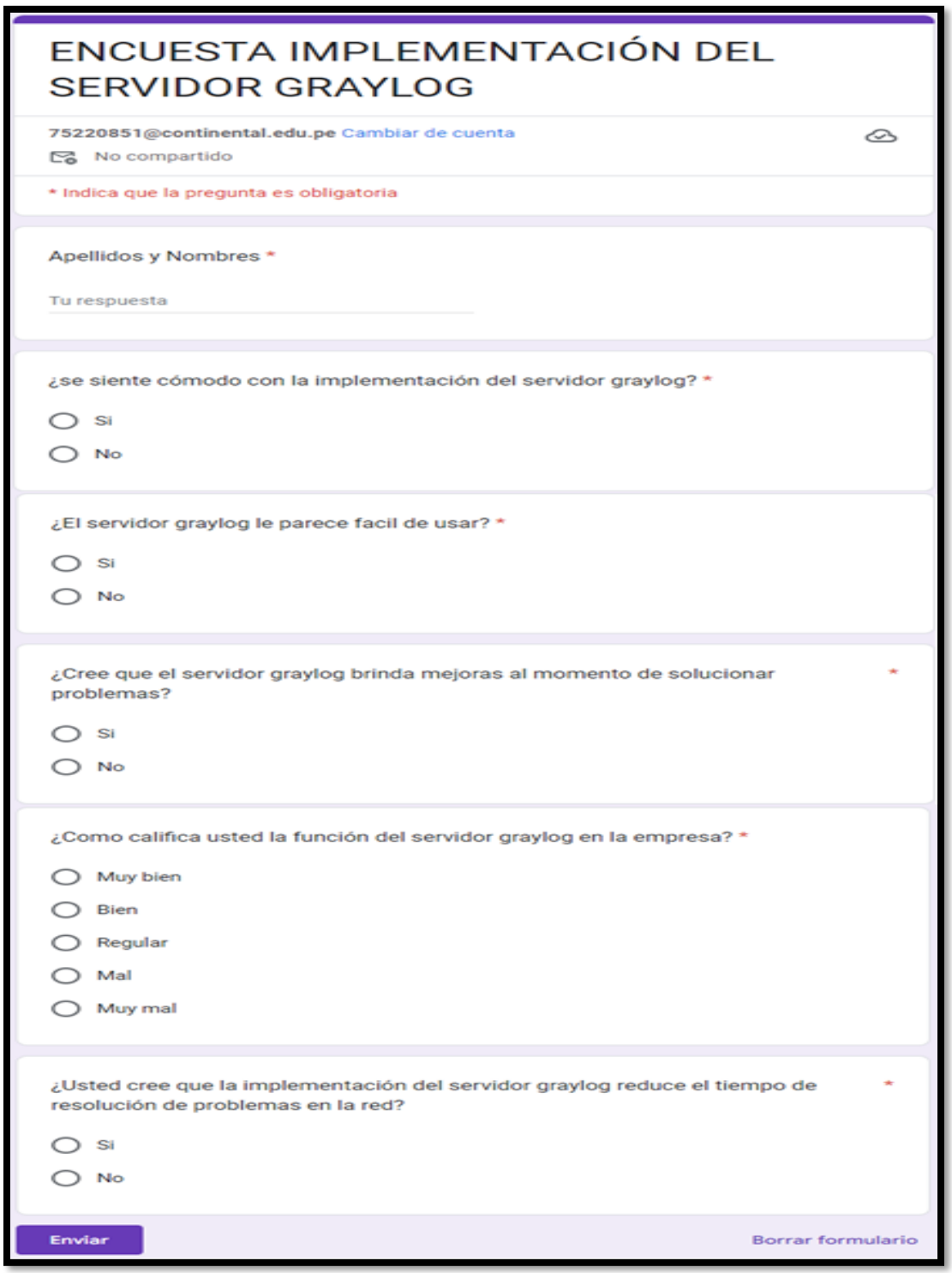
Ingresamos por web con nuestro usuario y contraseña

Ip privada: http://172.16.25.8:9000/

Ip publica: http://45.173.200.5:9000

ANEXO G

ENCUESTA DE SATISFACCIÓN SOBRE LA IMPLEMENTACIÓN DEL SERVIDOR GRAYLOG A LOS TRABAJADORES DE LA EMPRESA TELECABLE



ENCUESTA IMPLEMENTACIÓN DEL SERVIDOR GRAYLOG

75220851@continental.edu.pe Cambiar de cuenta

No compartido

* Indica que la pregunta es obligatoria

Apellidos y Nombres *

Tu respuesta

¿se siente cómodo con la implementación del servidor graylog? *

- Si
- No

¿El servidor graylog le parece facil de usar? *

- Si
- No

¿Cree que el servidor graylog brinda mejoras al momento de solucionar problemas? *

- Si
- No

¿Como califica usted la función del servidor graylog en la empresa? *

- Muy bien
- Bien
- Regular
- Mal
- Muy mal

¿Usted cree que la implementación del servidor graylog reduce el tiempo de resolución de problemas en la red? *

- Si
- No

Enviar Borrar formulario