UNIVERSIDAD JOSÉ CARLOS MARIÁTEGUI

VICERRECTORADO DE INVESTIGACIÓN

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS E INFORMÁTICA

TESIS

IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD PERIMETRAL BAJO UN SOFTWARE LINUX EN UNA INSTITUCIÓN EDUCATIVA DE ILO – 2021

PRESENTADO POR

HEBER JESUS CHAVEZ CHOQUE

ASESOR

Mg. ALBERTO ENRIQUE COHAILA BARRIOS

PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN INGENIERIA DE SISTEMAS E INFORMÁTICA CON MENCIÓN EN SEGURIDAD Y AUDITORÍA INFORMÁTICA

MOQUEGUA – PERÚ

2023

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE FIGURAS

RESUMEN

En el presente trabajo se tiene como objetivo principal Implementar un sistema de seguridad perimetral bajo un software Linux en un entorno virtual para mejorar la seguridad perimetral de la I.E. Almirante Miguel Grau Seminario Ilo – 2021, el tipo de investigación es aplicada con un nivel explicativo con un enfoque cuantitativo, además tiene un diseño experimental, para la obtención de datos y posterior análisis se consideró una muestra de 96 personas, tanto para el pre-test como el post-test, el análisis de los datos se realizó por medio del software Excel.

Se trabajó con dos variables, siendo la dependiente seguridad perimetral y la independiente el software Linux, que está compuesto por dimensiones, de las cuales la funcionalidad y confiablidad obtuvieron un resultado favorable en la funcionalidad de la información además se obtuvo mejoras evidentes debido a que las variaciones porcentuales que fueron de 40% y 7% para indicadores de confidencialidad e integridad respectivamente. En conclusión, se logró la implementación del software Linux para el sistema de seguridad perimetral que influye favorablemente en la funcionalidad de los sistemas virtuales de información de la I.E. en Ilo.

Palabra clave: Confidencialidad, funcionalidad, confiabilidad

ABSTRACT

The main objective of this work is to implement a perimeter security system under a Linux software in a virtual environment to improve the perimeter security of the I.E. Almirante Miguel Grau Seminar Ilo - 2021, the type of research is applied with an explanatory level with a quantitative approach, it also has an experimental design, for data collection and subsequent analysis a sample of 96 people was considered, both for the pre-test and post-test, the data analysis was performed using Excel software.

We worked with two variables, being the dependent one perimeter security and the independent one Linux software, which is composed of dimensions, of which functionality and reliability obtained a favorable result in the functionality of the information, in addition, evident improvements were obtained due to the percentage variations that were 40% and 7% for confidentiality and integrity indicators respectively. In conclusion, the implementation of the Linux software for the perimeter security system was achieved, which favorably influences the functionality of the virtual information systems of the I.E. in Ilo.

Keyword: Confidentiality, functionality, reliability.

INTRODUCCIÓN

La información es ahora el activo más valioso para toda organización, y en un esfuerzo por manejar cualquier incidente de seguridad informática que pueda poner en peligro la confidencialidad, integridad y disponibilidad de esta información, han surgido dispositivos de seguridad perimetral, incluyendo IDS, IPS, Firewalls y demás (Preciado y Vargas, 2016).

El interés de las personas por la creación y el manejo de herramientas diseñadas para realizar asaltos informáticos de forma sencilla, al tiempo que se identifican nuevas vulnerabilidades en los sistemas, ha aumentado como consecuencia de los avances tecnológicos realizados en beneficio de las empresas (Bonilla y Rojas, 2019).

El problema es que, en el momento de un ataque informático, cada componente de la infraestructura de red produce sus propios registros, según el fabricante. Como estos registros son tan grandes e incompatibles entre sí, su procesamiento es una tarea difícil. Por ello, es necesario estandarizarlos y centralizarlos, facilitando la generación de alertas y la identificación de ataques informáticos en tiempo real (Preciado y Vargas, 2016).

Muchos de los ataques que se generan hoy en día no muestran ningún patrón claro. Se requieren herramientas tecnológicas modernas para identificar o detectar las amenazas, contenerlas si se materializan, poder eliminarlas y poder restaurar los servicios afectados en un momento en el que la empresa no se vea impactada negativamente o el daño sea bajo (Bonilla y Rojas, 2019).

CAPÍTULO I. PLANTEAMIENTO DEL ESTUDIO

1.1. Descripción de la realidad problemática

El factor tecnológico a lo largo del tiempo ha evolucionado ante la demanda de seguridad exigida y en vista de ello nacen los sistemas de seguridad perimetral, los cuales tienen como fin brindar mayor confiabilidad a los usuarios internos o externos al acceder a ciertos servicios.

Por ello surge el método de defensa de las redes informáticas como la seguridad perimetral, la misma que busca instalar equipos de comunicación con políticas de seguridad que puedan funcionar de manera óptima en la red interna y externa permitiendo o restringiendo el acceso a usuarios de servicios de red. Igualmente, es importante mencionar que la distribución Linux es una de las plataformas más seguras en cuanto a sistemas operativos y servicios en tecnología, pero no es comercialmente más conocido por la complejidad de su uso y por el bajo nivel de conocimiento de sus beneficios, sin embargo, cuenta con una ventaja importante al no requerir licencia para su uso, siendo de acceso libre. Si bien el software libre actualmente es bastante tradicional en el ambiente informático se torna riesgoso para la seguridad de la red,

teniendo que analizar cada paquete de tráfico para ser aceptado o en caso contrario rechazado.

En la actualidad las instituciones educativas requieren el uso de tecnologías informáticas para responder al fenómeno de la digitalización, del cual el sector educación no es ajeno. Sin embargo, con ello las Instituciones Educativas se ven expuestas a los riesgos que conllevan dichas tecnologías y a la necesidad de implantar mejores herramientas de control y optimización de estos recursos.

Según el Ministerio de educación (2019) para el año 2022 todas las entidades nacionales urbanas contarán con equipamiento digital y conexión a internet como parte de sus objetivos de digitalización pedagógica, por lo que el resguardo y protección de información y servicio de red, debe ser tomada en cuenta como una prioridad, para que dicha tecnología sea realmente utilizada en bien del aprendizaje escolar evitando el mal uso de las mismas.

1.2. Definición del problema

En la actualidad tener acceso a herramientas tecnológicas, a la red y poder emplearlas para el aprendizaje se ha vuelto importante, pero, también ha traído consigo los peligros de ataques y amenazas en la red, páginas web con virus, y más, que ponen en riesgo la protección de la información y datos confidenciales. La I.E. Almirante Miguel Grau Seminario – Ilo, de estudio, es una institución reconocida con más de 10 años al servicio de la educación en los niveles de inicial, primaria y secundaria. Cuenta con talleres y salas de cómputo que se emplean como herramientas de aprendizaje dentro de la educación que proporcionan a sus estudiantes.

Los alumnos, profesores y el personal administrativo utilizan constantemente los equipos tecnológicos y tienen acceden a la red para buscar y almacenar información, donde se ha observado que no hay políticas de restricción a ciertos contenidos en la red de dudosa procedencia que generan virus, hay acceso libre a diferentes tipos de páginas web no educativas, de ocio y juegos, que al unirse con las descargas de archivos y programas dañinos que pueden generar daños operacionales en los equipos utilizados. Esto a su vez limita el ancho de banda (internet) que no permite que el internet llegue a abastecer todas las salas y equipos de cómputo, siendo el nivel de primaria el más perjudicado.

De igual manera no existe un servidor de archivos que garantice la seguridad al momento de compartir información; por ello al no tenerlo controlado, seguro y restringido no es posible la utilización de las fuentes de estudio como apoyo a lecciones de aprendizaje en el aula y para realizar tareas administrativas, lo que deja en evidencia la vulnerabilidad del sistema de seguridad en la red de la institución y la falta de protocolos de monitoreo.

Dado que la protección de datos es esencial, por el contenido de información que es de carácter confidencial, se ha propuesto la implementación de un sistema de seguridad perimetral basado en un software Linux, dentro de un entorno de virtualización, acompañado de protocolos de que monitoreen accesos, cambios y más en la red, asimismo la seguridad de las mismas y de la información, que permita la prevención frente a las amenazas latentes de la red, los accesos no autorizados.

Por lo que se formula la pregunta ¿La implementación de un sistema de seguridad perimetral bajo un software Linux en un entorno virtual reducirá la vulnerabilidad de la seguridad de la información en una I.E. de Ilo - 2021?

1.3. Definición del Problema

1.3.1. Interrogante principal

¿La implementación de un sistema de seguridad perimetral bajo un software Linux en un entorno virtual mejorará la seguridad perimetral de una I.E. en Ilo - 2021?

1.3.2. Interrogantes Básicas

- ¿Cómo es la funcionalidad del software Linux en un entorno virtual en la seguridad perimetral de una I.E. en Ilo - 2021?
- ¿Cómo es la confiabilidad del software Linux en un entorno virtual en la seguridad perimetral de una I.E. en Ilo - 2021?
- ¿Cuál es nivel de seguridad perimetral que perciben los docentes y el personal administrativo de una I.E. en Ilo antes y después de la implementación del sistema de seguridad perimetral bajo un Software Linux en un entorno virtual?

1.4. Objetivos de Investigación

1.4.1. Objetivo general

Implementar un sistema de seguridad perimetral bajo un software Linux en un entorno virtual para mejorar la seguridad perimetral de una I.E. en Ilo - 2021.

1.4.2. Objetivos específicos

- Determinar la funcionalidad del software Linux un entorno virtual para la seguridad perimetral de una I.E. en Ilo - 2021.

- Determinar la confiabilidad del software Linux un entorno virtual para la seguridad perimetral de una I.E. en Ilo - 2021.
- Determinar el nivel de seguridad perimetral que perciben los docentes y el personal administrativo de una I.E. en Ilo antes y después de la implementación del sistema de seguridad perimetral bajo un Software Linux en un entorno virtual.

1.5. Justificación e Importancia de la Investigación

La investigación se realizó con la finalidad de ofrecer un entorno seguro de uso de la red en el personal docente y administrativo que labora en la institución asimismo permitirá que los estudiantes interactúen libremente con buscadores de información seguros para su aprendizaje y estudio, mediante la implantación de un sistema de seguridad perimetral que ofrezca confiabilidad y seguridad de la información manipulada, la cual es privada.

En vista de ello es valioso que se plantee una metodología eficiente y eficaz con el fin de optimizar el nivel de seguridad informática, pues mediante dicho sistema se pretende brindar resguardo a la información, además dicho sistema busca proteger los elementos vulnerables de la comunidad estudiantil. Asimismo, mediante el método de defensa de dicho sistema se establecerá políticas de seguridad en el perímetro externo y en los diversos niveles para forjar confiabilidad en cuanto al acceso a la red solo a usuarios identificados con los equipos que se unen a la red para adherirse a servicios específicos y a su vez rechazar el acceso a otros, con el fin de tratar los datos de manera segura (SIMAD, 2012).

1.6. Variables de Operacionalización

1.6.1. Variable dependiente

Tabla 1

Tabla operacional de la variable dependiente

VARIABLE DEPENDIENTE (Y)	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	ESCALA DE MEDICIÓN
Seguridad perimetral	Es el sistema que tiene como propósito resguardar el perímetro de intrusos, se protege básicamente las redes privadas del sistema informático. Los principios básicos del sistema es resistir a ataques exteriores, identificar ataques sucedidos, aislar los servicios en base a la exposición de ataques y por último filtrar el tráfico de ser necesario. (Davantis, 2019)	Brinda mayor confiabilidad a los usuarios internos o externos al acceder a ciertos servicios, mediante herramientas informática que identifican y restringen la accesibilidad de diferentes usuarios.	Ataques Informáticos	Nivel de ataques informáticos.	N° de reportes 0-5: Bajo; 6-10: Medio; 11 a más: Alto
				Tipos de ataques cibernéticos	Fuerza Bruta, Phishing, envenenamiento por IP, Redireccionamiento, Malware, Error de configuración, Boots, Ddos, Otros.
				Herramientas de seguridad	Antivirus, Firewalls, Proxy, IDS, Monitoreo de red, otros.
			Gestión de datos	Nivel de eficiencia de gestión de datos	Porcentaje de filtros: 0: Bajo; 1-2: Medio; de 3 a más:Alto Capacidad de Ancho de banda: 0Mgb-3 Mgb: Bajo; 4Mgb a 10 Mgb:Medio; 11Mg a más alto

Nota. La tabla anterior refleja la operacionalización de la variable Seguridad Perimetral. Adaptación tomada de la investigación de Bautista (2018).

1.6.2. Variable Independiente

Tabla 2

Tabla operacional de la variable independiente

VARIABLE INDEPENDIENTE (X)	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	ESCALA DE MEDICIÓN
Monitoreo de los protocolos de administración de red	Es un protocolo que les permite a los administradores gestionar los dispositivos de red y diagnosticar sus problemas. (Villa gómez, 2017)	Brinda la posibilidad de controlar y delimitar los diferentes requerimientos de seguridad según la necesidad del administrador de red.	Monitoreo de tráfico	Monitoreo de tráfico pasivo	Frecuencia de monitoreo del nivel de tráfico de red. De 1 a 4 veces por mes: Baja; 5 a 9: media; de 10 a más: alta
				Monitoreo de tráfico activo	Número de Mensajes que envían los dispositivos SNMP a una dirección configurada. De 0- 4 msj al día: tráfico bajo; 5-9: tráfico medio; de 10 a más: tráfico alto.

	Conocimientos sobre sistemas de seguridad	Nivel de conocimientos sobre sistemas de seguridad	sí: Alto, no: Bajo

Nota. La tabla anterior refleja la operacionalización de la variable Software Linux. Adaptación tomada de la investigación de Bautista (2018)

1.7. Hipótesis de la Investigación

1.7.1. Hipótesis general

$H0_1$: La Implementación del sistema de seguridad perimetral bajo un software Linux en un entorno virtual mejora la seguridad perimetral de una I.E. en Ilo - 2021.

Ha_1: La Implementación del sistema de seguridad perimetral bajo un software Linux en un entorno virtual no mejora la seguridad perimetral de una I.E. en Ilo – 2021.

1.7.2. Hipótesis especificas

$H0_2$: La funcionalidad del software Linux un entorno virtual para la seguridad perimetral de una I.E. en Ilo - 2021 es buena.

$Ha_{2:}$ La funcionalidad del software Linux un entorno virtual para la seguridad perimetral de una I.E. en Ilo - 2021 no es buena.

$H0_3$: La confiabilidad del software Linux un entorno virtual para la seguridad perimetral de una I.E. en Ilo – 2021 es buena.

Ha_3: La confiabilidad del software Linux un entorno virtual para la seguridad perimetral de una I.E. en Ilo – 2021 no es buena

$H0_4$: El nivel de seguridad perimetral que perciben los docentes y el personal administrativo de una I.E. en Ilo antes y después de la implementación del sistema de seguridad perimetral bajo un Software Linux en un entorno virtual es distinta.

Ha_4: El nivel de seguridad perimetral que perciben los docentes y el personal administrativo de una I.E. en Ilo antes y después de la implementación del sistema de seguridad perimetral bajo un Software Linux en un entorno virtual no es distinta.

CAPÍTULO II: MARCO TEÓRICO

2.1. Antecedentes de la Investigación

2.1.1. Antecedentes nacionales

- Bautista (2018), en su estudio, *"Implementación de un servidor Linux y su influencia en la seguridad perimetral de la red local de la empresa Junefield Group S.A., Lima 2017" UCV.* Perú.

El objetivo central del estudio era montar un servidor Linux y ver cómo afectaba a la seguridad perimetral de la red local de Junefield Group S.A. El cual se desarrolla bajo una metodología Top Down, el cual se desarrolla en cuatro etapas, la caracterización de necesidades, diseño lógico y físico, pruebas y optimización del servidor en Endian. Entre los resultados basados en el análisis de datos derivados del estudio se logró establecer un cambio significativo en la seguridad perimetral de la red local de la compañía Junefield Group S.A. Pudiendo concluir que la implementación de dicha propuesta generará una solución eficiente a la problemática de rendimiento y seguridad en la Red de Salud Valle del Mantaro.

– Albujar (2018), en su estudio *"Diseño de un sistema de seguridad de red basado en la integración de los servidores Radius – Idap en Linux para fortalecer elacceso de la red de la clínica Millenium Chiclayo 2016".* UNPRG. Chiclayo.

La investigación planteó como objetivo central fue lograra expansión, eficiencia y mayor amplitud con el propósito de optimizar la atención de los pacientes y familiares de este acompañado de un plan definidos de expansión a nivel nacional y un control consciente de los recursos de la organización apoyado de un trabajo fortalecido en equipo basado en un diseño de sistema de seguridad de red asentado en la integración de los servidores Radius – Idap en Linux. Bajo una metodología CISCO Top – Down Network Design. Teniendo como resultados que la implementación del proyecto planteado logrará la conexión entre las diferentes áreas de la clínica en estudio fortaleciendo la transferencia de información; proporcionando a la vez una estructura robustecida mediante un sistema de seguridad de red basado en la integración de los servidores Radius – Idap en Linux, resolviendo las caídas de la Red LAN y WLAN. Pudiendo concluir que el diseño de seguridad de red planteado en el estudio en mención logra cubrir con el objetivo del trabajo reforzando el control de acceso a usuarios de la clínica Millenium Chiclayo mediante la implementación de herramientas de software libre identificando la veracidad de las redes inalámbricas y autentificando la conexión de los determinados equipos.

– Díaz (2019), en su proyecto de investigación, *"Implementación de un prototipo de monitoreo de dispositivos de comunicación y usuarios finales utilizando el*

protocolo SNMP centrado en software libre para una organización e-Commerce." UNMSM. Perú.

El objetivo central de la investigación fue desarrollar y construir un prototipo que admita monitorear en tiempo real los dispositivos de comunicación y los usuarios finales a través del protocolo SNMP y software libre. Se aplicó la metodología en tres partes: la recopilación de la documentación técnica, la identificación de la empresa, por último, la implementación de un prototipo de sistema de monitoreo propuesto. Como parte de los resultados de la implementación de una propuesta bajo el sistema GNU/Linux se determinó que la misma brinda ventajas en cuanto al costo, nivel de conocimientos requeridos para el manejo del sistema operativo. En conclusión, el prototipo planteado permitió examinar los diferentes dispositivos de comunicación y terminales de red de datos de la organización estudiada denotando el índice de actividad y anomalías en el funcionamiento del mismo. Demostrando la eficiencia de la herramienta no licenciada en el mismo nivel de competencia que una aplicación con requerimiento de licencia.

- Oré (2019), en su estudio; *"Implementación de un Sistema de Monitoreo Para Asegurar la Continuidad de los Servicios en un Data Center Utilizando Protocolo SNMP".* UTP. Perú.

La investigación plantea como objetivo principal implementar un sistema que monitoree la red, que observe el comportamiento de la infraestructura de comunicación en Netsecure Perú. Bajo un marco metodológico de tipo descriptivo enmarcado bajo un diseño cuasiexperimental. Como principales resultados se presenta que la seguridad de la prolongación de servicios manipulados en la data center mediante la

implementación de protocolos SNMP para la organización en estudio; anexando formalidades y sistemas mayormente usados en empresas diferentes para el seguimiento y control de la estructura tecnológica. Pudiendo concluir que mediante el análisis de las aplicaciones del monitoreo de uso más común resaltaron que el PRTG NETWORK MONITOR resulta el más accesible y adecuado para su implantación en la empresa Netsecure Perú dado su practicidad de diseño, amigable configuración y facilidad para escalar conforme a las necesidades de complejidad que requiera la red y los servicios de la empresa en mención.

- Huertas (2022), en su estudio; *"Seguridad de la información y la gestión de riesgos en el Instituto de Educación Superior Tecnológico Privado DETECSUR, Tacna – 2020".* Universidad José Carlos Mariátegui. Perú.

El objetivo principal fue establecer cómo se interrelacionan la gestión de riesgos y la seguridad de la información en el IESTP Detecsur de Tacna. A partir de un cuestionario distribuido a 15 colaboradores de la empresa, se desarrolló un estudio fundamental, descriptivo-correlacional, no experimental, de corte transversal. Para determinar el grado de correlación entre las variables en estudio y las dimensiones correspondientes, se utilizó el estadístico de normalidad de Shapiro-Wilk y la correlación Rho de Spearman. Los resultados indicaron que existía una fuerte asociación significativa (R=.709; p.05).

2.1.2. Antecedentes internacionales

- Marín et al. (2020), *"Implementación de un sistema de seguridad perimetral informático usando VPN, firewall e IDS",* Revista Universidad Católica de Oriente, 84-99.

La investigación a través del empleo de un firewall, un sistema de detección de intruso y una red privada virtual busco elevar la seguridad de la red de una microempresa al mitigar el riesgo de un ataque cibernético. La metodología empleada se basó en tres etapas, desde el proceso de análisis del software idóneo para el IPS, seguido de su desarrollo de las tres herramientas y posterior a ello la integración de las herramientas en uno solo sistema. Para la evaluación de prueba del sistema se empleó la distribución Kali del sistema operativo Linux. Dando como resultados un sistema de defensa que pudo neutralizar los ataques de denegación y fuerza bruta. Concluyendo que la implantación mejora la seguridad de la red, siempre que se cumplan ciertos requisitos como la activación continua del escudo y las reglas de seguridad. asimismo, se recomendó la capacitación del personal para su concientización en temas de seguridad.

- Morales et al. (2020)*, "Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información",* RISTI, 553-565.

La investigación busco aplicar un sistema de seguridad perimetral para mitigar los riesgos externo e internos en la seguridad de la información, mediante el uso de servidores virtuales de una institución pública. Como metodología se empleó el método practico para la implementación, de diseño experimental, la cual paso por la etapa de reconocimiento de equipos, el levantamiento del software y la etapa de prueba y

evaluación en la infraestructura tecnológica. Entre los resultados obtenidos se encontró una buena comunicación entre las redes, equipos, los permisos de navegación, acceso a internet y un aumento de la capacidad del CPU. Concluyendo con la mejora de la seguridad, así como el control de acceso y protección eficaces, garantizando la integridad, confidencialidad y disponibilidad de la información de la institución frente a las amenazas de la red.

- Guamán (2015), en su investigación, *"Diseño de un sistema de gestión de seguridad de la información para instituciones militares".* Escuela Policiaca Nacional de Ecuador.Ecuador.

La investigación proyectó como principal objetivo diseñar un sistema de gestión de seguridad de data dirigido a Entes Militares. En la cual se aplicó una metodología dividida en tres partes, primero está el estudio diagnóstico, luego está la factibilidad y finalmente la creación del sistema de gestión de seguridad de información para instituciones militares bajo la Norma ISO 27001: 2005, al mismo tiempo empleó un conjunto de metodologías para evaluar los riesgos.

En conclusión, la falta de programa de gestión de seguridad respecto a la data agrava el mantenimiento de dichos datos, asentadas en las normas de la ISO 27001:2005, por ello la implementación de dicho sistema hará que todos los usuarios asuman una obligación frente a la seguridad y reconocimiento respecto al trato responsable de la información.

- Gálvez (2019), en su tesis *"Análisis y propuestas para la seguridad de redes internas LAN y redes perimetrales utilizando TCP/IP y GNU/Linux en*

pequeñas y medianas empresas del Ecuador". Pontificia Universidad Católica del Ecuador. Ecuador.

La misma que busco como principal objetivo la determinación de herramientas libres que garanticen seguridad frente a intrusos o personas inescrupolosas que busquen robar información. La metodología aplicada fueron los sistemas de software libre GNU/Linux además de la herramienta IPCOP. En conclusión, la seguridad perimetral requiere desarrollarse a nivel de red encaminado a advertir ataques de hackers y piratas electrónicos e incluso el hurto de data mediante centrales externas, siendo ideal que el nivel de seguridad esté vinculado a las políticas de planes de seguridad.

- Ruales (2016), en su estudio *"Auditoría de Seguridad perimetral en dispositivos de capa 3 para entornos empresariales utilizando la heramienta Kali Linux".* Universidad de Guayaquil. Ecuador.

El estudio formuló como propósito primordial el desarrollo de un análisis para la determinación de puntos sensibles de la seguridad en dispositivos de transferencia comunicacional, al igual que servidores conectados a la red perimetral de una institución. La metodología aplicada fue ITILv3 la más idónea para la seguridad informática.

En conclusión, un buen sistema de seguridad perimetral lógico contempla por lo menos la protección de la red frente a intrusos externos e internos, además de un adecuado uso de las herramientas como Nmap, IDS, entre otros que permiten a la empresa tener conocimiento sobre las acciones de protección de su información confidencial.

- Alvarado (2018), *"Implementación de políticas de seguridad y control de navegación a través de un firewall basado en Linux para la empresa TRIBUTAX Services S.A.",* Universidad de Guayaquil, Ecuador.

El estudio tuvo como objetivo detectar las vulnerabilidades de acceso a internet en la empresa Tributax services, y su mitigación a través de la instalación del software Linux para una protección a nivel interno que restringa acceso a páginas dañinas para el sistema. La metodología empleada fue el NIST SP 800-30 compuesta de 9 pasos en el análisis de riesgo. La población de estudio se conformó por los trabajadores de la empresa y el encargado del área tecnológica. Para lo cual se empleó la entrevista y encuesta como técnicas en la obtención de información. Luego del proceso de identificación se pasó a la etapa de implementación que trajo como resultados un acceso a internet más seguro y reducción de riesgo frente a ataques en red. Concluyendo con la protección a nivel confidencial, disponible e íntegro de la información, así como la protección de los equipos.

- Díaz (2019), en su investigación titulada *"Implementación modular de un sistema de centralización y correlación de eventos de seguridad de la información (SIEM)".* Universidad Autónoma Benemérita de Puebla. México.

La investigación antes mencionada tuvo como objetivo fue estudiar las soluciones SIEM analizando los módulos de implementación y reconocimiento de las fortalezas de diferentes aplicaciones con el fin de seleccionar e implementar la más adecuada a las necesidades reales de la organización. Siguiendo una metodología CISCO Top – Down Network Design de cuatro etapas. Mediante la cual se obtuvo

como resultado la identificación de las particularidades más relevantes para la implementación de las soluciones SIEM, tales como: capacidad de análisis, motor de detección de amenazas, herramientas de análisis de información, capacidad de respuesta y soporte de normativas de seguridad.

Pudiendo concluir que para lograr un análisis eficiente de registros se requiere una adecuada planificación bajo los lineamientos de normativas aplicables, tanto para el funcionamiento operativo como para el resguardo de seguridad tomando en cuenta las necesidades de la empresa.

2.2. Bases Teóricas

2.2.1. Seguridad Perimetral

Seguridad en la red

La conectividad y la globalización ha permitido que a través de internet se encuentren inmensas cantidades de información, y la sociedad se encuentra inmersa en ella. La información se ha vuelto importante para las personas, empresas, instituciones u organizaciones, las cuales producen, recopilan, sistematizan datos e información, que son usado para tomar decisiones. Al conectarse a la red, entras aun mundo donde estas sujeto a riesgos entre ellos la seguridad y robo de información ya sea por virus, hackers, violaciones de información. Por tanto, la protección de datos es una prioridad esencial para evitar el robo de información y su uso fraudulento, la seguridad informática se vuelve un elemento clave que necesita protocolos de seguridad que certifica la protección de los datos. Asimismo, los datos externos provienen de los usuarios y los internos de la empresa misma, representan activos para una empresa, dado que la información comprendida es sensible (Mora y Villero, 2020).

Para Mora y Villero (2020) las características de un sistema de seguridad se fundamentan en:

- Confidencialidad, se refiere a que solo el personal con autorización tenga acceso a la información.
- Integridad, se busca que los archivos originales no sean modificados.
- Autentificación, la importancia de comprobar la veracidad de la identidad del autor de la información.

Seguridad informática

La seguridad informática es definida como las medidas que se utilizan para la protección del hardware, el software y los recursos informáticos que una empresa u organización emplea para la realización de sus actividades, dado que su enfoque busca garantizar la integridad y privacidad de la información, y que estos sean usados de manera correcta (Figueroa et al., 2017).

Se considera una disciplina, un conjunto de métodos, técnicas que se emplean para la protección de las redes e infraestructura de los sistemas informáticos como los antivirus, firewalls, entre otros. Una de las medidas más conocidas en el ámbito de la seguridad es restringir el acceso al sistema o parte del mismo, donde solo las personas autorizadas tienen acceso a un cierto tiempo de información la cual cuenta también con algunas limitaciones. Cuando el usuario no tiene conocimiento de la vulnerabilidad de sistema informático, las amenazas surgen debido a la descarga de archivos de procedencia no segura que pueden estar dañados o con virus, o eliminar archivos importantes para el sistema informático (Figueroa et al., 2017).

Seguridad de la información

Para Figueroa et al. (2017) la información es el activo en riesgo que debe ser protegida, conocida también como propiedad intelectual que está conformada por datos o conocimientos de gran valor para una organización o una persona. Es una disciplina que se encarga de evaluar riesgos y amenazas, para la realización de actividades referidas a la información como la creación, almacenaje y su utilización de manera confiable.

Las amenazas pueden ser internas o externas, son latentes frente a las vulnerabilidades propias de la tecnología o de los procesos propios de la información. Por ello la información se apoya en la política de seguridad, la cual mediante un plan determina las medidas y procedimientos que garantizan la seguridad de la misma (Figueroa et al., 2017).

Existe una norma para la seguridad de la información, la ISO 27001 cuya implementación sirve para reducir amenazas y riesgos u otros beneficios, dado que establecer garantías para el negocio, los interesados y la opinión pública (Figueroa et al., 2017).

Métodos de ataque a la seguridad informática

La vulnerabilidad, expresa la posibilidad de daños, es la debilidad que compromete la seguridad del sistema informático. Estas vulnerabilidades pueden traer grandes pérdidas económicas para empresas e instituciones, de igual manera en las instituciones educativas donde se mantienen información personal de los alumnos y sus padres, por lo que si el sistema es vulnerable y ocurre el robo de información se

pondría en riesgo la seguridad de los alumnos y sus familias en muchas áreas (Arévalo et al., 2020).

Según Arévalo et al. (2020) las vulnerabilidades se dan debido al:

- Diseño, propio de los protocolos que hay en la red, de los programas, y las políticas de seguridad deficientes e inexistentes.
- Implementación, principalmente por errores al momento de la programación y otros por descuido del fabricante.
- Uso, se da cuando no se aplica una buena configuración, por desconocimiento, falta de preocupación de los usuarios y la falta de algún responsable de informática o con conocimientos necesarios en el tema.

Se detalla la guía de administración de redes con Linux de Kirch y Dawson (2000) los ataques más comunes en la seguridad informática dentro de una organización:

- Acceso no autorizado: hace referencia a individuos que a pesar de no ser parte de la organización pueden acceder y manipular su información.
- Debilidades propias de un programa: los programas tienen sus diseños propios y no necesariamente con niveles de seguridad altos, lo que los hace inherentemente vulnerables a ataques.
- Denegación de servicio: este tipo de ataques genera que el programa o servicio no funcione o no permita que otros hagan uso del mismo, se generan al nivel de la red, mediante datagramas malintencionados bien

preparados generando fallos en la red. También se presenta a nivel de aplicación, mediante ordenes enviadas a un programa que genera el detenimiento del programa y se encuentre saturado o muy ocupado.

- Suplantación de identidad: se usando una aplicación simula las acciones de otro, el atacante sigue el rastro IP presente en los paquetes de red, al actuar como un Host inocente, de ahí surge la necesidad de verificar las órdenes y datagramas, que tienen orígenes no válidos.

Eavesdropping, el ataque más sencillo de todos, el cual está configurado para escuchar y captura datos que no están dirigidos a él, fisgonean documentos para obtener información como nombres y contraseñas a través de la conexión de red con difusiones.

Seguridad perimetral

La seguridad perimetral se entiende como los elementos y sistemas que ayudan en la protección de las redes privadas y seguridad frente a intrusos, sirve como defensa frente a robos de información, ataques o amenazas que reduce considerablemente los riesgos de pérdida o robo de datos por parte de terceros. Asimismo, representa una política de seguridad entre la red privada y el internet.

Es una forma de defender una red que se basa en la creación de recursos de securización para el perímetro exterior de la red y las distintas capas. Esto permite mantener altos niveles de confianza, así como la capacidad de ofrecer acceso a servicios específicos a ciertos usuarios internos o externos mientras se restringe el acceso a otros (Espinoza, 2012).

La seguridad perimetral contempla aspectos como la concentración de sistemas y elementos ya sean mecánicos o electrónicos para su protección en instalaciones sensibles de intrusión (SIMAD, 2012).

Actualmente existen diferentes herramientas de seguridad perimetral, que ayudan a disminuir los riesgos de estar en la red, además de asegurar la confidencialidad e integración de los datos como los firewalls, honey pots, iptables y más. Dado que su fin es prevenir y evitar que la seguridad de los datos este comprometida (Marín et al.,2020).

Dimensiones del sistema de seguridad

a) Confidencialidad

Refiere a que el acceso a la información debe ser solo para el personal autorizado, además de que debe estar a buen recaudo para evitar que otras personas accedan a ella, lo que es posible con un acceso que requiere autorización y control. Dado que la información es un recurso valioso y fundamental para una empresa, por tanto, debe ser mantenido en secreto (Mora y Villero, 2020).

Se pretende prevenir la divulgación no autorizada, dado que la sostenibilidad de una organización, así como su situación en el mercado pueden verse afectada.

b) Integridad

Hace referencia a que la información debe estar inalterable ante cualquier suceso o ataque, cuya modificación debe ser realizado siempre con una previa autorización, de forma que la información sea viable y exacta (Mora y Villero, 2020).

Los ataques, vulnerabilidades y riesgos se presentan desde diversas formas y orígenes, no solo a nivel computacional, dichos ataques son principalmente en daños a

la información, su modificación o eliminación, de igual forma en los softwares, servidores, datos de producción y la infraestructura de seguridad. situación donde el hombre es la parte más débil de la cadena de aseguramiento de la investigación.

La integridad engloba desde la información hasta la infraestructura de seguridad que la rodea y protege, la seguridad tanto física como lógica, por lo que aparte de medios tecnológicos, ve esencial capacitar y contar con un personal calificado. Donde se ve la importancia de tener protocolos de seguridad, un adecuado manejo del sistema de seguridad. Incluido el análisis de riesgos y evaluación de vulnerabilidades (Chilán y Pionce, 2017).

c) Disponibilidad

Hace referencia a la accesibilidad y capacidad de uso de la información cuando se es requerido, lo que significa un funcionamiento permanente sin interrupciones, donde el acceso a cualquier usuario no se vea perjudicado, de modo que sea visible la misma información para los elementos autorizados. Donde un sistema no disponible es lo mismo que la no existencia del sistema (Chilán y Pionce, 2017).

Seguridad perimetral Firewall

Es un servicio que filtra información que ingresa y que sale de una organización, es la primera línea de seguridad frente a cualquier actividad sospechosa, la cual, a través de un monitoreo constante del contenido. Supervisa el tráfico de red, bloqueando tráfico de red no deseado protegiendo la red local, al mejorar el dominio de control de ataques y amenazas en tiempo real (Marín et al.,2020).

Uno de los instrumentos de firewall que se emplean de forma común dentro de Linux es Ipstables; el mismo que admite al administrador de una red el diseño y

configuración del firewall. De igual manera, el administrador puede modelar la cadena o reglas dentro del sistema Linux.

Método de implementación

En caso de la implementación del programa Linux se desarrolla en función de paso que consiste en la identificación actual de la situación del estado en el que se encuentra la seguridad de las computadoras y la accesibilidad de las mismas a ciertas páginas que no contribuyen a la formación de los estudiantes.

En consecución de lo que se evalúa, se implanta un programa de prueba de manera que se midan los cambios que se perciben durante su instalación y manejo del software.

Ventajas y desventajas de la seguridad perimetral firewall

Para Cuenca (2016) se tienen como ventajas del Firewall:

- Gestiona los accesos de internet a la red privada. Puesto que cada uno de los servidores del sistema son vulnerables al asalto de otros servidores en internet sin el apoyo de la herramienta de Firewall. La dureza de cada servidor es primordial en la seguridad de la red privada, la seguridad depende del potencial de fragilidad del mismo sistema.
- Mantiene a los usuarios no deseados fuera de la red, mediante la construcción de un Check Point, los usuarios no deseados son los hackers, espías, evitando su entrada y salida a la red, previniendo posibles ataques. Una de las ventajas más importantes es que facilita la

gestión; una vez concentrada e integrada el sistema de seguridad, resultando ser más eficiente a comparación de distribuirlo por áreas.

- Proporciona un punto donde se puede monitorear la seguridad, la cual emite una alerta al primer comportamiento sospechoso, este se puede ver al conectarse a internet. Además, que uno no sabe cuándo se efectuará un posible ataque, y es muy necesario tener que llevar registros del tráfico en firewall.

2.2.2. Software Linux

Linux

Linux se le denomina como la aplicación estrella del software libre, dado que se torna como un sistema multitarea, multiusuario, compatible con UNIX. Asimismo, en diversos momentos el software libre es confundido con el Linux, pero esto no es conveniente dado que el sistema del software libre no siempre se basa en Linux. Sin embargo, existen otras aplicaciones que funcionan en Linux como el Acrobat Reader, PDF (Gónzalez et al, 2003).

Por su parte Hernández (2015) refiere que Linux es el mayor representante del software de tipo libre, dado que su estructura sistémica libre es parte de diversos instrumentos desarrollados para servidores al igual que para clientes naturales. Además, los hackers Linux han ido adaptando las herramientas de GNU al núcleo de Linux para crear las primeras distribuciones GNU/Linux.

a) Historia de Linux

Según Gónzalez et al (2003) mencionan que:

“En el ámbito del mundo del software la historia de Linux es muy popular. Por el año 1991 un estudiante llamado Linus Torvalds quiso aprender cómo era el uso del modo protegido 386 en una máquina adquirida. Luego Linus emitió un mensaje en su grupo de noticias de Minix, en el cual anuncio su inicio desde cero en cuanto a un núcleo de sistema operativo excluyendo el código del mismo, dado que el fin era que el sistema no tendría las barreras de Minix. Luego para octubre del mismo año salió la versión 2.0, mediante la cual se permitía ejecutar terminales bash y el compilador GCC y en los meses posteriores a ello las aportaciones se fueron incrementando y en 1992 Linus publica su versión 0.95 camino a la versión 1.0, luego en 1993 publica la versión 0.99 pl 14 y por último la versión Linux 1.0 se publicó 1994 en base a las condiciones de Licencia GPL como menciona el propio Torvalds todo con la finalidad de distribuir y popularizar su núcleo”

Luego del éxito que tuvo Linux gracias a Linus, su principal competidor Tanenbaum atacó de forma desproporcionada, puesto que el sistema de Linux era monolítico es decir una sola pieza integra todos los manejadores y no microkernel, cuyo núcleo presenta diseño modular permitiendo hacerlo más pequeño. Por lo que dicho debate fue parte de un artículo.

b) Antecesor de Linux

Uno de los antecesores de Linux fue UNIX, dado que en sus inicios Linux surgió como una copia de Minix y Unix propietario. Sin embargo, Linux se desarrolló en código abierto y orientado a las PC domésticas, si bien UNIX se inició por el año 1969 con el fin de crear un sistema operativo donde un ordenador de gran magnitud pueda abarcar a un millar de usuarios simultáneos, su ambición generó fallas, a pesar

de ello Unix destacó por ser un sistema pionero independiente de la arquitectura hardware, que a su vez ha generado éxito a diferentes sistemas de hardware (Jorba, 2010).

c) Modo de trabajo de Linux

El modo de trabajo de Torvalds en esos tiempos no era muy típico, puesto que su desarrollo se basó en una relación de correos, donde más que discusiones existía un deseo desarrollador. Por ello Torvalds prefería que el proyecto se plasmara en la lista, pidiendo además que el parche se enviara a la misma. Asimismo, Linux optaba por el envío de dicha codificación inmerso en el desarrollo del mensaje con el objetivo de que él y los otros miembros puedan comentarlo. De igual forma Torvalds generó la idea de desarrollo paralelo de ambas vertientes del núcleo controlado, cuya versión es par y la inestable que es impar. En síntesis, Linux no cuenta con un esquema de entregables guiados en fechas límites, si no que plantea que estará listo cuando esté listo, en pocas palabras la decisión depende básicamente del propio Linux (Gónzalez et al, 2003).

d) Métodología de implementación

Según Aldave (2021), menciona que en caso de la implementación se sigue los siguientes procesos, se empieza por la instalación de los servidores en donde se rige por:

- La elección del sistema que se va operar
- Implementación y creación de contraseñas para los programas
- Activación del Firewall

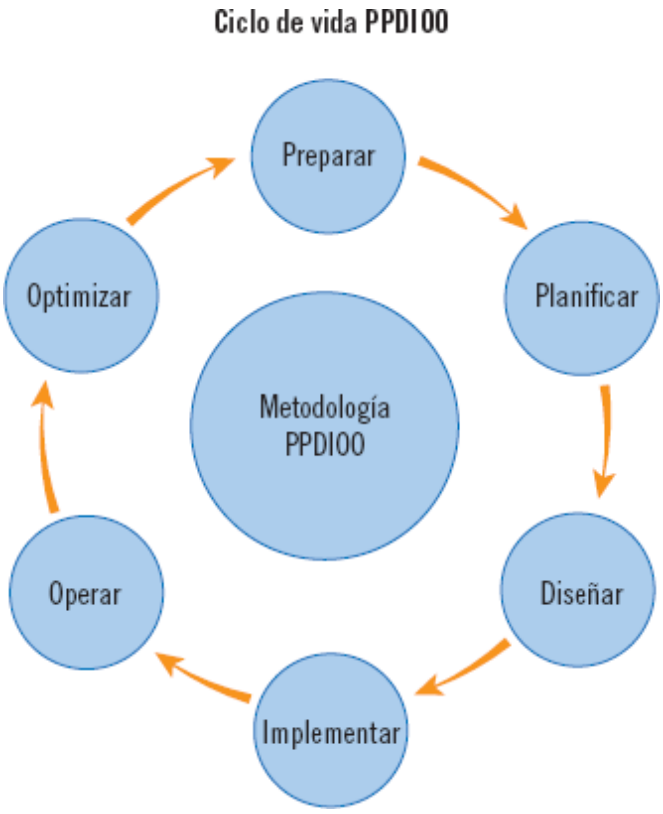
- Configuración e instalación de servicios, sistema de respaldo y scrips personales
- Automatización de tareas
- Intalación y seguimiento a programas de seguridad
- Mantenimiento de los servidores

Asi también se hará uso de la metodologia PPDIOO que consiste en un ciclo de vida cuya función es mantener las actualizaciones y convertirse en su sistema de gestión de negocios; este metodo se enfoca en definir las actividades que son requeridas por la tecnología que permite la optimizacion de su desempeño del ciclo de vida de la red. (Lagla, 2019)

Dentro de los beneficios que tiene la metodologia estan el manejo sobre la complejidad de la red en expansión, asi también cuenta con mejorar la estabilidad, disponibilidad, escalabidad y seguridad con ayuda del sistema planeación, diseño, mantenimiento y la optimización. Asi también ayuda al incremento de la red en la gestion del negocio y retorno de inversión, de esta manera contribuyen a la disponibilidad de la red. Dentro de las fases o componentes de la metodologia se encuentran los siguientes.

Figura 1

Ciclo de vida PPDIOO



Nota. El gráfico muestra el ciclo del PPIOO, con todas las fases correspondientes, adaptado de Saavedra, 2021.

Preparar: Se establece los importes financieros para identificar la tecnología que se encarga de dar soporte a la red.

Planear: Se realiza la evaluación y caracterización de red, en función de la mejora de prácticas y funcionamiento.

Diseñar: Se desarrolla los requerimientos y componentes necesarios de diagramas de red.

Implementar: Se realiza la integración de dispositivos que no intervengan en el funcionamiento de la red y que el monitoreo se mantenga vifente.

Operar: Se tienen administración de todas las actualizaciones, desempeño y corrección de errores.

Optimizar: La administración de la web es proactiva, se absuelven cuestiones que talvez afecten al funcionamiento de la red.

e) Distribuciones de GNU/Linux

El sistema Linux no es el único sistema debidamente estructurado, pues existen tres elementos primordiales de software que componen un sistema GNU/Linux tales como:

- Kernel Linux; es la pieza clave del sistema, pero sin aplicaciones de utilidad y compiladores el sistema no está completo.
- Las aplicaciones GNU; para el desarrollo Linux se llegan a complementar con el software de la FSF como parte del proyecto GNU.
- Software de terceros, el sistema GNU/Linux se complementa con software de terceros incorporando un conjunto de aplicaciones de mayor uso; además, suele ser recurrente incluir algún software propietario.

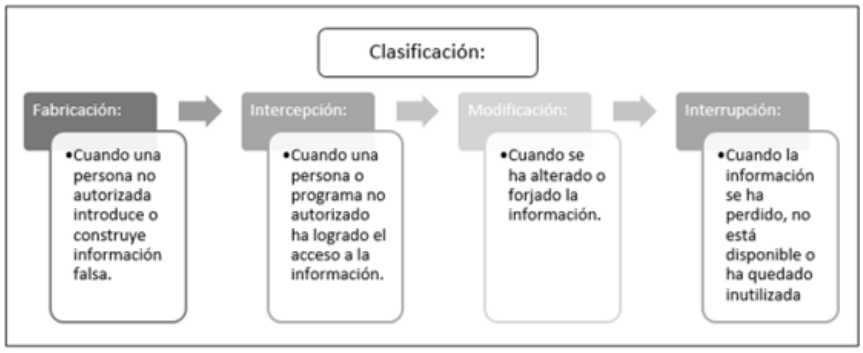
En síntesis, debido a que gran parte del software son de código abierto o libre como Kernel, software GNU o de terceros, esto hace que su evolución sea más rápida, obligando al sistema GNU/Linux a elegir el software que debe instalarse en el sistema (Jorba, 2010).

f) Acciones en contra de la seguridad de la Información

Dentro de los parámetros de acciones realizadas con objeto de comprometer la seguridad de la data según la Oficina de Seguridad para las Redes Informáticas (2007) pueden clasificarse en:

Figura 2

Acciones en contra de la seguridad de la Información

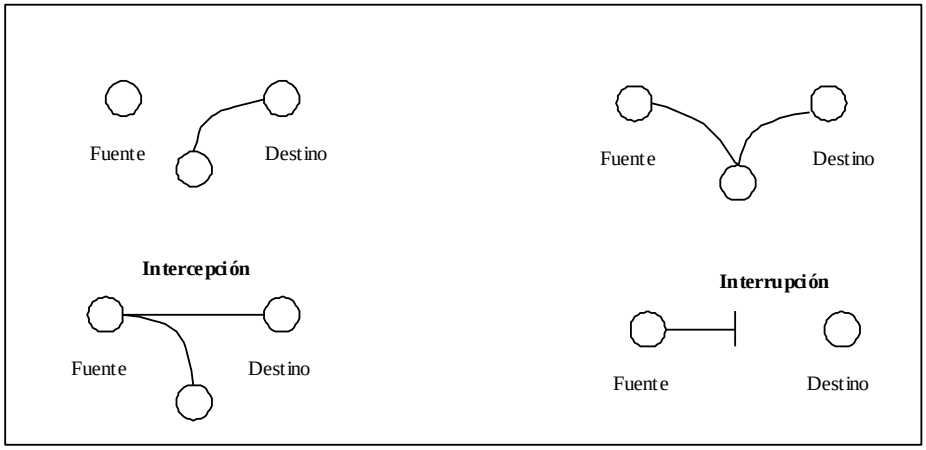


Nota. El gráfico representa la clasificación de las acciones de seguridad adaptado de "Oficina de la Seguridad para redes informáticas", por Oficina de Seguridad para redes informáticas, 2014, p. 16.

Asimismo, en la siguiente figura se puede apreciar dichas acciones:

Figura 3

Acciones de la seguridad informática



Nota. El gráfico representa la Clasificación de las acciones de seguridad. Adaptado de "Oficina de Seguridad para redes informáticas", por Oficina de Seguridad para redes informáticas, 2014, p. 20.

Dimensiones

- Funcionalidad

Hace referencia a las capacidades y funciones que deberia tener un sotftware, de forma que satisfaga las necesidades requeridas. Dicha dimension tiene como indicadores (Aizprua et al., 2019):

- Nivel de estabilidad del servidor
- Cumplimiento de servicio que brindan a la red

- Confiabilidad

Hace referencia las capacidades del software de seguir operando y este disponible para su uso en un determinado tiempo. El cual cuenta con los indicadores (Aizprua et al., 2019):

- Tolerancia a fallos, que ve que el sistema no colapse frente a situaciones no previstas, como un mal uso de la interfaz o fallas debido a causa externas como el ambiente.
- Recuperabilidad, que ve pro restablecer un rendimiento luego de ocurrido la falla, como la interrupción en la red.

Entorno virtual en Linux

Dentro del ámbito de la enseñanza el entorno virtual constituye una serie de facilidades informáticas y telemáticas tanto para la comunicación y el intercambio de información donde se realizan procesos de enseñanza y aprendizaje. No obstante, la naturaleza del medio impone la participación en determinados momentos del proceso. Asimismo, el afrontamiento de un entorno virtual de enseñanza presenta el problema

de heterogeneidad debido al ancho de banda. A su vez, el diseño de un entorno virtual de aprendizaje involucra dos niveles que se mencionan seguidamente (Méndez, et al. , 2017).

Dentro del entorno virtual en la actualidad se presentan diversas tecnologías, como lo son QEMU/KMV, VMWARE, LINUX, entre otros. Donde resalta la tecnología Open Source de virtualización como lo es PROXMOX en su versión 6.0, el mismo que involucra un disco para la instalación de un servidor físico o para la instalación del sistema en máquinas virtuales (Ochobits, 2015).

a) Interfaz del usuario

Se tiene en cuenta tres tipos de usuarios tales como profesores, alumnos y administradores del sistema para el nivel de hardware y software.

b) Modulo de Enseñanza- Aprendizaje

En este módulo se implementan todos los servicios para el desarrollo de un adecuado proceso de enseñanza y aprendizaje. Asimismo, el interfaz para el usuario tiene su base en un navegador con la finalidad de lograr simplicidad e independencia de la plataforma empleada, dicha interacción se da a partir de formularios en HTML.

c) Virtualización con Proxmox

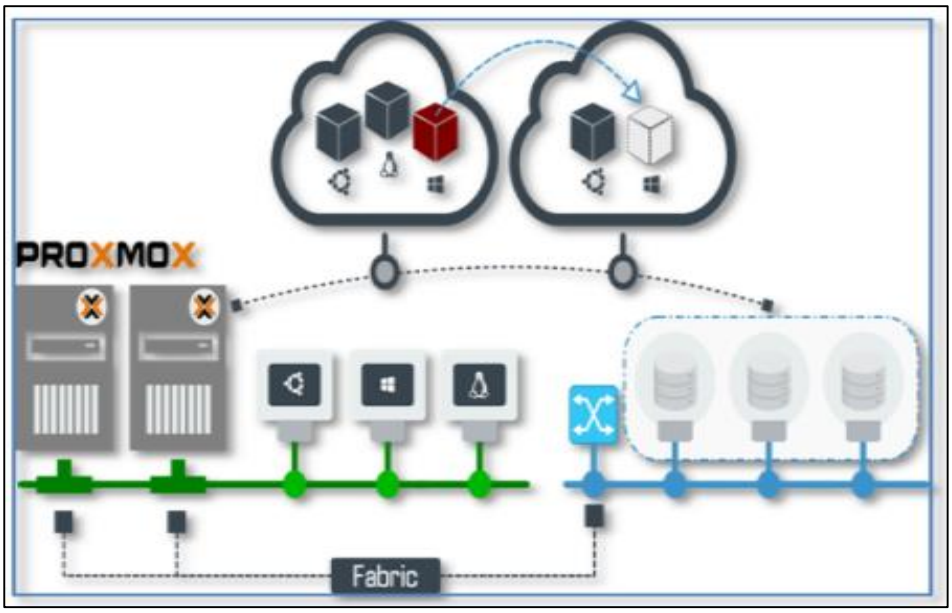
Fue diseñado para administrar cientos o incluso miles de máquinas virtuales, es un software libre y sin costo. Esta baso en dos tecnologías de virtualización una de ellas es Kernel (KVM), el cual asienta las creaciones de máquinas virtuales en sistemas de Linux en Hardware para una virtualización completa y Open Vz, para la virtualización de contenedores. Las ventajas del sistema son:

- Es gratuito, se innova constantemente y las actualizaciones son de acceso libre.
- No depende de los proveedores
- Tiene un Núcleo Linux
- La ejecución de tareas es sencilla y se puede hacer a través de la interfaz web de Proxmox de nombre HTML5.
- Ofrece alta disponibilidad y escalabilidad sin límite porque permite trasladar máquinas en cada nodo sin necesidad de apagar la máquina virtual.
- Es aplicable para la mayoría de sistemas operativos
- Tiene una grande comunidad de usuarios
- Cada nodo tiene su propio administrador web, el cual mediante un nodo orquestador centraliza el control.
- LXC provee un entorno virtual que tiene su propio espacio de procesos y redes.
- Permite administrar, programar y restaurar backups.
- Mediante el Snapshot Live, se pueden hacer copias instantáneas de las Máquinas Virtuales incluyendo el contenido de la RAM, su configuración y el estado de los discos virtuales.
- Permite una conexión de manera directa con el administrador grafico o virtual.

– Permite a través de gráficos, mostrar la información de las máquinas virtuales, el tráfico de red y el grado de aplicación del procesador y otros aspectos.

Figura 4

Virtualización en Proxmox



Nota. La imagen muestra el Proceso de Virtualización a través de Proxmox. Adaptado de Proxmox. Elaborado por Proxmox.

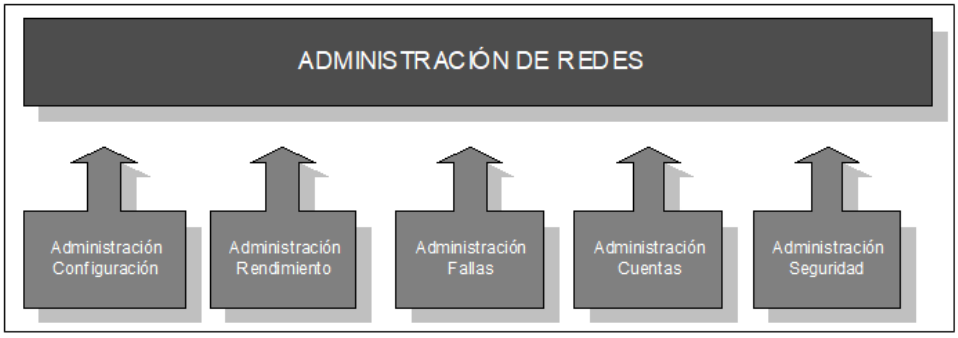
La figura detalla el proceso de virtualización a través del uso de un switch que hace funcionar los clústeres de dos dispositivos necesarios para el acceso a las máquinas virtuales. Seguido del uso de un segundo swicth que asigna recursos de almacenamiento en red, lugar donde los discos duros virtuales están ubicados.

Gestión de redes en Linux

Dentro de la administración de redes se encuentran las siguientes funciones:

Figura 5

Áreas de Administración de Redes



Nota. La figura representa la administración de Redes. Adaptado de "Funciones de la administración de redes" por V. Sánchez, 2018, p. 10.

A. Administración de seguridad

Dentro de la administración de la seguridad se tiene en cuenta:

- Seguridad física.
- Seguridad Lógica.

B. Gestión de redes

Dentro de los formatos regulares más sencillos se acentúan los destinados al descubrimiento de equipos de red, la competencia de administrar equipos de seguridad, el bloqueo de los mismos y la competencia de brindar servicios de alta eficiencia (QoS) dentro de diferentes equipos, como:

- Syslog.
- Protocolo para gestión de Red simple.

Puertos TCP tradicionales y puertos TCP al usar SSL

Tabla 3

Puertos TCP tradicionales y puertos TCP al usar SSL

Protocolo	Puerto TCP asignado	Protocolo protegido por SSL	Puerto TCP asignado
https	80	https	443
Smtp	25	Ssmtp	465
Pop3	110	Spop3	995
telnet	23	Telnets	992
ftp	21	Ftps	989 (data), 990 (control)
nntp	119	Nntps	563
idap	389	Ssl-idap	646

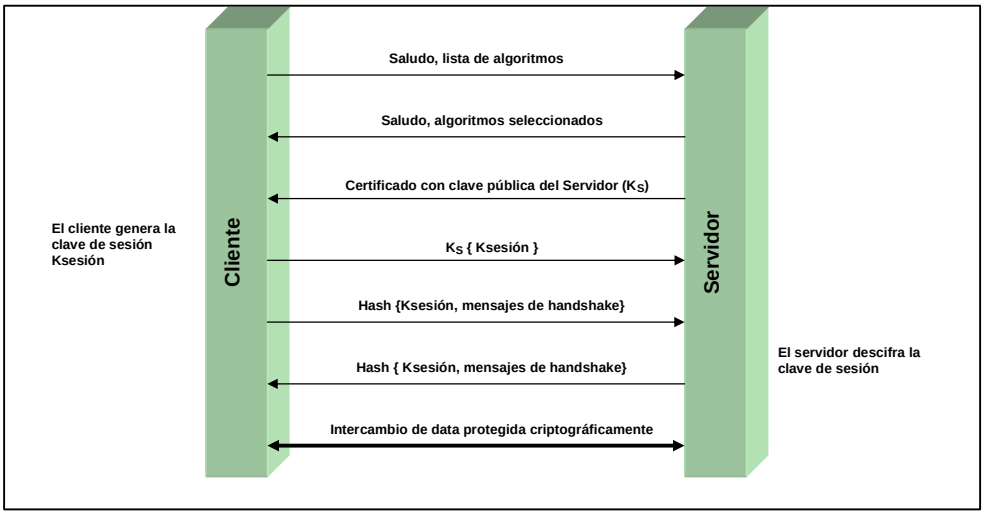
Nota. En la presente tabla se aprecia los puertos TCP tradicionales y puertos TCP SS.

Adaptado de *"Principales Puertos TCP"* por Villagómez, 2017, p.8.

Modelo de operación del protocolo SSL

Figura 6

Modelo de operación bajo el protocolo SSL



Nota. El gráfico representa el Modelo de operación del protocolo SSL. Adaptado de "Protocolo SS", por I. García, Revista Dialnet, p.20.

Estructura y Datagrama de Internet

Tabla 4

Estructura y Datagrama de Internet

Versión	**Long. Cab**	**Tipo de servicio**	**Longitud total**
Identificación		Flags	Offset fragmento
Tiempo de vida		Protocolo	FCS cabecera
Dirección IP fuente			
Dirección IP destino			
Opciones			Relleno
DATOS			

Nota. En la presente tabla se aprecia la estructura y Datagrama de Internet, Adaptado de “Internet Protocol”, por IONOS, 2018, p.4.

Algunos de los puertos más comunes y los servicios que se ejecutan sobre ellos son los siguientes:

Tabla 5

Puertos más comunes y los servicios que se ejecutan

Puertos más comunes y Servicios Ejecutores	
23 Telnet	Telnet proporciona una conexión de terminal a un sistema remoto.
25 SMTP	Se encarga de evitar y almacenar correo electrónico.
53 DNS	Sistema de nombre dominio.
80 HTTP	World Wide Web (Telaraña mundial)
110 POP3	Acceso remoto al correo electrónico
143 IMAP	Otro método de acceso remoto al correo electrónico
161SNMP	Sistema de gestión de red simple

Nota. En la presente tabla se aprecia los puertos más comunes y servicios financieros. Adaptado de “Internet Protocol” por IONOS, 2018, p.25.

Protocolo Syslog

Para almacenar, interpretar y mostrar los mensajes, los administradores de la red cuentan con diversidad de opciones, los cuales brindarán un incremental impacto dentro del esquema de la red, donde la metodología con mayor injerencia es el protocolo Syslog, el cual permite acceder a los mensajes que el sistema brinda a los dispositivos. Asimismo, Syslog para el envío de notificaciones a recopiladores, por lo general emplea el puerto UDP 514. (Walton, 2018)

Del mismo modo, Walton (2018) menciona que el protocolo Syslog admite que un dispositivo pueda emitir mensajes de notificación por medio de una red para que estos sean almacenados en un dispositivo.

a) Configuración del Syslog

El protocolo Syslog manifiesta una configuración básica similar en dispositivos Cisco IOS y los IOS XR. Donde se incluye fecha y hora en el mensaje generado, además se desactiva el servicio en la consola y elimina el buffer de memoria para almacenar mensajes de Syslog, posterior a ello se especifica el nivel de severidad de los mensajes de syslog, luego prosigue la definición de dirección IP del servidor Syslog para almacenar dichos mensajes y por último se precisa el nivel de severidad de los mensajes que han de emitirse a los servidores de Syslog en una escala de 0 a 7, donde 0 representa eventos de gran criticidad y 7 a los menos críticos (Walton, 2018).

b) Funcionamiento de Syslog

Para dispositivos pertenecientes a la red Cisco, el protocolo Syslog inicia con el envió de referencias por parte del sistema y el análisis del comando debug ante el desarrollo del proceso de inspección interna del equipo. Igualmente los mensajes

Syslog pueden enviarse por medio de una red a un servidor del Syslog externo, los mismos que brindan la oportunidad de ser recuperados sin ingresar al dispositivo, esto debido a que dichos mensajes pueden enviarse a un búfer interno, los cuales pueden verse a través del CLI del dispositivo. Entre los destinos más frecuentes para los mensajes Syslog están el búfer de registro,las líneas de consola y el de servidor de Syslog. Igualmente, se puede tener un control de los mensajes por medio de un dispositivo Telnet, SSH (Walton, 2018).

- **Formato de los mensajes de Syslog.** Para generar mensajes como consecuencia de los fenómenos de red cada alerta dirigida por el sistema Syslog presenta determinado rango de gravedad e instalación. Mientras menor sean los rangos de nivel mayor necesidad de alarmas Syslog se manifestarán.
- **Servidor de Syslog.** Para los indicativos de Syslog es necesario la instalación de un servidor en una estación de trabajo en la red, donde se presentan las versiones de freeware y shareware. Asimismo, el servidor Syslog proporciona una interfaz práctica para utilizar y ver el resultado, donde se analiza los mensajes por medio de columnas predefinidas fáciles de interpretar.

Protocolo SNMP

Se le conoce como el protocolo administrativo de red simple, además es adoptado mayormente para administrar y monitorizar elementos de red, en el cual gran

parte de sus factores de red en el grado profesional se acompañan de un agente SNMP incluido (ManageEngine, 2010).

Asimismo, el protocolo SNMP es conocido tambien como el protocolo simple de Administración de redes, el cual busca facilitar la transacción de data administrativa para los dispositivos de red e incluso brinda a los administradores el seguimiento funcional de la red, brindando soluciones a las problemáticas apoyando su desarrollo. En la siguiente tabla se puede apreciar diversas carácterísticas (Doctors y Vecchiotti, 2012).

Tabla 6

Familia de protocolos de internet

Familia	Familia de protocolos de internet
Función	Hace más fácil el intercambio de información de administración entre dispositivos de red
Versión final	SNMPv3
Puertos	131/UDP, 162/UDP
Ubicación en la pila de productos	IP (IPv4 e IPv6)
Estándares	RFC 1157 (SNMP, 1990) RFC 3410 (SNMPv3, 2002)

Nota. En la presente tabla se aprecia la familia de protocolos de internet. Adaptado de *"Sistema de gestión y monitorización de fallas para clientes de Sannet"* por A. Doctors, 2012, p. 14.

Además, por medio del SNMP se puede transformar los parámetros administrativos, el mismo que permitirá el acceso a las variables mediante un

community name, donde se distinguirá la estación de supervisión, elementos activos de la red, variables MIB además del protocolo UDP (Guerrero, 1998).

c) Componentes básicos del SNMP

Una red administrada por medio del protocolo SNMP manifiesta tres componentes necesarios (Guerrero, 1998):

- En primer lugar, los dispositivos administrados, que se desarrollan mediante un modelo de red el cual involucra un agente SNMP, encargado de recolectar y almacenar información de administración.
- En segundo lugar, están los agentes; un modelo de software administrativo de red resistente a un equipo controlado.
- En tecer lugar, están los sistemas administradores de red o conocido bajo las siglas NMS, donde se realizan aplicaciones que son controladas por dispositivos administrados.

d) El SNMP en Linux

Dentro de los programas más reconocidos del SNMP se encuentra el CMU-SNMP, que fue diseñado por la Universidad de Carnegie y posteriormente migrado a Linux por Schoenfelder, E. y Schoenwaelder, J. con la finalidad de lograr la compatibilidad hacia el estándar SNMPv1, el mismo que incluye las funcionalidades recientes del SNMPv2.

Otra de las ventajas del paquete es que brinda a los diseñadores la oportunidad de desarrollar herramientas con mayor grado de dificultad de administración, las mismas que se centran en las capacidades de red de la difusión. Además, la instauración

del mismo dentro del sistema Linux es sumamente sencillo, pero en cuanto a la instalación original es distinta, dada su organización apoyada en los ejecutables pre-compilados de los implementos de gestión. Por lo que primero debe decidir si opta por la distribución con fuentes o ejecutables, asimismo, en cualquier caso la distribución binaria se instala y funciona sin manifestar problemas en Linux.

e) Protocolo puertos

Los protocolos de red se componen por un conjunto de reglas con la finalidad de enviar información a través de un canal de comunicación. Asimismo, dentro del protocolo puertos se encuentran el protocolo de internet, de acceso a la red de aplicación y de transporte (Jorge, 2012).

2.3. Marco conceptual

- **Software libre;** Este software se caracteriza por ser libre, imprescindible y con amplia disponibilidad, pero el hecho de que sea libre no significa que sea gratis (Gónzalez et al, 2003).
- **Linux;** Dicho sistema surgió en 1991 tomando como base a UNIX, adquiriendo el nombre de Linux y adaptándose al sistema GNU, dando lugar a las primeras distribuciones GNU/Linux, las mismas que incluían todas las herramientas para servidores y usuarios finales (Torres et al, 2006).
- **Seguridad perimetral;** La seguridad perimetral involucra un perímetro mediante el cual un dispositivo puede ofrecer la comunicación entre las

redes a través de un router secuenciado por un dispositivo de seguridad conocido como firewall (Davantis, 2019).

- **Protocolo Syslog;** Para este tipo de protocolo se precisa cierto tipo de mensaje con tres campos el cual se comunica por medio del puerto UDP 514, permitiendo a la vez llevar registros de las diversas máquinas en un solo punto (Oscar, 2010). Asimismo, el protocolo Syslog se encarga de proveer transporte y funcionalidad para el envío de mensajes por medio de las redes IP para así agrupar servicios de Log. Además, dentro de las estructuras de Syslog se maneja una estructura sencilla y como protocolos de puertos de comunicación pudiéndose aplicar el UPD o el TCP (Méndez, 2016).
- **Protocolo SNMP;** Dentro de las principales funciones del Protocolo SNMP está el facilitar la monitorización y control, centrando todos los componentes de una red tipo informática (Digital Guide Ionos, 2019). Del mismo modo el protocolo SNMP, es aceptado de manera amplia debido al conjunto de comandos tales como: GET que se usa para recuperar uno o más valores del dispositivo almacenado, GET NEXT el cual recupera el valor del próximo OID del árbol MIB, GET BULK el cual recupera datos de una tabla MIB grande, SET es de gran ayuda para que los administradores puedan modificar o asignar el valor del dispositivo almacenado, TRAPS es la señal para el administrador SNMP por parte del agente, INFORM es un tipo de comando parecido

al TRAP que incluye la confirmación del administrador SNMP y RESPONSE cuyo comando transporta valores y señales de acciones regidas por el administrador (Fava, 2015).

- **Proxmox;** Pudiéndose entender a Proxmox VE como la plataforma completa de código abierto dirigida a la virtualización organizacional que genera la unificación del hipervisor KVM y los contenedores LXC; el nivel de almacenaje referente por software y la operatividad de red mediante una misma plataforma, generando la administración de los clústeres de alta disponibilidad de forma sencilla al igual que los instrumentos de recuperación frente a una calamidad en la interfaz de gestión web (Proxmox, 2019).
- **Proxmox VE "Virtual Environment";** El Proxmox es una potente plataforma de virtualización con un nivel 100% empresarial y sin límites en su uso como servidor (Nodo) para colocar máquinas virtuales o integrarlo a un Cluster (Goldman, 2016).
- **NethServer versión 6.10;** Se trata de una distribución basada en Linux que se orienta a actuar como servidor en pequeñas y medianas oficinas, por lo general se basa en las populares distribuciones CentOs y Red Hat Enterprise Linux (De luz, 2016).
- **Zabbix y Grafana;** Se trata de un script de Shell simple (bash) que instala los paquetes Docker, Docker – compose y jq es implementa los

contenedores Zabbix desde las imágenes oficiales de Zabbix docker a través del uso de Docker – compose (Ersen, 2020).

- **Moodle en Ubuntu Server;** El escenario Moodle se tornó en una plataforma de gestión de aprendizaje en línea la cual es de código abierto bajo la licencia Pública General GNU más funcional y dinámica y Moodle está disponible para entonos web bajo extensiones Ubuntu Server (Damián, 2019).
- **Sistema de Prevención de Intrusión**; EL IPS es una metodología que acopla métodos cortafuegos y otros Sistemas de detección de Intrusos (IDS); siendo una aplicación asentada en Linux, que permite el monitoreo del tráfico del sistema o de la red, haciendo una indagación constante de abuso o actividad maliciosa que posteriormente pueda generar notificaciones al sistema. Logra prevenir agravios que accedan a la red local analizando y registrando los paquetes de datos y haciendo un reconocimiento a aquellos paquetes de datos propios del sensor que, al identificar al agresor, se declina el acceso, bloqueándolo y registrando como amenazantes.
- **Sistema de Prevención y Detección de Intrusiones.** Sistema de prevención y detección de intrusos (IDPS), que se divide en dos, dentro de los que se presentan los sistemas que utilizan los métodos IDS e IPS, la utilización de IDS se genera únicamente para monitorear el nivel de tráfico de red o el análisis de los paquetes de datos cuando existe una

intrusión y por otro lado se tiene al IPS, el mismo que puede usarse para la detección o bloqueo de amenazas. Existen dos tipos de detección de amenazas tanto para IDS e IPS, asentado en host o en red.

- **Cortafuegos.** Se definen como un mecanismo cuyo propósito es resguardar hardware y software. Dicho resguardo se genera mediante filtrado, limitación o negación de acceso a una cantidad o la totalidad de enlaces/actividades concernientes a un segmento de una red privada con redes externas que no se encuentran incluidas en su alcance.
- **Snort.** Definida también como una herramienta ejecutada bajo el sistema Linux, la misma que se puede configurar para la detección de intromisiones o amenazas, siendo capaz de analizar paquetes que traspasan la red de tráfico en tiempo real e inicio de sesión dentro de la base de datos. De igual manera, logra detectar diferentes amenazas originadas de forma externa a la red; pudiéndose utilizar en plataformas de sistemas operativos Linux, Fress BSD, Debian y Windows.

CAPÍTULO III: MÉTODO

3.1. Tipo de investigación

La investigación es aplicada, debido a que las características de la investigación reúnen las condiciones para la realización de un estudio de tipo experimental. Dado que busca la ampliación de conocimientos y la solución de problemas mediante la aplicación directa de un sistema de red perimetral en la red local de la institución de estudio.

El nivel de investigación es explicativo dado que pretende establecer las causas de un hecho que se estudia, y explicar el porqué de los sucesos y las condiciones que manifiesta o la relación entre dos o más variables. El estudio servirá para explicar los resultados e impactos de implementación en la red local.

La investigación tiene un enfoque cuantitativo, porque mediante la recopilación de información se verifica la hipótesis a través de la medición numérico y el análisis estadístico, para comparar los resultados y determinar la relación en variables, patrones de comportamiento o la prueba de teorías.

3.2. Diseño de investigación

La investigación tiene un diseño experimental dado que se realizó un primer análisis en base a la situación inicial (pre - test) y un análisis final una vez implementado el sistema de seguridad perimetral (post - test), lo que determinó el impacto de la variable independiente en la dependiente.

3.3. Población y muestra

3.3.1. Población

La institución cuenta con un total de 107 profesores y 20 administrativos que laboran en la institución educativa, utilizan los equipos y la red en sus actividades diarias. Por tanto, la población de estudio se conforma por 127 personas que están directamente involucradas con el uso de la red.

3.3.2. Muestra

La muestra se determinó mediante la fórmula para poblaciones finitas:

$$n = \frac{127 \times 1.96^2 \times 0.5 \times 0.5}{0.05^2 \times (-1) + 1.96^2 \times 0.5 \times 0.5}$$

$$n = 95.63$$

La muestra está conformada por 96 personas dentro del personal administrativo y docente de la Institución Educativa.

3.4. Técnicas e instrumentos de recolección de datos

La información fue recopilada en la institución de estudio, mediante el uso de un cuestionario como instrumento para la obtención de los resultados que respondan a la seguridad perimetral.

Cuestionario: Fue adaptado en base a la investigación de Bautista Pillaca (2018), el cual tiene preguntas que responden a las dimensiones de confidencialidad, integridad y disponibilidad de la variable seguridad perimetral. El cuestionario cuenta con 17 preguntas que estan divididas para la dimensión de confidencialidad (1-9), dimensión integridad (10-14) y dimensión disponibilidad (15-17), que son evaluadas a traves de 4 opciones; bajo (1), regular (2), alto (3) y muy alto (4). Dicha adaptación se aplicó a través de la técnica de encuesta al personal administrativo y docente de la institución educativa de estudio en dos momentos del tiempo, uno antes de la implementación y otro después de la implementación.

Prueba, se hizo una simulación de prueba con la implementación en Linux y entorno virtual con el cual se pudo apreciar la funcionalidad y confiablidad del mismo.

3.5. Técnicas de procesamiento y análisis de datos

Para el análisis de los datos obtenidos a través de la aplicación del cuestionario que contiene ítems diseñados se evaluó los aspectos más relevantes de la variable dependiente. El procesamiento de la información se llevó a cabo mediante el Software estadístico Excel, en el cual se desarrolló el análisis de datos y la presentación de resultados.

Se aplicó una prueba de normalidad para el pre-test y post-test con el fin de conocer el tipo de datos del estudio.

Se hizo una simulación de prueba con la implementación del sistema de seguridad perimetral en Linux en una I.E. de Ilo para la medición del funcionamiento y la confiabilidad del mismo. Se elaboró un esquema de alta disponibilidad de

protección perimetral bajo un software Linux en un entorno de virtualización. Mediante las siguientes etapas:

1. Detectar las vulnerabilidades de la seguridad perimetral de una I.E. de Ilo.
2. Diseño de un modelo inicial de protección perimetral de red para la red local de una I.E. de Ilo, según las necesidades de seguridad de la institución.
3. Desarrollo y configuración de la segmentación y direccionamiento del sistema de seguridad perimetral firewall basado en software Linux.
4. Establecimiento temporal de una interfaz del dispositivo administrador con la IP local de una I.E. de Ilo para continuar el proceso de la implementación en software Linux.
5. Instalación de PROXMOX para la virtualización en Linux y la instalación de protocolos de seguridad Syslog y SNMP, como parte de la gestión del sistema de seguridad.
6. Integración del sistema de seguridad perimetral basado en software libre Linux con la gestión del monitoreo de los protocolos Syslog y SNMP bajo un entorno virtual en una I.E. de Ilo. (Ver anexo 5)

CAPÍTULO IV: RESULTADOS

4.1. Análisis de la situación actual

La Institución Educativa (IE) desea brindar seguridad y mitigación de ciberataques a su red interna haciendo uso de filtros y/o políticas de seguridad, estos equipos se encargarán de realizar funciones orientadas a la protección de ataques a las aplicaciones web e infraestructura interna del colegio, así como también de mantener y administrar un registro completo de los LOG, seguimiento y/o monitoreos generados por cada uno de estos respectivamente.

Actualmente, la institución educativa no cuenta con un nivel de seguridad perimetral, permitiendo que la organización sea vulnerable a ataques informáticos, de esta manera se realizará un análisis de la situación actual de la clínica en materia de seguridad informática, y así diseñar un sistema de seguridad perimetral considerando la infraestructura, los servicios, los protocolos, las aplicaciones, el acceso a Internet e Intranet.

Actualmente lo problemas encontrados con mayor frecuencia son:

Tabla 7

Análisis de vulnerabilidad 1

1	El sistema web permite la réplica de sus archivos mediante el uso de herramientas de software de clonación. La clonación de sitios web engaña a los usuarios, mostrando una web como si fuera la original, para luego acceder a la información de ellos.	Activo: Sistema web Afecta: Confidencialidad Amenaza: Clonación

Nota: Elaboración propia

Tabla 8

Análisis de vulnerabilidad 2

2	Al ingresar a un sitio web se descarga la mayor parte de archivos de dicho sistema web.	Activo: Sistema web Afecta: Integridad Amenaza: Ingreso de archivos maliciosos

Nota: Elaboración propia

Tabla 9

Análisis de vulnerabilidad 3

3	El sitio web carece de un certificado SSL/TLS, necesario para mantener la seguridad del tráfico de red. Los ciberdelincuentes utilizan la vulnerabilidad del sitio web para interceptar las transmisiones de información entre puntos.	Activo: Sistema web Afecta: Integridad y confidencialidad Amenaza: Pérdida y/o robo de información

Nota: Elaboración propia

Tabla 10

Análisis de vulnerabilidad 4

4	Los puertos presentan vulnerabilidades que permiten a los atacantes sobrecargar un servidor objetivo abriendo y manteniendo muchas conexiones HTTP simultáneas entre el atacante y el objetivo. Asimismo, permite a un atacante debilitar la complejidad del cifrado.	Activo: Sistema web Afecta: Confidencialidad y disponibilidad Amenaza: Robo de información

Nota: Elaboración propia

4.2. Resultados del Pre-Test

Una vez se haya recopilado el resultado de las encuestas, se procede a realizar el análisis de la información, para corroborar la situación actual y como lo perciben las personas involucras.

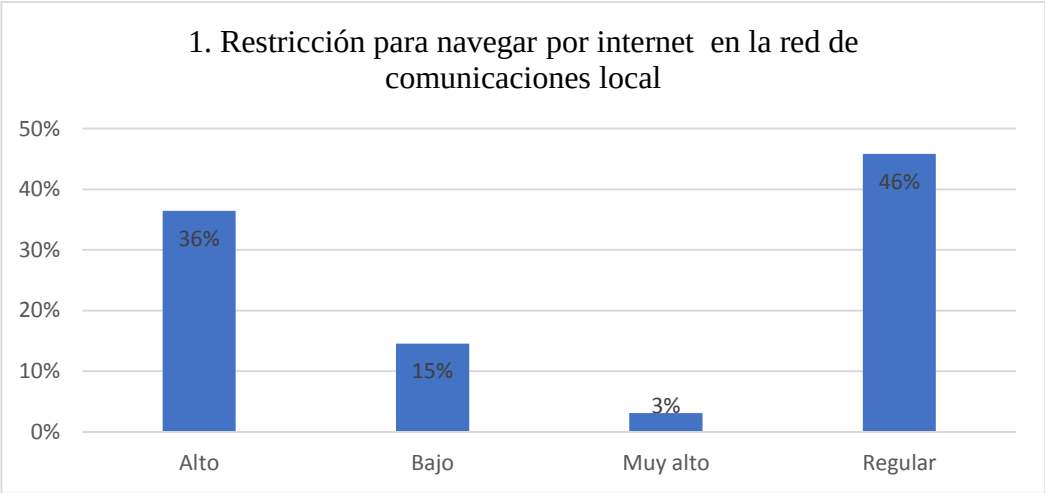
4.2.1. Análisis de la Dimensión Confidencialidad

Indicador: Nivel de políticas de seguridad

Para el análisis del primer indicador, se toman en cuenta las preguntas que ayudarán a entender mejor la percepción de las personas en cuanto a las políticas de seguridad.

Gráfico 1

Restricción para navegar por internet en la red de comunicaciones local

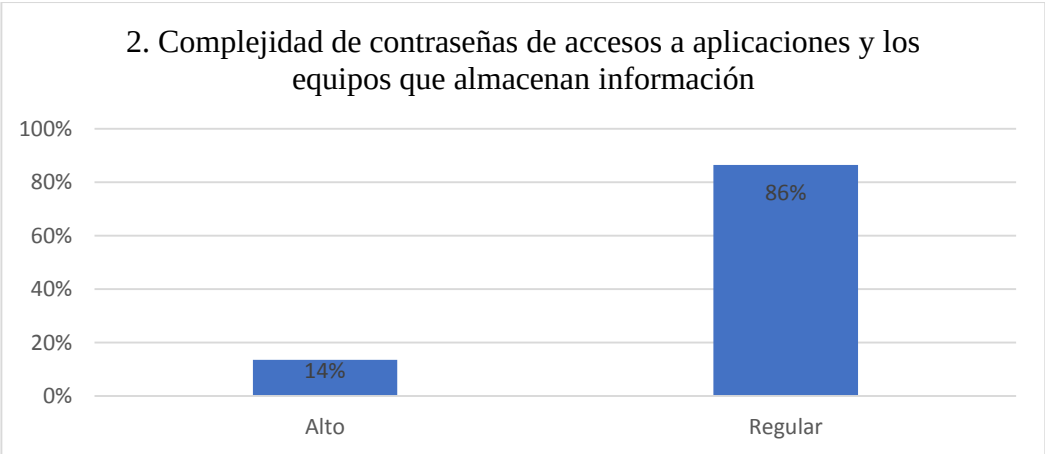


Nota: Elaboración propia

Los resultados muestran que para la mayoría de personas que contestaron la encuesta, con un 46%, tienen una percepción regular acerca de las restricciones en la red de comunicaciones local, por otro lado, un 36% lo percibe de manera alta, es decir que identificaron más restricciones o comportamientos y finalmente un 15% asegura no son frecuentes las restricciones.

Gráfico 2

Complejidad de contraseñas de accesos a aplicaciones y los equipos que almacenan información

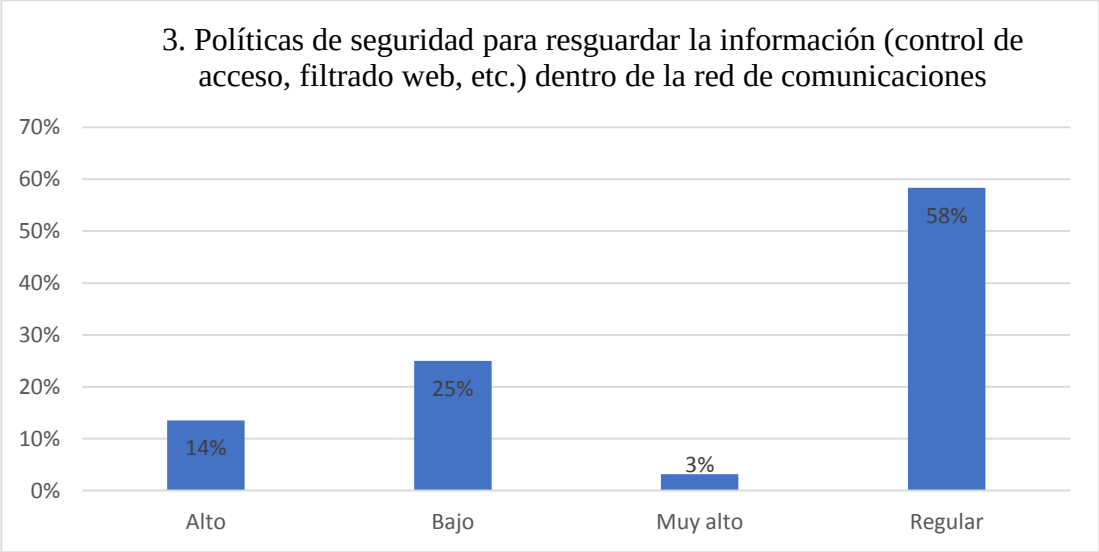


Nota: Elaboración propia

Para el caso de contraseñas para acceder a aplicaciones, la mayoría de las personas encuestadas con un 86% asegura que son de categoría regular, mientras que un 14% considera que son categoría alta, por lo que no tendrían un acceso rápido a las páginas.

Gráfico 3

Políticas de seguridad para resguardar la información dentro de la red de comunicación

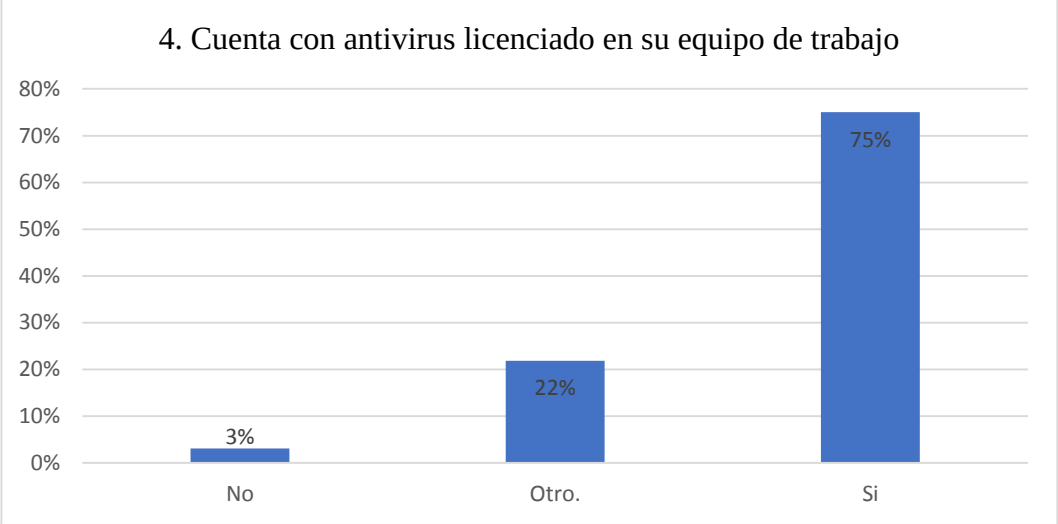


Nota: Elaboración propia

En la percepción acerca de la seguridad de información que existen, la mayoría con un 58% lo califica como regular, es decir que se puede filtrar la información, así como también un 25% lo considera de nivel bajo, en este caso los usuarios no se encuentran satisfechos con las políticas de seguridad.

Gráfico 4

¿Cuenta con antivirus licenciado en su equipo de trabajo?

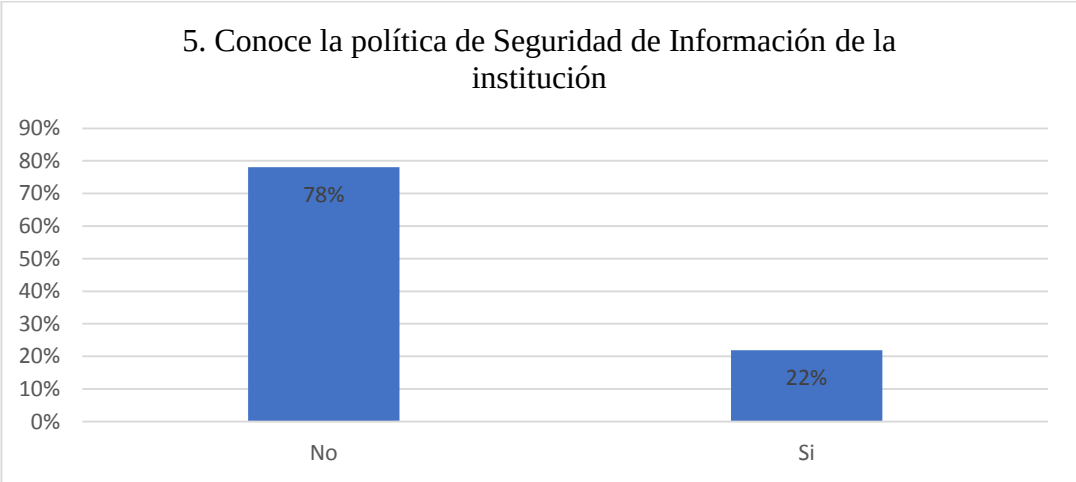


Nota: Elaboración propia

Las personas manifiestan en un 75% que, si cuentan con un programa de antivirus licenciado, es decir que resguardan por medio de un programa el cuidado de su información, un 22% no cuenta con un programa de antivirus, pero si con otras herramientas que ayudan al cuidado de su información, un 3% no cuenta con ningún programa de respaldo.

Gráfico 5

Conoce la política de seguridad de información de la institución

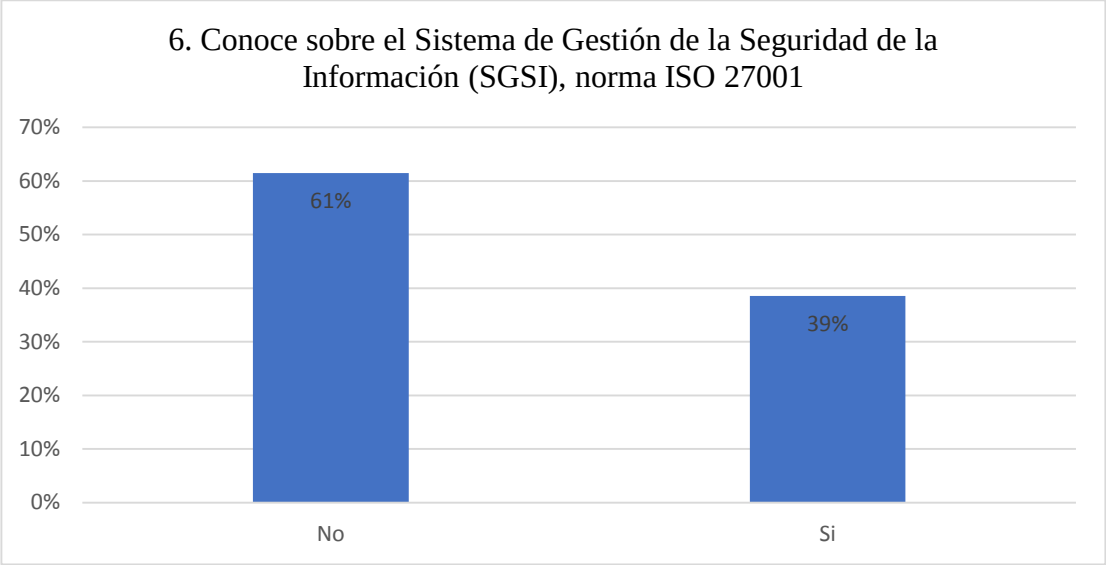


Nota: Elaboración propia

En caso de la política de seguridad de información un 78% asegura que no conocen los términos de seguridad, esto puede ser por la poca difusión o por la falta de interés de las personas, el otro 22% asegura que si conocen los términos bajo los cuales se rigen la institución.

Gráfico 6

Conoce sobre el sistema de gestión de la seguridad de la información (SGSI), normas ISO 27001



Nota: Elaboración propia

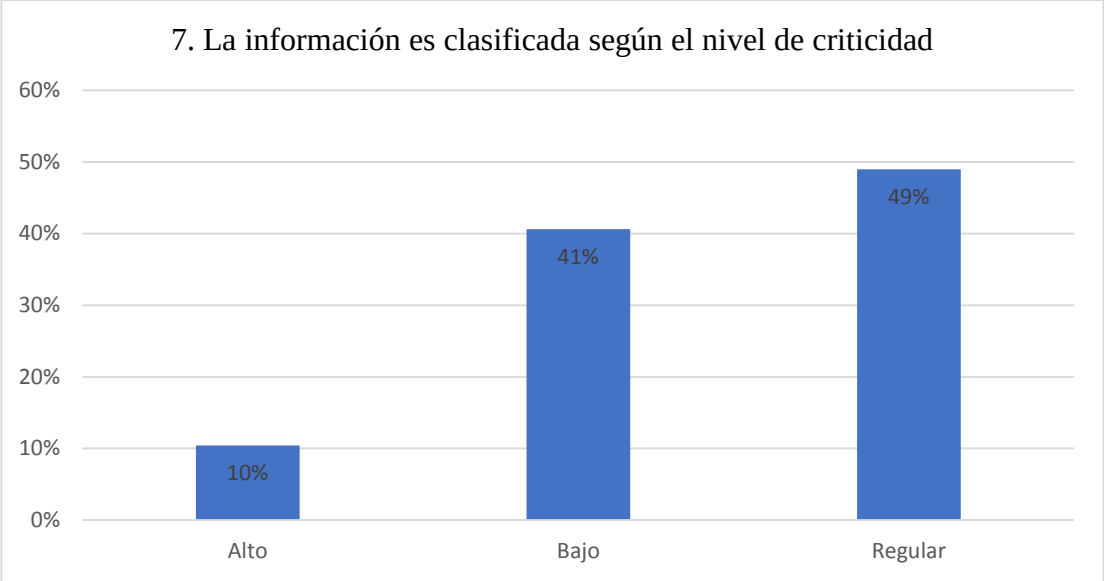
Para esta situación en caso del conocimiento acerca del sistema de gestión de seguridad o de la norma ISO 27001, la mayoría de las personas encuestadas con un 61% aseguran que no conocen los principios de ambas normas, sin embargo, un 39%, asegura que, si conocen por lo que están informados de los principios y regularidades del sistema de información.

Indicador: Nivel de confidencialidad

Se analiza las respuestas para identificar el nivel de confidencialidad percibido dentro de la institución.

Gráfico 7

La información es clasificada según el nivel de criticidad

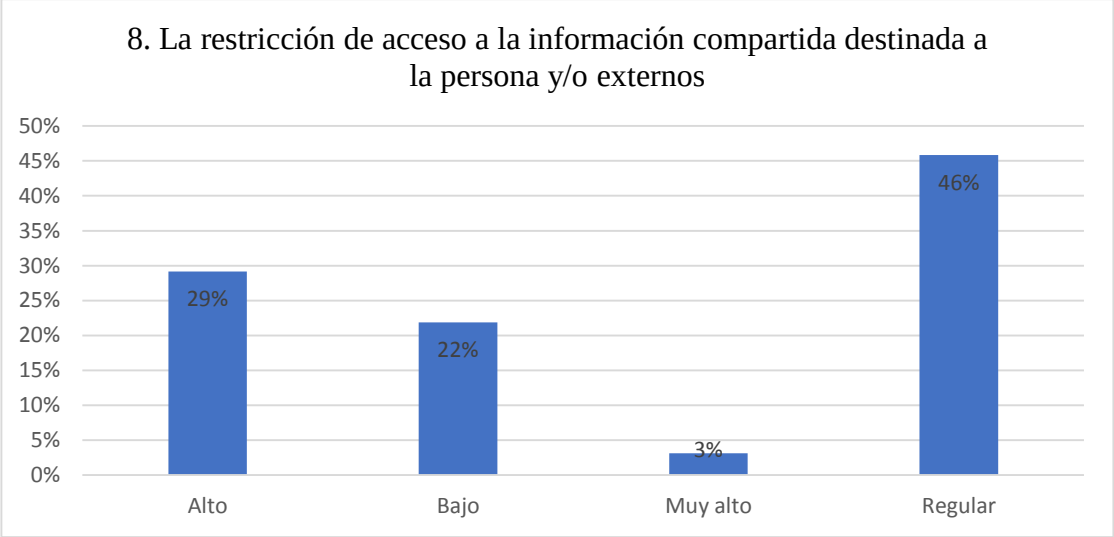


Nota: Elaboración propia

Para el aspecto de información clasificada según el nivel de criticidad, la mayoría percibe que es de forma regular, con un 49%, en caso del 41% afirma que es de forma baja, no se encuentran satisfechos con la información clasificada; sin embargo, un 10% asegura que el nivel de criticidad es de manera óptima, la cual calificaron como alto.

Gráfico 8

La restricción de acceso a la información compartida destinada a la persona y/o externos

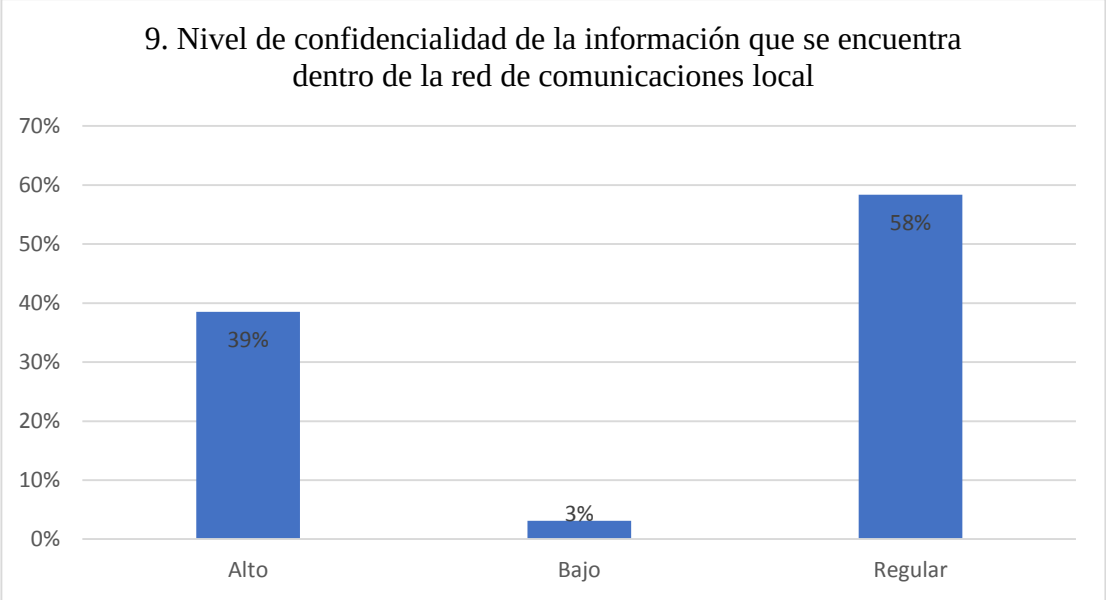


Nota: Elaboración propia

En caso de la restricción de acceso a la información compartida el 46% siendo la mayoría lo califica como regular, es decir que no perciben restricciones mayores o de fácil acceso; un 29% percibe una alta restricción mientras que un 22% asegura que hay una baja restricción por lo que se puede acceder sin inconvenientes a la información compartida.

Gráfico 9

Nivel de confidencialidad de la información que se encuentra dentro de la red de comunicaciones local



Nota: Elaboración propia

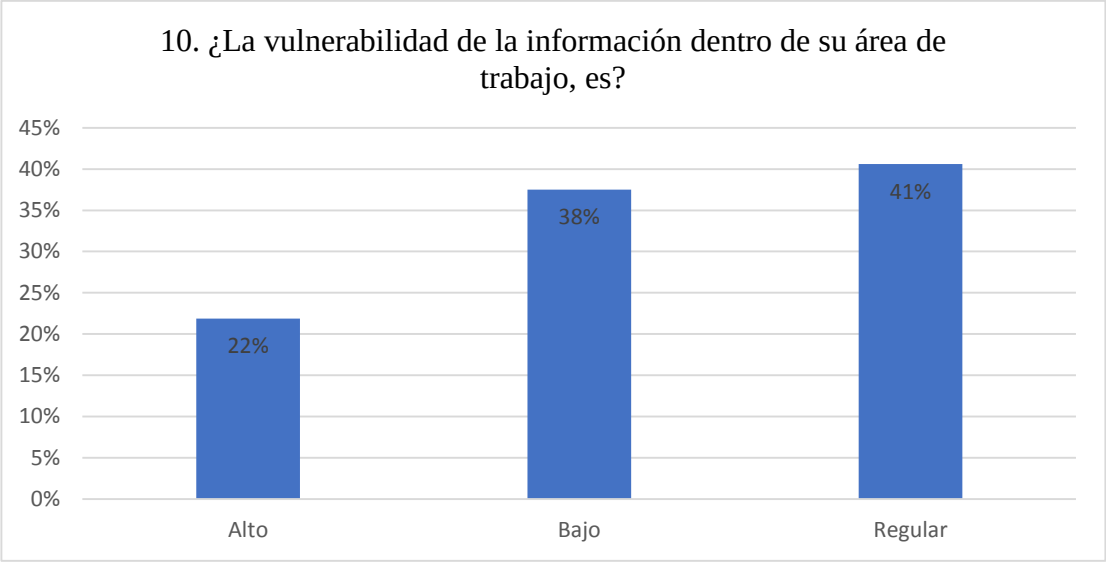
Para el caso de percepción acerca de la confidencialidad, la mayoría con un 58% afirma que es regular es decir que consideran que corren riesgo a que otras personas puedan a acceder a la información de las personas, un 39% afirma que es totalmente confidencial es decir confían en el nivel que proporciona la plataforma, asimismo, un 3% asegura que el nivel es bajo, es decir que se sienten expuestos a un robo de información.

4.2.2. Análisis de la Dimensión Integridad

Indicador: Nivel de riesgo de los datos

Gráfico 10

¿La vulnerabilidad de la información dentro de su área de trabajo, es?

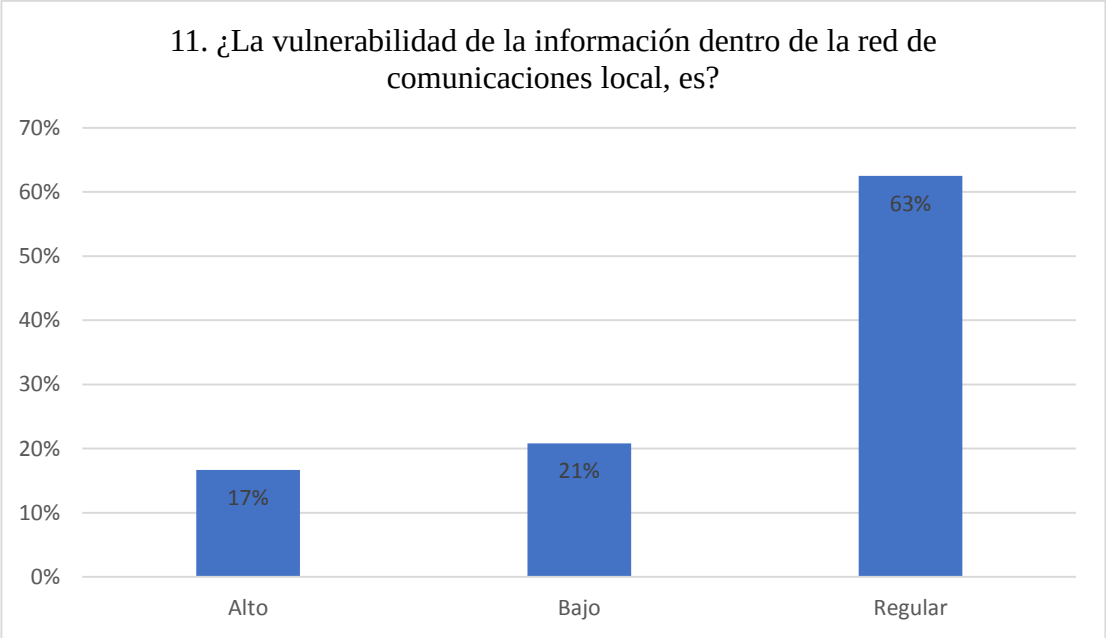


Nota: Elaboración propia

La vulnerabilidad de la información es calificada como regular con un 41%, las personas no se sienten seguras, pero tampoco sienten que haya riesgo para el acceso o filtración de su información, un 38% percibe que es de nivel bajo, por lo que no se consideran estar en riesgo por su información, mientras que un 22% si considera que hay una alta vulnerabilidad.

Gráfico 11

¿La vulnerabilidad de la información dentro de la red de comunicaciones local, es?



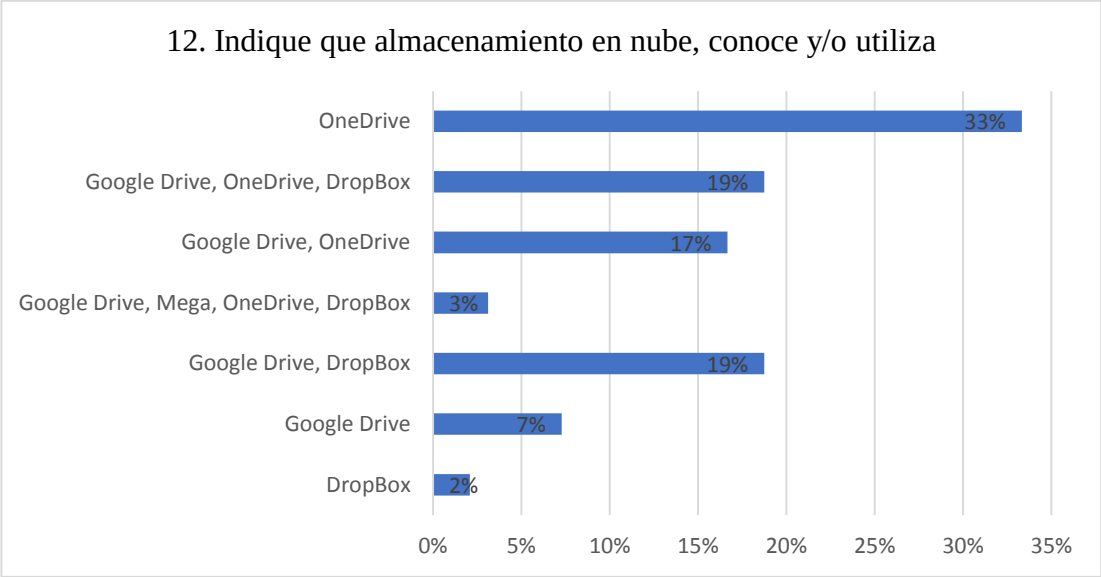
Nota: Elaboración propia

En caso de la percepción de vulnerabilidad de información en la red de comunicaciones es regular en caso de un 63% de las personas encuestadas, un 21% considera que no hay riesgo a la filtración de información, debido a que lo califican como vulnerabilidad baja, sin embargo, un 17% considera que hay una vulnerabilidad alta, es decir que percibe alto riesgo al robo o filtración de información en la red de comunicaciones local.

Indicador: Manipulación de datos

Gráfico 12

Indique que almacenamiento en nube, conoce y/o utiliza

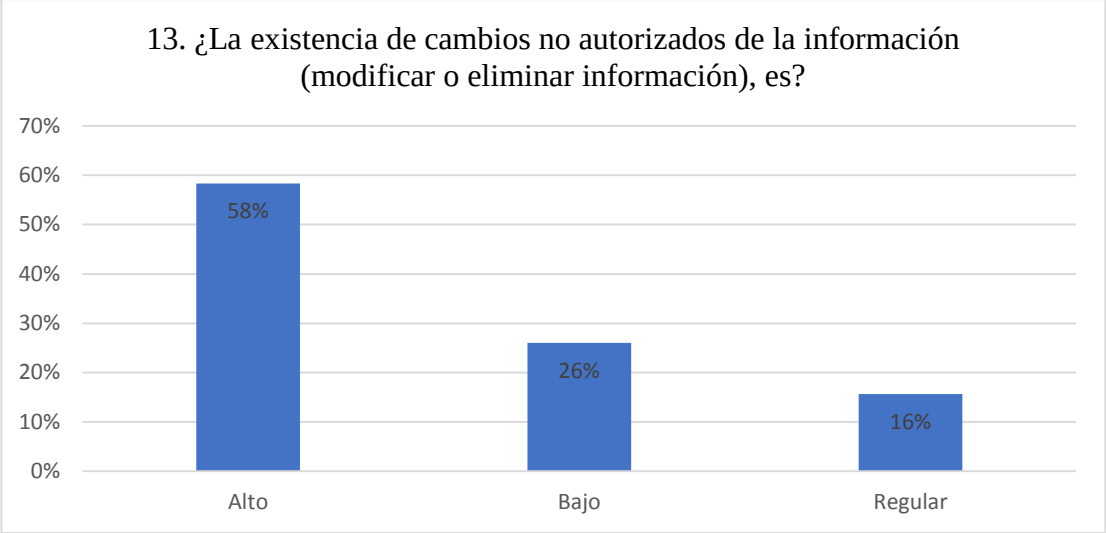


Nota: Elaboración propia

En este caso se identifica una variedad de respuestas, sin embargo, un 33% usa el servidor de OneDrive, un 19% tiene conocimiento de plataformas como Google Drive, One Drive y Dropbox, otro 17% conoce Google Drive y One drive, otro servidor que se pudo identificar es Mega, por lo que se puede interpretar que los encuestados hacen uso de plataformas en red para el almacenamiento de información.

Gráfico 13

¿La existencia de cambios no autorizados de la información (modificar o eliminar información), es?

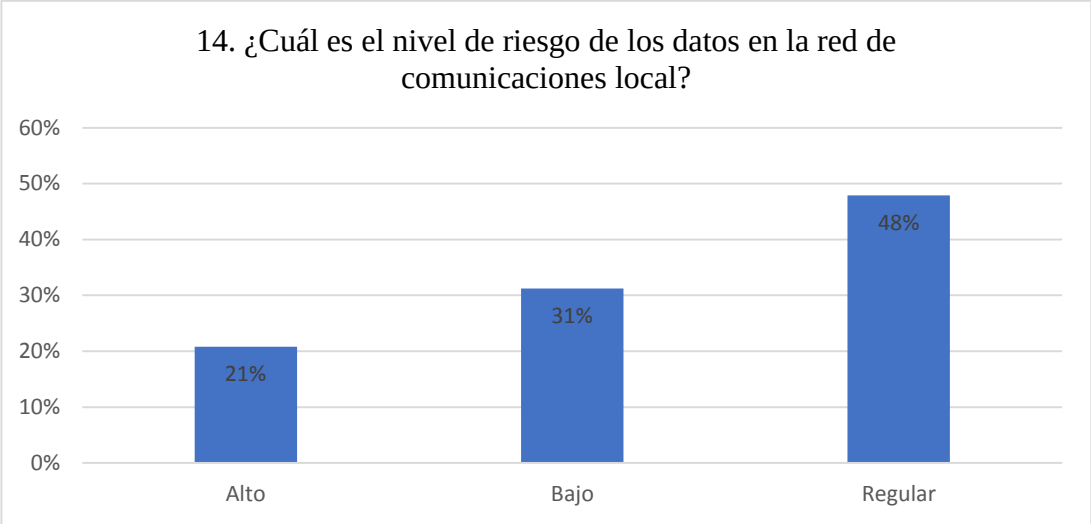


Nota: Elaboración propia

Para la existencia de cambios no autorizados de información los encuestados en un 58% consideran que es alto, es decir que hay modificaciones o eliminación de información de manera constante, para un 26% los cambios se dan de forma baja, no hay riesgo de modificaciones constantes, y para un 16% los cambios son de forma regular.

Gráfico 14.

¿Cuál es el nivel de riesgo de los datos en la red de comunicaciones local?



Nota: Elaboración propia

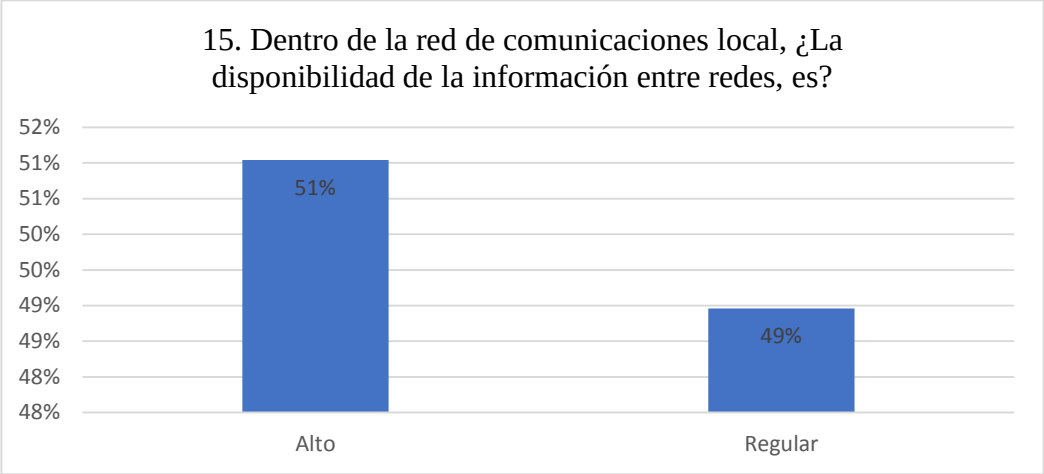
El nivel de riesgo de los datos en la red de comunicaciones es 48% regular según la percepción de los encuestados, es decir que no se sienten muy inseguros de los datos que proporcionan, por otro lado, un 31% se sienten seguros debido a que lo califican como bajo el nivel de riesgo; y el 21% considera que hay un alto riesgo de los datos en la red de comunicaciones.

4.2.3. Análisis de la Dimensión Disponibilidad

Indicador: Nivel de disponibilidad de los datos

Gráfico 15

Dentro de la red de comunicaciones local, ¿La disponibilidad de la información entre redes, es?

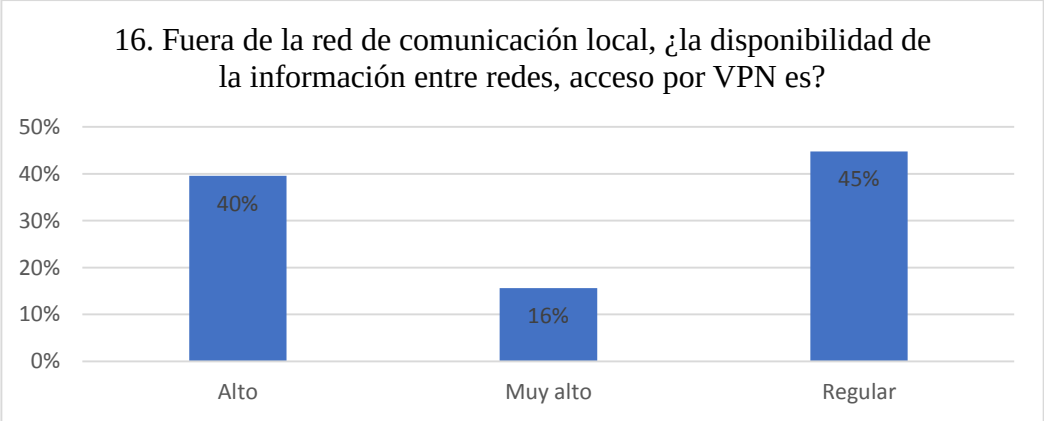


Nota: Elaboración propia

Para la disponibilidad de la información según la percepción de los encuestados se percibe que el 51% lo califica como alto, califican que, si existe una buena disponibilidad de información entre las redes, mientras que un 49% lo califica como regular, no percibe que exista demasiada disponibilidad.

Gráfico 16

Fuera de la red de comunicación local, ¿la disponibilidad de la información entre redes, acceso por VPN es?

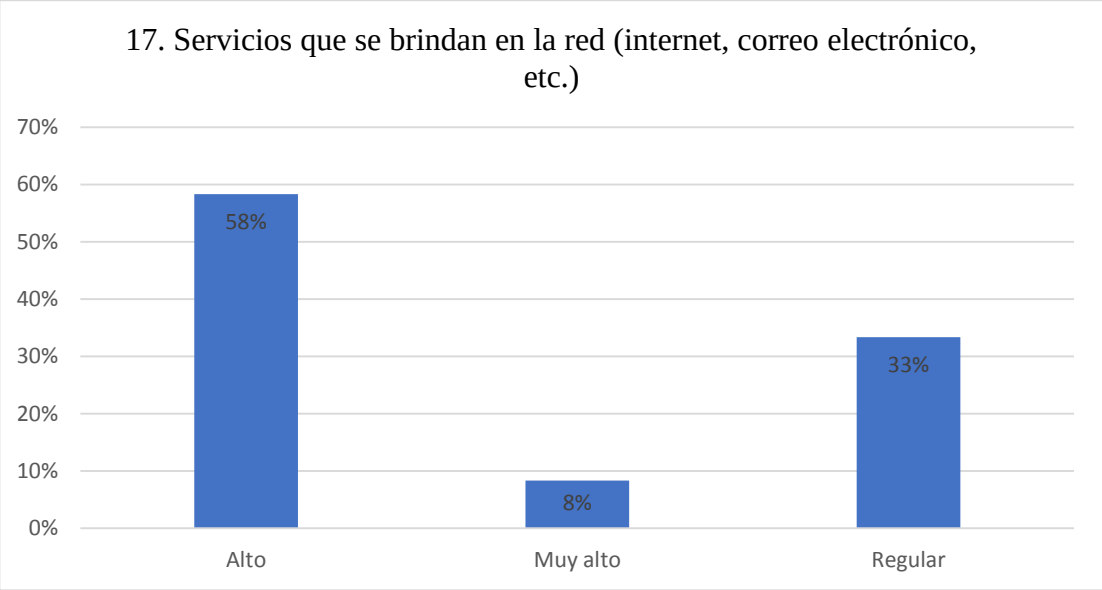


Nota: Elaboración propia

El 45% de los encuestados manifiestan que la disponibilidad es regular, es decir que enviar y recibir datos por la red no es muy eficiente, por otro lado, el 40% lo califica como alta es decir que se encuentran satisfechos por el intercambio de información y un 16% se encuentra muy satisfecho con la disponibilidad.

Gráfico 17

Servicios que se brindan en la red (internet, correo electrónico, etc.)



Nota: Elaboración propia

Los servicios que se brindan en la red, tienen buena aceptación debido a que el 58% lo califica como alto, un 8% se encuentra satisfecho lo califican como muy alto, tienen acceso a la recepción e intercambio de información, y 33% lo considera como regular, por lo que se percibe que encontraron falencias o no encontraron lo que necesitan.

4.3. Implementación de seguridad perimetral

La Institución Educativa (IE) requiere contratar los servicios de implementación de seguridad administrada, el cual integra al servicio de Seguridad

perimetral basado en Firewall de próxima generación. Esta solución contribuirá también a la consecución exitosa de los procesos técnicos y administrativos del personal y de esta manera apoyará al cumplimiento de sus actividades y objetivos estratégicos institucionales.

La Implementación por prestarse debe garantizar por requerimiento la seguridad de la información, salvaguardar el secreto de las telecomunicaciones y proteger la transferencia de datos personales, para lo cual se ha analizado y diseñado la mejor solución a implementarse, materia de la presente oferta técnica.

Como parte del servicio, se tiene la implementación de Sophos XG Home Edition los cuales estarán virtualizados en servidores ubicados en la institución.

Se ha considerado como parte de la solución de seguridad el siguiente equipamiento para la atención de los requerimientos indicados en el punto anterior**.**

4.3.1. Solución de Ciberseguridad Perimetral e interconectividad entre laboratorios TIC's

Para esta solución se implementará lo siguiente:

- Implementación de entorno de virtualización Proxmox en centro de datos.
- Implementación de una (01) máquinas virtuales tipo firewall Sophos XG Home Edition 18.5 en la IE de ILO, esta implementación cuenta con licenciamiento TRIAL gratuito entregado por Sophos.

Figura 7

SEDE ILO: Licencia Sophos XG Home Edition

Nota: Adaptación propia

Asimismo, la solución implementada en el Firewall cuenta con los siguientes módulos de seguridad disponibles.

Figura 8

Módulos disponibles del Firewall

Nota: Adaptación propia

4.3.2. Detalles de la solución

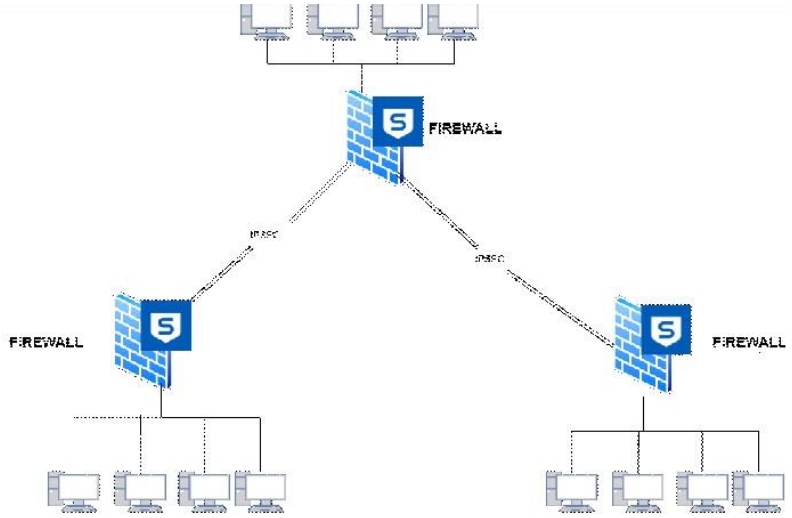
La solución establecida en el proyecto permitirá el buen manejo de recursos a través de la virtualización, asimismo el control de la seguridad perimetral e

interconectividad entre laboratorios con la licencia y servicios actualizados de esta solución.

IE AMGS	:	MOQUEGUA ILO
ID, Máquina Virtual	:	100
Modelo	:	C01001288FY6FA4

Figura 9

Estructura de interconectividad de laboratorios TIC's entre equipos firewall implementados



Nota: Adaptación propia

4.3.3. Objetivo de la solución

- Brindar seguridad y mitigar los posibles ciberataques a través de políticas de seguridad.
- Laboratorios TIC's seguros con filtro de contenido.

4.3.4. Servicio de implementación LAB PRIMARIA (principal)

Este laboratorio TIC's se considera como punto principal de interconexión entre los demás Secundaria e Inicial a través del tipo de conexión TRUNK, por lo que tiene recursos mayores para cumplir los requerimientos solicitados.

Asimismo, la solución tomada para este proyecto fue la virtualización completa de máquinas virtuales, tomando como entorno de virtualización principal PROXMOX VE, el cual alberga la solución de seguridad SOPHOS XG en una máquina virtual.

El presente informe detallara los aspectos principales de configuración de la implementación realizada en dos puntos:

- Implementación de entorno de virtualización PROXMOX.
- Implementación de Firewall Perimetral.

4.3.5. Implementación de entorno de virtualización PROXMOX

Para desplegar y gestionar máquinas virtuales y contenedores, se puede utilizar el entorno de virtualización de servidores de código abierto conocido como Proxmox. Tiene una interfaz basada en la web, sencilla y fácil de usar, que hace que sea fácil crear, configurar y administrar máquinas virtuales (Barrionuevo Mercedes et al., 2017).

Información de Hardware empleado para virtualización

Para construir un sistema informático virtual, la virtualización utiliza software para imitar las características del hardware.

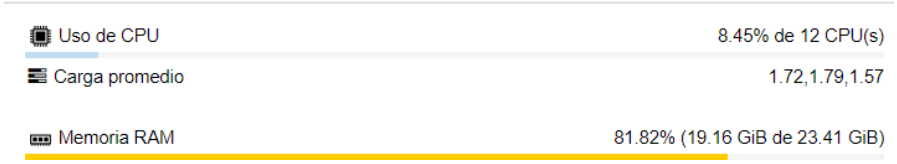
A continuación, se detallan las características técnicas del hardware empleado:

Servidor

El servidor empleado cuenta con una memoria RAM de 23.41 GiB, este a su vez cuenta con una disponibilidad del 81.82% conjunto a un 8.45% de uso de CPU y una carga promedio de 1.72, 1.79, 1.57.

Figura 10

Información de hardware



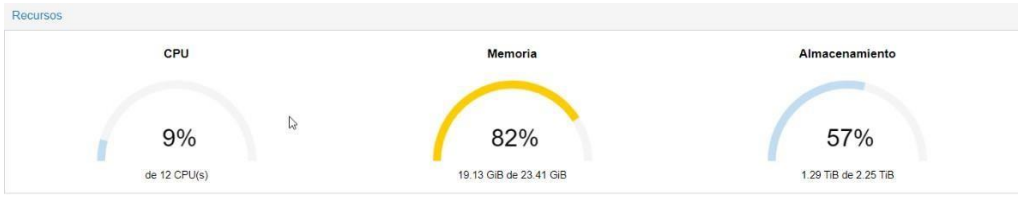
Nota: Adaptación propia

Actualmente el servidor presenta una utilización de CPU del 9%, un 82% de utilización de memoria RAM y 57% de almacenamiento.

La imagen a continuación detalla el resumen de uso actual de recursos.

Figura 11

Resumen de consumo de recursos



Nota: Adaptación propia

4.3.6. Interfaces físicas y virtuales

Proxmox proporciona la facilidad de crear redes virtuales, por lo que se aprovechara esta característica para crear 3 zonas necesarias para la infraestructura:

- Zona LAN: Red de informática que cubre áreas geográficas pequeñas con un alcance de 1-5 km, es decir con extensión física limitada. De este modo, distintos dispositivos pueden comunicarse entre ellos (Lederkremer, 2019).

- Zona WAN: Red informática con un diámetro de entre 100 y 1.000 kilómetros; más concretamente, una red de comunicaciones cuya conectividad atraviesa las fronteras locales, regionales o nacionales. El hardware utilizado, como enrutadores, conmutadores, módems, cortafuegos, etc., es más diverso en comparación con otros tipos de redes. (Lederkremer, 2019).
- Zona DMZ: Esta red local, que suele estar en Internet, se sitúa entre la red interna de una organización y una red externa. La función de una DMZ es permitir las conexiones de la red externa a la DMZ, pero suele prohibir las conexiones de la DMZ a la red interna (los equipos de la DMZ no deben conectarse directamente a la red interna). En caso de que los intrusos pongan en peligro la seguridad de los equipos situados en la zona desmilitarizada, la red interna queda protegida al tiempo que se permite a los equipos de la DMZ prestar servicios a la red externa (Lederkremer, 2019).

A continuación, se muestran las interfaces tanto Físicas como virtuales:

Figura 12

Interfaces físicas en Proxmox

eno1	Dispositivo de ...	Sí	Sí	No
eno2	Dispositivo de ...	Sí	Sí	No
eno3	Dispositivo de ...	Sí	Sí	No
eno4	Dispositivo de ...	Sí	Sí	No
enx42f2e9...	Dispositivo de ...	No	No	No

Nota: Adaptación propia

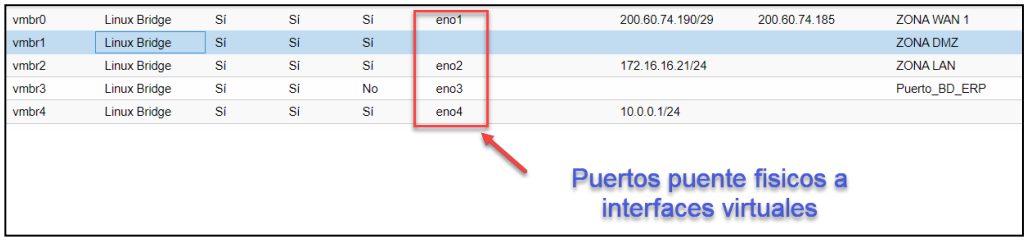
Puertos Puente

Este tipo de configuración es una forma común donde se establece una conexión directa entre la interfaz física con la virtual.

La imagen detalla la lista de interfaces virtuales conectadas directamente a las interfaces físicas en modo puente.

Figura 13

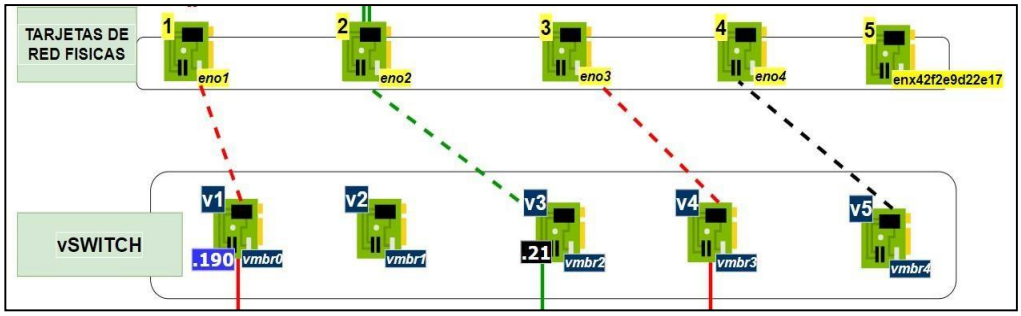
Interfaces virtuales en modo puente



Nota: Adaptación propia

Figura 14

Interfaces virtuales en modo puente II



Nota: Adaptación propia

Direccionamiento Asignado a interfaces

Cada interfaz de red mantiene un direccionamiento respectivo para tener conectividad con las máquinas virtuales.

Observación 1: Las máquinas virtuales que tengan asignadas una interfaz virtual, deberá mantener el direccionamiento respectivo.

Observación 2: En la imagen se observa la interfaz de red VMBR4 está conectada directamente a la interfaz física eno4, esta interfaz sirve para conectarse directamente al servidor en caso se haya perdido conectividad desde otras interfaces esto ayudara a poder apagar las máquinas virtuales de manera segura ante cualquier incidente.

Para este de funcionamiento el administrador tendrá que conectar una laptop directamente a la interfaz física "eno4" y configurar la laptop con el direccionamiento IP 10.0.0.2/24 (dejar en blanco los parámetros Gateway y DNS).

Figura 15

Direccionamiento asignado a interfaces

Nota: Adaptación propia

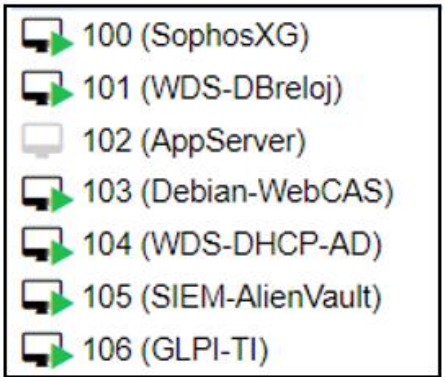
4.3.7. Información de Máquinas Virtuales implementadas

Los ordenadores basados en software, conocidos como máquinas virtuales, ofrecen las mismas características que los ordenadores reales.

A continuación, se detallan las Máquinas Virtuales implementadas:

Figura 16

Lista de Máquinas virtuales implementadas



Nota: Adaptación propia

4.3.8. Respaldo de Máquinas virtuales

Cada máquina virtual cuenta con el respaldo ejecutado con fecha 06/06/2020. Se debe tener una bitácora de respaldo ante cualquier cambio a realizar.

Observación:

La funcionalidad de snapshot sobre VMs no está disponible sobre discos virtuales alojados en almacenamientos basados en LVM, es por esta razón que se opta realizar el respaldo directo de las máquinas virtuales a excepción de las siguientes Máquinas virtuales:

- Sophos XG (100): Considerada una solución de seguridad de red puede identificar completamente una infección de red, junto con su usuario y su origen, y actuar bloqueando automáticamente el acceso a otros recursos de la red.
- Windows 2012 (104): Un sistema operativo conjunto de aplicaciones que permiten gestionar los recursos de un ordenador. Este tipo de sistema empieza a funcionar en cuanto se enciende el ordenador para manejar el hardware en los niveles más fundamentales.

A continuación, se detalla los respaldos y snapshots realizados a cada máquina virtual:

Tabla 11

Cuadro de MV con respaldo

ID	Nombre de Máquina Virtual	Snapshot	Backup
100	Sophos XG	X	X
101	WDS-DBReloj		X
102	APPServer		X
103	Debian-WebCAS		X
104	WDS-DHCP-AD	X	X
105	SIEM-AlienVault		
106	GLPI-TI		X

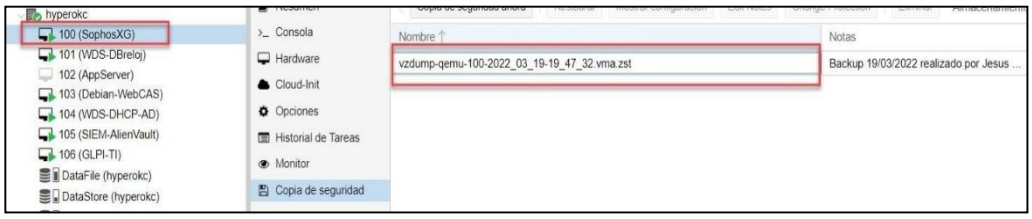
Nota: Adaptación propia

Sophos XG – 100

Sophos XG Firewall ofrece una visibilidad inigualable de los usuarios de riesgo, las aplicaciones desconocidas y no deseadas, los ataques sofisticados, las cargas útiles sospechosas, el tráfico cifrado y mucho más.

Figura 17

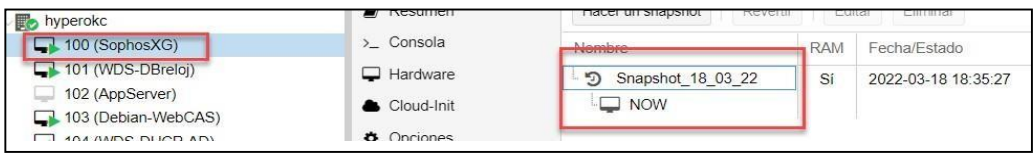
Respaldo de MV Sophos XG



Nota: Adaptación propia

Figura 18

Snapshot de MV Sophos XG



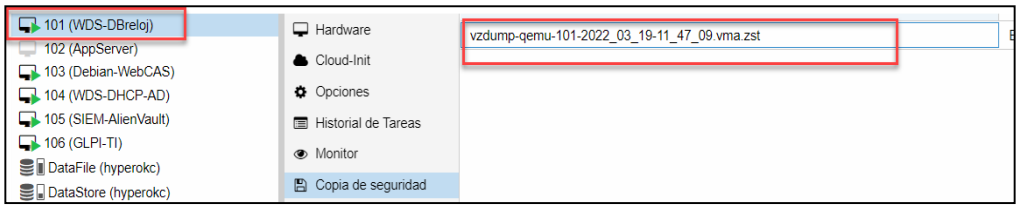
Nota: Adaptación propia

WDS-DBReloj – 101

Un sistema de distribución inalámbrica (WDS) es un dispositivo que hace posible que los puntos de acceso (AP) de una red se comuniquen de forma inalámbrica entre sí. Sin el uso de una red troncal física, el WDS permite ampliar una red inalámbrica utilizando múltiples puntos de acceso.

Figura 19

Respaldo de MV WDS-DBReloj

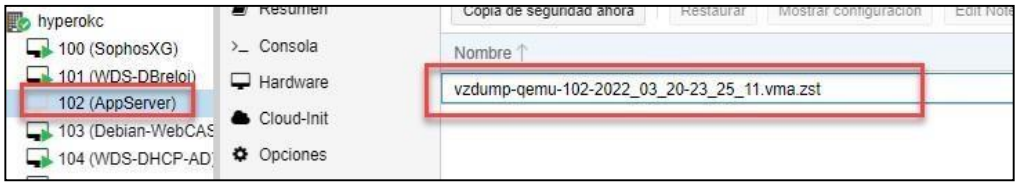


Nota. Adaptación propia

APPServer – 102

Figura 20

Respaldo de MV Debian-AppServer



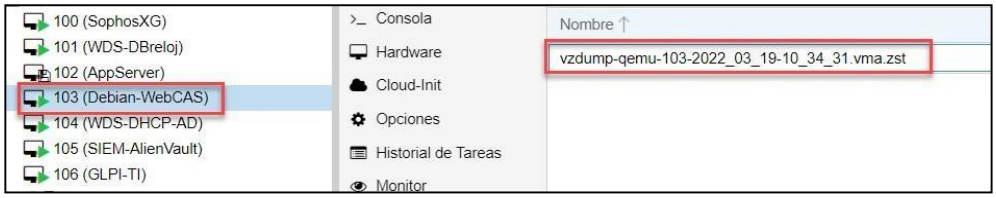
Nota. Adaptación propia

Debian-WebMoodle – 103

Moodle es una plataforma de aprendizaje diseñada para proporcionarle a educadores, administradores y estudiantes un sistema integrado único, robusto y seguro para crear ambientes de aprendizaje personalizados.

Figura 21

Respaldo de MV Debian-WebMoodle



Nota: Adaptación propia

WDS-DHCP-AD – 104

Los servicios de implementación de Windows se denominan servicios WDS. Los servicios WDS, para los que los clientes previstos deben soportar el arranque remoto, son un software que permite a un administrador configurar remotamente nuevas máquinas cliente sin tener que estar presente en cada ordenador cliente individual.

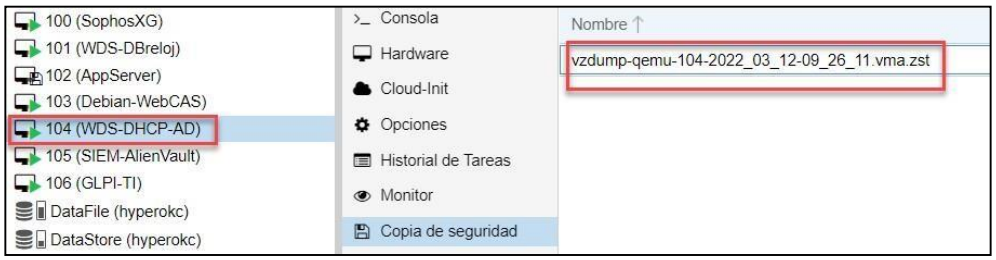
Figura 22

Snapshot de MV WDS-DHCP-AD

Nota. Adaptación propia

Figura 23

Respaldo de MV WDS-DHCP-AD



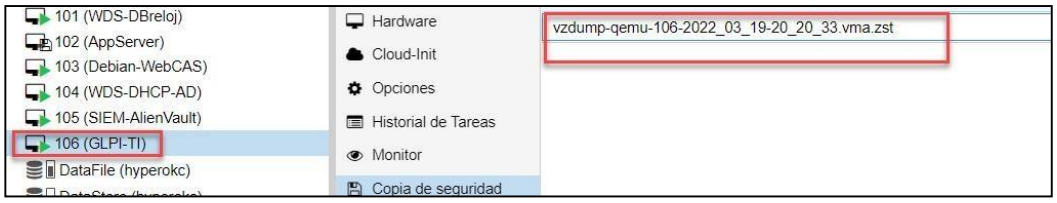
Nota: Adaptación propia

GLPI-TI – 106

GLPi es un programa de gestión de servicios de TI (ITSM) de código abierto y un servicio de asistencia que permite a su empresa mejorar su infraestructura de TI.

Figura 24

Respaldo de MV GLPI-TI



Nota. Adaptación propia

4.3.9. Gestión del Equipamiento

Direccionamiento IP de Gestión de Proxmox

Para gestionar la plataforma de Proxmox y máquinas virtuales, se detalla las direcciones IP y modo de acceso. Un dispositivo puede ser identificado por su dirección IP en Internet o en una red local. El término "Protocolo de Internet" se refiere al conjunto de directrices que controlan la estructura de los datos transferidos a través de una red local o de área amplia.

Tabla 12

Gestión de Proxmox

PLATAFORMA	IP	ACCESO WEB	ACCESO DESDE ZONA
PROXMOX	172.16.16.21	https://172.16.16.21:8006	LAN
	200.60.74.190	https://200.60.60.190/29:8006	WAN
	10.0.0.1	https://10.0.0.1:8006	Conexión directa desde **eno4**

Nota. Adaptación propia

Usuario de Administración

Para el caso de la gestión del equipo instalado se le ha entregado el usuario de administración en modo lectura y escritura, se describe a continuación los usuarios:

Tabla 13

Usuario de Administración

PLATAFORMA	USUARIO	PERFIL
PROXMOX	root	Administrador

Nota: Adaptación propia

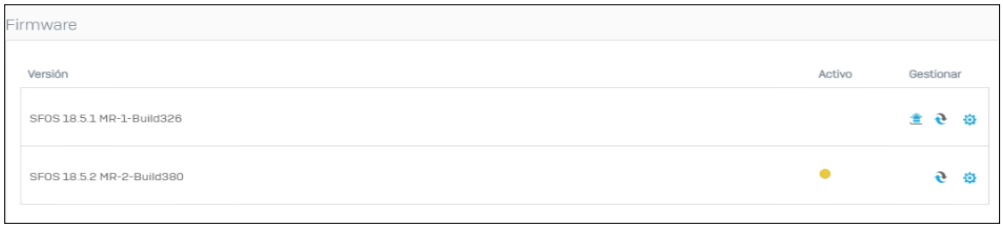
4.4. Implementación de Firewall Perimetral

Al impedir los ataques a los puertos con vulnerabilidades del servidor y del ordenador, los accesos no autorizados y la mayoría de los códigos dañinos automatizados, un cortafuego perimetral da más seguridad a su red informática. Puede protegerse contra los ataques DoS con un cortafuego de seguridad perimetral. protección contra el acceso no autorizado y el robo de credenciales.

4.4.1. Información de Firewall Perimetral IE

Figura 25

Información del Firmware instalado



Nota. Adaptación propia

4.4.2. Información de Firewall como Máquina Virtual

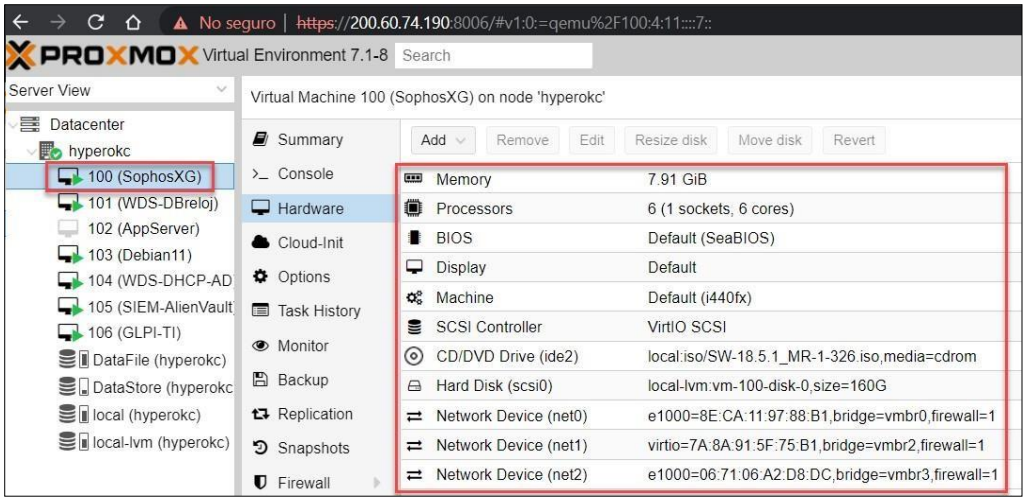
Un firewall es un mecanismo de seguridad que se utiliza para evitar el acceso no deseado y no fiable a las redes privadas conectadas a Internet.

El firewall se encuentra virtualizado bajo el entorno de virtualización PROXMOX-VE, este mismo tiene características específicas para su funcionamiento.

La imagen a continuación muestra los detalles y características de la Máquina Virtual asignados para el Firewall Sophos XG.

Figura 26

Descripción de equipos



Nota: Adaptación propia

4.4.3. Interfaces

El punto de compromiso y comunicación entre los humanos y los ordenadores en un dispositivo es la interfaz de usuario, o UI. Puede incluir pantallas de escritorio, teclados, ratones y otros dispositivos señaladores. Además, se refiere a la forma en que un usuario se relaciona con un sitio web o un programa.

Ubicación de modulo:

Ir a CONFIGURAR → RED →interfaces

Figura 27

Lista de interfaces de red

Nota. Adaptación propia

LAN: se configuró la interfaz PORT1 con la dirección IP 172.16.16.16/24 para la comunicación entre el equipo Firewall y el Switch Core del cliente, la red 172.16.16.0/24 corresponde a una red de paso creada solo para la comunicación entre ambos equipos. El equipo firewall dejara pasar las VLAN a través de la IP del Switch Core (172.16.20.2/28) usando una sola ruta estática configurado en el Switch Core.

Asimismo, se detallan las VLAN creadas en el Firewall con sus respectivos ID y direccionamiento IP:

Ubicación de modulo:

Ir a CONFIGURAR → RED →interfaces/vlan

Figura 28

Lista de Vlan creadas

Nota. Adaptación propia

WAN1: se configuro la interfaz PORT2 con la dirección IP 200.60.60.187/29 para la comunicación entre el equipo firewall y los equipos Routers.

Sobre este enlace se encuentra establecida una conexión de tipo VPN:

- VPN SSL móvil para conectividad remota de usuarios fuera de la red.
- WAN2: se configuro la interfaz PORT3 con la dirección IP 200.60.60.188/29. esta subred fue declarada para establecer 2 funciones:
- Publicar Servicio web ie.amgs.edu.pe

4.4.4. Retransmisión DHCP

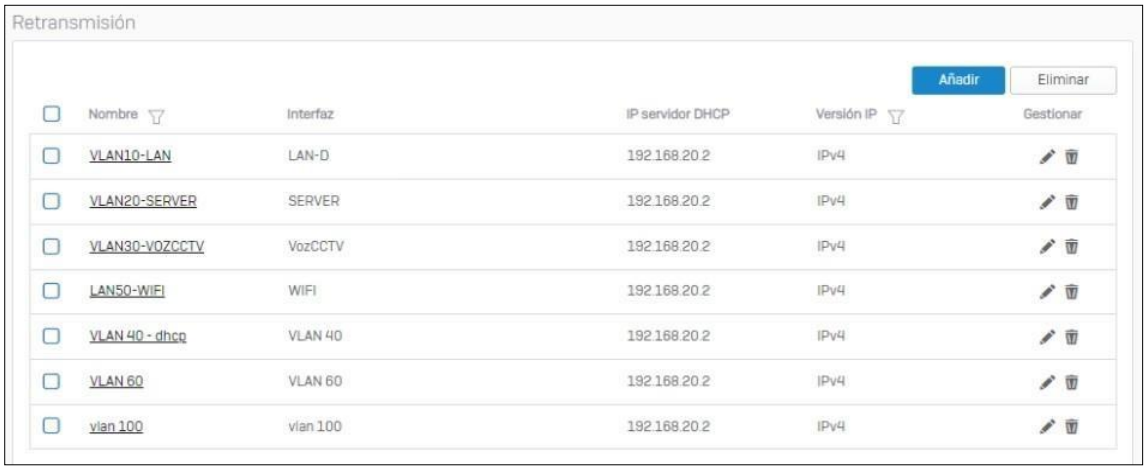
El firewall está configurado para retransmitir DHCP a las Vlan creadas de acuerdo con el direccionamiento establecido en el servidor Windows Server, este mismo tiene la dirección IP 192.168.20.2 (VLAN 20).

Ubicación de modulo:

Ir a CONFIGURAR → RED→ DHCP →Retransmisión

Figura 29

Retransmisión DHCP



Nota. Adaptación propia

4.4.5. Perfiles de Seguridad

Perfil de Filtrado Web

Según lo solicitado por el cliente se crearon los siguientes grupos de filtrado web los cuales fueron aplicados a las políticas de firewall para establecer los permisos de navegación a Internet a través del filtrado por URL.

Ubicación de modulo:

Ir a PROTEGER → WEB→ Políticas

Figura 30

Perfiles Web Filter

Nota. Adaptación propia

Perfil de Control de Aplicaciones

Se crearon los siguientes perfiles de Control de Aplicaciones, los cuales son utilizados para establecer los permisos de navegación hacia Internet a través del filtrado por aplicaciones.

Ubicación de modulo:

Ir a CONFIGURAR → APLICACIONES→ Filtro de Aplicaciones

Figura 31

Perfiles de Control de Aplicaciones

Nota: Adaptación propia

Antivirus

Programa que protege, busca, identifica y elimina los virus de un ordenador. Suelen ejecutarse automáticamente en segundo plano tras su instalación para ofrecer protección en tiempo real contra los ataques de virus.

Se configuró los siguientes perfiles de antivirus perimetral.

Este mismo analiza el tráfico de red entrante y saliente (por ejemplo, solicitudes DNS, solicitudes HTTP y paquetes IP) en busca de amenazas.

Ubicación de modulo:

Ir a CONFIGURAR → SERVICIOS DEL SISTEMA→ Protección contra Malware

Figura 32

Perfiles de Antivirus

Nota. Adaptación propia

IPS

Software que implementa el control de acceso en una red informática para defenderse de los asaltos y la explotación.

Se Habilito y configuró los siguientes perfiles de protección contra intrusos.

Ubicación de modulo:

Ir a CONFIGURAR → SERVICIOS DEL SISTEMA→ Protección contra Malware.

Figura 33

IPS Habilitado / Firmas Actualizadas

Nota. Adaptación propia

Figura 34

Perfiles de IPS

Nota: Adaptación propia

4.4.6. Políticas de Seguridad

Las políticas de seguridad informática son declaraciones escritas de las directrices que debemos cumplir quienes tenemos acceso a los recursos tecnológicos e informáticos de una empresa.

Se crearon las siguientes políticas de seguridad, los cuales son utilizadas para establecer los permisos de navegación hacia Internet.

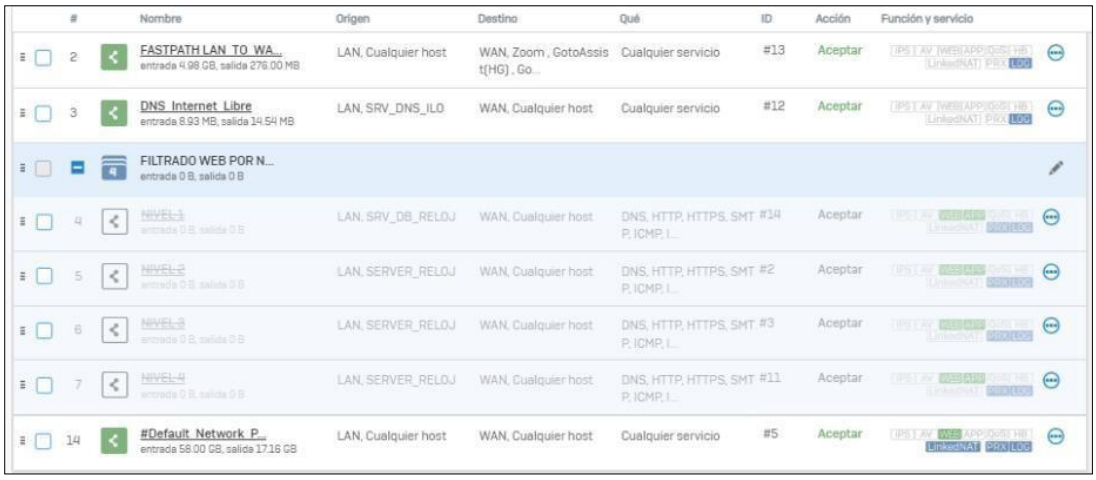
Observación: las políticas que se encuentran deshabilitadas para ejecutar pruebas por IP, así mismo estos pueden incluir los grupos de usuarios del servidor de Directorio Activo, dichos grupos serán asignados a cada política según su nivel de permisos de navegación hacia internet.

Ubicación de modulo:

Ir a PROTEGER → REGLAS Y POLITICAS → Reglas de Firewall

Figura 35

Políticas de LAN hacia WAN



Nota. Adaptación propia

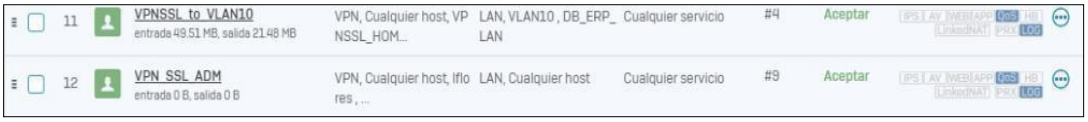
Figura 36

Políticas de LAN hacia WAN

Nota. Adaptación propia

Figura 37

Políticas de LAN hacia VPN SSL REMOTO Y VICEVERSA



Nota: Adaptación propia

Figura 38

Políticas de LAN hacia LAN (Comunicación entre VLAN)

Nota: Adaptación propia

Figura 39

Política WAF (ie.amgs.edu.com.pe)

Nota. Adaptación propia

4.4.7. Protección de Aplicaciones Web (WAF)

Protege el servidor de aplicaciones web backend de una variedad de amenazas. El trabajo del WAF es proteger la seguridad del servidor web inspeccionando los paquetes de solicitud HTTP / HTTPS y los patrones de tráfico.

Servidor Protegido

Se listan los servidores y sus puertos respectivos los cuales serán protegidos por el módulo de seguridad WAF.

Ubicación de modulo:

Ir a PROTEGER → SERVIDOR WEB → Servidores Web

Figura 40

Servidor Protegido

Nota: Adaptación propia

Figura 41

Detalle de Servidor web protocolo HTTPS

Nota: Adaptación propia

Políticas de Protección de Servidor

Se crearon las siguientes políticas de seguridad para la protección del servidor cas.okcomputer.com.pe.

Ubicación de modulo:

Ir a PROTEGER → SERVIDOR WEB → Políticas de protección

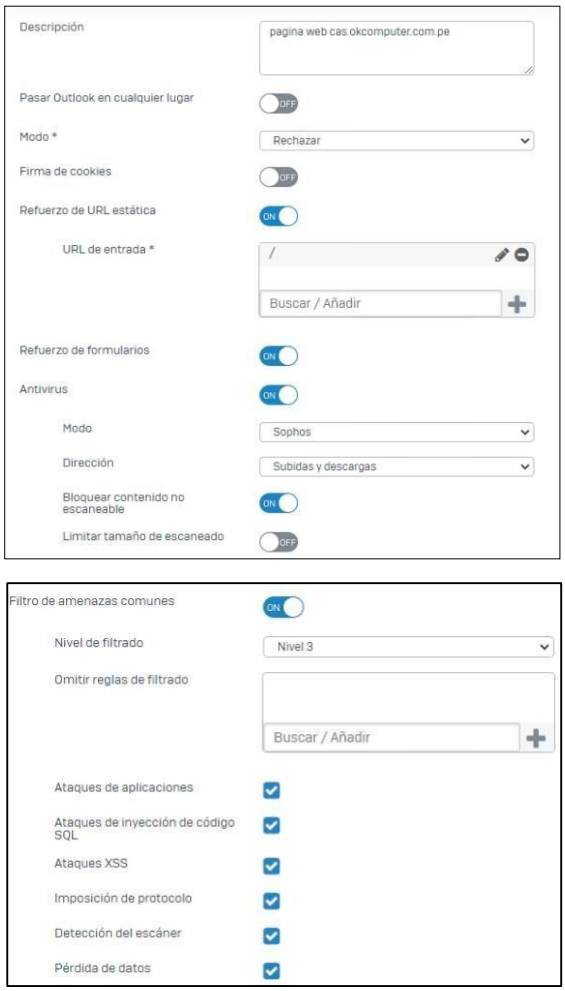
Figura 42

Políticas de Protección de Servidores

Nota: Adaptación propia

Figura 43

Detalle de Política de Protección del Servidor IE.AMGS.EDU.PE (HTTPS).



Nota: Adaptación propia

Perfiles de Protección Web

Una forma de medida de seguridad empleada como parte del proceso de Criterios Comunes es un perfil de protección. El objetivo principal de un perfil de protección es evaluar la eficacia de numerosos protocolos de seguridad otorgando a cada uno de ellos un grado o nivel. Este método permite evaluar la eficacia de las medidas de seguridad de una red, así como de los distintos sistemas y partes que la componen en su conjunto.

Se configuró los siguientes perfiles de protección web.

Ubicación de modulo:

Ir a PROTEGER → REGLAS Y POLITICAS → Reglas de Firewall

Figura 44

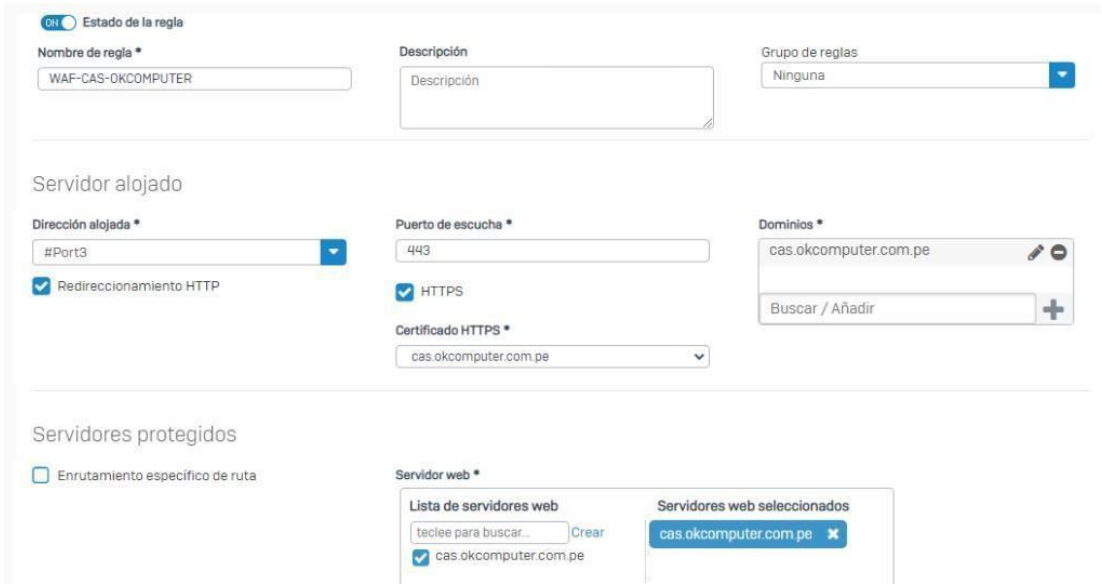
Perfiles de Protección Web

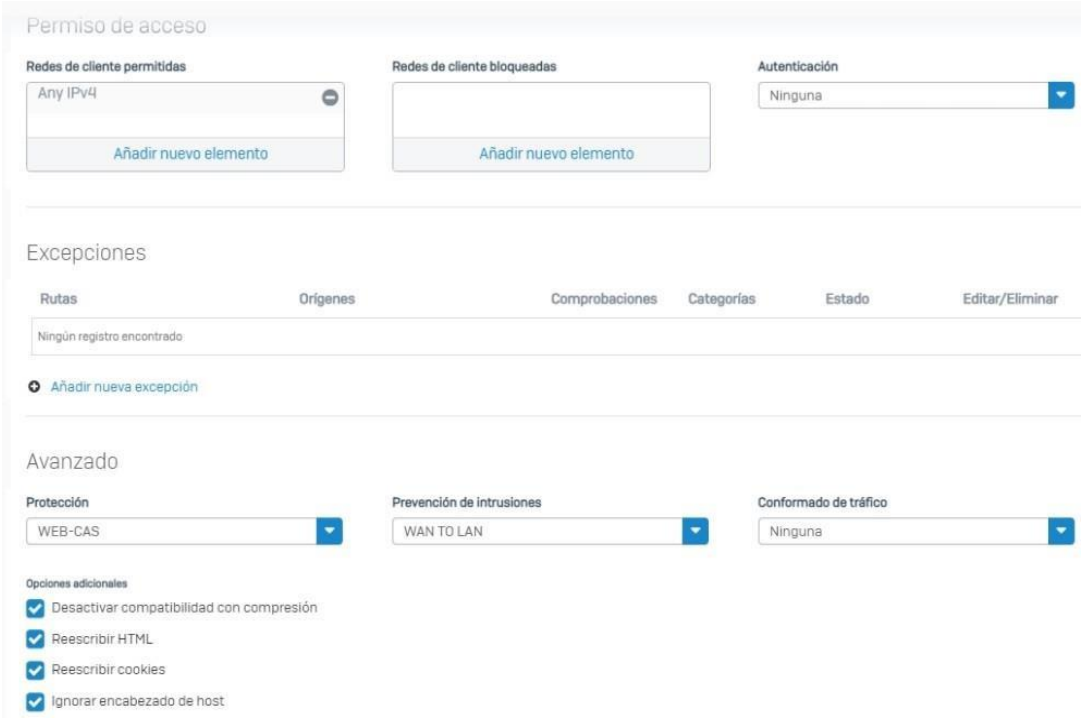
Nota. Adaptación propia

Se muestran los perfiles de protección correspondientes a los puertos 443 (HTTPS).

Figura 45

Detalle de Perfil WAF





Nota. Adaptación propia

4.4.8. Conexiones VPN

El firewall VPN cuenta con dos tipos de conexiones VPN, estas mismas sirven para interconexión con las sedes sucursales y la conexión remota de los colaboradores hacia la red interna permitida a través de las políticas establecidas. La conexión VPN es:

- VPN SSL Remoto

Una VPN SSL suele ofrecer dos servicios: acceso seguro a nivel de red a través de un túnel SSL seguro entre el cliente y la red de la empresa, así como acceso remoto seguro a través de un portal web. La seguridad y la privacidad de los datos son las principales ventajas de una VPN SSL.

4.4.9. VPN SSL Remoto

Esta conexión permite el acceso a recursos de red para hosts individuales mediante túneles cifrados de punto a punto a través de Internet. El acceso remoto requiere certificados digitales y un nombre de usuario y contraseña previamente creado en el Firewall.

Ubicación de modulo:

Ir a CONFIGURAR → VPN→ VPN SSL (acceso remoto)

Actualmente existen 2 perfiles de configuración:

- VPNSSL_to_VLAN10: Perfil que permite la conectividad solo a la vlan10 de la institucion, usuarios administrativos
- VPN_SSL_ADM: Este perfil tiene acceso a todas las VLAN de la IE.

Figura 46

Detalle de Conexión VPN SSL REMOTO

Nota. Adaptación propia

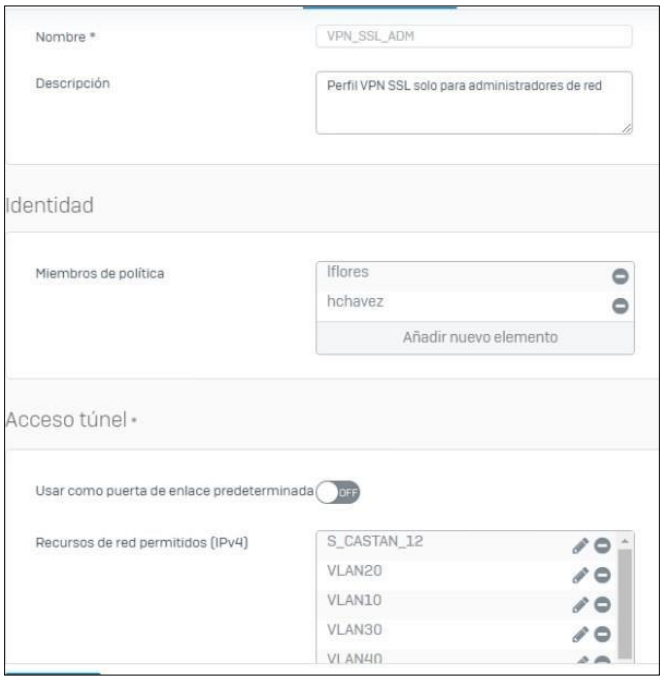
Figura 47

Detalle de Conexión (VPNSSL_TO_VLAN10)

Nota. Adaptación propia

Figura 48

Detalle de Conexión (VPN_SSL_ADM)



Nota. Adaptación propia

4.4.10. Administración Centralizada – SOPHOS CENTRAL

Un Sophos Central puede gestionar todos sus productos de Sophos desde una única ubicación con el uso de una consola centralizada.

Puede registrar los dispositivos de Sophos Firewall con Sophos Central y administrar los dispositivos de forma centralizada.

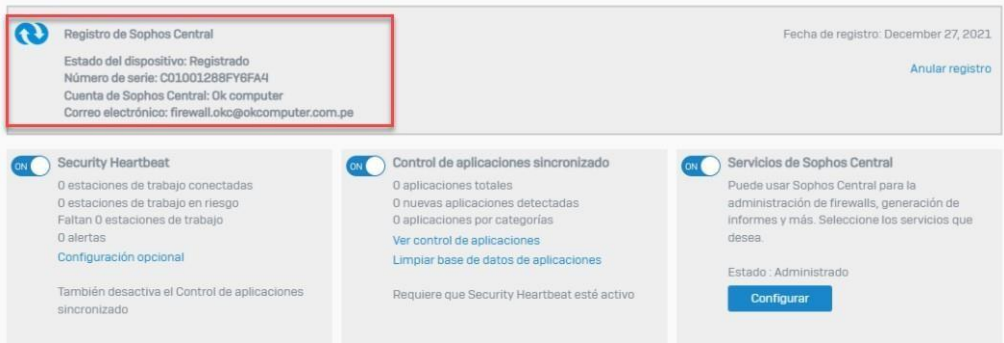
El firewall ya se encuentra registrado a Sophos central, por lo que no es necesario administrar de forma externa a través de una IP publica, en adelante la administración de este Firewall se realizará a través de la plataforma web de Sophos Central.

Ubicación de modulo:

Ir a SISTEMA → SOPHOS CENTRAL

Figura 49

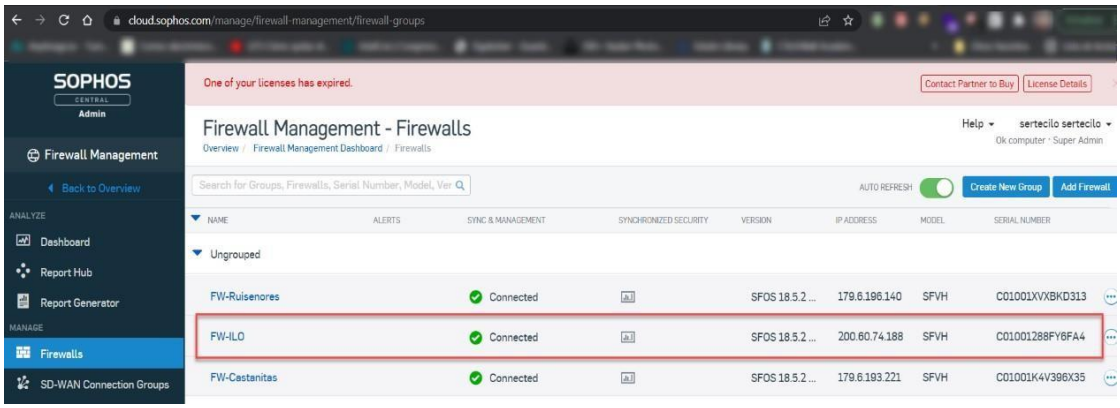
Detalle de registro a Sophos Central



Nota. Adaptación propia

Figura 50

Sophos Central – FW IE



Nota: Adaptación propia

4.4.11. Integración con Directorio Activo

La función de integración de Active Directory de Sophos Firewall permite que el dispositivo asigne usuarios y grupos de AD a SOPHOS para la autenticación. Esto permite que el dispositivo identifique fácilmente a los usuarios de la red. SOPHOS se comunica con los servicios de directorio de Windows para autenticar a los usuarios en función de grupos, dominios y unidades organizativas.

Para aplicar este tipo de autenticación fue necesario instalar STAS como recolector de inicios de sesión para luego enviarlos a Sophos, de esta manera podría haber una comunicación de inicio/cierre de sesión entre el servidor AD y Sophos.

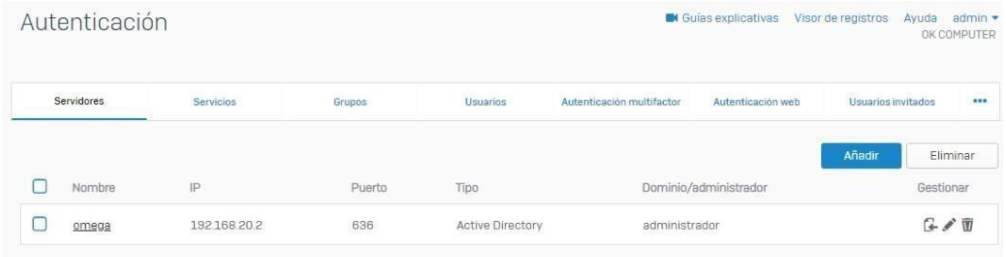
Ubicación de modulo:

Ir a CONFIGURAR → AUTENTICACION→ Servidores

A continuación, se muestran las configuraciones realizadas en el servidor de directorio activo y Sophos.

Figura 51

Servidor AD registrado en Sophos XG



Nota. Adaptación propia

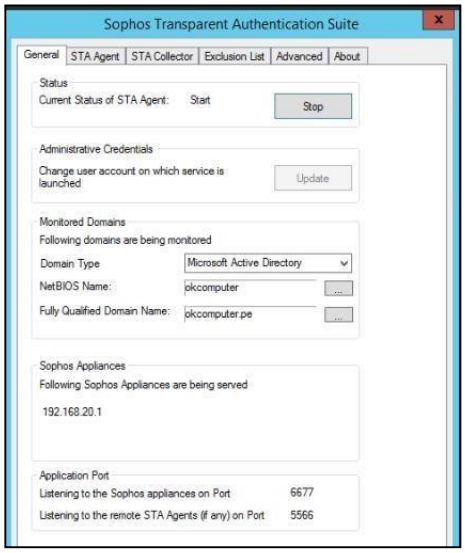
Figura 52

Unidades Organizativas agregadas a Sophos

Nota: Adaptación propia

Figura 53

Programa STAS instalado en AD



Nota. Adaptación propia

4.4.12. Respaldo y restauración de Configuraciones Sophos XG

La gestión de copias de seguridad, actualizaciones del firmware puede administrarse desde la plataforma de Sophos.

Actualmente se ha configurado la programación de envío diario de copias de seguridad al correo, Mientras que el respaldo de configuraciones puede realizarse subiendo el archivo de copia de seguridad más reciente y digitar la contraseña de cifrado.

Ubicación de módulo:

Ir a SISTEMA → COPIAS DE SEGURIDAD Y FIRMWARE

Para aplicar este tipo de autenticación fue necesario instalar STAS como recolector de inicios de sesión para luego enviarlos a Sophos, de esta manera podría haber una comunicación de inicio/cierre de sesión entre el servidor AD y Sophos.

4.4.13. Gestión del Equipamiento

Direccionamiento IP de Gestión de Firewall

Para el caso de la gestión del equipo por parte del cliente se ha configurado la siguiente dirección IP local para su respectiva administración.

Tabla 14

Direccionamiento IP de Gestión de Firewall

MÁQUINA VIRTUAL	IP	ACCESO WEB
SOPHOS XG	172.16.16.16	https://172.16.16.16:4444 SOPHOS CENTRAL

Nota. Adaptación propia

Usuario de Administración

Para el caso de la gestión del equipo instalado se le ha entregado el usuario de administración en modo lectura y escritura, se describe a continuación los usuarios:

Tabla 15

Usuario de Administración

MAQUINA VIRTUAL	USUARIO	PERFIL
SOPHOS XG	admin	Administrador
	hchavez	Administrador

Nota: Adaptación propia

4.5. Implementación LABORATORIO Secundaria

Este laboratorio se considera como jornada escolar completa JEC el cual tendrá interconexión con el laboratorio de primaria por conexión TRUNK.

Asimismo, la solución tomada para este proyecto fue la virtualización completa de máquinas virtuales, tomando como entorno de virtualización principal PROXMOX VE, el cual alberga la solución de seguridad SOPHOS XG en una máquina virtual.

El presente informe detallara los aspectos principales de configuración de la implementación realizada en dos puntos:

- Implementación de entorno de virtualización PROXMOX.
- Implementación de Firewall Perimetral.

4.5.1. Implementación de entorno de virtualización PROXMOX

Información de Hardware empleado para virtualización

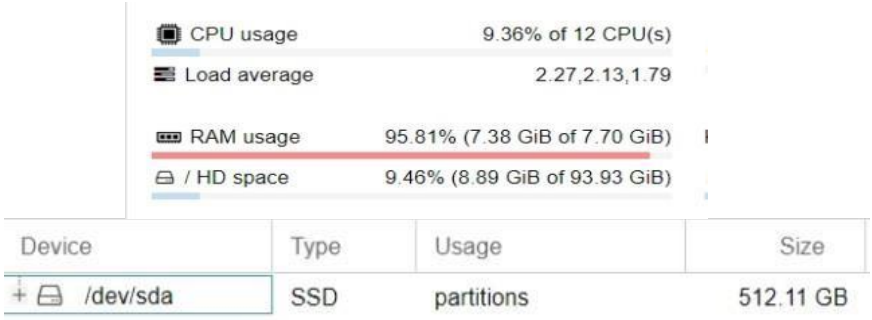
A continuación, se detallan las características técnicas del hardware empleado.

Servidor

Compuesto por una memoria RAM de 7.70 GiB, 12 CPU(s) y un espacio HD de 93.93 GiB.

Figura 54

Información de hardware



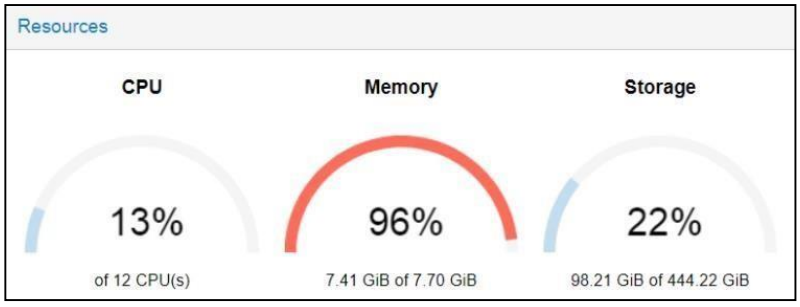
Nota: Adaptación propia

En cuanto al consumo de recursos se detalla que tiene una utilización del 13% de CPU, 96% de la memoria RAM y un almacenamiento del 22%.

La imagen a continuación detalla el resumen de uso actual de recursos.

Figura 55

Resumen de consumo de recursos



Nota. Se considera agregar un módulo adicional de RAM a este servidor, ya que el consumo actual es de 96% del total. Adaptación propia.

4.5.2. Interfaces físicas y virtuales

Proxmox proporciona la facilidad de crear redes virtuales, por lo que se aprovechara esta característica para crear 2 zonas necesarias para la infraestructura:

- Zona LAN: La Red de Área Local o LAN es aquella red informática con un rango de cobertura de 1 a 5 km para ubicaciones geográficas pequeñas.
- Zona WAN: Red de área amplia de distribución que abarca zonas geográficas mayores mediante ondas de radio de alta frecuencia.

Observación: Se consideró crear estas zonas como medida preventiva en caso se adquiera un servicio de ISP con ip pública, mientras tanto solo se considera el uso del equipo con el ISP que utiliza direcciones IPS dinámicas.

A continuación, se muestran las interfaces tanto Físicas como virtuales:

Figura 56

Interfaces físicas en Proxmox

eno1	Dispositivo de ...	Sí	No	No		
eno2	Dispositivo de ...	Sí	No	No		
eno3	Dispositivo de ...	No	No	No		
eno4	Dispositivo de ...	Sí	No	No		
enx42f2e9673c27	Dispositivo de ...	No	No	No		
vmbr0	Linux Bridge	Sí	Sí	Sí	eno1	10.10.10.12/24
vmbr1	Linux Bridge	Sí	Sí	Sí	eno2	192.168.12.252/24
vmbr2	Linux Bridge	Sí	Sí	No	eno4	10.0.0.1/24

Nota. Adaptación propia

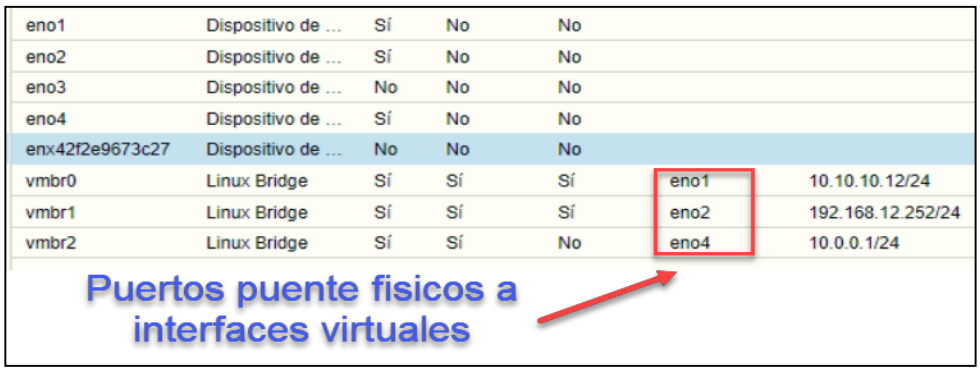
Puertos Puente

Este tipo de configuración es una forma común donde se establece una conexión directa entre la interfaz física con la virtual.

La imagen detalla la lista de interfaces virtuales conectadas directamente a las interfaces físicas en modo puente.

Figura 57

Interfaces virtuales en modo puente

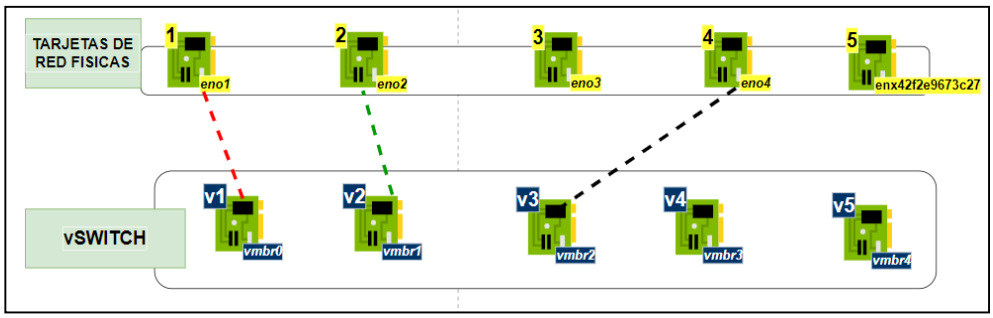


Nota. Adaptación propia

Para mayor entendimiento analizar la imagen a continuación:

Figura 58

Interfaces virtuales en modo puente II



Nota: Adaptación propia

Direccionamiento Asignado a interfaces

Cada interfaz de red mantiene un direccionamiento respectivo para tener conectividad con las máquinas virtuales.

Observación 1: Las máquinas virtuales que tengan asignadas una interfaz virtual, deberá mantener el direccionamiento respectivo.

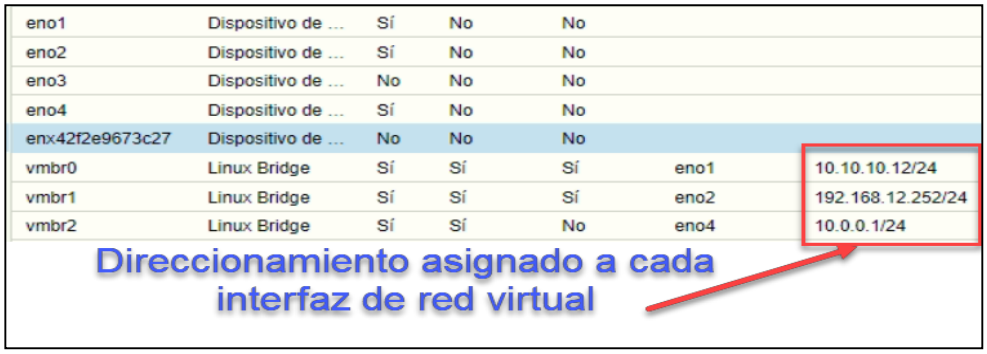
Observación 2: En la imagen se observa que la interfaz de red VMBR2 está conectada directamente a la interfaz física eno4, esta interfaz sirve para conectarse directamente al servidor en caso se haya perdido conectividad desde otras interfaces

esto ayudara a poder apagar las máquinas virtuales de manera segura ante cualquier incidente.

Para este de funcionamiento el administrador tendrá que conectar una laptop directamente a la interfaz física “eno4” y configurar la laptop con el direccionamiento IP 10.0.0.2/24 (dejar en blanco los parámetros Gateway y DNS).

Figura 59

Direccionamiento asignado a interfaces



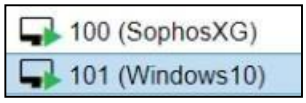
Nota. Adaptación propia

4.5.3. Información de Máquinas Virtuales implementadas

A continuación, se detallan las Máquinas Virtuales implementadas:

Figura 60

Lista de Máquinas virtuales implementadas



Nota: Adaptación propia

4.5.4. Respaldo de Máquinas virtuales

Cada máquina virtual cuenta con el respaldo y snapshot ejecutado con fecha 06/06/2020.

A continuación, se detalla los respaldos y snapshots realizados a cada máquina virtual:

Tabla 16

Cuadro de MV con respaldos

ID	Nombre de Máquina Virtual	Snapshot	Backup
100	Sophos XG	X	X
101	Windows 10	X	X

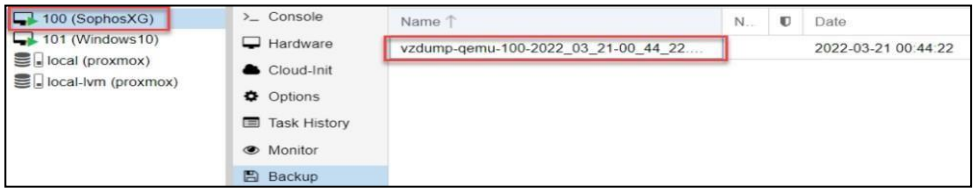
Nota. Adaptación propia

Sophos XG – 100

El acceso a otros recursos de la red puede limitarse automáticamente en respuesta a una infección de la red mediante un sistema de seguridad que pueda identificar completamente al usuario y la fuente.

Figura 61

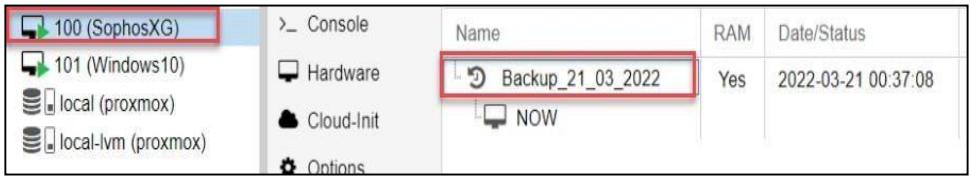
Respaldo de MV Sophos XG



Nota. Adaptación propia

Figura 62

Snapshot de MV Sophos XG

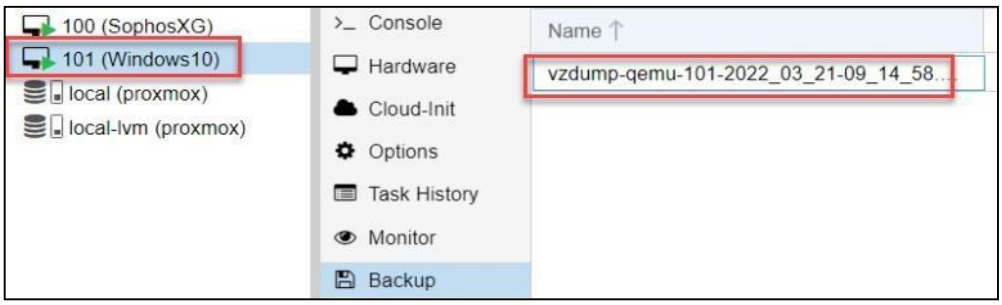


Nota. Adaptación propia

Windows 10 – 101

Figura 63

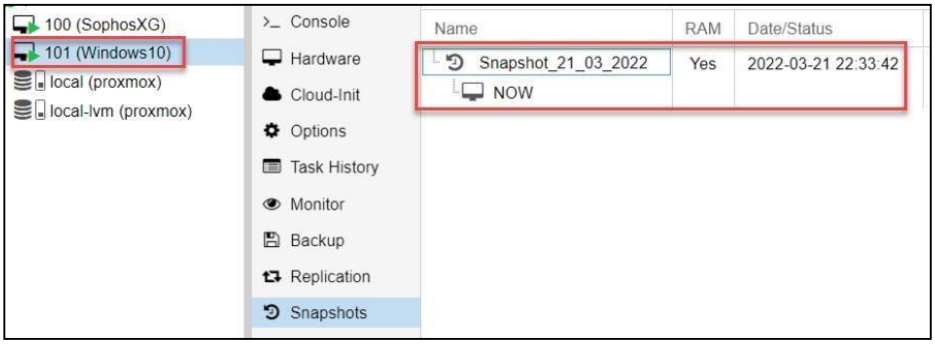
Respaldo de MV Windows 10



Nota. Adaptación propia

Figura 64

Snapshot de MV Windows10



Nota. Adaptación propia

4.5.5. Gestión del Equipamiento

Direccionamiento IP de Gestión de Proxmox

Para gestionar la plataforma de Proxmox y máquinas virtuales, se detalla las direcciones IP y modo de acceso.

Tabla 17

Direccionamiento IP de Gestión de Proxmox

PLATAFORMA	IP	ACCESO WEB	ACCESO DESDE ZONA
PROXMOX	192.168.12.252	https://192.168.12.252:8006	LAN
	10.10.10.12	https://10.10.10.12:8006	WAN
	10.0.0.1	https://10.0.0.1:8006	Conexión directa desde **eno4**

Nota. Adaptación propia

Usuario de Administración

Para el caso de la gestión del equipo instalado se le ha entregado el usuario de administración en modo lectura y escritura, se describe a continuación los usuarios:

Tabla 18

Usuario de Administración

PLATAFORMA	USUARIO	PERFIL
PROXMOX	root	Administrador

Nota. Adaptación propia

4.6. Implementación de Firewall Perimetral

4.6.1. Información de Firewall Perimetral LAB. Secundaria

Figura 65

Información del Firmware instalado

Nota. Adaptación propia

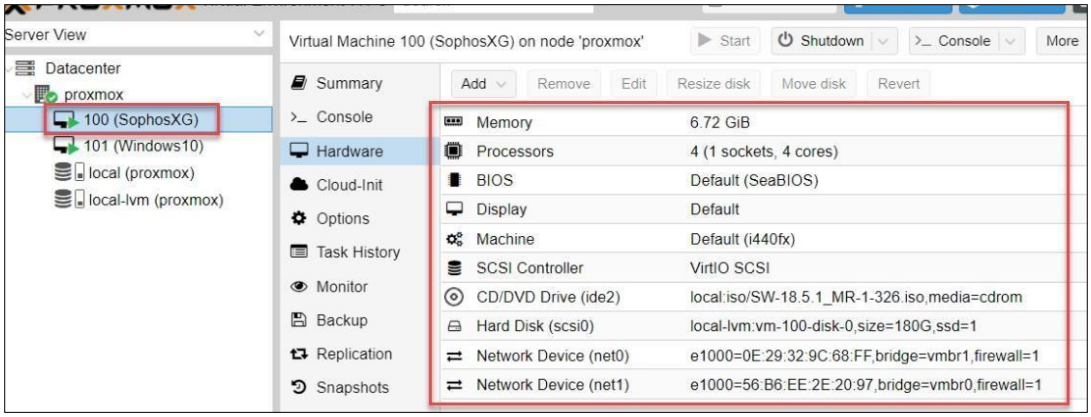
4.6.2. Información de Firewall como Máquina Virtual

El firewall se encuentra virtualizado bajo el entorno de virtualización PROXMOX-VE, este mismo tiene características específicas para su funcionamiento.

La imagen a continuación muestra los detalles y características de la Máquina Virtual asignados para el Firewall Sophos XG.

Figura 66

Descripción de Máquina Virtual Sophos XG



Nota. Adaptación propia

4.6.3. Interfaces

Para ubicar el módulo de las interfaces se debe de seguir la siguiente secuencia:

Ir a CONFIGURAR → RED →interfaces

Figura 67

Lista de interfaces de red

Nota. Adaptación propia

LAN: se configuro la interfaz PORT1 con la dirección IP 192.168.12.1/24. El equipo firewall está conectado directamente a un switch no administrable tomando como direccionamiento para toda la red 192.168.12.0/24.

WAN: Se configuro la interfaz PORT2 con la dirección IP 10.10.10.10/24 para la comunicación entre el equipo firewall y el Router.

Sobre este enlace se encuentran establecido la interconexión con la sede ILO a través de la conexión VPN IPSEC

4.6.4. Servicio DHCP

Un protocolo cliente/servidor conocido como Protocolo de Configuración Dinámica de Host (DHCP) asigna automáticamente a un host del Protocolo de Internet (IP) su dirección IP y otros datos de configuración necesarios, como la máscara de subred y la puerta de enlace predeterminada. En otras palabras, DHCP asigna direcciones IP a otros ordenadores de la red a través de un servidor central (un servidor, una estación de trabajo o incluso un PC). Este protocolo puede transmitir datos IP a través de una LAN o entre muchas VLAN.

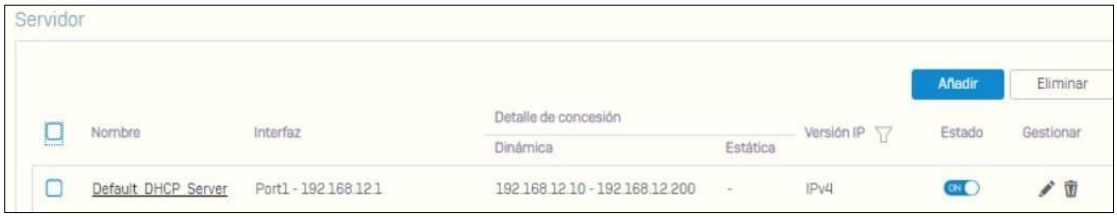
El firewall está configurado para brindar direccionamiento IP a través del protocolo DHCP.

Para ubicar el módulo se debe de seguir la siguiente secuencia:

Ir a CONFIGURAR → RED→ DHCP →Servidor

Figura 68

Servicio DHCP configurado



Nota. Adaptación propia

4.6.5. Perfiles de Seguridad

Un grupo de parámetros a los que se les ha dado un nombre constituyen un perfil de seguridad. Este conjunto de parámetros garantiza la seguridad en los ordenadores de sobremesa y dispositivos móviles adicionales. En otras palabras, puedes conceder a todos los usuarios y grupos los permisos que se incluyen en el perfil de seguridad. Los perfiles de seguridad facilitan el cambio de permisos para usuarios y grupos.

Perfil de Filtrado Web

Según lo solicitado por el cliente se crearon los siguientes grupos de filtrado web los cuales fueron aplicados a las políticas de firewall para establecer los permisos de navegación a Internet a través del filtrado por URL.

Para ubicar el módulo se debe de seguir la siguiente secuencia:

Ir a PROTEGER → WEB→ Políticas

Figura 69

Perfiles Web Filter

Nota. Adaptación propia

Perfil de Control de Aplicaciones

Se crearon los siguientes perfiles de Control de Aplicaciones, los cuales son utilizados para establecer los permisos de navegación hacia Internet a través del filtrado por aplicaciones.

Para ubicar el módulo se debe de seguir la siguiente secuencia:

Ir a CONFIGURAR → APLICACIONES→ Filtro de Aplicaciones

Figura 70

Perfiles de Control de Aplicaciones

Nota. Adaptación propia

Antivirus

Se configuró los siguientes perfiles de antivirus perimetral.

Este mismo analiza el tráfico de red entrante y saliente (por ejemplo, solicitudes DNS, solicitudes HTTP y paquetes IP) en busca de amenazas

Para ubicar el módulo se debe de seguir la siguiente secuencia:

Ir a CONFIGURAR → SERVICIOS DEL SISTEMA→ Protección contra Malware

Figura 71

Perfiles de Antivirus

Nota. Adaptación propia

IPS

Se Habilito y configuró los siguientes perfiles de protección contra intrusos.

Para ubicar el módulo se debe de seguir la siguiente secuencia:

Ir a PROTEGER → PREVECION DE INTRUSIONES→ Políticas IPS

Figura 72

IPS Habilitado / Firmas Actualizadas

Nota. Adaptación propia

Figura 73

Perfiles de IPS

Nota. Adaptación propia

4.6.6. Políticas de Seguridad

Se crearon las siguientes políticas de seguridad, los cuales son utilizadas para establecer los permisos de navegación hacia Internet.

Observación: las políticas que se encuentran deshabilitadas se habilitarán entorno de prueba, se incluirán las direcciones IP a los que se aplicara el filtro personalizado.

Para ubicar el módulo se debe de seguir la siguiente secuencia:

Ir a PROTEGER → REGLAS Y POLITICAS → Reglas de Firewall

Figura 74

Políticas de LAN hacia WAN

Nota. Adaptación propia

Es un canal que puede ser switch-switch o switch-router, a través del cual se transfiere la información que viene y va a más de una VLAN. El enlace troncal es una

configuración de canal para los puertos de conmutación de una red Ethernet que permite enviar muchas VLAN a través de un único enlace.

El firewall cuenta con conexión TRUNK para la interconexión con los recursos del LAB de Primaria.

Puerto TRUNK

La conexión permite establecer conectividad con los equipos Firewall Sophos del laboratorio de primaria denominado principal (sala de comunicaciones) través de la configuración Site to Site. Esto es de acuerdo con la política establecida

Para ubicar el módulo se debe de seguir la siguiente secuencia:

Ir a CONFIGURAR → VPN→ Conexiones IPSEC

Esta conexión permite la conectividad con los recursos. Detalle de conexiones establecidas:

Tabla 19

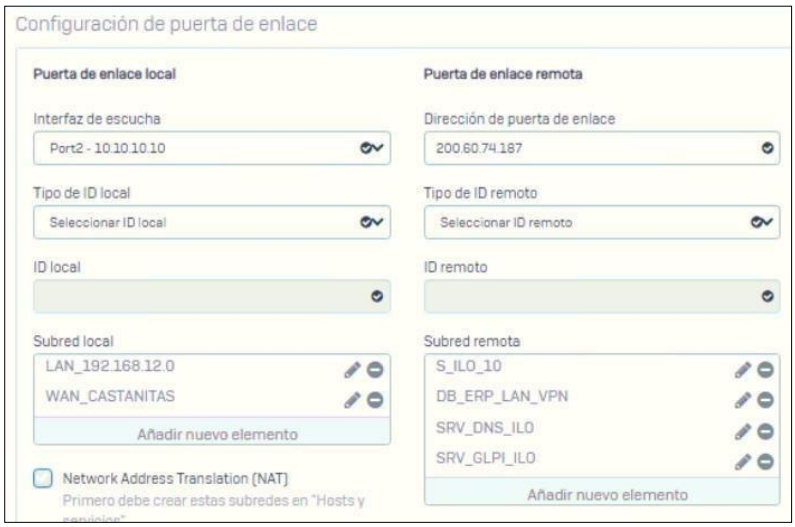
Conexiones

Lab. Secundaria	Lab. Primaria
192.168.12.0	192.168.11.0/24 192.168.20.2 192.168.20.5 192.168.20.10

Nota. Adaptación propia

Figura 75

Detalle de conexión entre laboratorios IE AMGS



Nota. Adaptación propia

4.6.7. Administración Centralizada – SOPHOS CENTRAL

Puede registrar los dispositivos de Sophos Firewall con Sophos Central y administrar los dispositivos de forma centralizada.

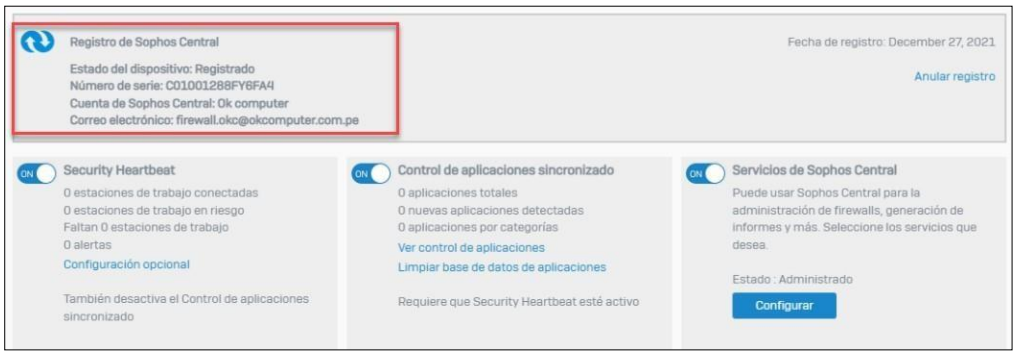
El firewall ya se encuentra registrado a Sophos central, por lo que no es necesario administrar de forma externo a través de una ip publica, en adelante la administración de este Firewall se realizara a través de la plataforma web de Sophos Central.

Para localizar el módulo hay que seguir los siguientes pasos:

Ir a SISTEMA → SOPHOS CENTRAL

Figura 76

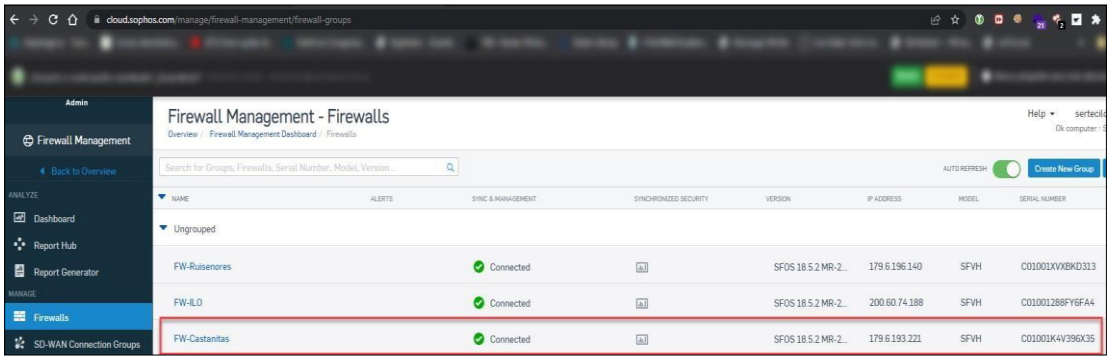
Detalle de registro a Sophos Central



Nota. Adaptación propia

Figura 77

Sophos Central – FW CASTAÑITAS



Nota. Adaptación propia

4.6.8. Respaldo Y restauración de Configuraciones Sophos XG

La gestión de copias de seguridad, actualizaciones del firmware puede administrarse desde la plataforma de Sophos.

Actualmente se ha configurado la programación de envío diario de copias de seguridad hacia el correo sertecilo@okcomputet.com.pe. Mientras que el respaldo de configuraciones puede realizarse subiendo el archivo de copia de seguridad más reciente y digitar la contraseña de cifrado.

Observación: Las credenciales de respaldo/restauración y contraseña maestra se encuentran detallados en el informe de credenciales.

Para localizar el módulo hay que seguir los siguientes pasos:

Ir a SISTEMA → COPIAS DE SEGURIDAD Y FIRMWARE

Para aplicar este tipo de autenticación fue necesario instalar STAS como recolector de inicios de sesión para luego enviarlos a Sophos, de esta manera podría haber una comunicación de inicio/cierre de sesión entre el servidor AD y Sophos.

4.6.9. Gestión del Equipamiento

Direccionamiento IP de Gestión de Firewall

Para el caso de la gestión del equipo por parte del cliente se ha configurado la siguiente dirección IP local para su respectiva administración.

Tabla 20

Direccionamiento IP

MAQUINA VIRTUAL	IP	ACCESO WEB
SOPHOS XG	192.168.12.1	https://192.168.12.1:4444 SOPHOS CENTRAL

Nota. Adaptación propia

Usuario de Administración

Para el caso de la gestión del equipo instalado se le ha entregado el usuario de administración en modo lectura y escritura, se describe a continuación los usuarios:

Tabla 21

Usuario de Administración

MAQUINA VIRTUAL	USUARIO	PERFIL
SOPHOS XG	admin	Administrador
	hchavez	Administrador

Nota. Adaptación propia

4.7. Resultados del Post-Test

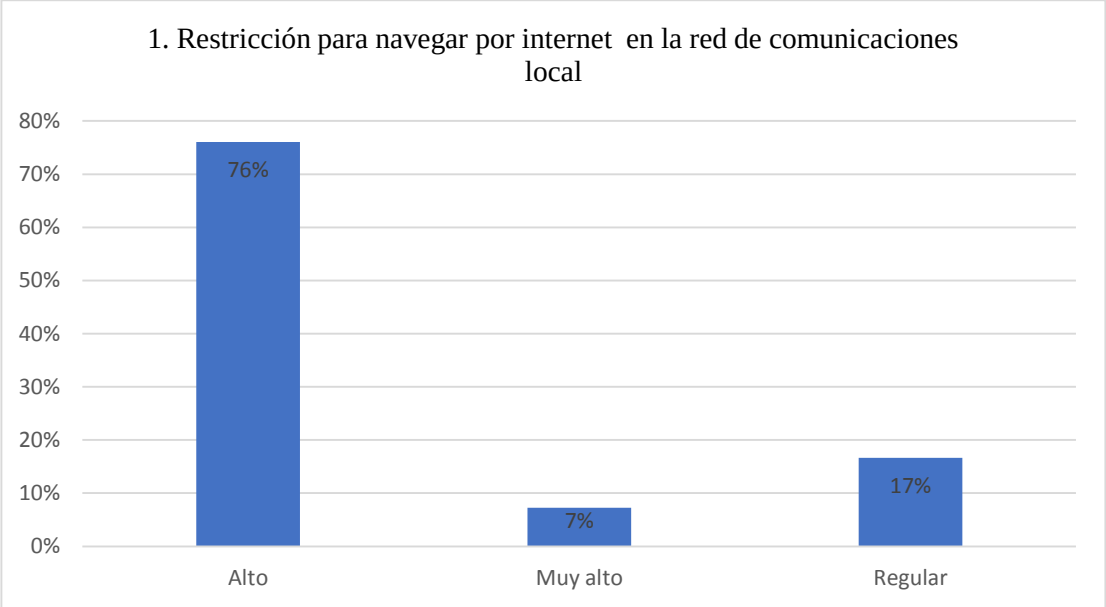
Se realiza el análisis de la encuesta después de la aplicación de la implementación, se realiza según las dimensiones planteadas.

4.7.1. Análisis de Dimensión Confidencialidad

Indicador: Nivel de políticas de seguridad

Gráfico 18

Restricción para navegar por internet en la red de comunicaciones local

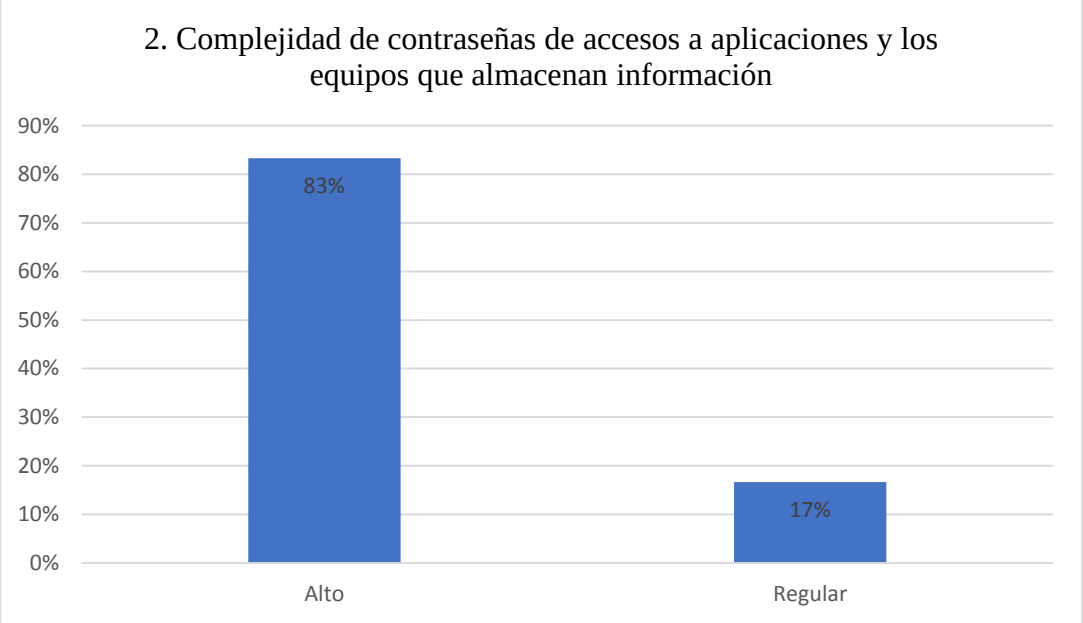


Nota. Adaptación propia

Después de la implementación se obtiene que para un 76% la restricción para navegar por internet es alto, es decir que encuentran dificultades para poder navegar, un 7% lo califica como muy alto, es decir que hay presencia de demasiadas restricciones, por lo que no se puede navegar libremente y un 17% afirma que es regular, es decir que no encuentran muchas restricciones.

Gráfico 19

Complejidad de contraseñas de accesos a aplicaciones y los equipos que almacenan información

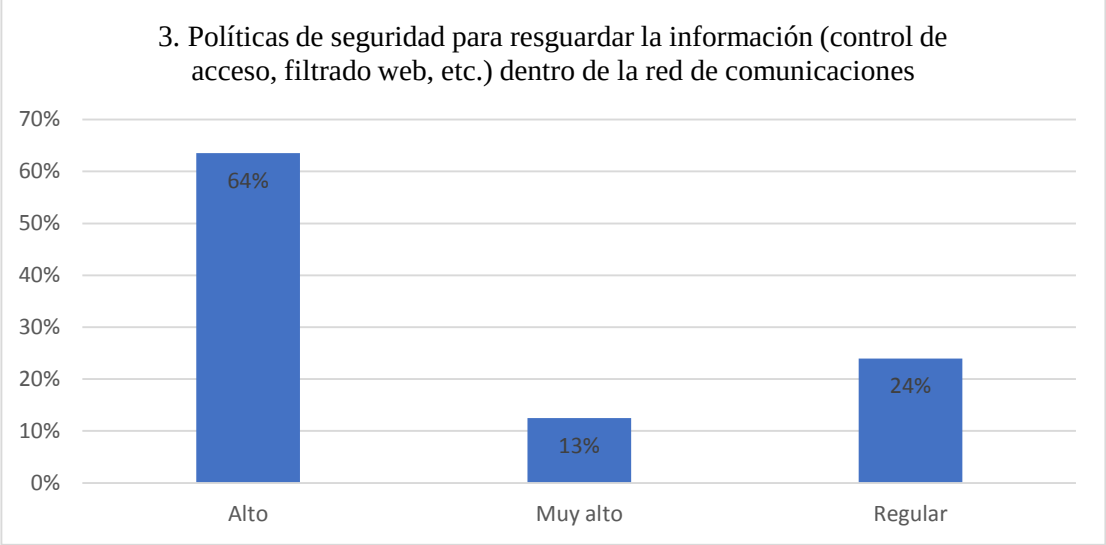


Nota. Adaptación propia

Los usuarios consideran que la complejidad de contraseñas es de nivel alto para un 83%, es decir que respaldan la información y no son vulnerables, para el otro 17% consideran que es regular por lo que todavía se puede implementar mejoras en el programa de seguridad.

Gráfico 20

Políticas de seguridad para resguardar la información (control de acceso, filtrado web, etc.) dentro de la red de comunicaciones

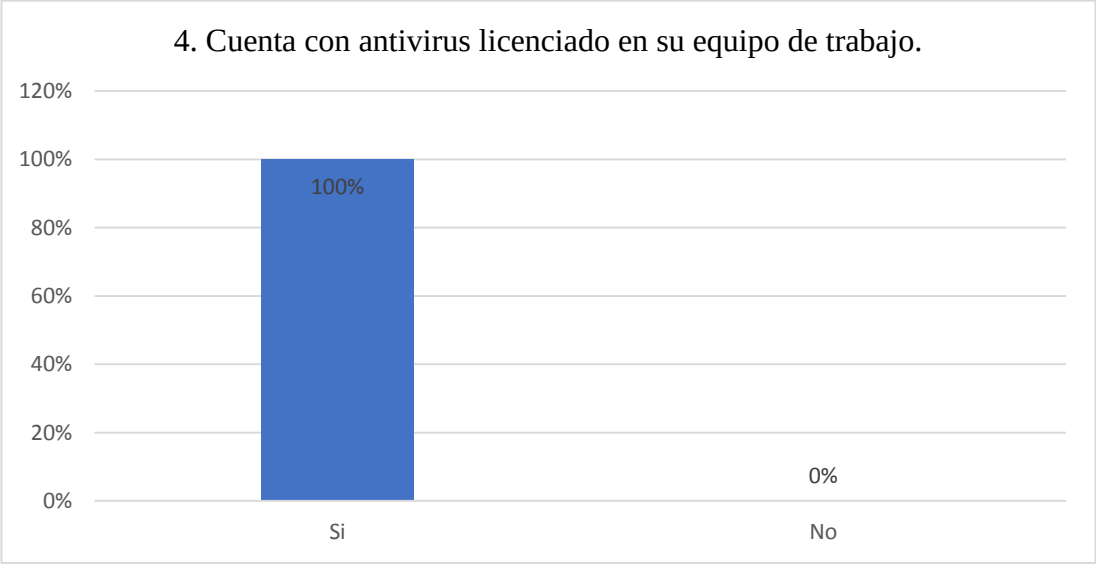


Nota. Adaptación propia

En caso de las políticas de seguridad con el nuevo software el 64% percibe que hay alta seguridad para resguardar la información, el 24% considera que es regular y el 13% lo califica como muy alto, es decir que se encuentran satisfechos por el funcionamiento del nuevo programa.

Gráfico 21

¿Cuenta con antivirus licenciado en su equipo de trabajo?

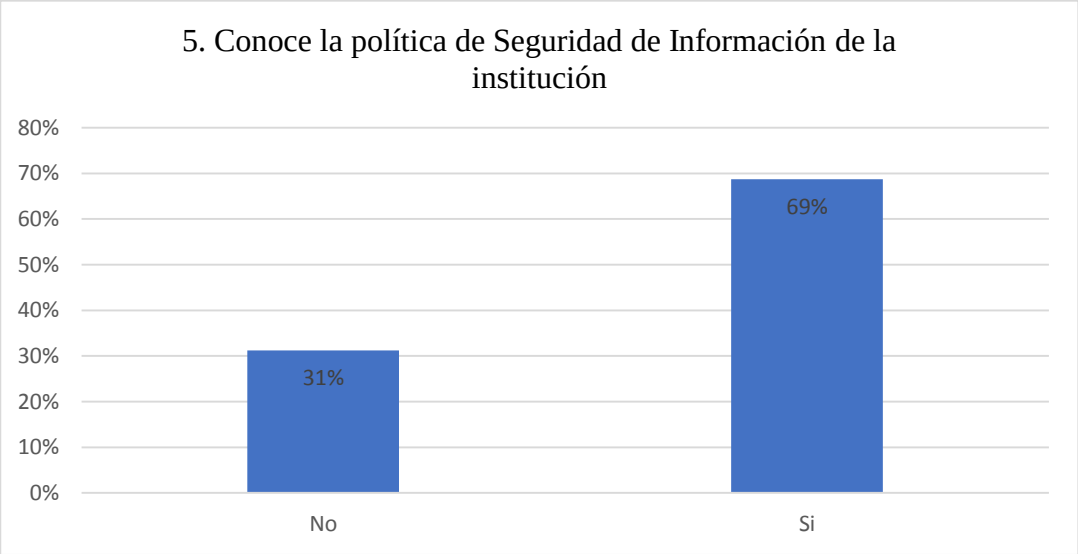


Nota. Adaptación propia

Para el cuidado de las computadoras se puede decir que el 100% cuenta con el antivirus licenciado, es decir todos resguardan el acceso a páginas que pueden infectar los programas o que se filtre la información.

Gráfico 22

Conoce la política de seguridad de información de la institución

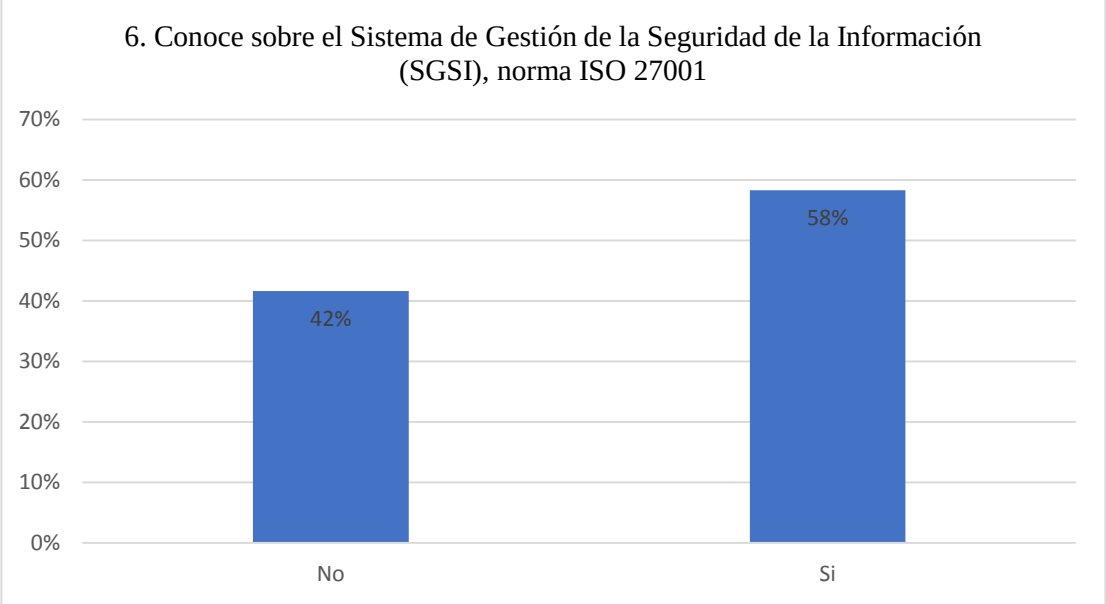


Nota. Adaptación propia

En el caso de conocimiento de las políticas de seguridad de información el 69% se encuentra informado de los términos de funcionamiento del programa que se implementó, sin embargo, el 31% no es conocedor de las políticas de seguridad.

Gráfico 23

Conoce sobre el Sistema de Gestión de la Seguridad de la información (SGSI), norma ISO 27001



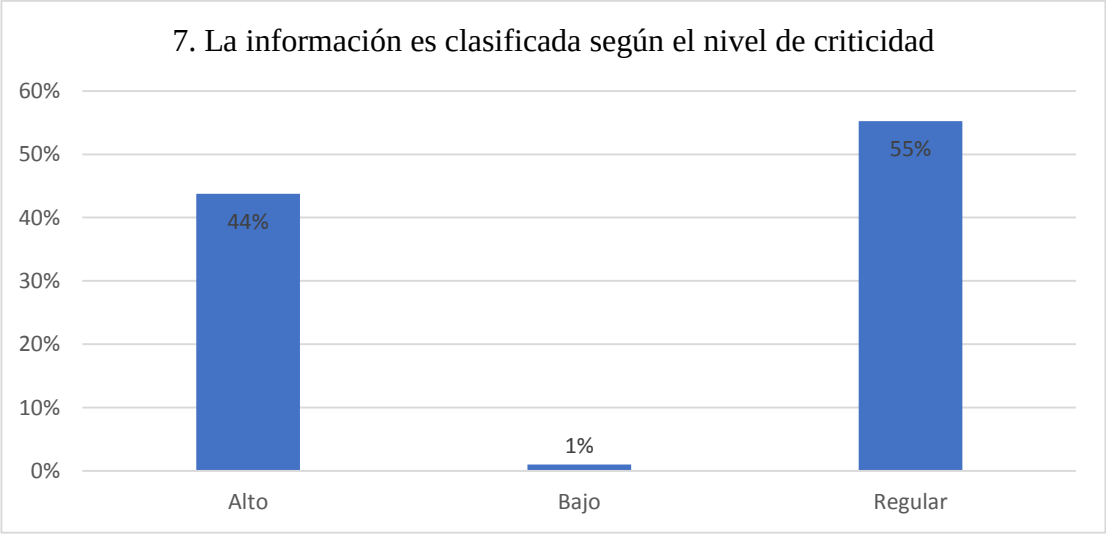
Nota. Adaptación propia

El 58% de los encuestados conoce los sistemas de gestión de la seguridad de la información, tienen información acerca de las políticas dentro de las normas, sin embargo, el 42% no tiene conocimiento de ninguna de las dos normas.

Indicador: Nivel de confidencialidad

Gráfico 24

La información es clasificada según el nivel de criticidad

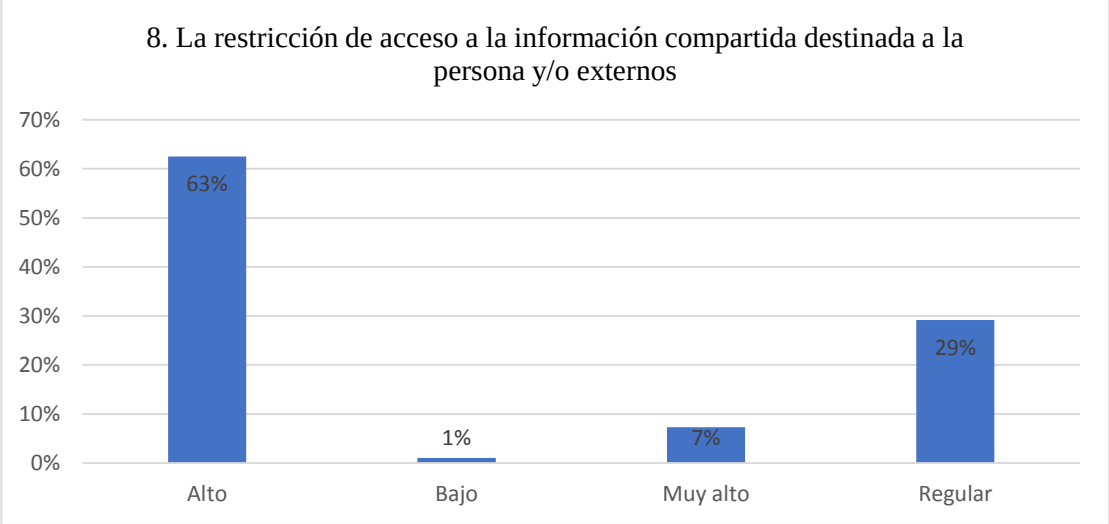


Nota. Adaptación propia

Para la clasificación según el nivel de criticidad el 55% lo califica como regular, es decir que hay buena clasificación de información evitando páginas de ocio o distracciones, el 44% lo califica como alto, no hay problemas en cuanto a la clasificación y el 1% considera que es bajo este aspecto.

Gráfico 25

La restricción de acceso a la información compartida destinada a la persona y/o externos

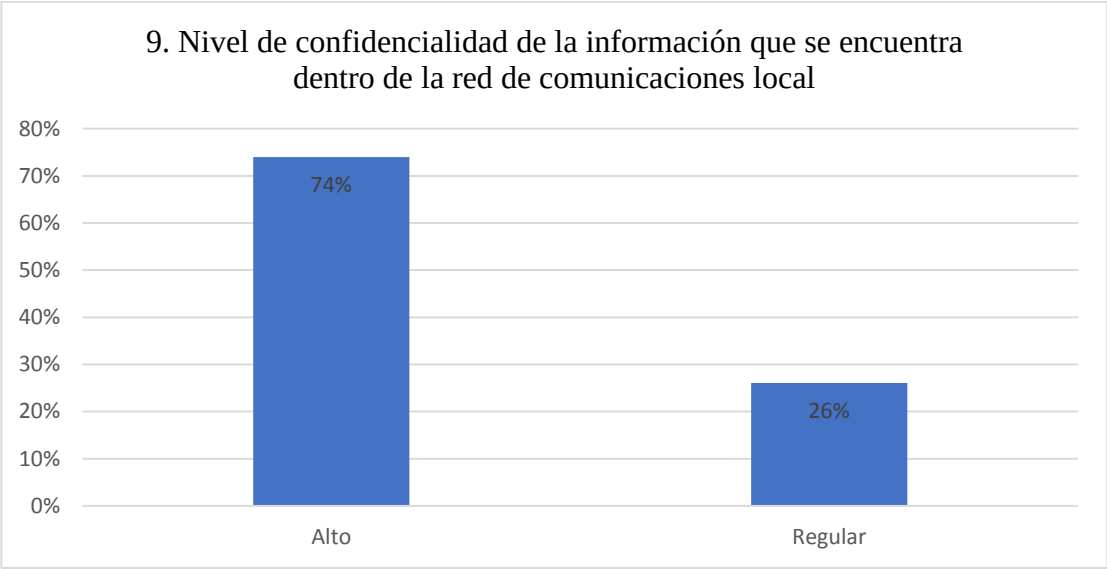


Nota. Adaptación propia

Para el caso de restricción de acceso a la información se tiene que 63% lo califica como alto, es decir que la implementación cumple con los estándares establecidos, el 29% considera que es de manera regular, el 7% percibe que es muy alto el grado de restricción de acceso a la información.

Gráfico 26

Nivel de confidencialidad de la información que se encuentra dentro de la red de comunicaciones local



Nota. Adaptación propia

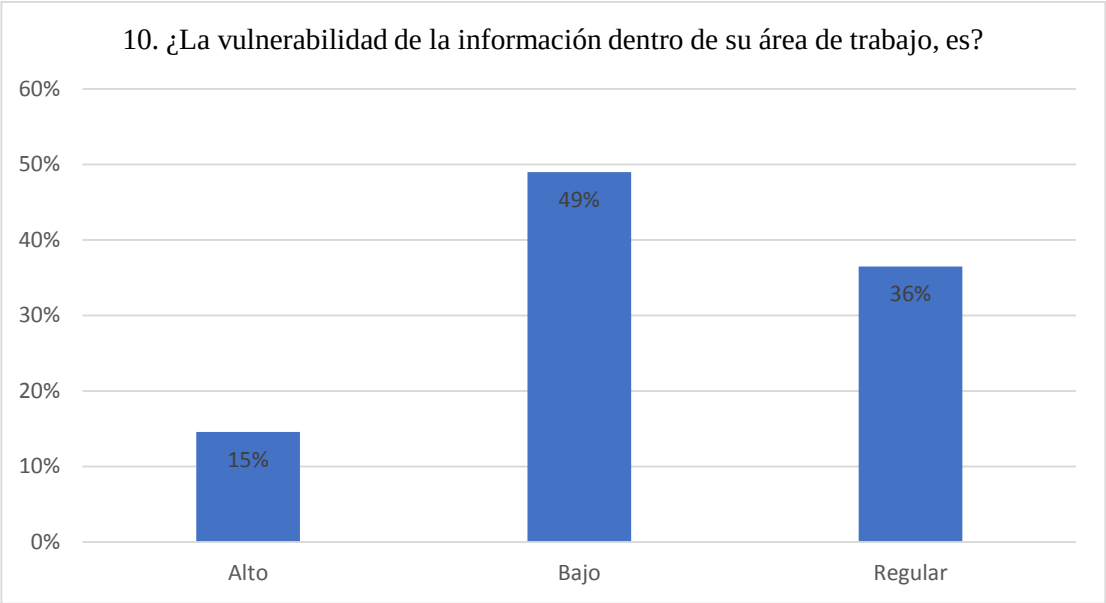
En caso del nivel de confidencialidad el 74% considera que es eficiente, se sienten seguros con la implementación, un 26% considera que es de forma regular, es decir que hay falencias o factores por los cuales no lo califican como alto el funcionamiento del programa.

4.7.2. Análisis de Dimensión Integridad

Indicador: Nivel de riesgo de los datos

Gráfico 27

¿La vulnerabilidad de la información dentro de su área de trabajo, es?

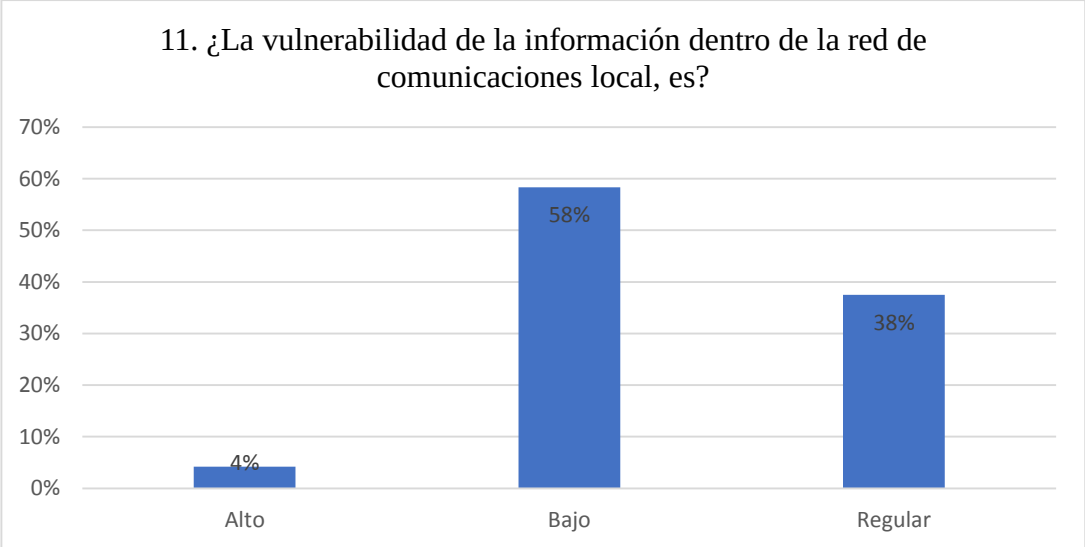


Nota. Adaptación propia

La vulnerabilidad se percibe como baja en 49%, es decir que al momento de navegar o colocar información no se sienten expuestos, en un 36% perciben que es de forma regular, lo que significaría que sienten riesgo al colocar información en otros programas, el 15% manifiesta que la vulnerabilidad es alta.

Gráfico 28

¿La vulnerabilidad de la información dentro de la red de comunicaciones local, es?



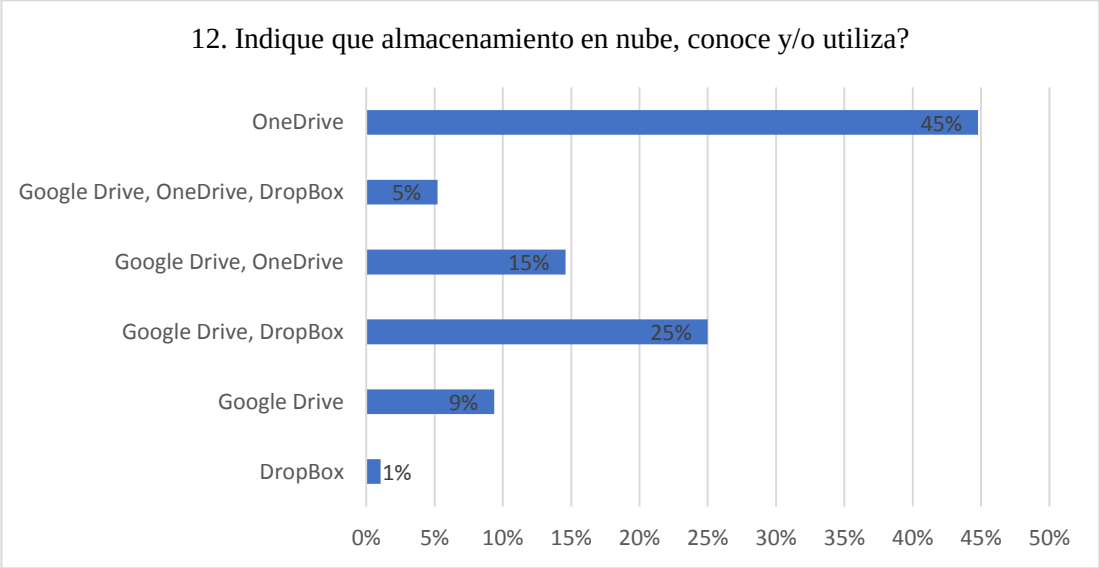
Nota. Adaptación propia

En caso de la red de comunicaciones local, se tiene que el 58% lo percibe como bajo, es decir que se sientes seguros del manejo de información en la red, el 38% considera que la vulnerabilidad es regular, no hay una eficiencia total, mientras que el 4% considera que hay vulnerabilidad alta.

Indicador: Manipulación de datos

Gráfico 29

Indique que almacenamiento en nube, conoce y/o utiliza

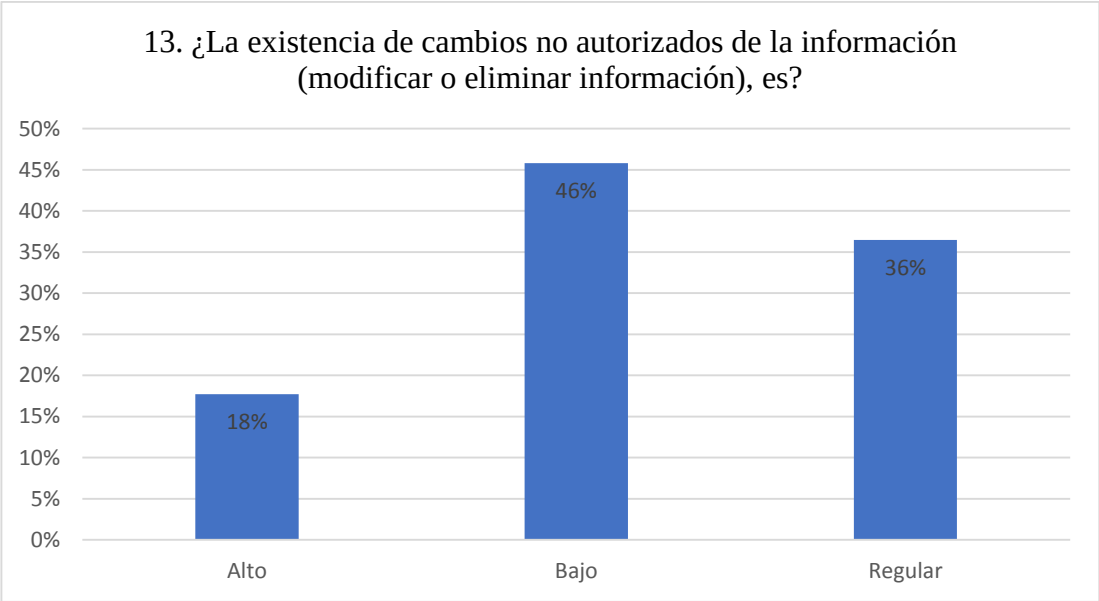


Nota. Adaptación propia

Para el conocimiento de almacenamiento en nube, las personas consideran en un 45% que conocen más OneDrive, en otro caso el 25% conoce Google Drive y Dropbox, siendo también plataformas de índice de confiabilidad alto.

Gráfico 30

¿La existencia de cambios no autorizados de la información (modificar o eliminar información), es?

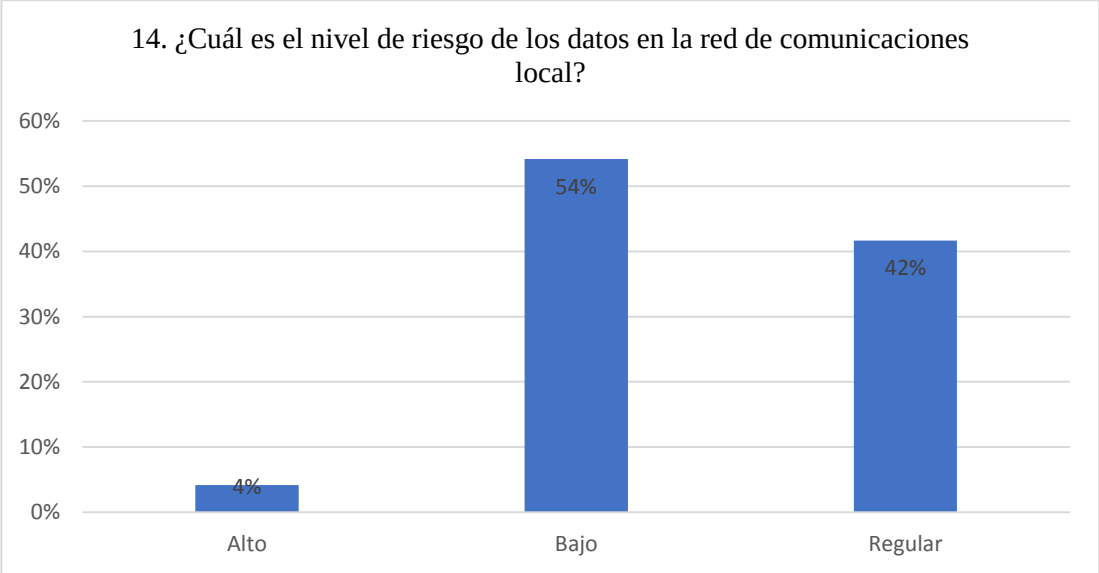


Nota. Adaptación propia

En caso de la existencia de cambios de información no autorizada el 46% de los encuestados percibe que es de nivel bajo, lo que quiere decir que no hay modificaciones o cambios no autorizados, por otro lado, el 36% manifiesta que los cambios se dan e forma reguilar y el 18% manifiesta que son altos estos cambios.

Gráfico 31

¿Cuál es el nivel de riesgo de los datos en la red de comunicaciones local?



Nota. Adaptación propia

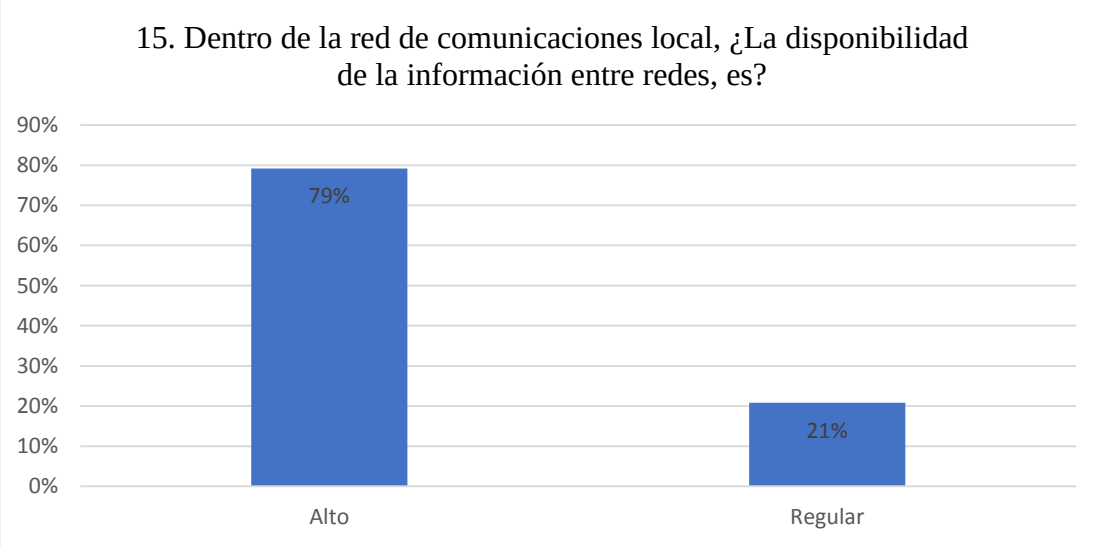
El nivel de riesgo de datos en la red según el 54% lo perciben como bajo es decir que no consideran que haya riesgo de los datos, un 42% considera que es de forma regular y para el 4% existe una percepción de alto riesgo para el manejo de sus datos en la red de comunicaciones local.

4.7.3. Análisis de Dimensión Disponibilidad

Indicador: Nivel de disponibilidad de los datos

Gráfico 32

Dentro de la red de comunicaciones local, ¿la disponibilidad de la información entre redes, es?

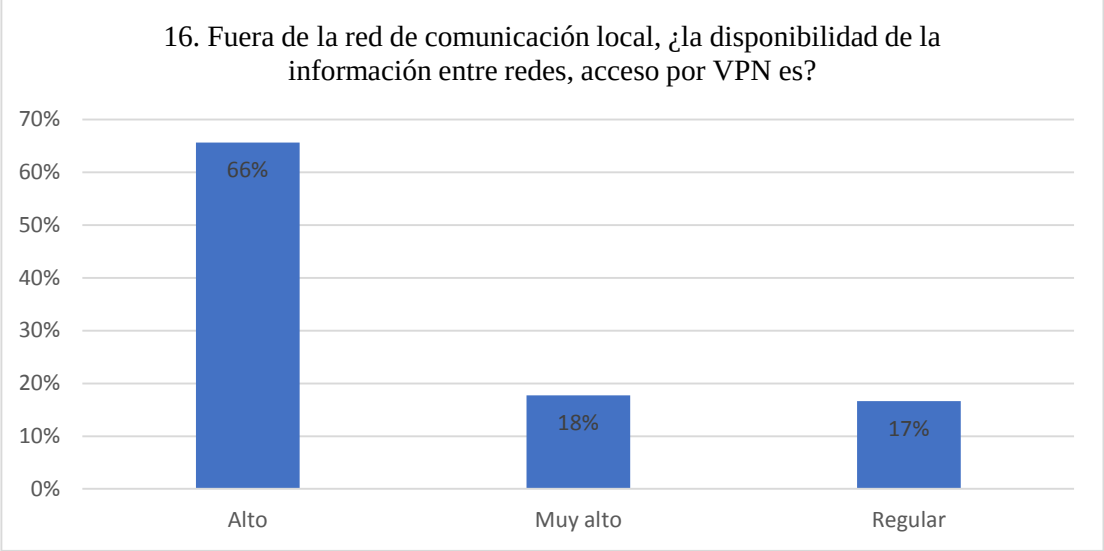


Nota. Adaptación propia

Para el 79% de las personas encuestadas la disponibilidad de información entre redes es de nivel alto, es decir que cuenta con variedad, el otro 21% consideran que es de nivel regular, no hay mucha disponibilidad de información.

Gráfico 33

Fuera de la red de comunicación local, ¿la disponibilidad de la información entre redes, acceso por VPN es?

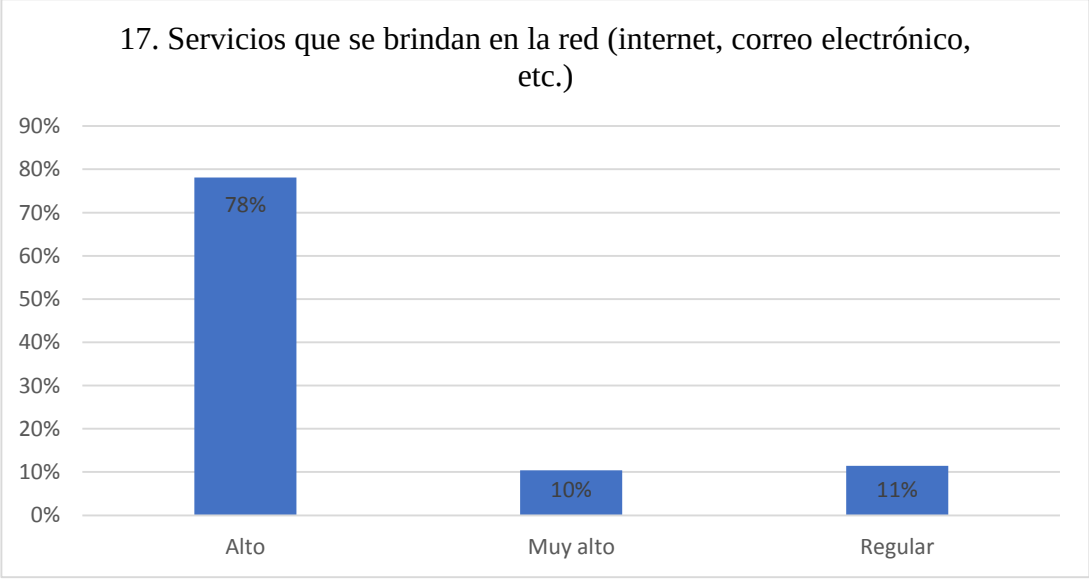


Nota. Adaptación propia

El 66% consideran que la disponibilidad de información entre redes por acceso VPN es alta, es decir que no tienen inconvenientes para el intercambio de información, el 18% considera que es muy alto, por lo que se encuentran satisfechos, el 17% considera que existe una disponibilidad regular.

Gráfico 34

Servicios que se brindan en la red (internet, correo electrónico, etc.)



Nota. Adaptación propia

Los servicios que se brindan en la red son de percepción alta para el 78%, el 10% considera que es muy alto los servicios que se brindan, no encuentran falencias dentro de su funcionamiento, en caso del 11% restante afirma que es de manera regular.

4.8. Comparación

En el análisis anterior se realizó la interpretación de los resultados obtenidos con la implementación del software, la mejora que se obtuvo es evidente debido a que en todas las dimensiones analizada y preguntas de medición se evidencia estos datos, así también estos datos se presentan en la Tabla N° 22.

Tabla 22

Comparación de datos Pre-test y Post-test

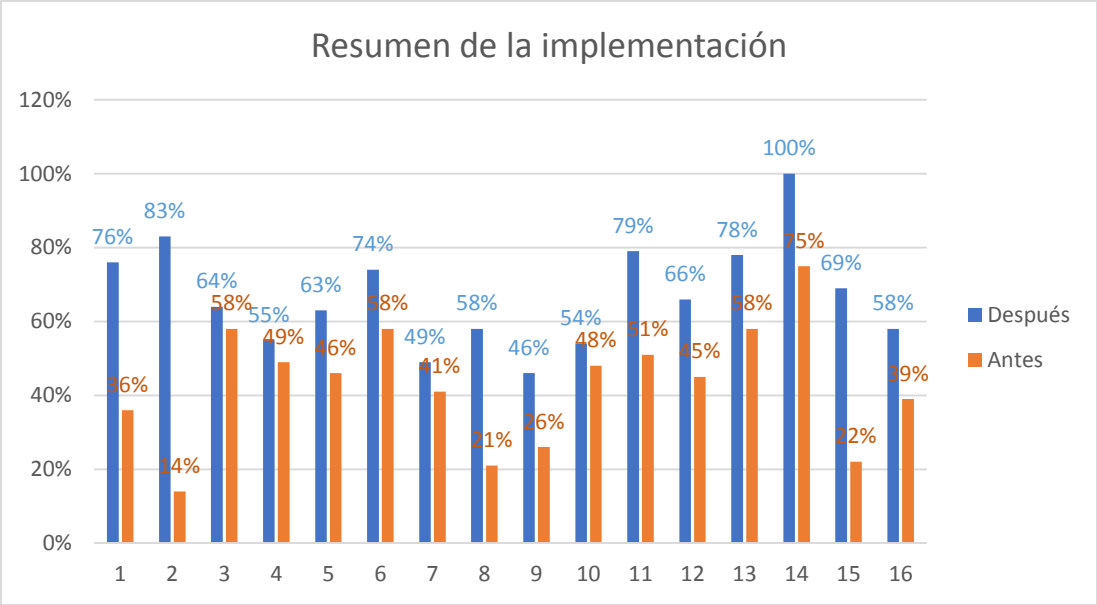
	ANTES	**DESPUES**
P1	Alto (36%)	Alto (76%)
P2	Alto (14%)	Alto (83%)
P3	Regular (58%)	Alto (64%)
P4	Si (75%)	Si (100%)
P5	Si (22%)	Si (69%)
P6	Si (39%)	Si (58%)
P7	Regular (49%)	Regular (55%)
P8	Regular (46%)	Alto (63%)
P9	Regular (58%)	Alto (74%)
P10	Regular (41%)	Bajo (49%)
P11	Bajo (21%)	Bajo (58%)
P13	Bajo (26%)	Bajo (46%)
P14	Regular (48%)	Bajo (54%)
P15	Alto (51%)	Alto (79%)
P16	Regular (45%)	Alto (66%)
P17	Alto (58%)	Alto (78%)

Nota. Adaptación propia.

Tal y como se observa en la tabla, la mejora es evidente para los encuestados quienes califican el funcionamiento del sistema de manera óptima; en diferentes aspectos de paso de una calificación regular a un alta, con lo que se puede concluir que el sistema está otorgando la seguridad y operación correcta.

Gráfico 35

Resumen de la implementación Antes - Después



Nota. Adaptación propia.

En el gráfico resumen que se presenta se observa la mejoría con la implementación del sistema, en los diversos aspectos evaluados muestra un incremento positivo que ayuda a evidenciar el cumplimiento de la función principal del software.

4.9. Discusión

Los resultados logrados a través de la investigación denotaron a través de la aplicación de encuestas para medir las variables mediante las dimensiones de confiabilidad, integridad y disponibilidad.

Respecto a la dimensión de confiabilidad en el caso de la variable seguridad de la información, se tiene en primera instancia que la restricción existente en el pre-test alcanza un nivel de 46% (regular), mientras que en el pos-test tiene una percepción de 76% (alto), lo que evidencia la mejora y la disminución de distracciones para los estudiantes. En comparación con el estudio de Bautista (2018), en el pre-test obtuvo un resultado de 32.8%, y al culminar la implementación tuvo una medición de 91%, alegando a la óptima implementación del software y al uso de programas que se contaban antes de realizar la mejora, sin embargo, en la Institución Educativa Ilo, no existía la presencia de programas o controladores que ayuden a mitigar estos problemas de manejo de información, con la implementación se logró tener el control acerca del acceso de información , y resguarde de datos evitando acceso a páginas o programas que sean una amenaza para la seguridad de información.

También con los resultados obtenidos se tiene una evidente mejora frente a los niveles de seguridad, ya que en otro indicador como las políticas de seguridad se obtuvo un 64% con la implementación, mientras que en el pre-test se alcanzó 14% de percepción alta, cumpliendo así con el objetivo de la eliminar ataques cyber.

Conforme a la dimensión de integridad en el caso de la variable seguridad de la información, en esta dimensión se analizó dos indicadores; nivel de riesgo de datos que tuvo un alcance de 22% antes de la implementación, donde el nivel de vulnerabilidad de la información era alto, sin embargo, en el post-test se obtuvo un 15% según percepción de los usuarios, en este caso también se evidencia que se logró reducir el riesgo al robo de información. Según el estudio de Pérez (2020), en la implementación del servicio Linux, logró proporcionar seguridad y control acerca del acceso como

también de la frecuencia de visita a las páginas, logrando mantener la mejora optima de la implementación, en el caso del estudio presente se logra obtener reportes de alerta y seguridad, con lo que se puede mitigar problemas que se identifiquen por acceso a páginas no verificadas o seguras. El otro indicador que se analizó fue de manipulación de datos, donde se determinó el índice de riesgo y vulnerabilidad de los datos que se proporcionan en web, en este caso se percibió que en el pre-test con un 58% percibían altos cambios no autorizados de la información, mientras que después de la implementación se identificó por 18% que estos ya no son muy frecuentes, lo que garantiza el eficiente funcionamiento del software.

Por otro lado, a la dimensión de disponibilidad en el caso de la variable seguridad de la información, se evaluó el indicador de disponibilidad de datos tanto en el lugar de trabajo como en la red de comunicación local, donde se identificó que la disponibilidad antes de la implementación fue de 51% alta según los usuarios, a comparación en el post-test se percibe un 79% de alta disponibilidad, en este aspecto se reafirma las ventajas y buen funcionamiento del software.

CAPITULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

Tras evaluar los resultados del tratamiento de los datos y de acuerdo con los objetivos iniciales, se formularon las siguientes conclusiones:

5.1.1. Conclusión general

Se implementó un sistema de seguridad perimetral bajo un software Linux en un entorno virtual para mejorar la seguridad perimetral en un Institución Educativa en Ilo. Para ello, se analizó los problemas más frecuentes y se realizó un test para medir la situación actual y las mejoras luego de la implementación. Dando como resultado una mayor seguridad para los laboratorios permitiendo un buen manejo de recursos a través de la virtualización asimismo el control de la seguridad perimetral e interconectividad entre laboratorios con la licencia y servicios actualizados, mediante la implementación de entorno de virtualización PROXMOX y la implementación de Firewall Perimetral.

5.1.2. Conclusiones específicas

Conclusión específica 1: Se concluye que la funcionalidad de la información de la institución educativa sin la implementación de un sistema de seguridad perimetral bajo un software Linux en un entorno virtual, en relación al objetivo específico 1, en el indicador de cumplimiento de servicios que brinda la red era de 69% y con la implementación mejoró a un 78% dando a entender que el software cumple con las características y estándares que contribuyen a la mejora continua. En caso del indicador de estabilidad logró mejorar de 39% a 42%. Entonces la implementación de un sistema de seguridad perimetral bajo un software Linux en un entorno virtual influye favorablemente en la funcionalidad de la información.

Conclusión específica 2: Se concluye que la confiabilidad de la información de la institución educativa sin la implementación de un sistema de seguridad perimetral bajo un software Linux en un entorno virtual, en relación al objetivo específico 2, era de 36% considerándose un indicador de tolerancia de fallas y con la implementación mejoró a un 76% dando a entender que las fallas se mitigaron y que la confiabilidad de información es más segura, sin riesgo a la filtración o cambios de información. Entonces la implementación de un sistema de seguridad perimetral bajo un software Linux en un entorno virtual influye favorablemente en la confidencialidad de la información.

Conclusión específica 3: Se concluye que el nivel de seguridad perimetral de la información de la institución educativa sin la implementación de un sistema de seguridad perimetral bajo un software Linux en un entorno virtual en relación al objetivo específico 3, era de 36% considerándose un indicador a la confidencialidad y con la implementación mejoró a un 76% dando a entender que las restricciones de

acceso a las páginas que sean distractoras u ocasionen ocio en los estudiantes; en caso de la integridad de información era de 22%, pero con la implementación se logró una disminución al 15% asegurando el respaldo de la información y datos que se proporcionan.

5.2. Recomendaciones

- Los resultados muestran que el nivel de seguridad de la información y de gestión de riesgos es adecuado; sin embargo, se aconseja poner en práctica las estrategias, como lo demuestran los programas de formación y sensibilización, así como el desarrollo y la utilización de indicadores de seguridad de la información.
- Reforzar las políticas de seguridad actualmente vigentes, teniendo en cuenta que la información es un activo muy importante y debe ser protegida de ataques enfocados al robo de información, modificación, entre otros.
- Debe existir constantemente capacitaciones a todo el personal que labora en la institución educativa., respecto a la seguridad de la información para evitar malas manipulaciones que puedan comprometer la seguridad.
- Se aconseja continuar con la investigación en el ámbito de las instituciones educativas y con los análisis anteriores para elegir el que mejor responda a los peligros actuales porque las amenazas y las vulnerabilidades, así como los sistemas de seguridad, evolucionan constantemente.

REFERENCIAS BIBLIOGRÁFICAS

Albujar, G. (2018). *Diseño de un sistema de seguridad de red centrado en la integración de los servidores Radius – Idap en Linux para facilitar el ingreso de la red de la Clínica Millenium Chiclayo 2016.* Chiclayo: UNPRG.

Alvarado Jaramillo, J. (2018). *Implementación de políticas de seguridad y control de navegación a través de un firewall centrado en Linux para TRIBUTAX Services S.A.* Ecuador: Univ. de Guayaquil.

Arévalo, F., Ordoñez, I., Peñaherrera, M., & Suárez, V. (2020). "Importancia de la seguridad de los sistemas de información frente el abuso y hurto de información". *Dominio de las ciencias*, 835-846.

Barrionuevo Mercedes, G., Giribaldi , M., Suarez , C., & Taffermaberry , C. (2017). *Virtualización en la Educación: Laboratorio Portátil de Redes.* XXIII Congreso Argentino de Ciencias de la Computación.

Bautista, O. (2018). *Implementación de un servidor Linux y su incidencia en la seguridad perimetral de la empresa Junefield Group S.A., Lima 2017.* Lima: UCV .

Bonilla Blanco, B., & Rojas Paternina, A. (2019). *Diseño y planificación de un centro de operaciones de seguridad informática aplicado como servicio por la organización A3SEC bajo marcos de trabajo propuestos por Sans, Isaca y Nist.* Universidad Piloto de Colombia.

Damián, A. (3 de septiembre de 2019). *Moodle, un sistema de gestión de aprendizaje en Ubuntu* . Ubunlog: https://www.solvetic.com/tutoriales/como-instalar-moodle-en-ubuntu-server-20-04/

Davantis. (4 de enero de 2019). *Seguridad Perimetral y sus beneficios*. DAVANTIS: https://www.davantis.com/que-es-la-seguridad-perimetral-y-cuales-son-sus-beneficios

De luz, S. (26 de Setiembre de 2016). *Conoce esta distro basada en CentOS/RHEL para crear tu propio servidor en casa u oficina*. Nethserver: https://www.redeszone.net//nethserver-conoce-esta-distro-basada-centosrhel-crear-propio-servidor-casa-u-oficina/

Díaz, D. (2019). *"Implementación de un prototipo de monitoreo de dispositivos de comunicación y usuarios finales utilizando el protocolo SNMP en software libre para una empresa e- Commerce".* Lima: UNMSM.

Digital Guide Ionos. (29 de mayo de 2019). *SNMP: El protocolo base para la gestión de redes*. Digital Guide Ionos: https://www.ionos.mx//servidores/know-how/

Doctors, A., & Vecchiotti, R. (2012). *Sistema de gestión y monitorización de fallas para clientes de Sannet* . Caracas : Centro de investigación de la Universidad Católica Andrés Bello.

Echevarría, M. (2014). Acceso abierto y software libre. *revista Universidad de Costa Rica*, 4-14.

Ersen, C. (18 de octubre de 2020). *Script de instalación automatizada de Zabbix y Grafana*. Fauno: https://faun.pub/zabbix-v5-0-and-grafana-automated-installation-script-6cd1a87cc36a

Espinoza, J. (2012). *Seguridad Perimetral* . Linares: CFT San Agustín .

Fabuel, C. (2013). *Implantación de un Sistema de Seguridad Perimetral.* Madrid : [tesis].

Fava, L. (2015). *Gerencia de redes de datos aplicando Java y SNMP.* La Plata: Centro de inv. de la Universidad de La Plata.

Figueroa, J., Rodríguez, R., Bone, C., & Saltos, J. (2017). La seguridad informática y de la información. *Polo del conocimiento*, 145-155.

Gálvez, R. (2019). *Análisis y propuesas para la seguridad de redes internas LAN y redes perimetrales utilizando TCP/IP y GNU/Linux en empresas del Ecuador.* Guayaquil: [tesis|.

Goldman, R. (2016). *Learning Proxmox VE* . Washington : Open Source .

Gomá, O. (2010). *Implementación de políticas de seguridad perimetral en la red LAN a través de un dispositivo UTM en la empresa Audifarma S.A.* Pereira: [tesis].

Gónzalez et al. (2003). *Software Libre* . Barcelona : Formación de Posgrado UOC .

González, J. (2011). El concepto de Software Libre . *Revista Tradumática* , 5-11.

Guamán, J. (2015). *Diseño de un sistema de gestión de seguridad de la información para instituciones militares* . Quito: [tesis].

Guerrero, D. (1998). *SNMP: Administración y Mantenimiento de Redes con Linux.* Madrid: Linux Jornal. http://redesdecomputadores.umh.es/snmp.htm

Heinz, F., & Da Rosa, F. (2007). *Guía práctica sobre Software Libre* . Montevideo: UNESCO .

Hernández, J. (2015). *Software Libre: Técnicamente Viable y socialmente justo.* Barcelona: Zero Fatory S.L.

Huertas Flores, E. (2022). *Seguridad de la información y la gestión de riesgos en el Instituto de Educación Superior Tecnológico Privado DETECSUR, Tacna – 2020.* Universidad José Carlos Mariátegui.

Jorba, J. (2010). *Introducción al sistema operativo GNU/Linux* . Barcelona: Centro de Investigación de la Universidad Oberta de Catalunya.

Jorge. (18 de junio de 2012). *Puertos y protocolos*. Sistemas Tu Web de Tecnología: https://nksistemas.com/curso-de-redes-y-protocolos/

Kirch, O., & Dawson, T. (2000). *Guía de administración de redes con Linux.* O'Reilly & Associates.

Lederkremer, M. (2019). *Redes Informáticas.* Six Ediciones. https://doi.org/https://books.google.es/books?hl=es&lr=&id=7frADwAAQBAJ&oi=fnd&pg=PA1&dq=Red+de+inform%C3%A1tica+que+cubre+%C3%A1reas+geogr%C3%A1ficas+peque%C3%B1as+con+un+alcance+de+1-5+km,+es+decir+con+extensi%C3%B3n+f%C3%ADsica+limitada.+De+este+modo,+distintos+dispos

López, G. (2015). *Sistema de seguridad perimetral para la red de datos de la Industria Floralp S.A. centrado en la plataforma de software libre.* Ibarra: [tesis].

Marín, J., Patiño, A., & Acevedo, J. (2020). Implementación de un sistema de seguridad perimetral informático usando VPN. *Rev. Universidad Católica de Oriente*, 84-99.

Méndez, A. (20 de julio de 2016). *Syslog Protocolo y servicios* . SILO Inc. : https://silo.tips/download/syslog-protocolo-y-servicios

Mora, E., & Villero, S. (2020). Importancia de la implementación de firewall en redes empresariales como mecanismo para la protección de información. *Ciencia e Ingeniería*, 28-35.

Morales, F., Toapanta, S., & Toasa, R. (2020). Implementación de un sistema de seguridad perimetral . *RISTI*, 553-565.

Ochobits, D. (28 de agosto de 2015). *Entornos virtuales*. ochobitshacenunbyte: https://www.ochobitsha.com/2015/08/28/entornos-proxmox/

Oré, A. (2019). *Implementación de un Sistema de Monitoreo para lograr la continuidad de los Servicios en un Data Center Utilizando Protocolo SNMP*. Lima: UTP.

Oscar. (13 de octubre de 2010). *Syslog : La piedra angular de los registros del sistema*. Ocubom: https://ocubom.wordpress.com/2010/10/13/-piedra-angular-de-los-registros-del-sistema/

Preciado Becerra, M., & Vargas Herrera, M. (2016). *Guía de contratación de servicios en la nube para empresas públicas y privadas en colombia que garantice un correcto análisis forense cuando se presenten incidentes de seguridad.* Bogotá: Universidad Piloto de Colombia.

Ruales, C. (2016). *Auditoría de Seguridad perimetral en dispositivos de capa 3 para entornos empresariales utilizando Kali Linux.* Guayaquil: [tesis de posgrado|.

Seoane et al. (2007). *Introducción al Software Libre* . Madrid : Some Rights Reserved.

SIMAD. (12 de abril de 2012). *Seguridad Perimetral frente a las amenazas*. SIMAD: http://www.si-mad.com/seguridad-perimetral-ante-las-amenazas-

Stallman, R. (2004). *Software libre para una sociedad libre* . Madrid: Traficantes de Sueños.

Torres, S., Gómez, W., & Culebro, M. (2006). *Software libre vs software propietario Ventajas y desventajas.* México DF.: Creative Commons.

Walton, A. (12 de Junio de 2018). *Syslog: Funcionamiento y Configuración*. CCNA desde cero: https:///syslog-funcionamiento-y-configuracion/

Yánez, C. (2008). *Diseño e implantación de plataforma de seguridad perimetral informática: Dirección ejecutiva de la Magistratura.* Barranquilla: [tesis] .

ANEXOS

ANEXO 1

TÍTULO: Implementación de un sistema de seguridad perimetral bajo un software Linux en una institución educativa de Ilo – 2021

INVESTIGADOR: Heber Jesús Chávez Choque

	PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	MÉTODO TIPO Y NIVEL DE INVESTIGACIÓN
GENERAL	¿La implementación de un sistema de seguridad perimetral bajo un software Linux en un entorno virtual mejorará la seguridad perimetral de una I.E. en Ilo - 2021?	Implementar un sistema de seguridad perimetral bajo un software Linux en un entorno virtual para mejorar la seguridad perimetral de una I.E. en Ilo - 2021.	La Implementación del sistema de seguridad perimetral bajo un software Linux en un entorno virtual mejora la seguridad perimetral de una I.E. en Ilo - 2021. La funcionalidad del software Linux un entorno virtual para la seguridad perimetral de	Variable Independiente (X): Software Linux. Dimensiones: Funcionalidad Confiabilidad . *Indicadores:* Nivel de Estabilidad del servidor Cumplimientos de servicio que brinda a la red Tolerancia de fallos	*Tipo de investigación* Aplicativa. *Diseño de la investigación*: Diseño experimental. *Población*: la población está conformada por 127 personas entre profesores y administrativos de la Institución Educativa
ESPECÍFICOS	¿Cómo es la funcionalidad del software Linux en un entorno virtual en la seguridad perimetral de una I.E. en Ilo - 2021?	Determinar la funcionalidad del software Linux un entorno virtual para la seguridad perimetral de una I.E. en Ilo - 2021.			

	¿Cómo es la confiabilidad del software Linux en un entorno virtual en la seguridad perimetral de una I.E. en Ilo - 2021?	Determinar la confiabilidad del software Linux un entorno virtual para la seguridad perimetral de una I.E. en Ilo - 2021.	una I.E. en Ilo - 2021 es buena. La confiabilidad del software Linux un entorno virtual para la seguridad perimetral de una I.E. en Ilo – 2021 es buena. El nivel de seguridad perimetral que perciben los docentes y el personal administrativo de una I.E. en Ilo antes y después de la implementación del sistema de seguridad perimetral bajo un Software Linux en un	Variable Dependiente (Y): seguridad perimetral. Dimensiones: Ataques informáticos. Gestión de datos. *Indicadores:* Nivel de ataques informáticos. Tipos de ataques cibernéticos. Herramientas de seguridad. Nivel de eficiencia de gestión de datos.	*Muestra* Mientras que la muestra a considerar en la investigación será un total de 96 personas entre profesores y administrativos pertenecientes a la Institución Educativa. Distribución de la muestra Instrumento de recolección de datos: Cuestionario
	¿Cuál es nivel de seguridad perimetral que perciben los docentes y el personal administrativo de una I.E. en Ilo antes y después de la implementación del sistema de seguridad perimetral bajo un Software Linux en un entorno virtual?	Determinar el nivel de seguridad perimetral que perciben los docentes y el personal administrativo de una I.E. en Ilo antes y después de la implementación del sistema de seguridad perimetral bajo un Software Linux en un entorno virtual.			

			entorno virtual es distinta.		