UNIVERSIDAD SAN PEDRO

FACULTAD DE INGENIERÍA

PROGRAMA DE ESTUDIOS DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

Seguridad perimetral de la red informática de la Compañía Minera Santa Luisa Unidad Pallca

Tesis para obtener el título profesional de ingeniero en informática y de sistemas

Autor

Caldas Tarazona, Gerson Waldir

Asesor

Martínez Carrión, Javier

Código ORCID: 0000- 0002- 0741-5458

Chimbote – Perú

2022

ÍNDICE

Palabras claves

Tema	Seguridad informática
Especialidad	Infraestructura de Tecnología de la Información

Keywords

Theme	Informatic security
Specialty	Information Technology Infrastructure

Línea de investigación

Línea	Infraestructura de tecnología de la información
Área	Ingeniería y tecnología
Sub área	Ingeniería informática
Disciplina	Telecomunicaciones

TÍTULO

Seguridad perimetral de la red informática de la Compañía Minera Santa Luisa Unidad Pallca

RESUMEN

La investigación realizada de seguridad perimetral para la compañía Minera Santa Luisa, tuvo como objetivo realizar la propuesta de la implementación para la mejora de la seguridad de la red informática, donde se consideró la protección de perímetros logicos, detectar las diferentes tentativas de intrusión y/o disuasión de intrusos en instalaciones especialmente sensibles. La metodología de estudio tuvo un componente investigativo de tipo descriptivo, teniendo en cuenta que será necesaria la recolección de información para lograr la propuesta de implementación de un equipo de seguridad perimetral y para lograr la implementación usaremos la metodología PPDIOO de CISCO. El resultado logrado de la investigación, fue proponer nuestro proyecto, con la cual se fortalecen los parámetros de seguridad que sean necesarios para mejorar los mecanismos que ayuden asegurar los dispositivos informáticos que presenta la red informática de la minería Santa Luisa.

ABSTRACT

The investigation carried out on perimeter security for the Minera Santa Luisa company, had the objective of making the proposal for the implementation to improve the security of the computer network, where the protection of physical perimeters was considered, detecting the different attempts of intrusion and/or or deterrence of intruders in particularly sensitive installations. The study methodology had a descriptive investigative component, taking into account that the collection of information will be necessary to achieve the proposal for the implementation of a perimeter security team and to achieve the implementation we will use the CISCO PPDIOO methodology. The result of the investigation was to propose our project, with which the security parameters that are necessary to improve the mechanisms that help secure the computer equipment of the Santa Luisa mining network are strengthened.

INTRODUCCIÓN

En la indagación bibliográfica efectuada, se han encontrado estudios referentes al tema de la investigación a realizar. En el contexto nacional tenemos los aportes de los siguientes investigadores como es el caso de:

Según Delgado (2018), en su tesis denominada "Implementación de una solución de seguridad perimetral Open Source en La Red Telemática de la Universidad Nacional Pedro Ruiz Gallo", tuvo por objetivo implementar una solución de seguridad perimétrica open source, para que cubra los requerimientos de una red perimetral DMZ y todos los servicios internos que contengan. Además, se muestra la instalación del software pfSense en un ambiente de pruebas controlado para luego ser puesto en producción. La investigación fue no experimental y descriptiva. Como población en este estudio hemos considerado 7 servicios los cuales la red telemática proporciona, por ello se define que la población es infinita. En promedio se pudo calcular 1067 ataques de accesos no deseados y que fueron divididos entre los 7 servicios que tiene la red. Los resultados obtenidos permitieron obtener hacer un análisis exhaustivo y hacer las recomendaciones necesarias para tener un nivel de seguridad óptimo.

Según Guevara y López (2016) en su tesis tuvieron como objetivo implementar un sistema criptográfico a través de algoritmos avanzados de encriptación para mejorar la seguridad perimetral de una red informática. Como metodología se usaron teorías relacionadas con un sistema criptográfico a través de algoritmos avanzados de encriptación denominada Metodología Cisco para el diseño de redes. La población que se consideró fue la cantidad de data enviada y recibida en la red perimetral de la institución "ABACO". Los tipos de investigación usados en el trabajo fueron las siguientes: tipo aplicada puesto que se aplicaron diversas teorías planteadas en investigaciones pasadas; y de tipo explicativa ya que se explicó cómo la variable independiente influye en la variable dependiente. Las conclusiones principales obtenidas fueron: se identificaron diversos factores que influyen en la seguridad perimetral de la red y que permitieron hacer una reestructuración del diseño.

Según Grados y Ventura (2014) en su tesis, tuvo por objetivo diseñar el sistema de seguridad perimetral para mejorar la performance de la red de datos mediante un sistema de seguridad perimetral. La metodología empleada para el diseño sistema de seguridad perimetral fue de Telecommunications Management Network (TMN) que es una metodología de redes de datos basada en modelos funcionales estándar de la ITU. La población y muestra elegida en la investigación fue con todas las personas relacionadas con la empresa. Las conclusiones más sobresalientes fueron: se analizaron y documentaron la situación actual de los sistemas de seguridad perimetral encontrando las principales necesidades de los colaboradores y los clientes que estén relacionados con la tecnología. Se concluye además que el diseño de un sistema perimetral mejora de manera significativa los servicios de comunicación de la organización.

Según Mero (2018) en su tesis tuvo como objetivo plantear un esquema de seguridad perimetral en la red de datos del Consejo Nacional Electoral Delegación Santa Elena, basado en estándares de gestión y principalmente en las normas y el uso de las mejores prácticas con la finalidad de tener una red efectiva y que pueda soportar de mejor manera las aplicaciones de la misma. Se usaron las mejoras prácticas propuestas por ITIL como metodología de la investigación. En cuanto a la población y muestra que se consideró para el desarrollo del presente proyecto fueron todas las personas integrantes del personal administrativo y las personas que trabajan directamente con la unidad de TICS de la empresa. Los tipos de investigación aplicados en el trabajo fueron: bibliográfico y de campo. Como resultado de la investigación realizada se concluye lo siguiente: Las herramientas de tecnología son inseguras en la medida que su utilización no sea la más adecuada en la organización, convirtiéndose así en objeto de amenazas y que la seguridad de la información es tarea de todos quienes laboran en la institución indistintamente del nivel en el que se encuentre y por tal motivo debe estar regida por políticas claras en seguridad de la información.

Según Aragón (2018) en su tesis denominada “Análisis y propuesta de mejoramiento del Sistema de Seguridad Perimetral aplicable a institución Publica

de Seguridad Social", la investigación tuvo como objetivo realizar un análisis del sistema de seguridad perimetral en base a las metodologías propuestas por Cisco Systems (PPDIOO, Top-Down), Check Point (SDP), IBM (ISF) que permitan el mejoramiento de la arquitectura de seguridad perimetral. La metodología que se utilizó estuvo basada en la metodología Check Point SDP, que permite el aprovechamiento de la actual segmentación de componentes, agrupación de servicios, naturaleza de servicios y aplicaciones, estructura de la red disponible. Entre las conclusiones se consideró que la arquitectura SDP Check Point es una metodología necesaria para la planeación y creación de sistemas de seguridad. Además, esta metodología se preocupa en proteger todo el contenido de la red y sus servicios partiendo desde una estación de trabajo hasta los servicios ofrecidos por la institución.

Según Bohorquez y Paez (2017), en su tesis tuvieron como objetivo proponer un sistema de seguridad perimetral con características de protección en la infraestructura física y lógica de las instalaciones del consorcio PTAR salitre que permitiera: realizar la implementación de un sistema de seguridad perimetral por anillos; generar el aseguramiento de la capa de red según modelo OSI; manejar la información por roles y perfiles de acceso. La metodología que se utilizó para el desarrollo fue dividida en fases de implementación, las cuales pueden ser aplicadas en el orden ascendente o descendente, según el criterio que deseen usar en el Consorcio. La población y muestra fueron los empleados vinculados al consorcio quienes respondieron las encuestas mediante correo electrónico. Entre las conclusiones se consideró realizar la implementación de un sistema de seguridad perimetral por anillos.

La fundamentación científica que sustenta la investigación se fundamenta con la variable de estudio que tiene que ver con los siguientes conceptos como:

Seguridad perimetral

De acuerdo con Fabuel (2013) esta seguridad constituye una barrera entre la red interna de una organización y el internet, en donde su finalidad es controlar los datos que ingresan o salen de la empresa. Su ventaja es que permite al administrador de la red concentrarse en los puntos de entrada sin dejar de lado los demás servidores y protegerlos así ante cualquier ataque externo.

El autor sostiene que existen diversos factores dentro de la seguridad perimetral, tales como:

- Se rechazan conexiones con servicios comprometidos
- Se permite ciertos tipos de tráfico de datos
- Proporciona un punto de interconexión con el exterior
- Redirige el tráfico que ingresa a los sistemas internos
- Oculta diversos tipos de servicios que no se pueden proteger desde la internet.
- Es capaz de auditar el tráfico interno y externo
- Oculta información, los nombres de los sistemas, las topologías, dispositivos, cuentas, entre otros.

Normas ISO

Son normas o estándares que fueron establecidas por la ISO (Organización Internacional para la Estandarización) y por la IEC (Comisión Electrotécnica Internacional) y que se encargan de definir estándares y protocoles que se relacionan con los sistemas de gestión y que se pueden aplicar a cualquier organización con la finalidad de mejorar y facilitar el comercio y el intercambio de la información.

Entre los más conocidos se tienen:

- ISO/IEC 27001. Aquella norma que regula los requisitos para la implementación de los sistemas de gestión de la seguridad de la información.
- ISO/IEC 27002. Es el código de las buenas prácticas para una buena gestión de la seguridad de la información.

- ISO/IRC 27033. Aquella norma que brinda una guía detallada de la seguridad, encargada de su gestión, de la aplicación de los servicios, y de la seguridad de la información,

a) Objetivos de la seguridad informática

De acuerdo con Voustass (2010), el objetivo de la seguridad informática es mantener los riesgos al mínimo sobre los recursos informáticos y garantizar la continuidad de los procesos de la empresa mientras se reducen los riesgos informáticos. Además, como segundo objetivo, se tiene que garantizar que todos los documentos y archivos informáticos deben tener la confiabilidad necesaria y en donde se cumplan seis características: permanencia, accesibilidad, disponibilidad, confidencialidad, integridad y aceptabilidad.

b) Clasificación de la seguridad informática

i. Seguridad activa y pasiva

- La seguridad activa está relacionada con todas las medidas que se usan para detectar amenazas y poder gestionar los mecanismos correctos para evitarlos. Como por ejemplo los antivirus o cortafuegos (Cervigón y Ramos, 2011).

- La seguridad pasiva es el conjunto de medidas que se usan para evitar que el impacto de un ataque sea menor, además de activar diversos mecanismos de recuperación. Como por ejemplo, las copias de seguridad (Cervigón y Ramos, 2011).

ii. Seguridad física y lógica

- La seguridad física se relaciona con los accesos físicos, estructuras, cámaras de seguridad, alarmas, extintores, entre otros (Díaz et al, 2014).
- La seguridad lógica tiene la finalidad de asegurar los sistemas informáticos. Como por ejemplo accesos a los sistemas, autenticación de usuarios, internet, protocolos, aplicaciones, etc. (Díaz et al, 2014).

Seguridad informática

Villegas et al. (2011) sostienen que la seguridad informática con el conjunto de procesos desarrollados por profesionales capacitados en políticas de seguridad y que sean capaces de garantizar la aplicación de salvaguardas en caso de una pérdida económica grave o de un incumplimiento o pérdida de la información.

A su vez, la UTTT (2012) afirma que la seguridad informática está relacionada con la protección de la infraestructura y de la información, haciendo uso de diversos protocoles y herramientas para disminuir los posibles daños.

Defensa de la Red

La defensa de una red permite asegurar la configuración de la misma, ya sea de manera interna o externa. Para esto se toma como base el modelo OSI que permite la aplicación de capas de aseguramiento de la red, tomando como base la parte física hasta la aplicación.

Red de Datos

De acuerdo con Tanenbaum (2010) la red es un sistema interconectado de computadoras que tienen la finalidad de compartir recursos, aplicaciones, información entre los usuarios. Una red puede conectar a usuarios dentro de una misma oficina o usuarios que estén fuera de ella.

a) Tipos de redes por alcance.

Se tienen los siguientes:

- Personal Área Networks (PAN) es una red de ordenadores usada para la comunicación entre los dispositivos del computador cerca de una persona.
- Local Área Networks (LAN). Aquella red que se limita a un área pequeña, como por ejemplo un cuarto o un solo edificio.
- Wireless Local Área Network (WLAN) o red de área local inalámbrica; es un sistema de área local o extensión de estas.
- Campus Área Network (CAN) llamada también red de campus. Es aquella red con alta velocidad y que se encarga de conectar redes dentro de un área geográfica limitada. Por ejemplo, hospitales, colegios, bases militares, etc.
- Metropolitan Área Networks (MAN) conocida como una red de área metropolitana. Se caracteriza por tener una alta velocidad, de banda ancha, cuya área de cobertura es más extensa. Por ejemplo, la conexión de diversos edificios dentro de una misma localidad.
- Wide Área Networks (WAN) es aquella red amplia que es capaz de extenderse sobre áreas muy extensas haciendo uso de satélites, internet, fibra óptica, entre otros.

b) Clasificación de redes por topología física.

- Red lineal. Aquella red que tiene un solo canal de comunicación que comunican a diferentes dispositivos. Dicho canal es conocido como troncal o bus.
- Ren en anillo o circular. Aquella red donde cada estación está conectada a la siguientes, y la última estación se conecta a la primera.
- Ren en estrella. Aquella red en donde las estaciones se conectan de manera directa a un punto central y todo el tráfico de la comunicación se realiza a través de esta.
- Red en malla. Aquella red en donde cada uno de sus nodos están conectados a los demás.
- Red en árbol. Aquella red en donde sus nodos están conectados en forma de árbol. Este tipo de redes tienen una semejanza a la red estrella, con la excepción que no tienen un nodo central.
- Red híbrida o mixta. Aquella red donde se combina cualquier tipo de red descrita anteriormente.

c) Protocolos de Redes.

En el caso de los protocolos son muchos modelos que aseguran un correcto funcionamiento de las redes. Se tienen, por ejemplo, el modelo OSI y el TCP/IP.

El modelo OSI presenta siete capas definidas y diferenciadas. Mientras que el modelo TCP/IP tiene cuatro capas que combinan funcionan con las capas del modelo OSI. Los protocolos están en las capas pero no están definidos como parte del modelo.

El modelo OSI fue creado por la Open System Interconnection (OSI por sus siglas en inglés) y tiene la finalidad de conectar sistemas abiertos con otros sistemas.

El modelo TCP/IP es el modelo más utilizado en la actualidad. Inicialmente fue propuesto por ARPANET y se utilizan en todas las redes locales. Su nombre se debe a la unión de dos principales protocolos, el TCP (capa de transporte) y el IP (capa de red).

d) Modelo de Referencia OSI

Tanenbaum (2010) sostiene que este modelo tiene diversos principios para lograr las siete capas. Estos principios son:

- Se crea una capa en donde se haga uso de un nivel diferente de abstracción.
- Cada capa tiene una función definida.
- Cada capa tiene una función específica que se elige teniendo en cuenta la definición de los protocolos.
- Se necesita elegir los límites de las capas a fin de que se disminuya el flujo de la información.
- El total de las capas debe ser lo suficiente como para no añadir funciones distintas.

Metodología PPDIOO

Este tipo de metodología (preparar, planear, diseñar, implementar, operar, optimizar) tiene como objetivo principal definir actividades mínimas requeridas que permitan asesor de manera correcta a los clientes. A su vez, se puede optimizar el desempeño mediante el ciclo de vida de la red.

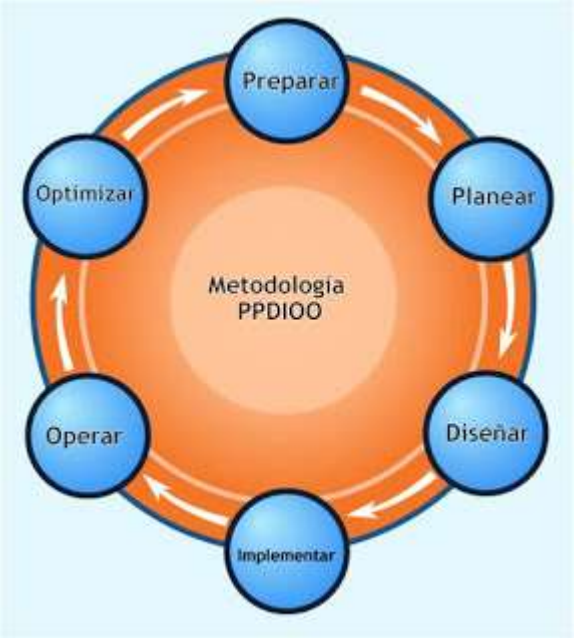

Figura 1. Etapas de la metodología PPDIOO

Las fases de la metodología PPDIOO son las siguientes:

a) Fase de preparación. En la fase de preparación es necesario crear un caso de negocio para justificar la estrategia de red. Además, se identifica la tecnología que debe soportar la arquitectura.

b) Fase planeación. Esta fase identifica los requerimientos de una red, haciendo una evaluación y análisis de las deficiencias encontradas. Se debe elaborar un plan de proyecto donde se consigne la administración de las tareas, responsables, las actividades a desarrollar y los recursos que se necesiten. Este plan debe seguirse en todas las fases.

c) Fase de diseño. Esta fase se encarga de desarrollar un diseño detallado de todos los requerimientos técnicos y económicos que se han conseguido en las fases anteriores. Además, en esta fase se incluye los diagramas de red. Con relación al plan del proyecto, este se actualiza con información más detallada.

d) Fase de implementación. En esta fase se acelera el retorno sobre la inversión al aprovechar el trabajo realizado en las últimas fases. Para la implementación se

debe incluir una descripción detallada, guías, tiempos y demás pasos para volver a alguna fase anterior en caso de fallas o de información adicional.

e) Fase de operación. Esta fase se encarga de mantener el estado de la red todos los días. Para esto se debe administrar correctamente y monitorear los componentes de la red, mantener el ruteo, y la identificación y la corrección de los errores. También se le conoce como la fase de la prueba final del diseño.

f) Fase de optimización. Aquí se identifican y se resuelven problemas antes que afecten a la red. Está en la capacidad de modificar el diseño en caso de que existan diversos problemas con el objetivo de mejorar el desempeño o resolver las cuestiones de aplicaciones (Fabuel, 2013).

La justificación de la investigación realizada se fundamenta desde los siguientes puntos de vista como el punto de vista social la investigación se justifica porque gracias a la implementación del Sistema de seguridad perimetral permitirá beneficiar a todos los usuarios de la red de datos brindando la seguridad que garantice la integridad de su información y evitar posibles tentativas de intrusión y/o disuasión de intrusos en instalaciones especialmente sensibles. Con respecto a la justificación científica el presente proyecto, involucra un conjunto de conocimientos que están asociadas con la seguridad perimetral que es muy necesaria hoy en día por la proliferación de las redes informáticas en los diversos tipos de organizaciones que hacen uso de las TICS en el desarrollo de sus actividades diarias. Las comunicaciones que se hacen a través de las redes informáticas privadas y públicas están expuestos a diferentes riesgos.

La problemática que actualmente con la coyuntura de la pandemia Covid-2019 y la necesidad de brindar el acceso presencial o remoto a los usuarios a los diferentes servicios informáticos de la Cía. Minera Santa Luisa – Unidad Pallca, y con los crecientes ataques informáticos en redes, expone la confiabilidad y seguridad de la información, permitiendo diferentes tipos de amenazas, tales como: el robo de la información, la denegación de algún servicio o la continuidad de la operación de la empresa. Por cierto tiempo la Compañía dejó de lado el tema

de la Seguridad informática y la implementación de políticas y dispositivos de seguridad en la red ocasionando algunos inconvenientes. Se encontró que en la Compañía tan solo contaban con un Proxy que cumplía las funciones de control de acceso y filtrado de contenidos, siendo un punto crítico y fácil de vulnerar, permitiendo a los usuarios navegar libremente por internet sin restricciones, también se detectó que había algunos usuarios conectados a la red mediante IP manuales, ocasionando saturación en la red, conflicto de IP, o ingresando a paginas inadecuadas en el horario de trabajo. Por esta razón en la Compañía Minera Santa Luisa – Unidad Pallca hemos creído conveniente implementar un equipo de seguridad perimetral Firewall para poder gestionar y filtrar las políticas y el total del tráfico que existe en la red, asimismo para evitar accesos no deseados en la red y ordenadores. Y finalmente para bloquear cierto tráfico que pueda salir de la misma.

Por ello luego de conocer la problemática podemos formular la siguiente interrogante:

¿Cómo implementar la seguridad perimetral de la red informática de la Compañía Minera Santa Luisa – Unidad Pallca?

Seguridad perimetral

Este término está referido a la seguridad que afecta a la frontera de la red de la empresa, denominada también perímetro. Dicha frontera está compuesta por diversas máquinas y dispositivos que se interrelacionan con el exterior y con otras redes. (CISCO, 2018).

Red de Datos

La red de datos son redes de comunicación debidamente diseñadas para la transmisión de información mediante el intercambio de datos. Las redes de estos datos en primer lugar son diseñadas para posteriormente ser construidas en arquitecturas especiales que ayuden a servir sus objetivos.

Las redes de datos por lo general se basan en la comunicación de paquetes y son clasificadas por el tamaño, la distancia y su arquitectura. (Tanenbaum, 2010).

En relación a la hipótesis se tiene:
Proponer la implementación de un sistema de seguridad perimetral de la Red de Datos de la Cía. Minera Santa Luisa Unidad Pallca, permitirá mejorar la seguridad de los datos de la empresa.

El objetivo general consiste en:
Proponer Implementar un sistema de seguridad perimetral de la Red de Datos de la Compañía Minera Santa Luisa Unidad Pallca.

Los objetivos específicos son: y tiene los siguientes objetivos específicos:
a) Determinar las vulnerabilidades de la red de datos para establecer las políticas de seguridad.
b) Definir la arquitectura del sistema de seguridad perimetral para lograr resguardar de manera física y lógica los datos de la Cía Minera Santa Luisa.
c) Proponer Implementar el sistema de seguridad perimetral haciendo uso de un equipo Firewall Fortinet FortiGate -200E para poder proteger de los datos que transitan por la red informática.
d) Evaluar el sistema de seguridad perimetral para comprobar el nivel de confiabilidad de la red de datos.

METODOLOGÍA

Tipo de investigación del Sistema de seguridad perimetral en la compañía se trabajó con el tipo de Investigación descriptivo.

El estudio corresponde al alcance descriptivo, debido a que la recolección de datos se realizó aplicando un cuestionario a los trabajadores del área de sistemas, dicho resultado nos permitió observar, comprender y describir el Sistema de Seguridad perimetral de la Red de Datos de la Compañía Minera Santa Luisa Unidad Pallca. Del mismo modo, el diseño del estudio tampoco es experimental porque los datos se recopilaron por una sola vez, utilizando una herramienta de recopilación de datos adecuada para el personal de la empresa.

Población y Muestra

En relación a la población empleada la conformaron el total de la cantidad de usuarios de la red de la Compañía Minera Santa Luisa - Unidad Pallca. La cantidad de usuarios de computadoras es de 70.

La Muestra en esta oportunidad para nuestro Proyecto, se consideró como muestra a toda la Población, es decir a los 70 usuarios, de la red de la Compañía Minera Santa Luisa - Unidad Pallca.

Como técnicas e instrumentos de recolección de información se tienen:

Tabla 2

Técnicas e Instrumentos

Técnicas	Instrumentos
Encuesta	Cuestionario
Análisis Documental	Textos, revistas, trabajos de investigación, tesis, etc.

Fuente: Elaboración propia

Se diseñaron diversas preguntas que finalmente otorgaron información relevante en relación a los servicios y la información que maneja la empresa.

Procesamiento y análisis de la información

La Recolección de datos, para efectos del desarrollo de ésta investigación, se aplicaron los instrumentos relacionados a las encuestas en sus técnicas de cuestionario, se tuvo en cuenta el instrumento de análisis de documentos en su técnica protocolos de investigación. Los tipos de datos que se obtuvo de los distintos indicadores en su mayoría fueron cualitativos.

El Procesamiento de los datos recolectados fueron procesados utilizando la estadística descriptiva, en donde se organizará la información sistemáticamente utilizando tablas de distribución de frecuencias unidimensional y bidimensional. Además, se utilizarán gráficos estadísticos para representar gráficamente a la información visualizando de una manera más directa los diferentes cambios de las variables; para su mejor apreciación se tendrá en cuenta el gráfico de barras.

RESULTADOS

En la propuesta de implementar un sistema de seguridad perimetral de la red de datos de la compañía minera Santa Luisa, se tomaron en cuenta las fases de elaboración, planeación y diseño de la Metodología PPDIOO. Según los objetivos específicos planteados tenemos el primer objetivo que hace énfasis en determinar las vulnerabilidades las cuales ayudaran a establecer las políticas de seguridad como se puede apreciar en la fase I.

Fase I: Preparación

Con respecto a los objetivos del proyecto de la compañía minera se consideran los siguientes:

- Mejorar los niveles de seguridad de la red de datos para controlar las entradas o salidas no autorizadas.
- Reducir la cantidad de ataques a la red de datos por agentes externos.
- Ampliar la infraestructura de la red de datos que permita migrar a nuevas tecnologías.

Las limitaciones organizacionales que tiene la compañía minera Santa Luisa y que pueden afectar el proyecto son las siguientes:

- Poco presupuesto anual que permita mejorar la infraestructura tecnológica y de comunicación.
- Poco personal capacitado en las diferentes especializaciones de la informática y telecomunicaciones
- Poca cultura informática por parte del personal de la empresa sobre la importancia de la seguridad informática.

Fase II: Planeación

Aquí se realiza el análisis y la distribución de la situación actual que la red presenta.

Actualmente la compañía minera tiene una red de datos que requiere mejorar las deficiencias que presenta en cuanto a conectividad de los dispositivos de red y las vulnerabilidades de seguridad que están expuestos todos los usuarios finales que hacen uso de las diferentes estaciones donde están funcionando las aplicaciones ofimáticas y los sistemas informáticos que utilizan en sus actividades diarias. Con respecto a la distribución física de la red de datos se deduce que es de tipo estrella, que usa un medio de comunicación con cable UTP nivel 5, dispositivos de conectividad como Swicth antiguos con no mucha capacidad. Toda la organización minera se encuentran conectada a la red de datos que permite transmitir y compartir información para el desarrollo diario de sus actividades. El centro de datos donde se ubica el servidor de la red de datos no cuenta con todos los equipos necesarios para hacer una buena administración.

Figura 2. Diagrama físico de la red actual – Oficinas principales – Nivel 1

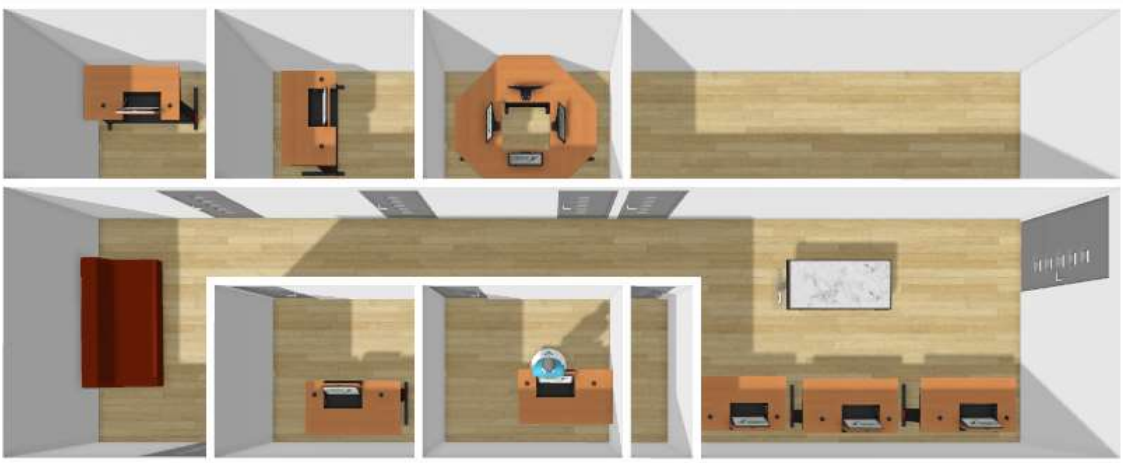

Figura 3. Diagrama físico de la red actual – Oficinas principales – Nivel 2

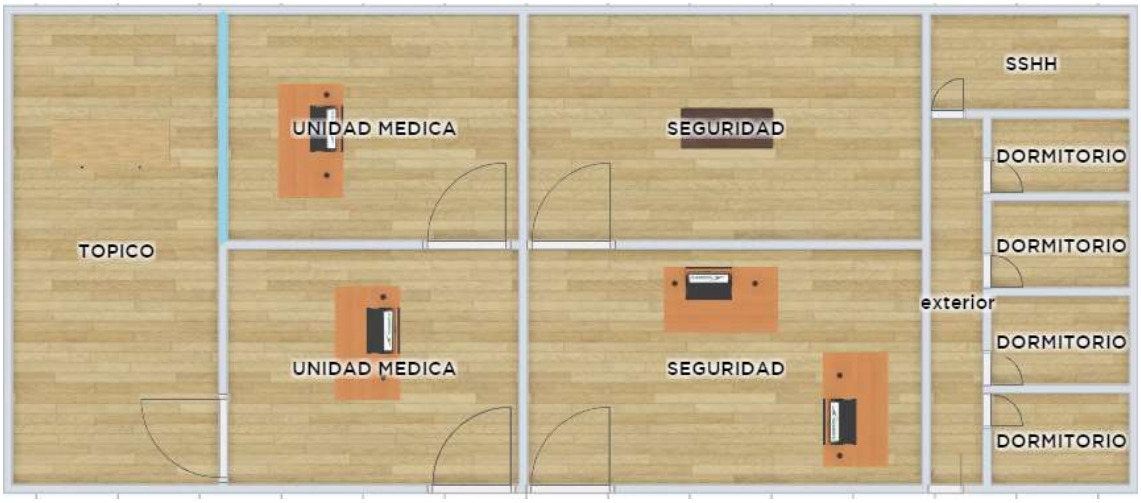

Figura 4. Diagrama físico de la red actual – Oficinas secundarias – Nivel 1

Figura 5. Diagrama físico de la red actual – Oficinas secundarias – nivel 2

Figura 6. Diagrama físico de la red actual – Almacén – Nivel 1

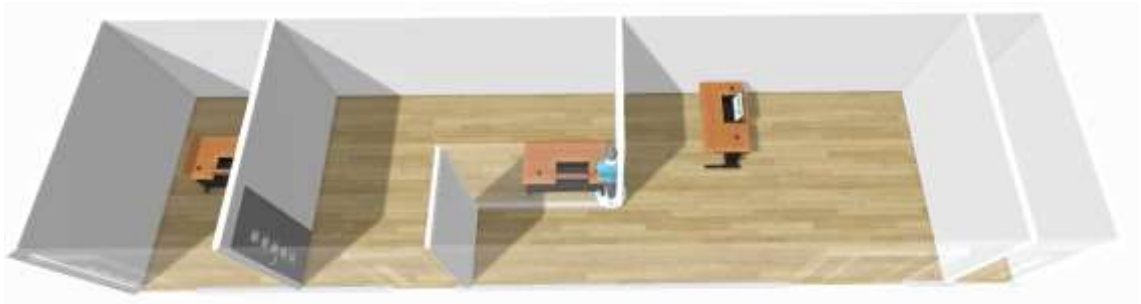

Figura 7. Diagrama físico de la red actual – Almacén – Nivel 2

Con respecto al segundo objetivo operacional que consiste en definir la arquitectura del sistema de seguridad perimetral para lograr resguardar de manera física y lógica los datos de la compañía Minera Santa Luisa. A continuación, tenemos las representaciones que permiten visualizar vista física y lógica.

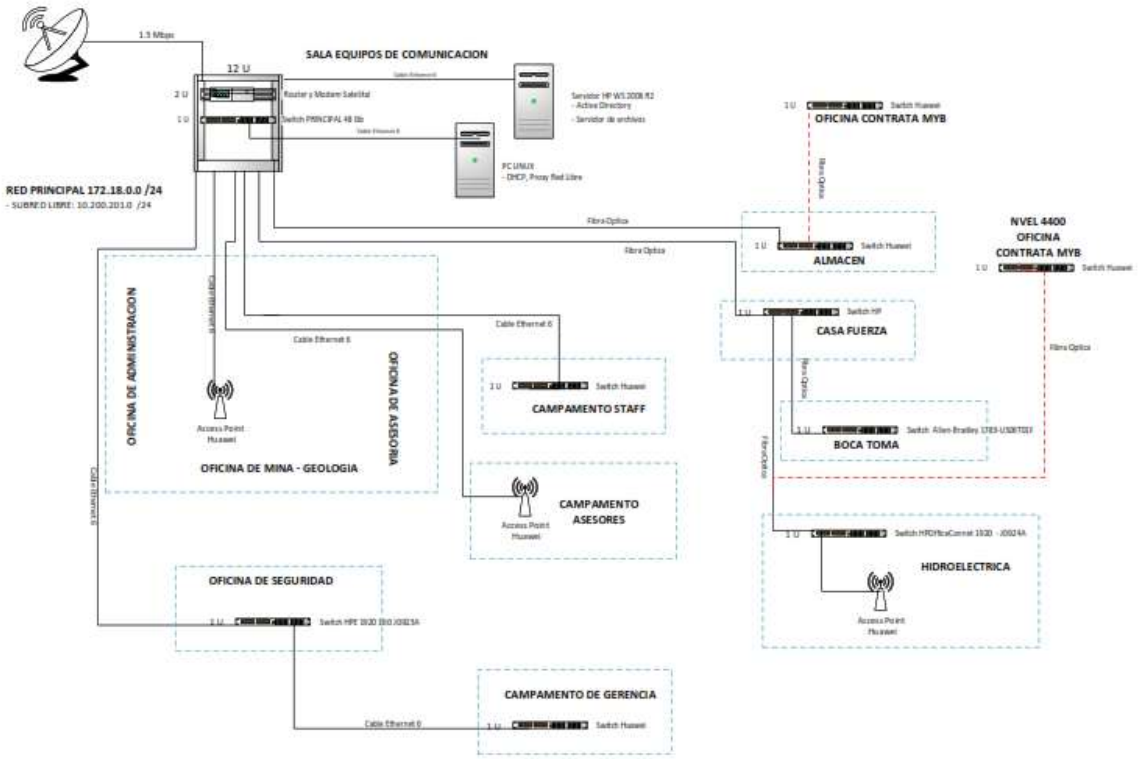

Figura 8. Diagrama lógico de la red actual

Actualmente la situación de la red de la organización es de la siguiente manera: El ambiente que hace de centro de datos no tiene las condiciones básicas como lo indica la norma ANSI/TIA 942 que permita albergar de forma correcta los equipos informáticos y de comunicación, con ello genera que no se pueda lograr una buena administración. Con respecto a los riesgos y vulnerabilidades de la red de datos se ha logrado tener un gran número de estadísticas tal como se puede apreciar en la siguiente imagen:

Figura 9. Análisis de vulnerabilidades de la red de datos

Análisis y evaluación del diseño de red que se propuso

Es necesario cuando se finalice el análisis de la infraestructura de TI de la organización nos centramos en el análisis de los requerimientos para poder realizar el sistema de seguridad perimetral de la red informática que cumpla con todas las especificaciones necesarias que garantice la seguridad de la información que fluye por los sistemas informáticos y otras aplicaciones informáticas. Además, se debe realizar un análisis del entorno para determinar las vulnerabilidades y amenazas lo cual permitirá seleccionar las políticas y realizar una adecuada configuración para mejorar la seguridad. Por ello es necesario poder revisar periódicamente los enrutamientos para tener información sobre las rutas por las que se transmiten los datos, tal como podemos observar en la siguiente figura 10.

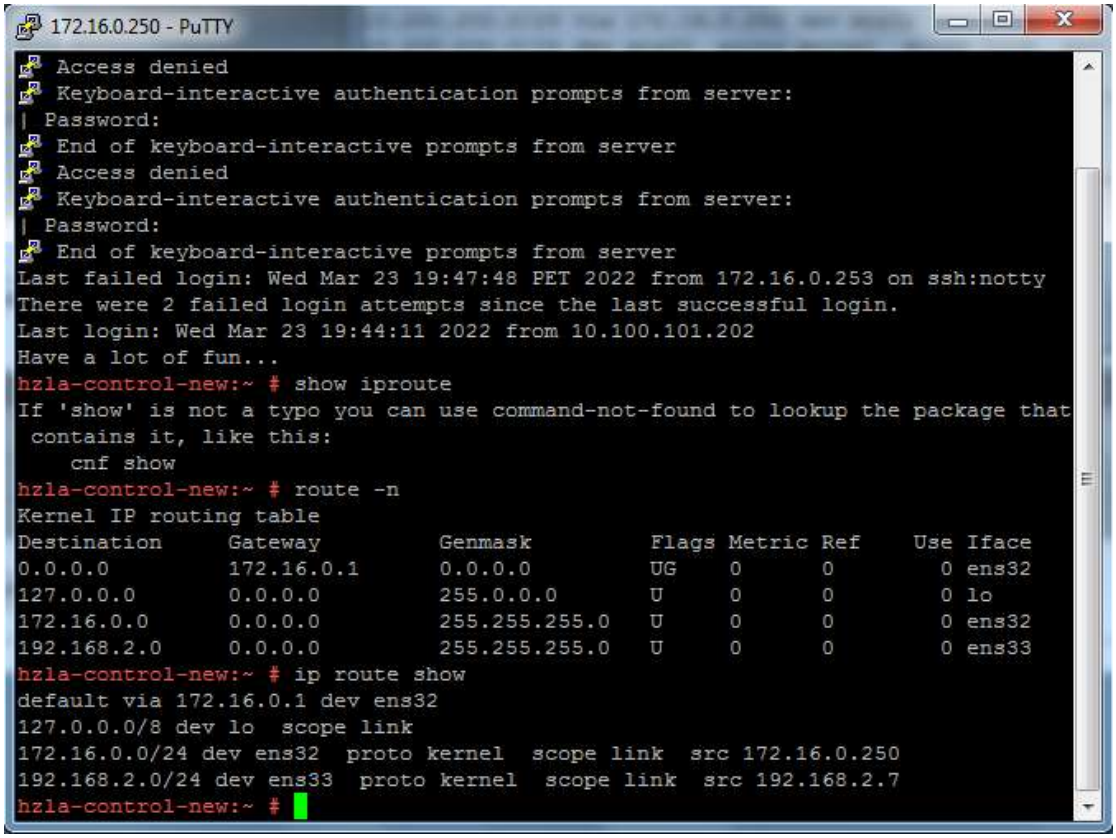

Figura 10. Enrutamientos de la red

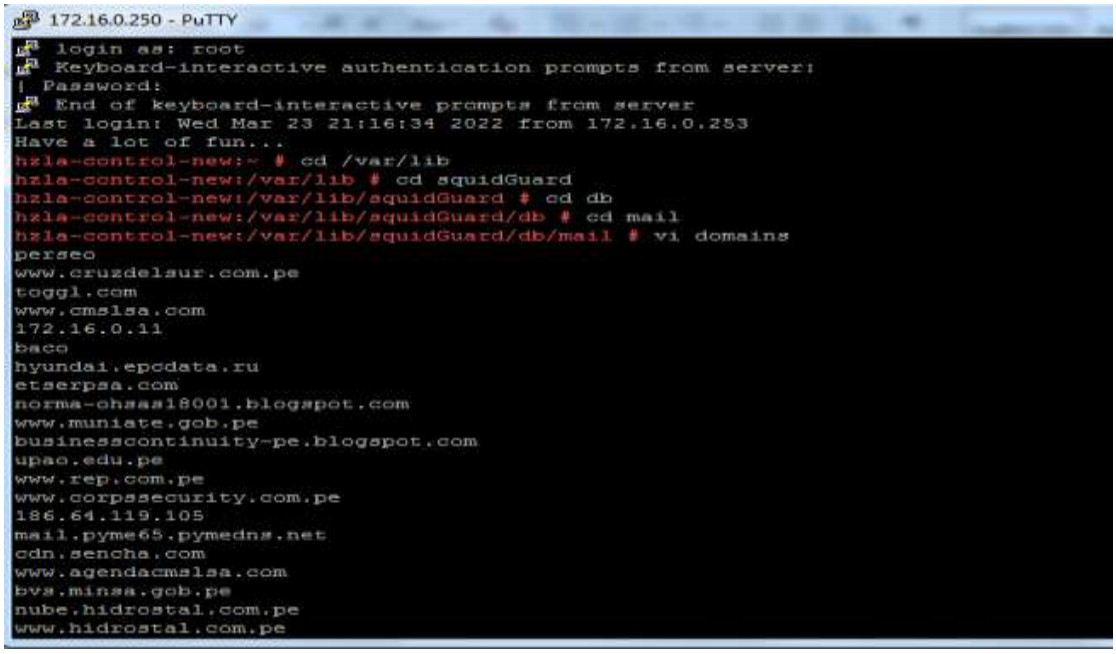

Figura 11. Inspecciones del tráfico de red

Requisitos de hardware

En la siguiente tabla se detalla el hardware y sus características técnicas que se requieren para llevar a cabo el sistema de seguridad perimetral:

Tabla 3
Requisitos de hardware

N°	Equipo / Dispositivo	Características técnicas	Cantidad
1	FortiGate – 200E	• 20/20/9 Gbps salida a través del Firewall. (1518 / 512 / 64 byte UDP packets) • 4 Gbps rendimiento VPN IPSEC • 900 Mbps rendimiento SSL VPN • 2.000,000 sesiones concurrentes (TCP) • 10,000 politicas de firewall • 135,000 nuevas sesiones/segundo (TCP) • 2000 enlaces entre sitios con tunel VPN IPSec VPN • 1.8 Gbps rendimiento NGFW • 3.5 Gbps Rendimiento Application Control • Gbps Rendimiento Inspección SSL • 300 sesiones VPN concurrentes	1

Fuente: Elaboración propia

Requisitos de Software

En la compañía minera Santa Luisa, con la finalidad de mejorar la seguridad informática para proteger sus datos, es necesario adquirir equipos informáticos de comunicación, de la misma manera que se debe adquirir programas para el manejo

de la gestión. El software necesario poder aplicar un sistema de seguridad se puede observar en la siguiente tabla:

Tabla 4
Requisitos de Software

Software (Aplicativos, Programas, otros)	**Características**	**Nro. de Licencias**
FortiOS 5.6	• Rediseño del Dashboard • Políticas NGFW: nuevos métodos de funcionamiento para aplicar, o en todo caso que la URL tenga una condición para hacer match. Esto se puede configurar debiendo elegirse entre lo tradicional o esto. • La funcionalidad del Proxy transparente y que se agrega al proxy ya existente conocido. • • Utilizar la BD internet services en las políticas. • No es necesario tener licencia para el servicio de control de las aplicaciones. • Soporte VxLAN • Protección para ataques DDoS.	1

Fuente: Elaboración propia

Requerimientos de seguridad eléctrica

Para el funcionamiento eficiente de los equipos es necesario que exista seguridad eléctrica para que el uso de la energía eléctrica y que los mantenimientos del sistema eléctrico sean seguros para las personas.

Tabla 5

Requisitos de seguridad eléctrica

N°	Equipos / Dispositivo	Características técnicas	Cantidad
1	Sistema de alimentación ininterrumpida(UPS)	01 BANCO DE BATERÍAS PARA UPS 32 BAT X 55AH - CONF. A 384 VDC - XTREME TEMP. SERIES Banco de Baterías tipo torre con 32 Baterías VRLA de 55Ah de capacidad de la serie Xtreme Temperature Version * Configuración de Voltaje DC - 384V / 01 string x 32 bat: 384V / 55Ah Tiempo de Autonomía estimado de 04 horas a 3.2kW de carga	1

Fuente: Elaboración propia

Desarrollo del plan del proyecto

a) Duración

   El plazo máximo para poner operativo el sistema de seguridad perimetral es de 160 días calendario.

b) Análisis costo beneficio

   Aquella relación entre las cifras que están en los estados financieros y otros documentos relacionados con la contabilidad y que tengan el objetivo de reflejar fielmente el comportamiento y cómo se aplica la seguridad informática.

   Seguridad perimetral = Gastos en seguridad - Beneficios en seguridad

   Los gastos en seguridad a considerar se reflejan en el presupuesto que se realiza cada año, como se puede apreciar en el siguiente apartado se está considerando los periodos 2019, 2020 y 2021. Con respecto a los beneficios en seguridad informática a implementar se considera aspectos como:

   - Demografía, es tener en consideración el tamaño real de la organización, de las personas que laboran a tiempo completo en el área de seguridad, cuál es la dependencia organizacional de la seguridad, los cargos de las personas y la ubicación geográfica.
   - Disminuir las fallas en la seguridad, está relacionado con las fallas más comunes que pueden existir. Se trata además de identificar las causas por las cuales no se denuncian, y si hay conciencia en los incidentes de la seguridad informática.

   - Mejorar las prácticas en la seguridad informática. Esto tiene que ver con identificar las diversas prácticas que tiene una organización sobre la seguridad y las herramientas más comunes que utilizan para desarrollar infraestructura tecnológica y estrategias para resolver las fallas de seguridad.
   - Las políticas de la seguridad. Se trata de investigar la efectividad que tienen las políticas de seguridad en una empresa, y cuáles son los

obstáculos que tienen para obtener una adecuada seguridad. Así como también establecer contactos nacionales o extranjeros para monitorear posibles ataques de intrusos.

c) Presupuesto

Tabla 6
Gastos en servicios

Actividades	**Años**		
	2019	**2020**	**2021**
Proteger la red	8,000	10,000	15,000
Protección de los datos críticos de la empresa	4,000	5,000	8,000
Protección de la propiedad intelectual	7,000	8,000	12,000
Protección de los datos de los clientes	5,000	6,000	10,000
Seguridad de las aplicaciones	15,000	20,000	22,000
Evaluación de seguridad internas y externas	5,000	8,000	10,000

Fuente: Elaboración propia

Tabla 7
Gastos de personal

Concepto	Tiempo	Pago mensual	Total
Implementación	4 meses	3,000	12,000
		Total:	12,000

Fuente: Elaboración propia

Tabla 8
Materiales

Concepto	Cantidad	Precio Unitario	Total
Fibra óptica	1	8,000	8,000
Patch core	20	60	1,200
Transeiver	10	500	5,000
		Total:	14,200

Fuente: Elaboración propia

Tabla 9
Equipos

Concepto	Cantidad	Precio Unitario	Total
Firewall	1	10,000	10,000
Switch	5	3,000	15,000
Gabinete de red	1	6,000	6,000
		Total:	31,000

Fuente: Elaboración propia

Tabla 10
Consolidado total

Concepto	Total
Personal	12,000
Materiales	14,200
Equipos	31,000
Total	57,200
Imprevistos 5%	2,860
Total Neto	60,060

Fuente: Elaboración propia

En esta fase podemos ver el desarrollo del sistema de seguridad perimetral para permitir mejorar la fiabilidad de la seguridad rede de datos.

Fase III: Diseño

Diseño lógico de la red de datos propuesta

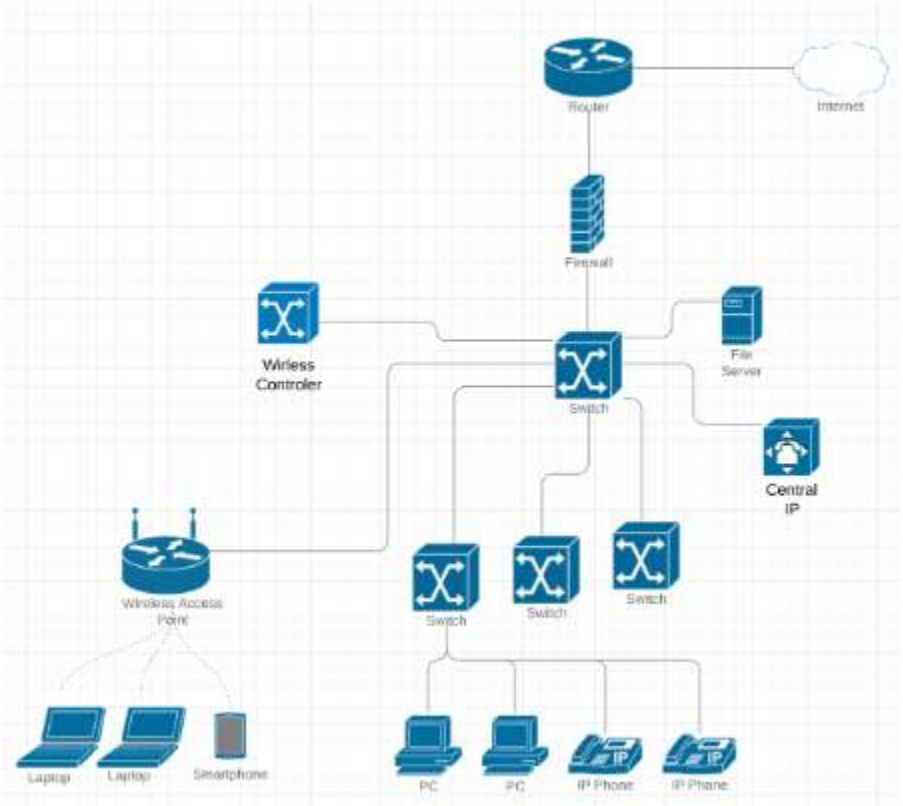

Figura 12. Arquitectura propuesta

Realizamos las configuraciones de las IP Publicas (190.119.170.162) y Local (172.18.0.254).

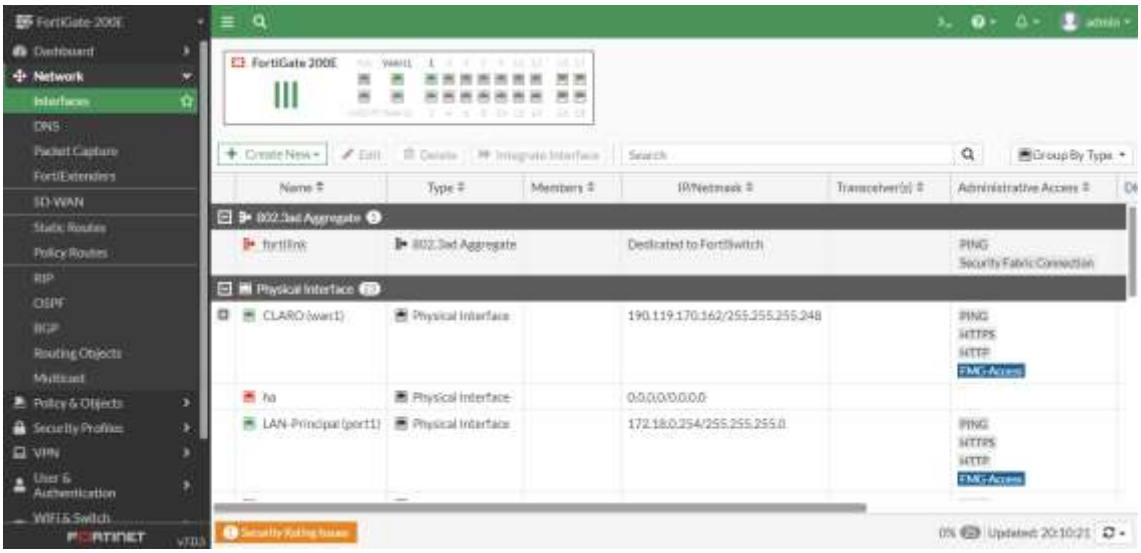

Figura 13. Configuración de las IP publica y local

Realizamos la configuración de los DNS, Local (172.18.0.3) y Publica (96.45.46.46).

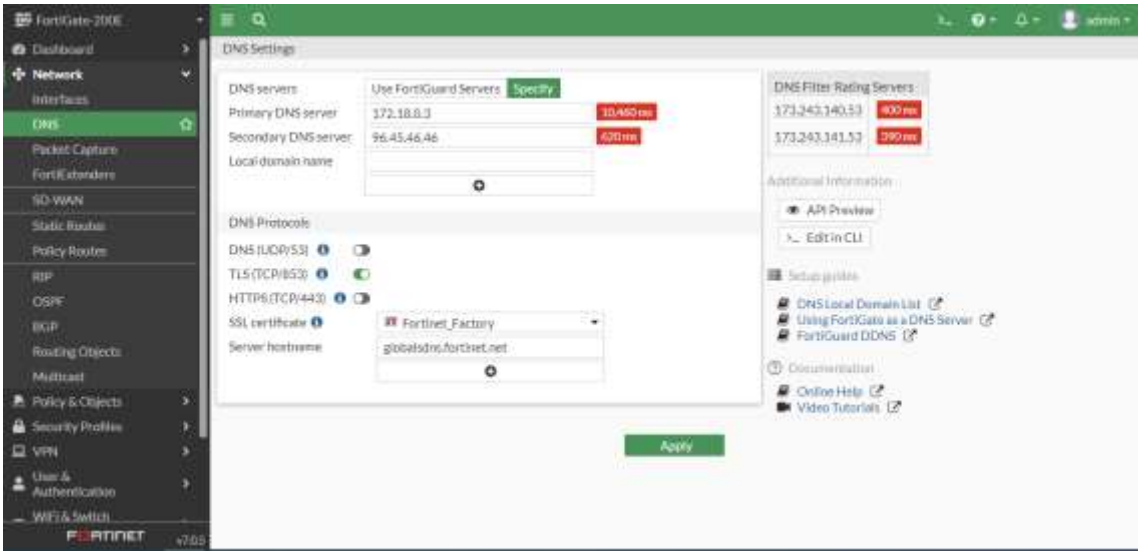

Figura 14. Configuración de DNS

Realizamos las configuraciones de las rutas estáticas:

- Rutas de la Unidad Huanzala (172.16.0.0/24 - 10.100.100.0/23)
- Rutas Sede Lima (172.16.4.0/24 – 10.200.204.0/24)
- Rutas Unidad Pallca (10.100.108.0/23 – 10.200.201.0/24)
- Rutas Cámara (50.0.0.0/24)
- Switch Core 172.18.0.50
- RPV 172.18.0.252

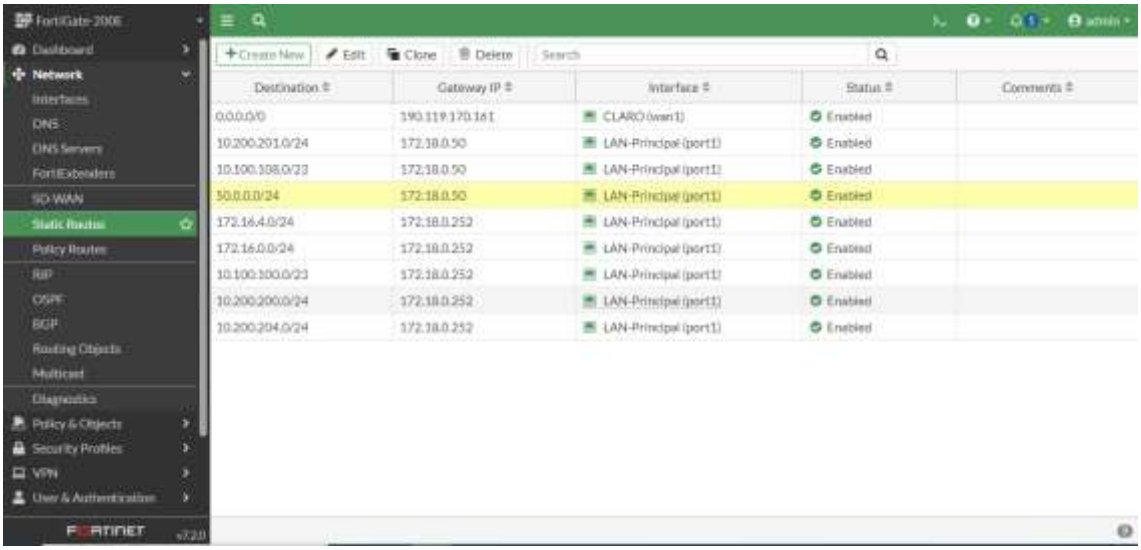

Figura 15. Configuración de rutas estáticas

Creación de Grupo de Políticas:

- Politica_Avanzada
- Politica_Intermedia
- Politica_Basica
- Politica_Contrata
- Horario_Libre
- Horario_Almuerzo
- Usuarios Libres Youtube

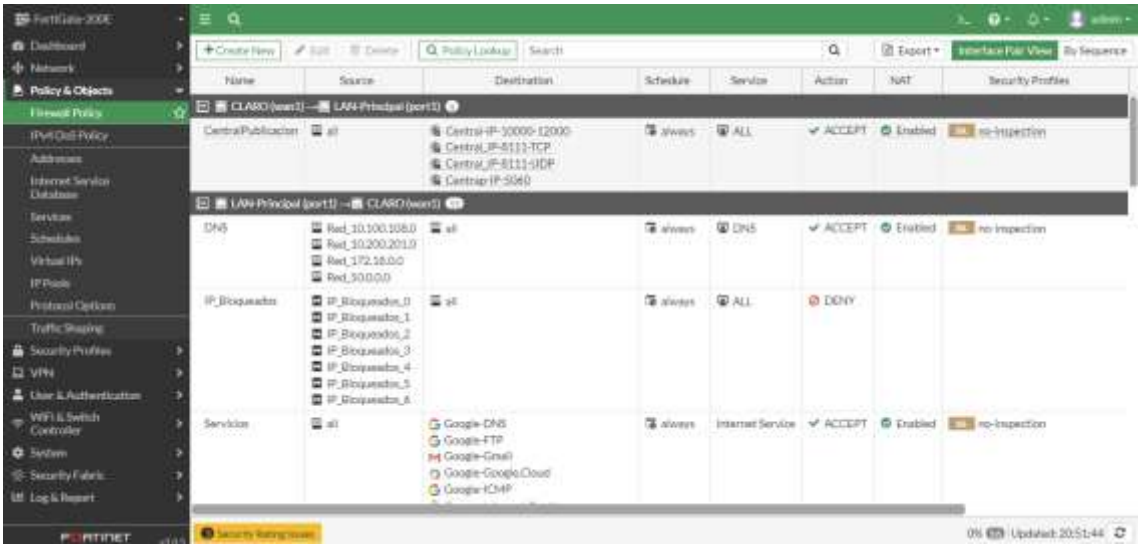

Figura 16. Configuración de políticas del Firewall

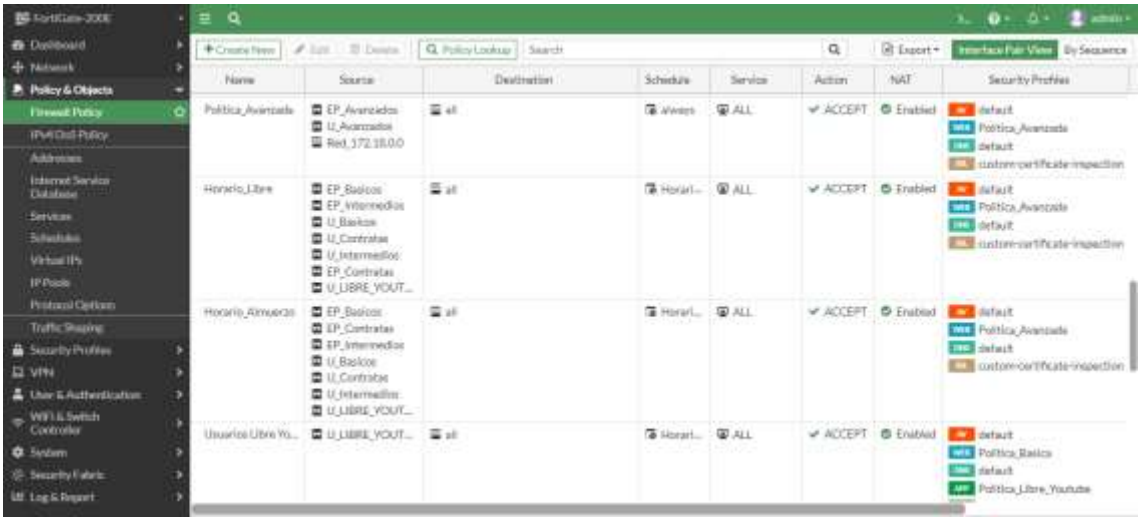

Figura 17. Configuración de políticas del Firewall

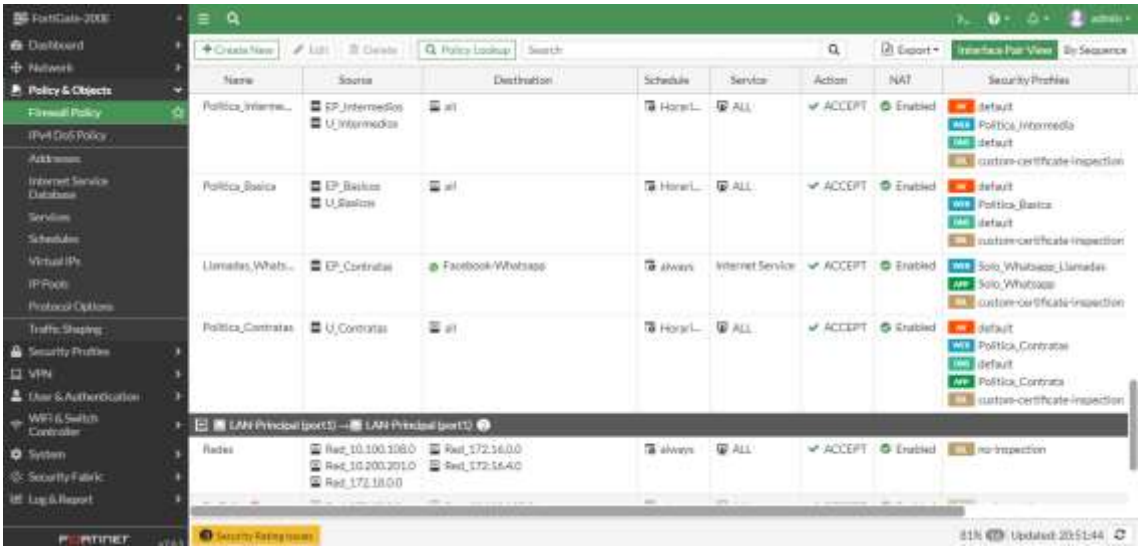

Figura 18. Configuración de políticas del Firewall

Creación de Rangos de Direcciones IP

- EP_Avanzado (10.100.109.10 - 50)
- EP_Basicos (10.100.108.50 - 200)
- EP_Contratas (10.100.109.200 - 250)
- EP_Intermedios (10.100.109.100 - 150)
- U_Avanzados (10.200.201.130 – 160)
- U_Basicos (10.200.201.50 – 100)
- U_Contratas (10.200.201.220 – 240)
- U_Intermedios (10.200.201.180 – 200)
- U_LIBRE YOUTUBE (10.200.201.210 – 220)

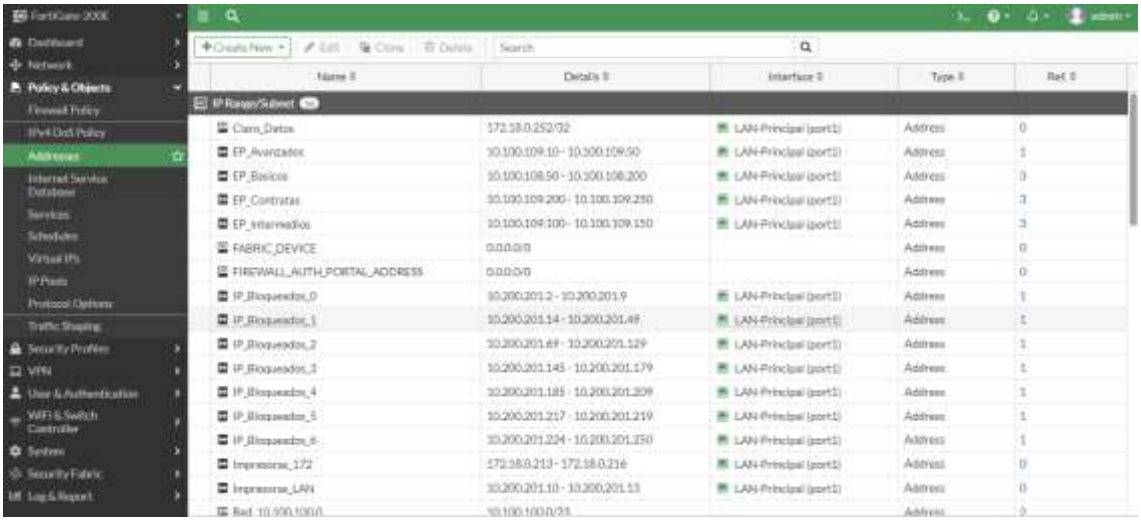

Figura 19. Creación de rangos de direcciones IP

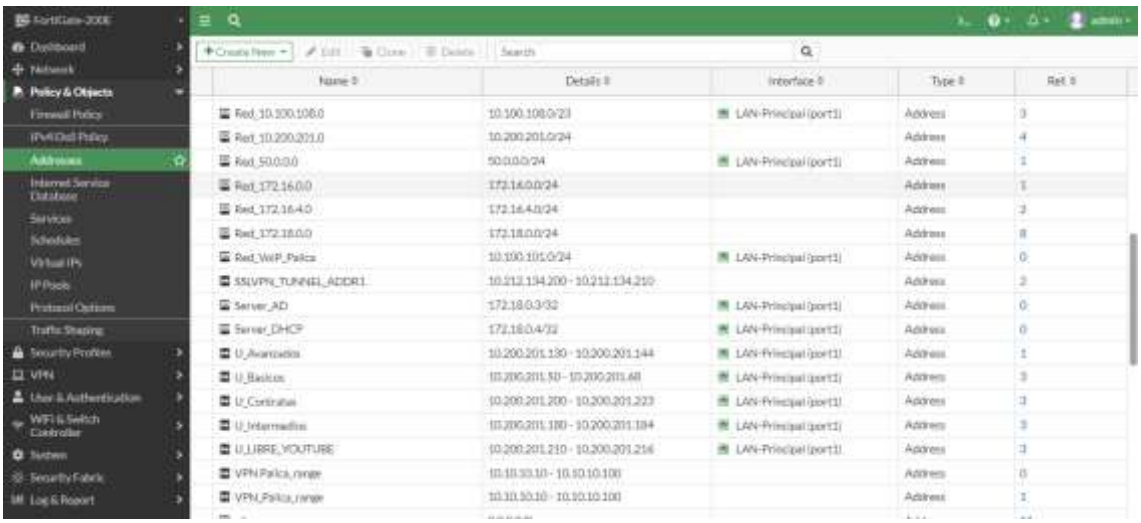

Figura 20. Creación de rangos de direcciones IP

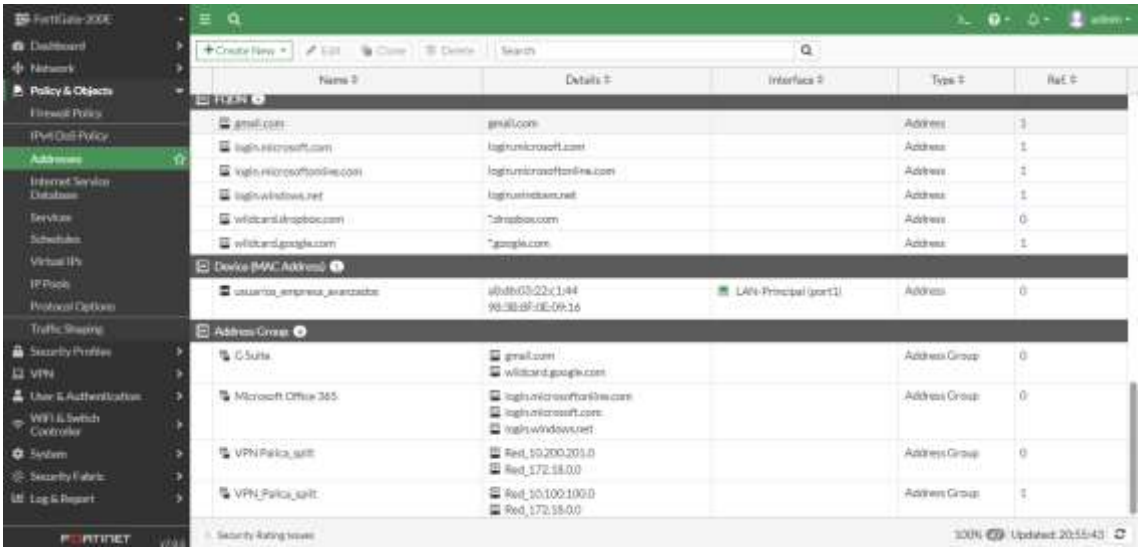

Figura 21. Creación de rangos de direcciones IP

Configuración de los servicios Habilitados

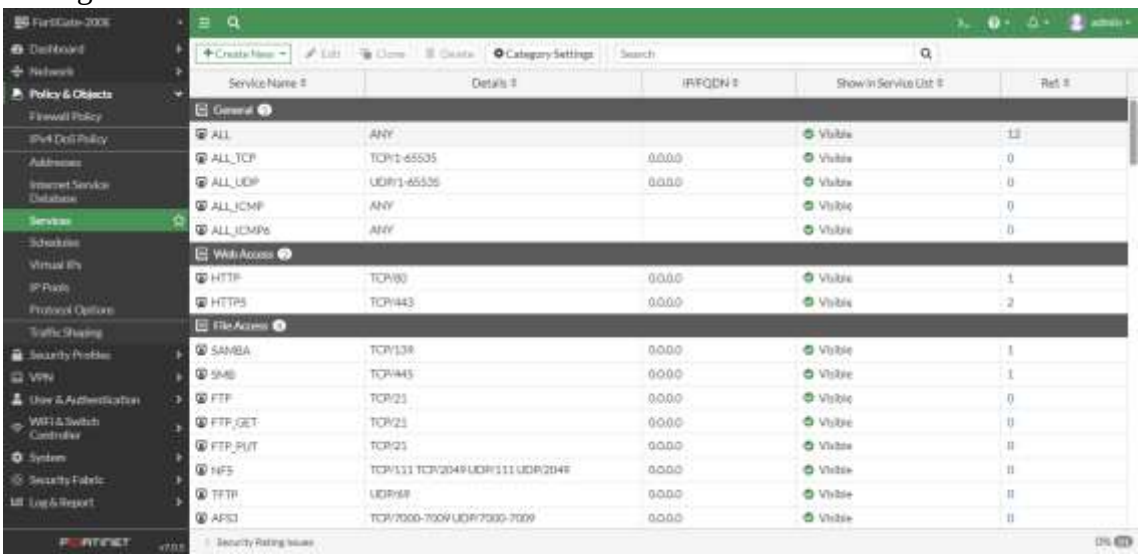

Figura 22. Configuración de permisos de los puertos

Configuración de horarios para un mejor manejo de la Red.

- Horario Almuerzo (Se libera el internet en el horario de 12 pm a 1 pm)
- Horario Libre (Se libera el internet en el horario de 6:17 pm a 11 pm)
- Horario_Pallca (Se aplican las políticas de red en horario de trabajo de 12 am a 6:17 pm)
- Always (Se mantiene el internet libre a el grupos de usuarios Avanzados)

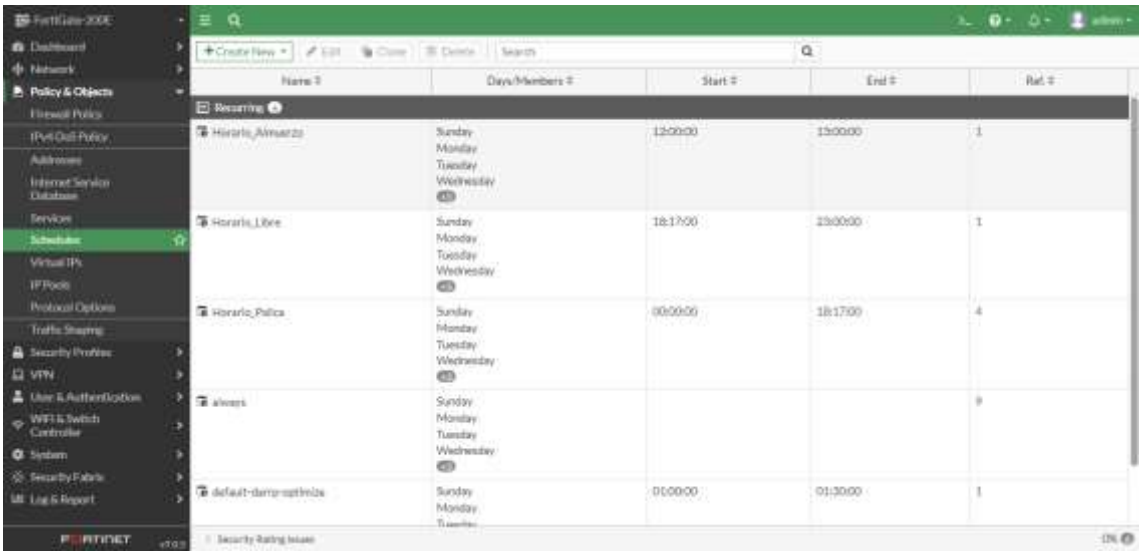

Figura 23. Creación de los horarios para permisos a la red

Configuraciones Antivirus por defecto

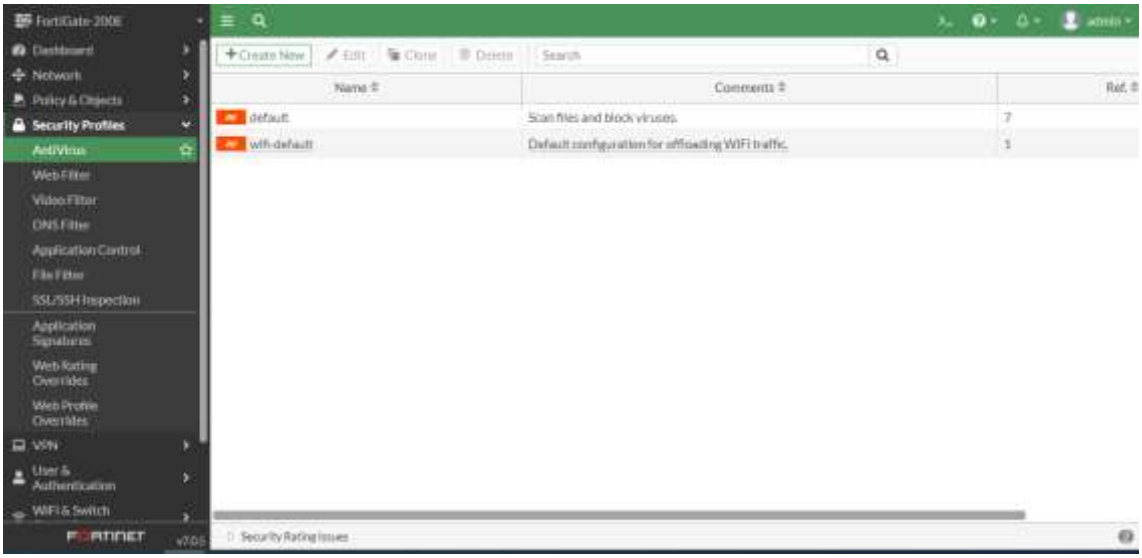

Figura 24. Configuración Wifi para el tráfico mediante WIFI

Configuraciones de Filtros Web por tipos de Tipos de Políticas

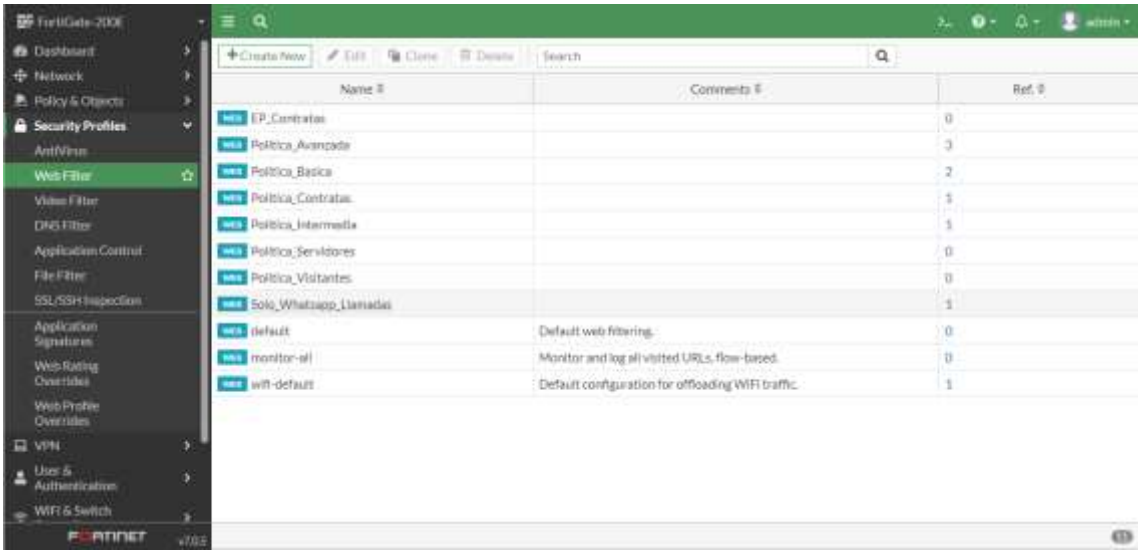

Figura 25. Creación de políticas web para los grupos creados

Configuración DNS por defecto

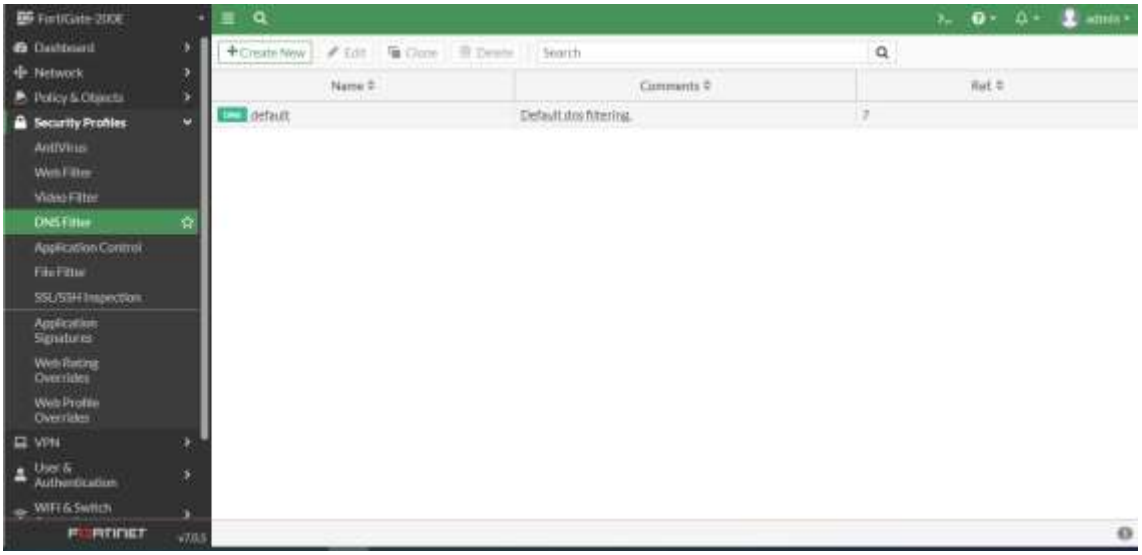

Figura 26. Configuración de DNS Filter

Configuraciones de restricciones de Aplicaciones por tipos de Politicas

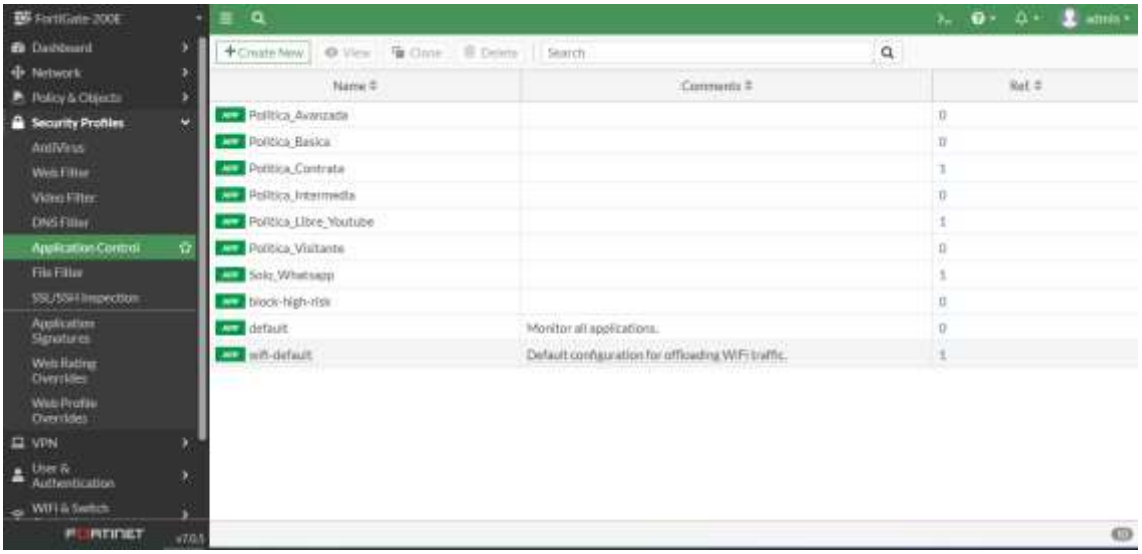

Figura 27. Configuración de accesos a las aplicaciones para cada política

Con respecto al cuarto objetivo específico que consiste en evaluar el sistema de seguridad perimetral para comprobar el nivel de confiabilidad de la red de datos. Tenemos lo siguiente:

Perfiles de seguridad de inspección

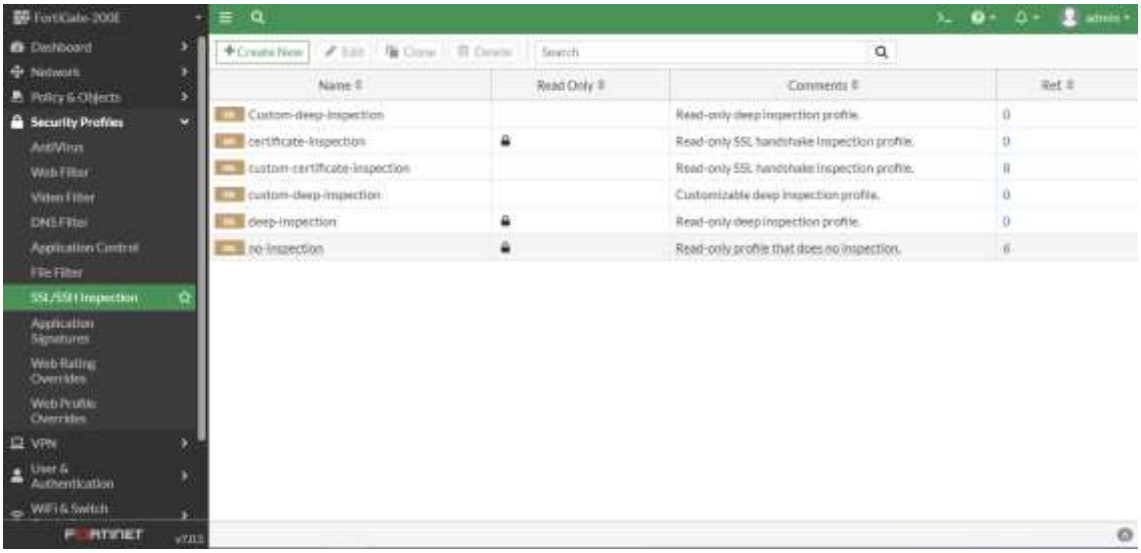

Figura 28. Inspecciones del tráfico de red

Reporte de Trafico de red en ejecución

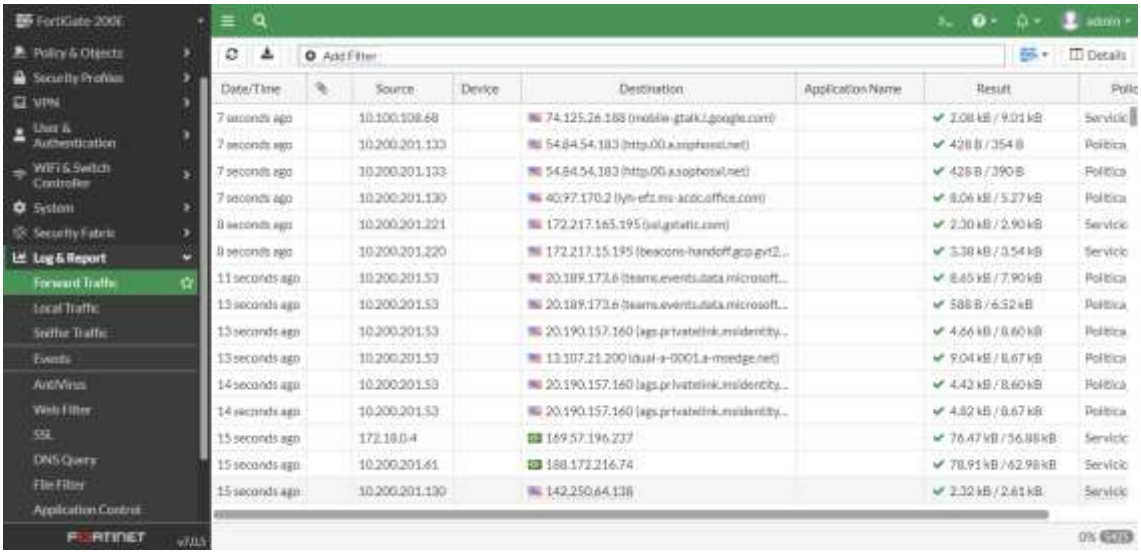

Figura 29. Trafico de red por cada estación

Reporte de Filtro Web

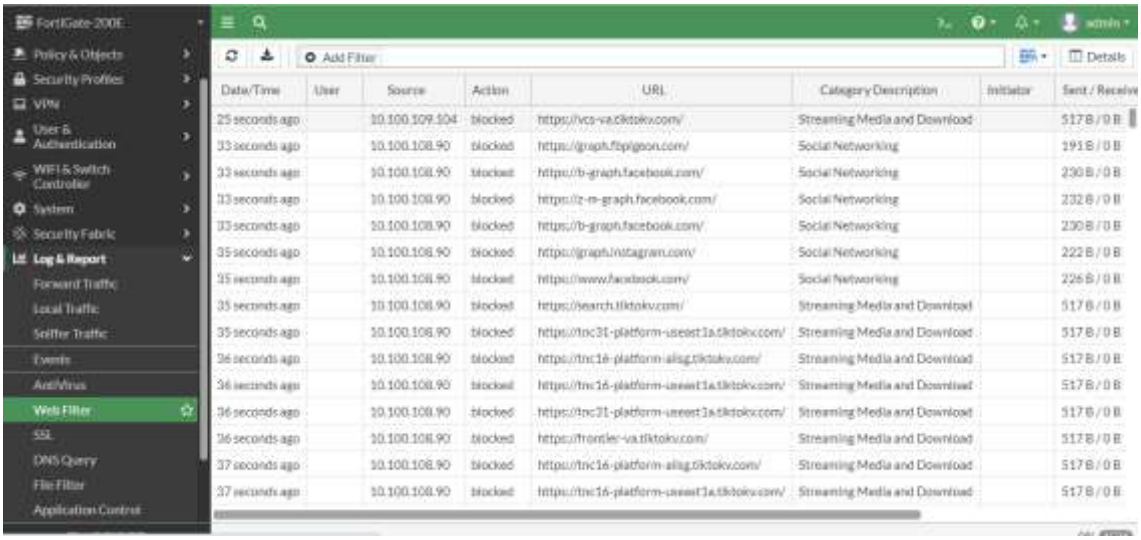

Figura 30. Filtro web por rango de IP

Reporte de Tráficos SSL

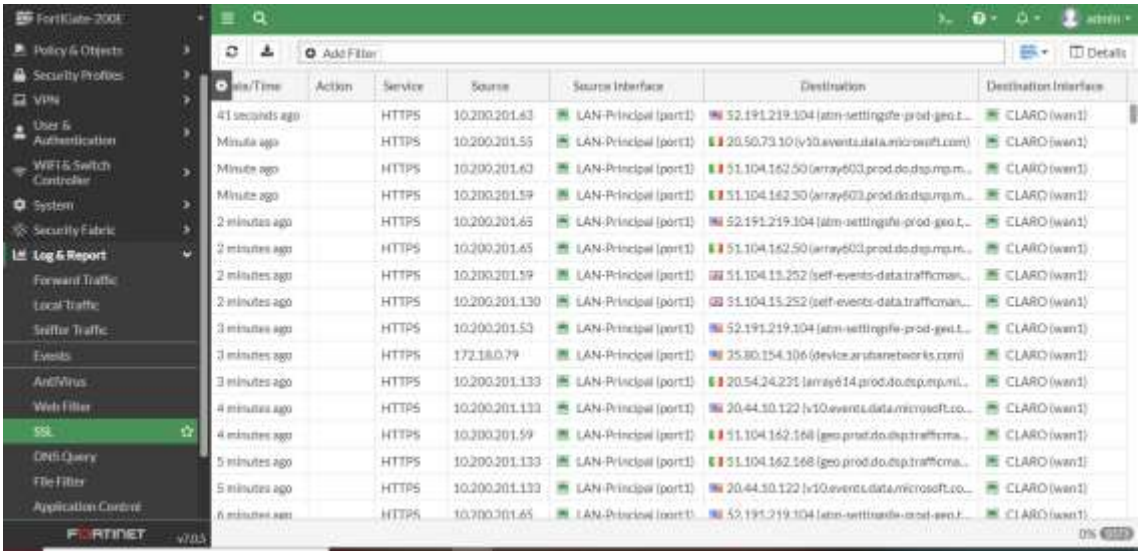

Figura 31. Trafico del protocolo SSL

Reporte de filtro de aplicaciones

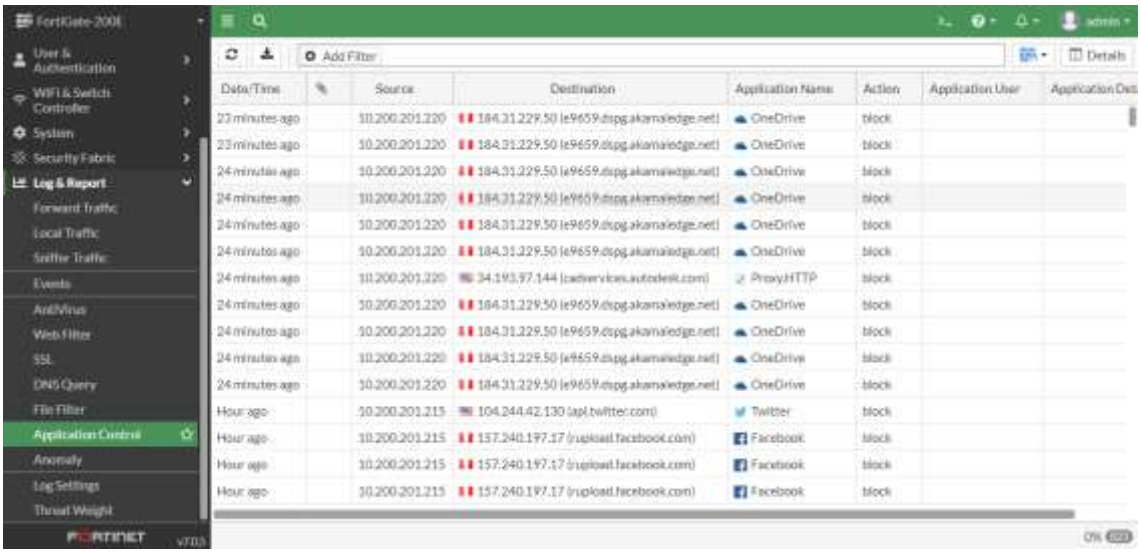

Figura 32. Trafico del control de aplicaciones

ANÁLISIS Y DISCUSIÓN

Luego de evaluar de manera presencial, es decir físicamente, en las instalaciones de la empresa, se constató la vulnerabilidad de la red de Datos (ver figura N° 9). Donde los usuarios podían vulnerar la Red de Datos. Posteriormente se implementó un Firewall y se logró corregir esta vulnerabilidad.

También se ha logrado definir una nueva arquitectura, respecto al antiguo diseño que se tenía. La antigua arquitectura estaba instalada dentro de un servidor virtual, lo cual no cumplía con los estándares de seguridad de Red de Datos.

Debido a que no existía seguridad en la Red de Datos dentro de la Empresa. Se implementó un Firewall Fortinet FortiGate -200E para la protección de los datos que transitan por la red informática,

Para la comprobación del proyecto se evaluó el sistema de seguridad perimetral para comprobar el nivel de confiabilidad de la red de datos, a través del equipo Fortinet FortiGate -200E, para lo cual se cuenta con los reportes donde indican los resultados (ver figura N° 29)

Ahora realizamos una comparación de nuestros resultados obtenidos con los antecedentes tenemos lo siguiente, por ello iniciamos con Delgado (2018) donde podemos decir que según sus resultados se coincide que es primordial aumentar el nivel de seguridad haciendo uso de un firewall que ayude a garantizar el nivel de servicio de la red informática.

Ahora con respecto a la investigación realizada por Guevara & López (2016) donde se enfoca en un sistema criptográfico para mejorar la seguridad, en nuestro caso todo ello el proceso de encriptamiento de los paquetes de la red es realizado por el sistema de seguridad que es soportado por los equipos que fueron adquiridos para realizar la implementación. En otro aspecto que se hace énfasis en mejorar la performance de la red de datos tenemos el trabajo realizado de Grados & Ventura (2014) en el cual señala gracias al uso de estándares ayuda a mejorar la satisfacción de los usuarios, con respecto a ello en nuestros resultados tenemos que gracias al sistema de seguridad perimetral se logró establecer políticas por grupos de usuario cumpliendo con una adecuada organización. Ahora tenemos la

investigación de Mero (2018) donde se coincide con sus resultados a pesar de haber realizado en una organización del sector público donde al igual que el trabajo anterior hace uso de normas y buenas prácticas que ayudan a reducir la inseguridad en una red informática haciendo uso de las herramientas. En el trabajo realizado por Aragón (2018) con respecto a sus resultados donde hace énfasis que el sistema implementado basado en una arquitectura donde las capas permiten la flexibilidad que en nuestro estudio también se logra gracias al tipo de tecnología utilizada en la implementación. En otro estudio realizado por Bohorquez & Paez (2017) que busca proteger la infraestructura física y lógica donde se hace énfasis en asegurar en el modelo OSI y una seguridad perimetral por anillos, es ahí donde encontramos una diferencia a nuestros resultados donde nuestra investigación se centra en proteger usando un cortafuego el cual permitirá controlar el tráfico de red a nivel de red y de aplicación.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- Se determinó y se documentó las vulnerabilidades que se presentaba en la red informática de la compañía lo cual ha permitido considerar las políticas de seguridad necesarias que se tomaron en cuenta en el sistema de seguridad perimetral.
- El definir la arquitectura necesaria para el sistema de seguridad perimetral ha permitido que se logre mejorar de formar considerable la seguridad física y lógica en la compañía minera Santa Luisa.
- Se logró proponer implementar sistema de seguridad perimetral haciendo uso de un equipo Firewall Fortinet FortiGate-200E para la protección de los datos que transitan por la red informática.
- Se logró evaluar funcionamiento del sistema de seguridad perimetral haciendo uso de casos de prueba para comprobar el nivel de confiabilidad de la red informática.

RECOMENDACIONES

- Se recomienda revisar periódicamente la situación de las vulnerabilidades de la red informática de la compañía para ir mejorando las políticas del sistema de seguridad perimetral.
- Es necesario planificar el mantenimiento preventivo y correctivo necesario de la arquitectura del sistema de seguridad perimetral, con la finalidad de garantizar su funcionamiento continuo.
- Se recomienda hacer un seguimiento del desempeño del sistema de seguridad perimetral implementado para evaluar que se cumple con la protección de los datos que transitan por la red informática.
- Periódicamente será necesario realizar casos de prueba para ir mejorando el funcionamiento del sistema de seguridad perimetral permitiendo de esa manera garantizar el nivel de confiabilidad de la red informática.

REFERENCIAS BIBLIOGRÁFICAS

Academy Microsoft, V. (Microsoft Virtual Academy de 2009). Programa de estudio en Seguridad Informática. Seguridad Informática. Guayaquil, Ecuador.

Andrés B. & Páez C. (2017), Diseño de un Sistema de Seguridad Perimetral en las instalaciones del Consorcio Expansión PTAR Salitre, Sede Bogotá. https://repository.ucatolica.edu.co/handle/10983/15322

Celi Campoverde, Y. E., Chalen Ortega, J. G., Lambert Sarango, Y., & Freire Cobo, L. E. (2009). Proyecto de tesis de grado sobre el "Desarrollo y Automatización del Control de Asistencia Docente y Cumplimiento del Programa de estudio" para la unidad EDCOM.

Fidias, O. (2012) EL Proyecto de Investigación 6ta Edición. Editorial Episteme ISBM 980-07-8529-9

https://www.researchgate.net/publication/301894369_EL_PROYECTO_DE_INVESTIGACION_6a_EDICION

Gobierno España, Ministerio de Educación, Cultura y Deporte, Normas ISO sobre gestión de seguridad de la información, 25 abril de 2020, [consultado: 10 setiembre 2022], Disponible en: http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_sobre_gestin_de_seguridad_de_la_informacin.html

Grados, J. & Ventura, G. (2014). Sistema de seguridad perimetral para mejorar performance de una red de datos empresarial. http://dspace.unitru.edu.pe/handle/UNITRU/11303

Guevara, T. & López, L. (2016). Implementación de un sistema criptográfico a través de algoritmos avanzados de encriptación para mejorar la seguridad perimetral de una red informática.

Hernández, E. (2006). Vulnerabilidad en redes. Madrid, España: Anaya Multimedia.

Instituto Universitario de Tecnología del Oeste Mariscal Sucre, Metodología PPDIOO, 27 de octubre de 2012, [consultado: 10 setiembre 2022], Disponible en: http://redplataformabibliotecakatherinebrech.blogspot.com/2012/10/normal-0-21-false-false-false-es-x-none_27.html

Guevara Tinoco, Roberto Carlos (2016), Implementación de un sistema criptográfico a través de algoritmos avanzados de encriptación para mejorar la seguridad perimetral de una red informática, Disponible en: https://hdl.handle.net/20.500.12802/350

López, P. (2010). Seguridad Informática. México: Editex.

Mero, S. (2018). Sistema de seguridad perimetral para la red de datos del Consejo Nacional Electoral delegación Santa Elena. http://dspace.uniandes.edu.ec/handle/123456789/8857

Profesorado, I. (2013). Instituto Nacional de Tecnologías Educativas y de formación del Profesorado. Obtenido de Instituto Nacional de Tecnologías Educativas y de formación del Profesorado (INTEF).

Valencia, J. J. M., Valencia, A. P., & Bedoya, J. C. A. (2020). Implementación de un sistema de seguridad perimetral informático usando VPN, firewall e IDS. Revista Universidad Católica De Oriente, 31(45), 84-99.

RNDS, Informe central Seguridad Perimetral, en línea, [consultado: 10 setiembre 2022], Disponible en: http://www.rnds.com.ar/articulos/015/rnds_060w.pdf

Ruiz, K. & Delgado, W. (2018), Implementación de una solución de seguridad perimetral Open Source en La Red Telemática de la Universidad Nacional Pedro Ruiz Gallo, Chiclayo – Perú. Recuperado: https://repositorio.udl.edu.pe/bitstream/UDL/122/3/UNIVERSIDAD-DE-LAMBAYEQUE.pdf

Stallings W. (2008). Fundamentos de seguridad en redes: aplicaciones y estándares. Madrid, España: Prentice Hall.

Stallings, W. (2004). Comunicaciones y redes de computadores. Madrid: Pearson Educación.

Tanenbaum, A. (2010). Seguridad en Redes de Computadoras. México: Prentice Hall.

Tanenbaum, A. & Wetherall, D. (2012). Redes de Computadoras. Mexico: Pearson Educación.

Villegas, M., Meza, M. y León, P. (2011). Las métricas, elemento fundamental en la construcción de modelos de madurez de la seguridad informática. Zulia, VEN. Telématique. Vol. 10. p 1-16.

Red Plataforma Biblioteca Katherine de Brech (2012). Metodología PPDIOO. Yaguara y Santa Rosalía, Caracas Venezuela.

ANEXOS Y APENDICES

Anexo I

CUESTIONARIO

TÍTULO: Encuesta a trabajadores

OBJETIVO: Obtener, información de los trabajadores respecto al funcionamiento de la Red de Datos

INSTRUCCIONES: Agradecemos el tiempo que usted asigne a la realización de la presente encuesta de la empresa. Contestar una sola respuesta por pregunta

PREGUNTAS: 10

		SI	NO
1	¿Está conforme con el servicio que brinda la red informática?		
2	¿La velocidad de transmisión y recepción de datos es adecuada para el trabajo que realiza diariamente?		
3	¿Ud. ha tenido algún incidente de seguridad en la red informática que provoque una pérdida de datos?		
4	¿Ud. ha tenido algún incidente con virus informáticos cuando hizo uso de la red informática para acceder a internet?		
5	¿Está de acuerdo con la importancia con mejorar la seguridad de la red informática?		
6	¿Está de acuerdo con que se implemente un sistema de seguridad perimetral que permita mejorar la seguridad de la red informática?		

7	¿Conoce si en su estación de trabajo existe alguna herramienta para el sistema de detección y prevención de intrusos?		
8	¿En la red informática cuenta con políticas para prevenir posibles ataques y tomar acciones ante un evento sospechoso?		
9	En su opinión, ¿le gustaría que exista un mejor control de seguridad en la red informática con respecto a la detección y prevención de intrusos?		
10	En su opinión, ¿cree usted que es demasiada inversión para una implementación del sistema de seguridad que ayudara a prevenir y detectar los intrusos de la red informática?		

Anexo 02

ANALISIS E INTERPRETACION

El procedimiento estadístico nos permite evaluar la confiabilidad de los instrumentos e implica realizar la organización de los datos recolectados para su posterior tratamiento mediante una herramienta ofimática que permite realizar el trabajo estadístico como es el Microsoft Excel. A continuación, se presenta los cuadros estadísticos que permiten revisar las características de la variable de estudio.

1. ¿Está conforme con el servicio que brinda la red informática?

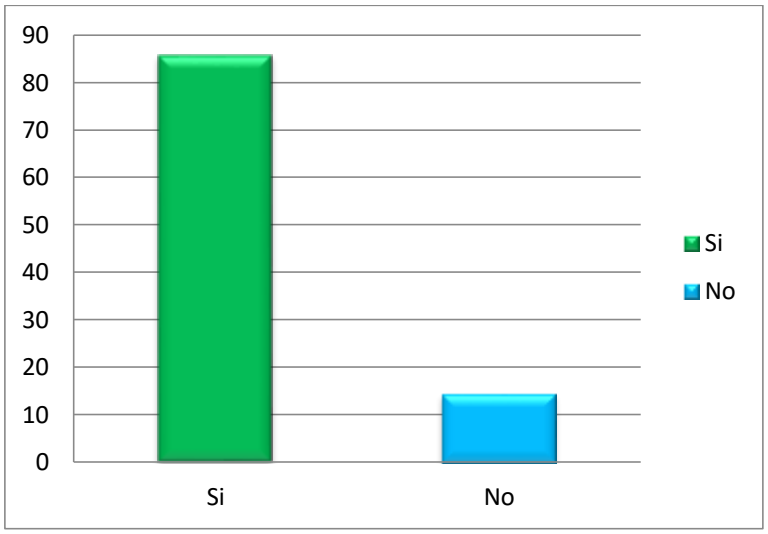

Figura 33. Conformidad de servicio. (Fuente: Tabla 11)

Interpretación: El grafico muestra la distribución de la conformidad sobre el servicio desde el punto de vista de los usuarios, donde podemos observar que el 86% considera que es un buen servicio y el 14% indica que no está conforme.

2. ¿La velocidad de transmisión y recepción de datos es adecuada para el trabajo que realiza diariamente?

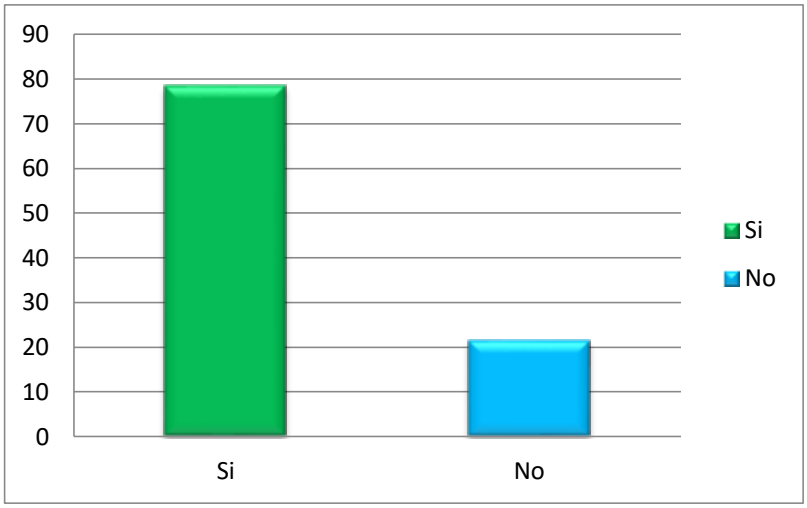

Figura 34. Velocidad de transmisión y recepción **(**Fuente: Tabla 12)

Interpretación: El grafico muestra la distribución de la opinión de los usuarios sobre la velocidad de transmisión y recepción donde tenemos que el 79% considera que es buena y un 21% indica que no está conforme.

3. ¿Ud. ha tenido algún incidente de seguridad en la red informática que provoque una pérdida de datos?

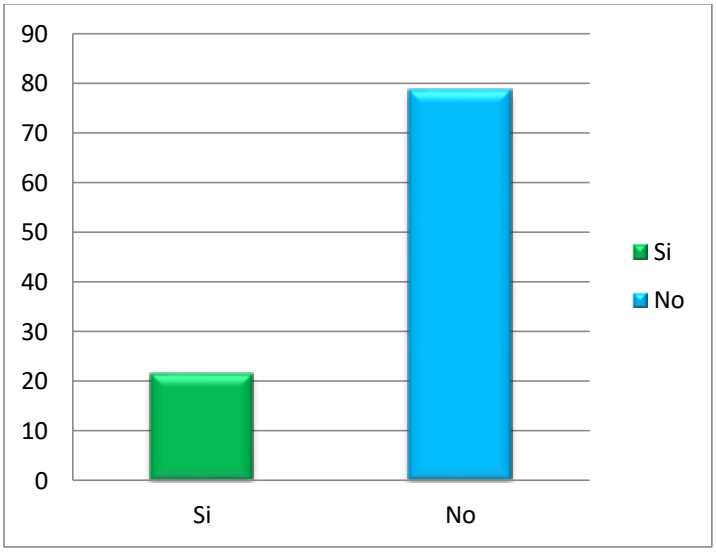

Figura 35. Incidencias de seguridad (Fuente: Tabla 13)

Interpretación: El grafico muestra el punto de vista de los usuarios con respecto a las incidencias de seguridad consideran que solo el 21% manifiestan que presentaron incidencias y un 79% indica que no está conforme.

4. ¿Ud. ha tenido algún incidente con virus informáticos cuando hizo uso de la red informática para acceder a internet?

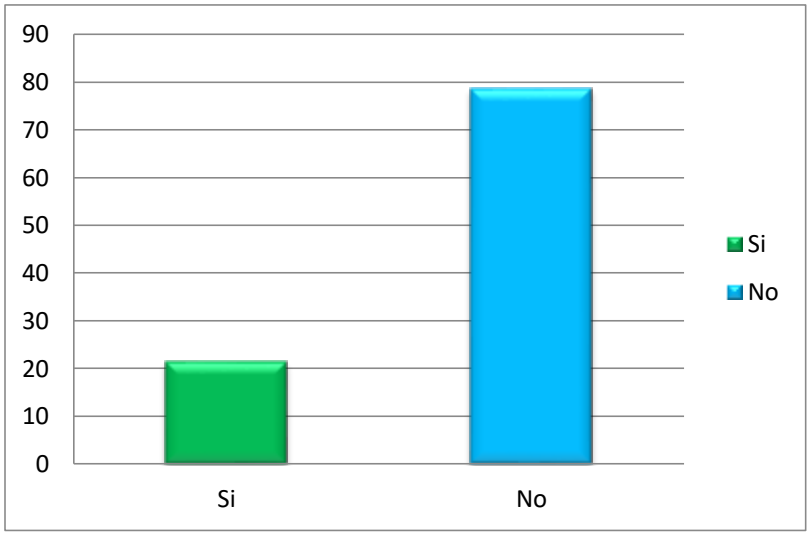

Figura 36. Incidentes con virus informáticos (Fuente: Tabla 14)

Interpretación: El grafico podemos observar que un 21% de los usuarios presentaron problemas con virus informáticos, lo cual significa un valor alto en este aspecto de la seguridad. Luego indica que el 79% considera que no tuvieron problemas con incidentes con virus.

5. ¿Está de acuerdo con la importancia con mejorar la seguridad de la red informática?

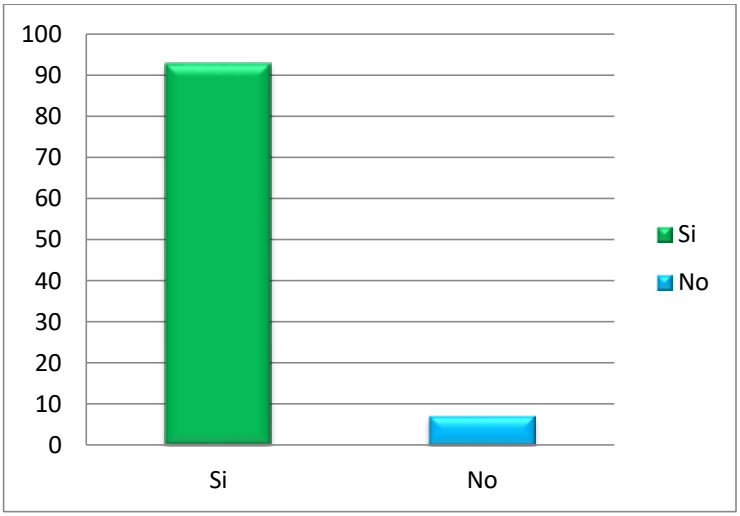

Figura 37. Importancia de seguridad informática (Fuente: Tabla 15)

Interpretación: El grafico podemos observar que el 93% de usuarios consideran importante la seguridad informática para la compañía; mientras que solo un 7% considera que no es importante aumentar la seguridad.

6. ¿Está de acuerdo con que se implemente un sistema de seguridad perimetral que permita mejorar la seguridad de la red informática?

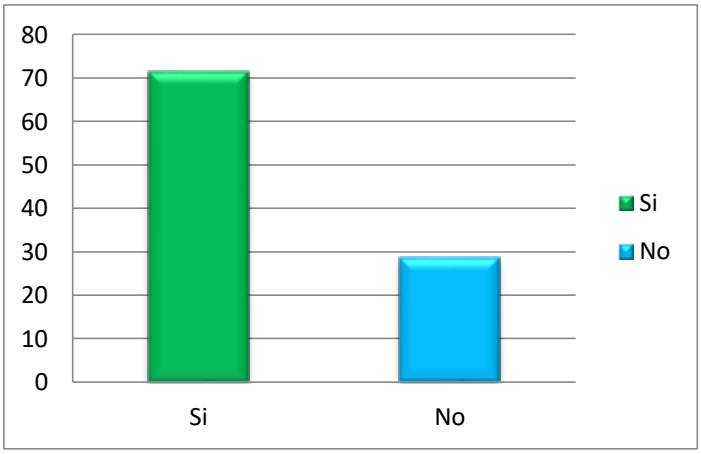

Figura 38. Implementar sistema de seguridad (Fuente: Tabla 16)

Interpretación: Como podemos observar en el siguiente grafico tenemos que el 71% de usuarios si están de acuerdo que se realice la implementación de un sistema de seguridad, mientras que un 29% indica que no es necesario.

7. ¿Conoce si en su estación de trabajo existe alguna herramienta para el sistema de detección y prevención de intrusos?

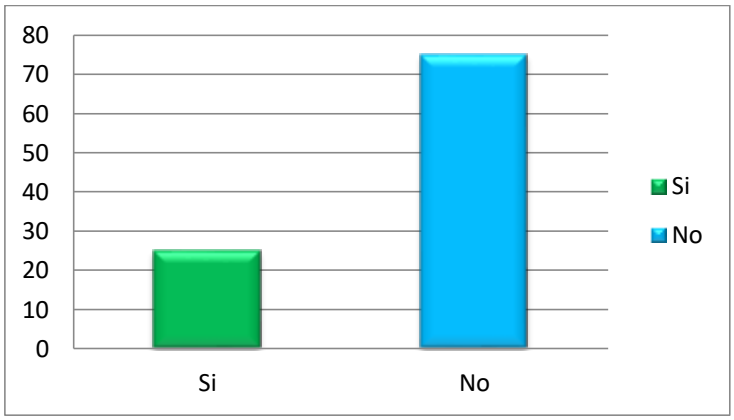

Figura 39. Herramienta de detección y prevención de intrusos (Fuente: Tabla 17)

Interpretación: El grafico podemos observar que un 25% de usuarios indican que si existe herramientas que ayudan a detectar los intrusos, mientras que un 75% indica que desconocen sobre esos mecanismos.

8. ¿En la red informática cuenta con políticas para prevenir posibles ataques y tomar acciones ante un evento sospechoso?

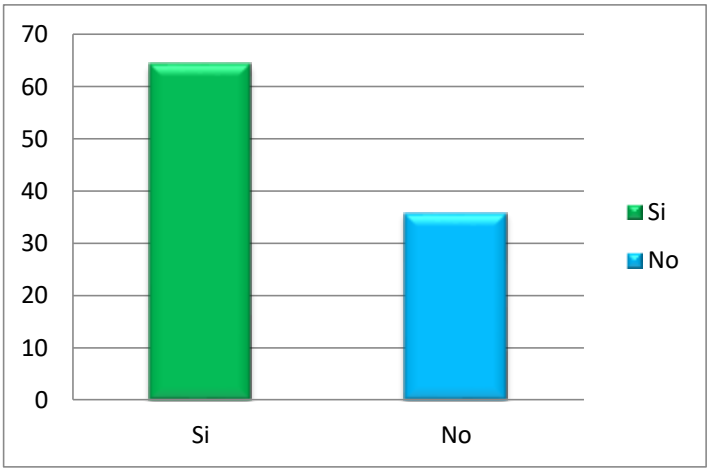

Figura 40. Políticas de prevención (Fuente: Tabla 18)

Interpretación: Según la opinión del 64% de usuarios nos indica que existen políticas de prevención contra los ataques que pueda sufrir la red informática, y un 36% de los usuarios manifiestan que no existen políticas.

9. En su opinión, ¿le gustaría que exista un mejor control de seguridad en la red informática con respecto a la detección y prevención de intrusos?

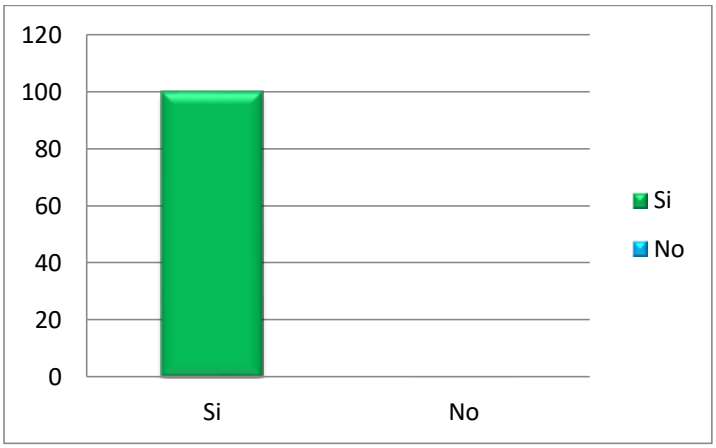

Figura 41. Mejora del control de seguridad (Fuente: Tabla 19)

Interpretación: Con respecto al mejoramiento del control de la seguridad tenemos que el 100% de todos los usuarios están en común acuerdo que se debe mejorar para evitar futuros problemas que puedan perjudicar los activos de información de los cuales son responsables.

10. En su opinión, ¿cree usted que es demasiada inversión para una implementación del sistema de seguridad que ayudara a prevenir y detectar los intrusos de la red informática?

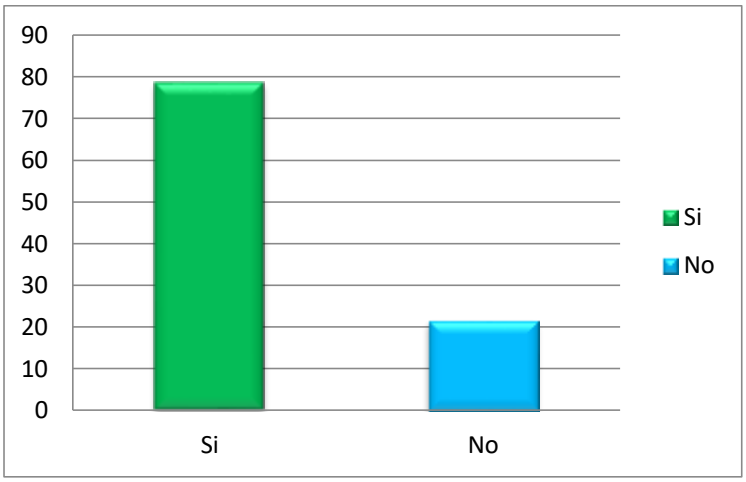

Figura 42. Inversión del sistema de prevención (Fuente: Tabla 20)

Interpretación: El grafico muestra la opinión de los usuarios de la red informática sobre la inversión que se debe realizar para la implementación del sistema de seguridad perimetral. Donde el 79% creen que es necesario realizar la inversión y solo un 21% no creen que es necesario.

Anexo 03: Matriz de Consistencia

Tabla 10

Matriz de Consistencia: Seguridad perimetral de la red Informática de la compañía minera santa luisa unidad Pallca

Problema	Hipótesis	Objetivo	Variables	Metodología
¿Cómo proponer implementar la seguridad perimetral de la red informática de la Compañía Minera Santa Luisa – Unidad Pallca?	La hipótesis de la investigación tiene un alcance descriptivo que consiste en proponer Implementar el sistema de seguridad perimetral de la Red de Datos de la Cía. Minera Santa Luisa Unidad Pallca, se mejorará la seguridad de los datos de la Empresa;.	**Objetivo General:** Proponer implementar un sistema de seguridad perimetral de la Red de Datos de la Compañía Minera Santa Luisa Unidad Pallca **Objetivos Específicos** - Determinar las vulnerabilidades de la red de datos para establecer las políticas de seguridad. - Definir la arquitectura del sistema de seguridad perimetral para lograr resguardar de manera física y lógica los datos de la Compañía Minera Santa Luisa. - Proponer implementar el sistema de seguridad perimetral haciendo uso de un equipo Firewall Fortinet FortiGate 60E para la protección de los datos que transitan por la red informática. - Proponer evaluar el sistema de seguridad perimetral para comprobar el nivel de confiabilidad de la red de datos.	**Variable 1** Seguridad Perimetral **Variable 2** Red de Datos	**Tipo de Investigación:** Nivel: Descriptivo **Diseño:** No experimental **Población:** 70 trabajadores **Técnicas e Instrumentos:** Encuesta

Fuente: Elaboración propia

Anexo 04: Matriz Operacional

Tabla 11

Matriz Operacional: Seguridad perimetral de la red Informática de la compañía minera santa luisa unidad Pallca

Variable	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores
Variable Seguridad perimetral	La seguridad perimetral informática se refiere a la seguridad que afecta a la frontera de la red de nuestra empresa también llamada perímetro. Esta frontera o perímetro, está formada por el conjunto de máquinas y dispositivos que interactúan con el exterior, con otras redes. (CISCO, 2028)	La seguridad perimetral considera la protección de los elementos de Hardware y Software, que pueden ser vulnerados por agentes internos o externos a la red de la empresa. Con la seguridad perimetral se implementan políticas y/o normas que ayudaran a realizar controles efectivos.	Controles Incidencias	- Nivel de acceso. - Alcance - Tipo de restricciones - Cantidad de incidencias. - Tiempo de respuesta. - Incidencias resueltas
Variable Red de datos	Se denomina red de datos a aquellas infraestructuras o redes de comunicación que se ha diseñado específicamente a la Transmisión de información mediante el intercambio de datos. Las redes de datos,	Los dispositivos podrán comunicarse mejor sin dificultades, y sus redes LAN estarán seguras para poder recepcionar y enviar	Hardware	- Rendimiento. - Topología - Tecnología

	generalmente, están basadas en la Comunicación de paquetes y se clasifican de acuerdo a su tamaño, la distancia que cubre y su arquitectura física.(Tanenbaum S. Andrew, 2010)	información a cualquier computadora que esté conectado.	Software	- Tipo de Licencia - Tipo de software - Sistema de archivos - Seguridad

Fuente: Elaboración propia