UNIVERSIDAD PRIVADA ANTENOR ORREGO

ESCUELA DE POSTGRADO

TESIS PARA OBTENER EL GRADO DE MAESTRO EN GERENCIA DE TECNOLOGÍA DE INFORMACION Y COMUNICACIONES

"INFLUENCIA DE LA SOLUCIÓN FIREWALL PARA LA SEGURIDAD PERIMETRAL DE LA RED DE DATOS EN LA MUNICIPALIDAD PROVINCIAL DE TRUJILLO USANDO FREEBSD PFSENSE"

ÁREA DE INVESTIGACIÓN:

Ciberseguridad de Información y Comunicaciones

AUTOR:

Br. Dionicio Guzmán, Antonio Isaac

Jurado Evaluador:

Presidente: Dr. González Herrera, Elmer Hugo
Secretario: Dr. Urrelo Huiman, Luis Vladimir
Vocal: Ms. Calderón Sedano, José Antonio

ASESOR:

Ms. Vásquez Pereyra, José Humberto

Código Orcid: https://orcid.org/0000-0002-9534-3748

Trujillo – Perú
2022

Fecha de sustentación: 2022/11/17

SOLUCIÓN FIREWALL PARA LA SEGURIDAD PERIMETRAL DE LA RED DE DATOS EN LA MUNICIPALIDAD PROVINCIAL DE TRUJILLO USANDO FREEBSD PFSENSE

Por: Br. Antonio Isaac Dionicio Guzmán

Aprobado:

Dr. Elmer Hugo González Herrera _____

(Presidente)

Dr. Luis Vladimir Urrelo Huiman _____

(Secretario)

Ms. Eduardo Elmer Cerna Sánchez _____

(Vocal)

Asesor: Ms. José Humberto Vásquez Pereyra

ACREDITACIÓN

El Ms. José Vásquez Pereyra, que suscribe, asesor de la Tesis con Título **"SOLUCIÓN FIREWALL PARA LA SEGURIDAD PERIMETRAL DE LA RED DE DATOS EN LA MUNICIPALIDAD PROVINCIAL DE TRUJILLO USANDO FREEBSD PFSENSE"**, desarrollado por la Br. en Ingeniería de Computación y Sistemas: **Antonio Isaac Dionicio Guzmán**, acredita haber realizado las observaciones y recomendaciones pertinentes, encontrándose expedita para su revisión por parte de los señores miembros del Jurado Evaluador.

Trujillo, 17 de noviembre del 2022.

El Asesor:

_____

Ms. José Humberto Vásquez Pereyra

El Autor:

_____

Br. Antonio Isaac Dionicio Guzmán

PRESENTACIÓN

Señores Miembros del Jurado:

De conformidad y en cumplimiento de los requisitos estipulados en el reglamento de grados y Títulos de la Escuela de Posgrado de la Universidad Privada Antenor Orrego, pongo a vuestra disposición la presente Tesis titulada: **"Solución Firewall para la Seguridad Perimetral de la red de datos en la Municipalidad Provincial de Trujillo usando Freebsd Pfsense"** para obtener el grado de Maestro en Gerencia en Tecnología de Información y Comunicaciones.

El contenido de la presente tesis ha sido desarrollado tomando como marco de referencia los lineamientos establecidos por la Facultad de Ingeniería, la Escuela de Posgrado y los conocimientos adquiridos durante nuestra formación profesional, además de consulta de fuentes bibliográficas.

Gracias.

Trujillo, 17 de noviembre del 2022

Br. Antonio Isaac Dionicio Guzmán

DEDICATORIA

A mis padres por ser mi fortaleza en mis momentos de debilidad y por brindarme una vida llena de mucho aprendizaje, experiencia, felicidad y permitirme el haber llegado hasta este momento tan importante de mi formación profesional.

A mis seres queridos y personas que ya no se encuentran que me ayudaron y motivaron para ser mejor persona y profesional.

A la persona que está a mi lado siempre apoyándome y motivándome para ser una mejor persona que se atrevió a seguirme para emprender una nueva aventura para crecer como profesionales.

AGRADECIMIENTOS

Quiero expresar mi agradecimiento al personal de las diferentes áreas y en especial a la Gerencia de Sistemas de la Municipalidad Provincial de Trujillo por brindarme todas las facilidades para conocer más sobre la problemática, dándome acceso a la información necesaria para el desarrollo de la presente tesis.

También agradezco al Ms. José Vásquez Pereyra, por su apoyo y asesoramiento en el desarrollo de la presente Tesis.

Y a todas las personas nos apoyaron de forma indirecta y que estuvieron siempre con nosotros durante todo el camino de este trabajo de tesis.

Muchas Gracias.

RESUMEN

SOLUCIÓN FIREWALL PARA LA SEGURIDAD PERIMETRAL DE LA RED DE DATOS EN LA MUNICIPALIDAD PROVINCIAL DE TRUJILLO USANDO FREEBSD PFSENSE

Por:

Br. Antonio Isaac Dionicio Guzmán

A través del tiempo la red de datos a ido evolucionando, gracias a las interconexiones que hay en internet en la actualidad hace posible que diversas organizaciones puedan sincronizar su información en tiempo real con sus sucursales que se encuentren lejos geográficamente, todo esto se puede tomar como un riesgo si no se tiene los medios necesarios para impedirlo.

De tal manera, la presente tesis desarrolla una propuesta para implementar una solución firewall para la seguridad perimetral de la red de datos en la Municipalidad Provincial de Trujillo usando Freebsd Pfsense.

El problema principal de esta organización, es que no cuenta con una seguridad perimetral que divida la red en una DMZ para servidores para la protección de sus datos, permitiendo separar la red de datos de clientes LAN en servicios internos poniéndolo a salvo ante cualquier ataque informático que se pueda ocasionar ante sus servicios externos.

Para solucionar dicho inconveniente se propone un Firewall como solución para la seguridad perimetral, el cual está orientado a una herramienta FreeBSD con la finalidad que pueda segmentar la red en diversas partes generando restricciones de acceso de acuerdo a las necesidades establecidas permitiendo así una mejor administración y seguridad de la red de datos.

Para la implementación de la solución se desarrolló la metodología Top-Down, se utilizó como virtualizador a Virtual Box 6.0, Linux Pfsense y para la generación de restricciones se aplicaron reglas ACL, Squid, NAT y Balanceo de Carga.

En conclusión, la implementación de un Firewall con seguridad perimetral aportó a la Gerencia de Sistemas de la Municipalidad Provincial de Trujillo a proteger su información segmentando su red de datos interna y externa ante posibles ataques informáticos que puedan comprometer la data almacenada en ellos.

ABSTRACT

FIREWALL SOLUTION FOR THE PERIMETER SECURITY OF THE DATA NETWORK IN THE PROVINCIAL MUNICIPALITY OF TRUJILLO USING FREEBSD PFSENSE

By:

Br. Antonio Isaac Dionicio Guzmán

Over time, the data network has been evolving, thanks to the interconnections that exist on the internet at present makes it possible for various organizations to synchronize their information in real time with their branches that are geographically far away, all this can be taken as a risk if you do not have the necessary means to prevent it.

In this way, the present thesis develops a proposal to implement a firewall for perimeter security in the data network of the Provincial Municipality of Trujillo.

The main problem of this organization is that it does not have a tool in hardware or software for the protection of its data network, which allows dividing the network of its internal services, safeguarding it against any computer attack that may be caused to its external services.

To solve this problem a Firewall is proposed as a solution for perimeter security, which is oriented to a FreeBSD tool with the purpose that it can segment the network in different parts generating access restrictions according to the established needs, thus allowing a better administration and security of the data network.

To implement the solution, the Top-Down methodology was developed, Virtual Box 6.0, Linux Pfsense was used as a virtualizer, and ACL, Squid, NAT and Load Balancing rules were applied to generate restrictions.

In conclusion, the implementation of a firewall with perimeter security will contribute to the Systems Management of the Provincial Municipality of Trujillo to protect your information by segmenting your internal and external data network before possible computer attacks that may compromise the data stored in them.

ÍNDICE

INDICE DE ILUSTRACIONES

INDICE DE TABLAS

CAPITULO I:

Introducción

1. Introducción

La presente investigación estudia la problemática de no contar con un firewall, en la actualidad, contar con un sistema de seguridad perimetral, que se encuentre ubicado entre la red de datos interna y externa ayuda a que la organización pueda laborar con menos riesgos ante posibles ataques informáticos no deseados dentro de ella. Por tal motivo se abarco la investigación en la Municipalidad Provincial de Trujillo a través de la implementación de un firewall de seguridad en el cual se tuvo que tomar en cuenta los recursos de la organización para poder definir las reglas con mayor exactitud tales como la cantidad de usuarios que maneja, los equipos de red, los tipos de software utilizados y el análisis de trafico de red tanto interna como externa de la organización, garantizando que la administración red sea más precisa.

Es por ese motivo que se consideró rearmar la arquitectura de red en la Gerencia de Sistemas con la finalidad de contar con un firewall que permita organizar la seguridad perimetral en la red de datos y evite una mala administración en ella que exponga el riesgo de los sistemas internos de la Municipalidad Provincial de Trujillo, teniendo todo lo expuesto se consideró que se cuenta con una red de datos considerablemente segura.

1.1. Antecedentes

Renzo Da Silva (2016), en su estudio titulado "EFECTO DE LA IMPLEMENTACIÓN DEL SISTEMA PFSENSE EN LA SEGURIDAD PERIMETRAL LÓGICA EN LOS SERVICIOS DE LA RED TRONCAL DE LA UNIVERSIDAD NACIONAL DE LA AMAZONÍA PERUANA, IQUITOS", fue desarrollado dentro de las instalaciones de La Universidad Nacional de la Amazonía Peruana (UNAP), el cual tiene una red troncal con un Firewall configurado con FreeBSD v6.3, configurada remotamente desde Lima. Se propuso como objetivo determinar el efecto de la implementación del sistema PfSense en la seguridad perimetral lógica en los servicios de la red troncal de la UNAP, para lo cual desarrollaron un diseño del sistema actual que brinda seguridad perimetral, identificaron los ingresos en el sistema de seguridad, lograron describir e implementar el sistema pfsense configurando las políticas para lograr la seguridad perimetral y por ultimo evaluaron el efecto del sistema implementado dentro de los servicios de la red troncal de la UNAP. La investigación llego con los siguientes resultados

llegando a identificar la arquitectura de la red actual de la organización y lograron reestructurar la red interna para una mayor seguridad gracias a la identificación de los ingresos al sistema de seguridad y por último se implementó el sistema de seguridad el cual dio buenos resultados al momento de evaluar los servicios configurados. El principal aporte del trabajo de investigación es poder implementar y configurar un servidor firewall para poder asegurar y optimizar la red empresarial.

Kenny Ruiz y Wilson Delgado (2018) en su estudio titulado "Implementación de una solución de seguridad perimetral Open Source en La Red Telemática de la Universidad Nacional Pedro Ruiz Gallo" muestra una solución de seguridad perimetral basado en open source, para cumplir con los requerimientos de una red DMZ, detallando la instalación del sistema de seguridad pfSense en un entorno de pruebas para realizar su pase a producción. nos da a conocer sobre la inseguridad cibernética y los riesgos que pueden presentarse en la información con la importancia, de detallar técnicamente los riesgos, amenazas contra la integridad de una red de datos que una institución educativa superior pueden ser adoptadas mostrando los materiales y métodos explicando el escenario de desarrollo en su tesis, en la implementación del sistema de seguridad sea hardware o software muestran los puntos que fueron tomados en cuenta para la selección de la solución más oportuna para el ambiente planteado y se aplicaron las configuraciones acertadas que permitan ejecutar las tareas de restricciones bloque y monitoreo. El principal aporte del trabajo de investigación es aprender diversas funciones que tiene un firewall dentro de una organización para el aseguramiento de los sistemas.

En su estudio (Leonardo, 2016) titulado como "SIMULACIÓN DE UN PERIMETRO DE SEGURIDAD LOGICA EMPLEANDO NUEVA GENERACION DE FIREWALLS PARA PREVENIR ATAQUES EXTERNOS E INTERNOS A LA GRANJA DE SERVIDORES DE UN PROVEEDOR DE SERVICIOS DE INTERNET EN UNA RED IP-MPLS", surge de la necesidad de controlar los accesos hacia los servidores del proveedor de internet detallando los diversos tipos de ataques generados por los hackers como la denegación de los servicios y el reconocimiento de los puertos, realiza una prueba de seguridad informática simulando diferentes ataques informáticos por ciberdelincuentes localizados en cualquier parte de la red global con la finalidad de dejar fuera de servicio los servidores y con la implementación del firewall impedirá que dichos

ataques sean denegados asegurando la operatividad de los servicios. El principal aporte de la investigación la simulación de un perímetro de seguridad empleado por una nueva generación de firewall evitando cualquier tipo de ataques internos o externos dentro de una red de servidores promoviendo la importancia de seguridad informática que se debe aplicar en una red empresarial.

Jaime Bonilla (2016) en su estudio titulado "DISEÑO E IMPLEMENTACIÓN DE UN FIREWALL L2 UTILIZANDO REDES DEFINIDAS POR SOFTWARE (SDN)", propuso como objetivo diseñar e implementar un Firewall capa 2 por SDN (Redes Definidas por Software) para beneficiar la tecnología en seguridad, para lo cual se desarrolló con un emulador de redes Mininet y se dividió en tres fases, la primera fase realizo un estudio teórico del SDN para tener los conceptos teóricos claros, en la segunda fase diseño el firewall para desarrollar un módulo controlador en el SDN aplicando reglas de seguridad y en la tercera y última fase emulo una red mediante el programa Mininet para experimentar un entorno de red y mostrar como la gestión y flujo de datos es más segura con la tecnología SDN. El principal aporte al trabajo de investigación es la protección perimetral dentro de la red de una organización porque ayuda a protegerse ante presuntos ataques que puedan afectar a la institución.

Carmen Jiménez (2014) en su estudio titulado "CONFIGURACIÓN E IMPLEMENTACIÓN DE UN SERVIDOR DE INTERNET CON FIREWALL BAJO ESTÁNDARES DE SEGURIDAD EN LINUX CENTOS 5.9 EN EL LABORATORIO DE REDES DE LA CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI EN EL PERÍODO MARZO – AGOSTO DEL 2013", propuso como objetivo configurar e implementar un Servidor de internet con firewall bajo estándares de seguridad en Linux CentOS 5.9 con el fin de proteger la data recopilada en cada uno de las organizaciones, para cumplir con las reglas de seguridad que son la confidencialidad, los más importante de proteger la información son de las infiltraciones y de accesos no autorizadas que puedan recopilar la información y poder así ocasionar daños y mal uso de la data recopilada. La investigación llego a los siguientes resultados el instalar equipos o software de firewall protegen y administran el tráfico de la red además se logró configurar con éxito los accesos de usuarios no autorizados a navegaciones prohibidas a internet tales como sitios o

servicios web. Se logro configurar un Servidor Firewall basado bajo normas de Seguridad Linux CentOS 5.9. El principal aporte al trabajo de investigación es como se debe realizar técnicas de bloqueos para poder proteger la información y mantener ordenada una red empresarial brindándonos una serie de pasos que se tienen que cumplir para llegar con dicho objetivo.

1.2. Enunciado del problema

¿Cuál es el impacto de la implementación de influencia de la solución firewall para la administración de la red de datos en la Gerencia de Sistemas para la Municipalidad Provincial de Trujillo usando una arquitectura de red perimetral?

1.3. Hipótesis

La implementación de una solución firewall para la seguridad perimetral basado en freebsd pfsense solucionara los problemas de vulnerabilidad en la red de datos de la Municipalidad Provincial de Trujillo.

CAPITULO II:

Planeamiento de Investigación

2.1. Planteamiento del Problema

2.1.2. Realidad Problemática

En la actualidad, contar con un sistema de seguridad perimetral nos permite organizar planes de seguridad para resguardar la información relevante, por tal motivo se requiere un firewall perimetral que permitirá tener una seguridad responsable e imprescindible que tiene como finalidad bloquear, prevenir y detener ataques no deseados y lograr controlar el uso del internet dentro de la organización. En Trujillo según (PAREDES VASQUEZ, 2016) en su tesis nos dice que la inseguridad informática se estable en dos categorías (i) inseguridad activa es cuando el usuario no tiene idea de cómo funciona un sistema es decir que una persona no desactiva los servicios de red que no utiliza. (ii) inseguridad pasiva cuando un administrador de sistemas no tiene los conceptos claros de seguridad informática y a nivel nacional en el Perú según lo publicado en (Optical News, 2018) se está registrando ataques informáticos en empresas privadas y públicas, lo cual seguirá creciendo en los siguientes años donde se observará caídas en las entidades afectados. La vulnerabilidad informática se debe a que la inversión en ella es muy baja en donde el 100% del presupuesto que manejan solo usan el 15% para la seguridad informática y por ultimo según (Gemalto, 2017) en el artículo publicado de su sitio web revela que a nivel mundial las organizaciones creen y confían estar protegidos contra los hackers, de acuerdo a un estudio hecho a 1050 organizaciones creen que bloqueando todas "las puertas informáticas" se encuentran seguros, un 94% piensa que es suficiente apartar de su red a los usuarios no autorizados, por otra parte un 65% no siente seguridad en sus datos si logran burlar su red de datos.

La Municipalidad Provincial de Trujillo es una entidad pública que se rige según lo estipulado en la ley orgánica de municipalidades y tiene competencia en todo el territorio de la provincia. Su autoridad no está restringida a la ciudad y no existe un órgano de gobierno de la ciudad como tal, dicha municipalidad está facultada para regular, promover y asegurar la conservación del patrimonio cultural de la ciudad y planificar el desarrollo urbano de la misma.

Tomando en cuenta el contexto anterior, la Gerencia de Sistemas de la Municipalidad Provincial de Trujillo no cuenta con un sistema de seguridad poniendo en riesgo toda la información que se maneja dentro de la institución quedando así un grado de vulnerabilidad

más elevado debido a los constantes cambios de mecanismos y técnicas de hackers encontrando lo siguientes problemas:

- Cantidad de ataques indeseados a los diversos aplicativos que se maneja dentro de la entidad.
- Carencia de servidores informáticos operativos debido a la baja calidad de seguridad.
- Limitada evaluación de análisis de riesgo ante posibles ataques inminentes y la falta de confianza de los usuarios.
- Deficiente diseño de monitoreo y control de todos los servicios internos en la entidad.

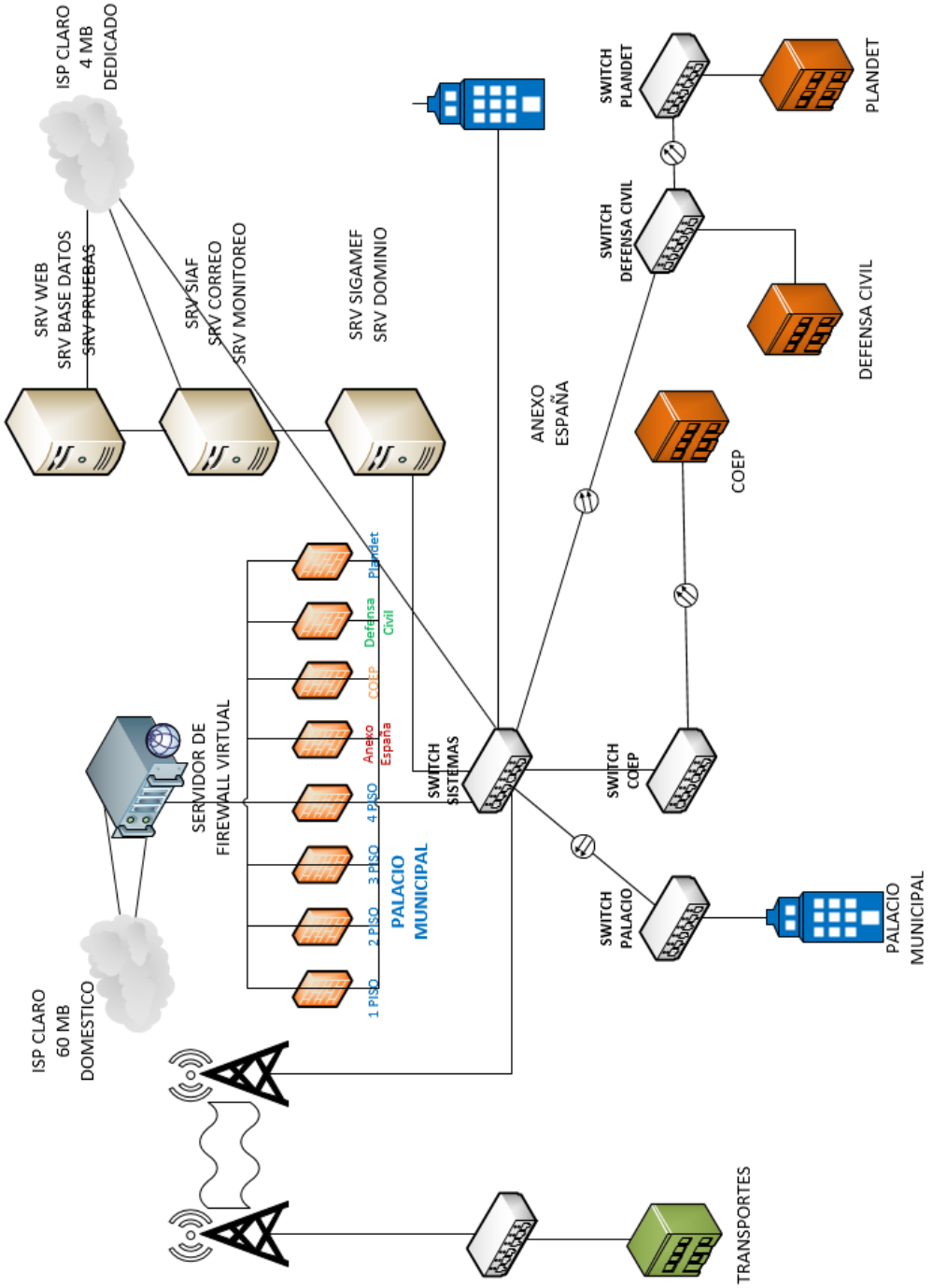
Debido a esto, se requiere implementar un firewall que cumpla con las reglas necesarias de seguridad perimetral, para ello se debe tomar en cuenta los recursos de la organización como la cantidad de usuarios, equipos de red, tipos de software utilizados y análisis del tráfico de red tanto interna como externa de la organización para mantener los accesos requeridos que permita dividir los servicios, el cual se adecuen a las necesidades de la organización además de cumplir con una debida arquitectura de red documentada, que se pueda visualizar cómo estará dividida la red perimetral con sus respectivas reglas.

En tal sentido, el presente documento de investigación lleva a cabo un análisis de la problemática de la seguridad perimetral en la Gerencia de Sistemas de la Municipalidad Provincial de Trujillo durante el periodo de diciembre del 2018 a mayo del 2019.

.

Ilustración 1

Distribución de red Actual



Nota. El gráfico muestra cómo se encuentra la arquitectura red con las diversas sedes de la entidad municipal.

Fuente: (Elaboración propia)

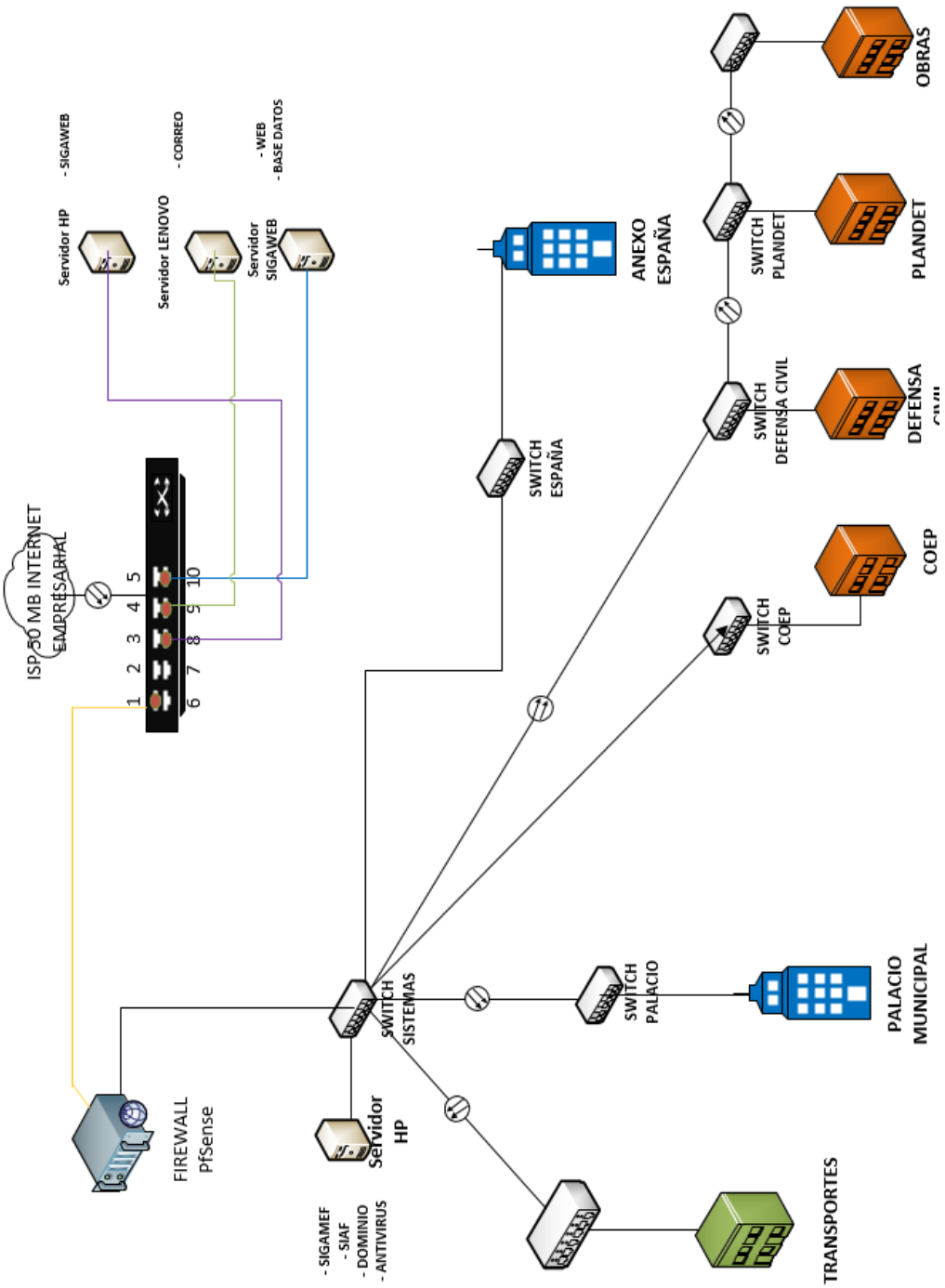
Basado en el diagrama mostrado, se determina que la distribución de la red actual con los diversos firewalls instalados, la administración de la red en la Gerencia de Sistemas presenta problemas en:

- Vulnerabilidad de los equipos internos.
- El nivel de confianza del usuario.

Por lo tanto, se propone la siguiente distribución de red de datos para la Gerencia de Sistemas de la Municipalidad Provincial de Trujillo.

Ilustración 2

Distribución de red con firewall PfSense



Nota. El gráfico muestra cómo se realizará la nueva arquitectura de red al utilizar el firewall PfSense.

Fuente: (Elaboración propia)

2.2. Marco Teórico

2.2.1. Solución Firewall para la seguridad perimetral

A. Firewall

Un firewall es una herramienta informática que brinda protección a un dispositivo o un grupo de dispositivos informáticos que se encuentran interconectadas dentro de un entorno LAN ayudando a denegar paquetes de datos no deseados que ingresan por la red de la organización haciendo un puente entre la red externa hacia la interna. (McAfee, 2021)

Función de un Firewall

El firewall opera como un muro en la red externa (internet) hacia la red interna (LAN). Las reglas que se establezcan como no permitidas para el tráfico de red en este sistema no pueden salir ni entrar dentro del entorno LAN (HP, 2021). El firewall tiene reglas establecidas que admiten:

- Autorizar un paquete (Allow).
- Bloquear un paquete (Deny).
- Redireccionar un paquete sin avisar al emisor (Drop).

Tipos de Firewall

1) **Firewall por Software:** Existen 2 tipos de firewalls en este entorno, la primera solución es gratuito: puede ser instalado en cualquier ordenador sin necesidad de una licencia completamente libre y sin costo alguno. La finalidad de este software es evitar el acceso de cierto tipo de información en los dispositivos personales. En la actualidad la mayoría de las PC cuentan con un firewall instalado. La segunda opción es comercial. Este software firewall cuentan con características similares al anterior, la diferencia es que se le añade niveles superiores de control y protección. En varias ocasiones son vendidos con otros sistemas de seguridad como antivirus. (Peña, 2020).

2) **Firewall por hardware:** Es un hardware que viene instalado en un router el cual lo usamos para conectarnos a internet, y así de esta manera todos los equipos que se encuentren conectados se encontraran protegidos por dicho firewall. (HP, 2021)

Ilustración 3

Firewall

Nota. El gráfico representa como está compuesto el firewall mediante hardware.

Fuente: (Tecnologia informatica, 2019)

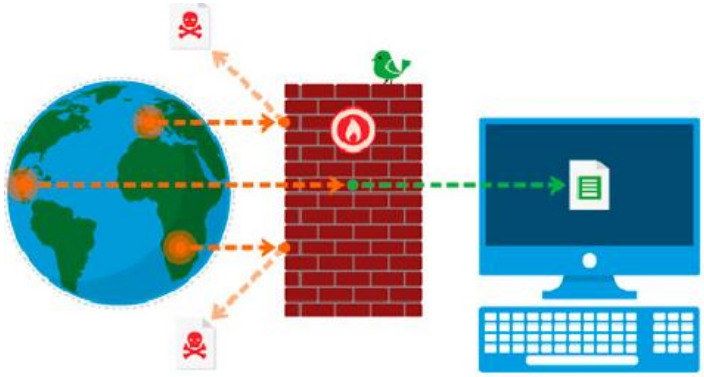
Necesidad de un firewall

Un firewall está estructurado para cuidar nuestro ordenador de diferentes tipos de amenazas, malware y ataques, como los siguientes (HP, 2021):

- Gusanos, conocidos también como “worms”, el cual estos aparecen en diversos ordenadores y se propagan vía internet logrando así el control del ordenador.
- Los intrusos informáticos que deseen ingresar en la computadora para controlarla y lograr realizar “ataques disfrazados” o a adueñarse de datos personales que estén almacenados en el disco duro.
- Negar el tráfico de red en la salida para no dejar pasar determinados protocolos sean usados para extender los virus que pueda albergar su ordenador.

Ilustración 4

Protección del Ordenador



Nota. El gráfico representa como un firewall puede proteger de diversas amenazas diagnosticando cada tráfico entrante.

Fuente: (Tecnologia informatica, 2019)

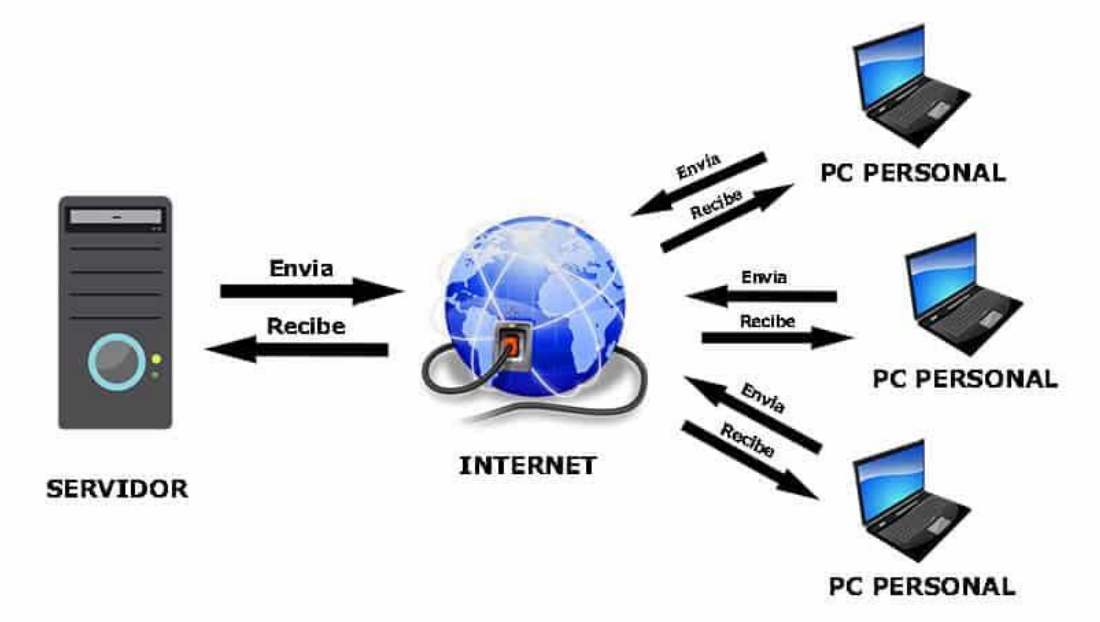
B. Servidor

Un servidor es un dispositivo que se encarga de administrar información de un grupo de clientes en red además en dicho dispositivo se puede transferir y almacenar gran cantidad de documentos, archivos, imágenes, videos, software necesario para la instalación en ordenadores clientes, base de datos, etc. (Ionos, 2020)

El servidor es un computador que tiene instalado o alojado en los diversos programas, que estén disponibles para otros computadores. Debido a eso se les concede el nombre de servidores ya que sirven diversas funcionalidades específicas y están disponibles para las peticiones de otros ordenadores. Por ejemplo, si se tiene un correo electrónico, este se recibe en un servidor de correos, si se quiere visualizar una página web, se recibe de un servidor web y así se cuentan con muchos servicios (rockconten, 2019).

Ilustración 5

Función del Servidor



Nota. El gráfico representa la funcionalidad que tiene el servidor para brindar información. **Fuente:** (Webebre, 2019)

Tipos de Servidores (docusign, 2020)

- **Servidor de Base de Datos:** Provee servicios de almacenamiento de información a diferentes programas o usuarios finales como se establece en la arquitectura cliente-servidor.
- **Servidor de Impresiones:** Dispositivo que se encarga de controlar todas las impresoras dentro de una organización.
- **Servidor de Correo y fax:** Guarda, enruta, recepciona y envía mensajes relacionados al destinatario de los clientes en la red.
- **Servidor de Telefonía:** Almacena las llamadas y mensajes de voz además de establecer un camino para las llamadas.
- **Servidor proxy:** Proporcionar seguridad dentro de la navegación de los usuarios finales.

- **Servidor de Acceso Remoto (RAS):** Controla el ordenador a través de diversos caminos de comunicación dentro de la red interna por medio de una conexión remota hacia el exterior.
- **Servidor Web:** Guarda información de lenguaje HTML, videos, documentos, imágenes y diversos archivos que está compuesto para la página web requerida.
- **Servidor de Base de Datos:** Provee servicios de almacenamiento de información a diferentes programas o usuarios finales como se establece en la arquitectura cliente-servidor.

Ilustración 6

Servidores

Nota. El gráfico representa las diversas funciones que tiene los servidores para cada aplicación o servicio que brinda.

Fuente: (Quispe G. , 2019)

Alojamiento de los servidores

Grande organización les conviene la adquisición del hardware de los servidores, los particulares y los autónomos que desean implementar proyectos en su propio servidor recurren habitualmente al alquiler. Los diversos proveedores especialistas ofrecen diversos modelos de servidores en alquiler en el que los diferentes usuarios no tienen que realizar mantenimiento por el funcionamiento del equipo físico. La gama de servidores abarca desde equipos dedicados cuyos dispositivos de hardware están disponibles a los usuarios

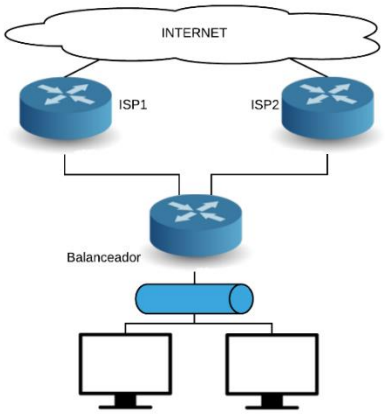
de manera exclusiva, hasta los servicios compartido de hosting para albergar a varios clientes virtuales en un solo hardware común (IONOS, 2021).

C. Balanceo de Carga

Es un método que se utiliza para repartir el trabajo a realizar entre diversos procesos, computadores, discos u otros medios. Está relacionado a los sistemas de multiprocesamiento que distribuyen la actividad de procesamiento y comunicación de forma unificada por medio de una red de datos con la finalidad que no haiga ningún aparato de "sobrecargado". El balanceo de carga es sumamente importante para los entornos de red en las que es difícil de acertar la cantidad de solicitudes que se envían a un servidor. Diversas páginas web con gran cantidad de peticiones suelen emplearse dos o más servidores con una arquitectura de balanceo de carga, permitiendo así que un servidor este muy saturado de solicitudes, automáticamente los usuarios son re direccionados a otro servidor con menos cantidad de usuarios en ese momento. (virtualizandoconcitrix, 2019).

Ilustración 7

Balanceo de carga



Nota. El gráfico representa como se debe realizar un balanceo de carga para que el servicio se mantenga en óptimas condiciones ante una posible caída de un ISP.

Fuente: (Rizolatti, 2020)

Algoritmos de balanceo de carga (ricardogeek, 2020)

Diferentes algoritmos de equilibrio de carga proporcionan diferentes beneficios; La elección del método de equilibrio de carga depende de sus necesidades:

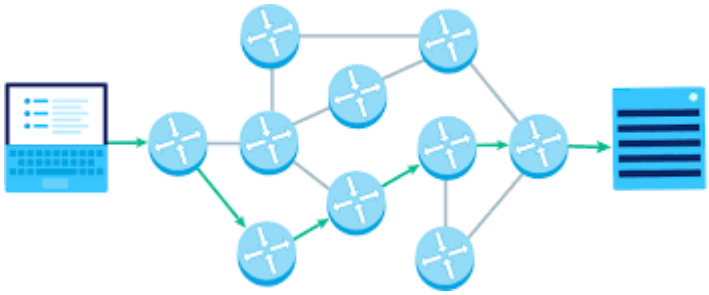
- Round Robin - Las solicitudes se distribuyen en el grupo de servidores de forma secuencial.
- Menos conexiones: se envía una nueva solicitud al servidor con la menor cantidad de conexiones actuales a los clientes. La capacidad de computación relativa de cada servidor se factoriza para determinar cuál tiene la menor cantidad de conexiones.
- IP Hash: la dirección IP del cliente se utiliza para determinar qué servidor recibe la solicitud.

D. Tolerancia a Fallos

Es la propiedad que posee un sistema que le permite continuar operando eficientemente en caso de una falla en alguno de sus componentes. La tolerancia a fallas es muy importante en aquellos sistemas que deben funcionar todo el tiempo sin interrupciones. Ante una posible falla, otro componente o procedimiento especial de respaldo pueden tomar el control para subsanar o amortiguar los efectos del fallo. Una forma de lograr tolerancia de fallas, es duplicar cada componente del sistema. (Ortiz, 2020).

Ilustración 8

Tolerancia a fallos



Nota. El grafico representa la automatización de tolerancia a fallos en caso un servicio de red este off-line automáticamente toma otra ruta para mantener en línea el servicio.

Fuente: (Fox, 2021)

Diseño de tolerancia a fallos

El diseño de tolerante a fallos está capacitado para que un sistema deba seguir funcionando a pesar que algún componente de cierto sistema falle, tal vez a un grado de nivel más comprimido, lo que es una mejor opción a que dicho sistema deje de funcionar completamente. Este diseño es usado en sistemas basados para diseñar en ordenadores la continuidad en mayor o menor medida las operaciones que se realiza con él, permitiendo reducir su rendimiento o incrementar el tiempo de respuesta en las fallas de los componentes. El sistema significa que al presentarse una falla de hardware o software no se interrumpe (Wikipedia, 2018).

Tolerancia a fallos frente a la alta disponibilidad

Tabla 1: ***Tolerancia a fallos vs Alta disponibilidad*** *(Rouse, 2016)*

Tolerancia a fallos	Alta disponibilidad
La tolerancia a fallos está estrechamente asociada con el mantenimiento de la continuidad del negocio a través de redes y sistemas informáticos de alta disponibilidad. Los entornos tolerantes a fallas se definen como aquellos que restauran el servicio instantáneamente después de una interrupción del servicio, mientras que un entorno de alta disponibilidad se esfuerza por cinco nueves de servicio operativo.	En un clúster de alta disponibilidad, los conjuntos de servidores independientes se acoplan de manera holgada para garantizar el intercambio de datos y recursos críticos en todo el sistema. Los grupos monitorean la salud de cada uno y proporcionan recuperación de fallas para asegurar que las aplicaciones permanezcan disponibles. A la inversa, un clúster tolerante a fallas consiste en varios sistemas físicos que comparten una única copia del sistema operativo de una computadora. Los comandos de software emitidos por un sistema también se ejecutan en el otro sistema.

E. Pfsense

Es una distribución Linux basada en FreeBSD, utilizado para implementar como firewall de seguridad. Es una versión open source, que se puede instalar en diversos ordenadores sin necesidad de una licencia de uso, tiene una interface web de fácil uso para su configuración de herramientas comunes como proxy, NAT, balanceo de carga, entre otros y cuando está bien implementadas las reglas convierte un equipo común en una herramienta firewall o en un enrutador muy eficaz y seguro para los servicios de redes LAN y WAN. (perulinux, 2019).

Tabla 2: Funciones de firewall (Elaboración propia)

FUNCIONES	PFSENSE	ENDIAN
FIREWALL	X	X
VPN	X	X
PROXY	X	X
SERVIDOR DHCP	X	X
SERVIDOR DNS	X	X
LIMITE DE ANCHO DE BANDA POR RED	X	
LIMITE DE ANCHO DE BANDA POR PUERTOS	X	
LIMITE DE ANCHO DE BANDA POR IP	X	
PORTAL CAUTIVO	X	X
TABLA DE ESTADO	X	
INTERFACE WEB	X	X
VLANS	X	
IP VIRTUALES	X	
NAT	X	
ENRUTAMIENTO	X	X

Ventajas de pfsense (Clouding.io, 2019)

- Es un tipo de software libre con una licencia FreeBSD. Se considera un tipo de solución gratuita que es considerada muy segura. Si se requiere de un soporte comercial, puede ser solicitado en la zona web de PFSense.
- Es práctico y versátil.
- Cuenta con una interface intuitiva. La parte de la instalación via consola como el configurador web es fácil: una vez familiarizado con la interface, el aprendizaje es rápidamente sencillo.

- La comunidad de centro de información y PFSense. En su foro tus cuestionarios son resueltos por personas especializadas, y además de contar con la documentación oficial.
- El Package Manager de PFSense cuenta en la actualidad con decenas de paquetes preinstalados que nos permiten ingresar al terminal de UTM (Unified Threat Management), dejándonos realizar gran parte de las funciones que se necesitan de este sistema. Además de contar con paquetes adicionales disponibles como SquidGuard (proxy), Snort (IDS/IPS), Asterisk, Mail scanner hay que considerar cuales realmente necesitamos para evitar convertirlo en un sistema multifunción.

F. BSD

Berkeley Software Distribution o BSD es un sistema operativo proveniente de Unix que se origina en la Universidad de California en Berkeley.

Según lo mencionado en (Wikipedia, 2020): "En los primeros años del sistema Unix sus creadores, los Laboratorios Bell de la compañía AT&T, autorizaron a la Universidad de Berkeley en California y a otras universidades, a utilizar el código fuente y adaptarlo a sus necesidades. Durante los años 1970 y 1980 Berkeley utilizó el sistema para sus investigaciones en materia de sistemas operativos. Cuando AT&T retiró el permiso de uso a la universidad por motivos comerciales, la universidad promovió la creación de una versión inspirada en el sistema Unix utilizando los aportes que ellos habían realizado, permitiendo luego su distribución con fines académicos y al cabo de algún tiempo reduciendo al mínimo las restricciones referentes a su copia, distribución o modificación".

Diversos sistemas operativos provienen del sistema implementado por Berkeley son Mac OS X, FreeBSD, PC-BSD, OpenBSD, NetBSD y SunOS. el sistema BSD ha logrado realizar grandes contribuciones en general de los sistemas operativos, como, por ejemplo:

- El control de trabajos.
- El manejo de memoria virtual paginado por demanda.
- El protocolo TCP/IP.
- El Fast FileSystem.

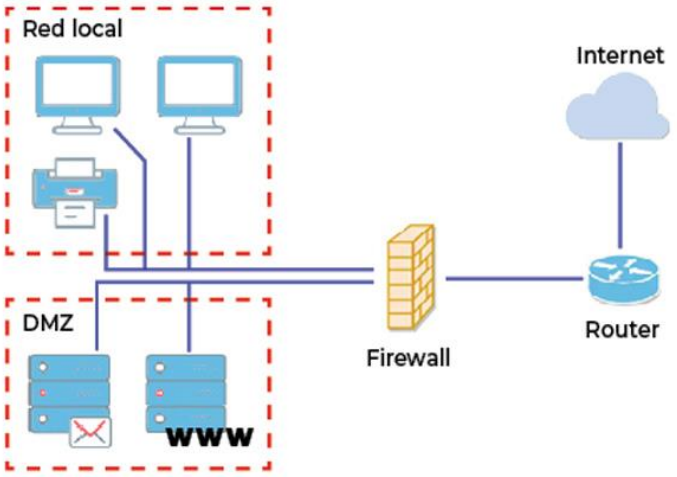
2.2.2. Seguridad perimetral de la red de datos

A. Red Perimetral

Es el espacio inseguro que se localiza dentro de la red interna de una institución y una red externa. La principal función de una DMZ es permitir que las conexiones de la red interna y externa a la DMZ estén aprobadas, por lo general las comunicaciones desde la DMZ solo se autorizan a la red externa (los equipos de la DMZ no pueden comunicarse con la red interna). Ayudando a que los equipos de la DMZ puedan brindar servicios a la red externa a la vez que cuidan la red interna en el posible caso que unos intrusos informáticos vulneren la seguridad de los equipos situados en la zona desmilitarizada dicha DMZ protegerá la red interna debido a que la zona desmilitarizada se convertirá en un laberinto sin salida. (wikipedia, 2020).

Ilustración 9

Red perimetral



Nota. El gráfico representa la segmentación de la red empresarial entre usuarios y servidores dentro del mismo lugar físico.

Fuente: (Bottini, 2021)

Las políticas aplicadas en la DMZ para la seguridad, se conforma de la siguiente (HP, 2021):

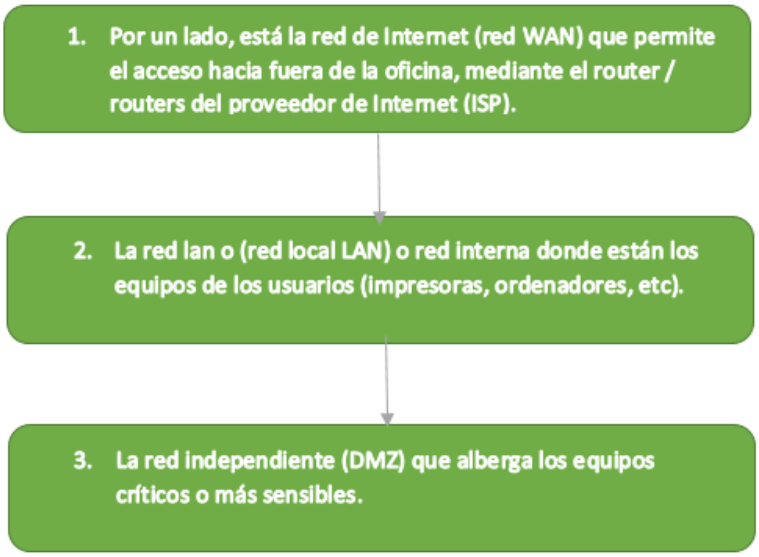
- Tráfico de red interna a la red externa autorizada
- Tráfico de red externa a la red interna prohibida
- Tráfico DMZ a la red externa rechazada
- Tráfico DMZ a la red interna prohibida
- Tráfico de red interna a la DMZ autorizada
- Tráfico de red externa a la DMZ autorizada

Filtrado DMZ

Al configurar la DMZ fundamental e importante es negar todo tipo de tráfico. Permitimos así solamente todo aquello que se requiera indispensable. En la zona DMZ se a incluido el servidor para anuncios, como DMZ host y reacciona sobre un servicio web con una ip específica. La aplicación en la que se va ingresar es de acceso web y por tal motivo el tráfico que va a ingresar entre las redes es tráfico web. Se tiene que establecer reglas dentro del firewall en su configuración empresarial que permitan acceder al servicio web (en las conexiones habitualmente de los puertos 80/http y 443/https) (tecnozero, 2019).

Ilustración 10

Escenario habitual DMZ



Nota. El gráfico representa como debe ser los pasos a elaborar una red DMZ.

Fuente: (Tecnozero, 2019)

Requisitos de red perimetral (barracuda, 2021)

Para la mayoría de las empresas modernas, no existe un único límite defendible entre los activos internos de una empresa y el mundo exterior.

- Los usuarios internos no se están simplemente conectando desde dentro del edificio, red o círculo interno de una organización. Se conectan desde redes externas y utilizan dispositivos móviles para acceder a recursos internos.
- Los datos y las aplicaciones ya no se alojan en servidores que las empresas poseen, mantienen y protegen físicamente. Los almacenes de datos, la computación en la nube y el software como servicio presentan desafíos inmediatos de acceso y seguridad para los usuarios internos y externos.

- Los servicios web han abierto una puerta amplia a las interacciones fuera de los límites de confianza normales. Para atender a múltiples clientes, o simplemente para comunicarse con otros servicios, tanto internos como externos, se producen interacciones inseguras en plataformas externas todo el tiempo.

Además, la protección individual de cada aplicación de software, servicio o activo puede ser bastante desafiante. Si bien el concepto de "perímetro de red" tiene significado para ciertas configuraciones de red, en el entorno actual se debe tratar de manera abstracta, en lugar de como una configuración específica.

B. Sistemas Operativos

Es un software libre o licenciado que le da vida a un ordenador para administrar y controlar todos los recursos de hardware y software que posee dicho computador y facilita la interacción con el usuario final. (concepto, 2021)

Tipos de Sistemas Operativos (concepto, 2021)**:**

- **Sistemas operativos para PC:** Estos tipos de sistemas son muy variados pero los sistemas más usados a nivel mundial son Windows, MAC y Linux. Windows se caracteriza por ser un sistema más intuitivo en sus interfaces, MAC es un sistema de Apple y se caracteriza por su mejor uso del hardware en los dispositivos y Linux es un sistema libre y se caracteriza por ser un sistema muy eficiente, rápido y seguro.
- **Sistemas operativos para móviles:** Estos tipos de sistemas son más utilizados en los celulares, tabletas y actualmente en los televisores este es en el caso de Android en IOS (Solo se encuentran en celulares y tabletas).

Tabla 3: Características de Sistemas Operativos *(Aco-Cas, 2015)*

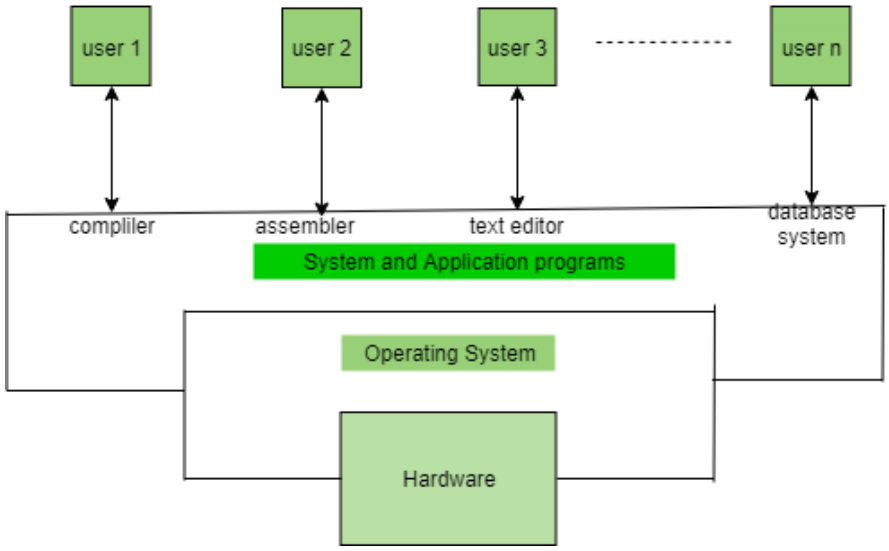
TIPOS	DESCRIPCION	EJEMPLO
MONOUSUARIO	° Solo puede ser ocupado por un único usuario a la vez. ° Administra recursos de memoria procesos y dispositivos de las PC´s.	Versiones domesticas de Windows
MULTIUSUARIO	° Puede proveer servicio y procesamiento a múltiples usuarios simultáneamente. ° Es pseudo-simultaneo. ° Combina procesador, memoria, disco duro, programas...	VMS UNIX
MONOTAREAS	° Solamente puede ejecutar un proceso del programa de computación a la vez	MS DOS
MULTITAREAS	° Permite que varios procesos se ejecuten al mismo tiempo. ° Comparten uno o mas procesadores	Linux Mac
MONOPROCESO	° Es capaz de manejar solamente un procesador de la computadora, de manera que si la computadora tuviera mas de uno se le seria útil.	DOS MACOS
MULTIPROCESO	° Es capaz de usar todos sus procesadores del sistema para distribuir su carga de trabajo. ° Trabajan de forma simétrica o asimétrica	Windows

Objetivo del sistema operativo

El objetivo fundamental de un sistema informático es ejecutar programas de usuario y facilitar las tareas. Se utilizan varios programas de aplicación junto con el sistema de hardware para realizar este trabajo. El sistema operativo es un software que administra y controla todo el conjunto de recursos y utiliza eficazmente cada parte de una computadora (ikastaroak, 2020).

Ilustración 11

Función del sistema operativo



Nota. El gráfico representa como está distribuido el sistema operativo de un computador y cuáles son sus funciones

Fuente: (M., 2019)

C. Red de Datos

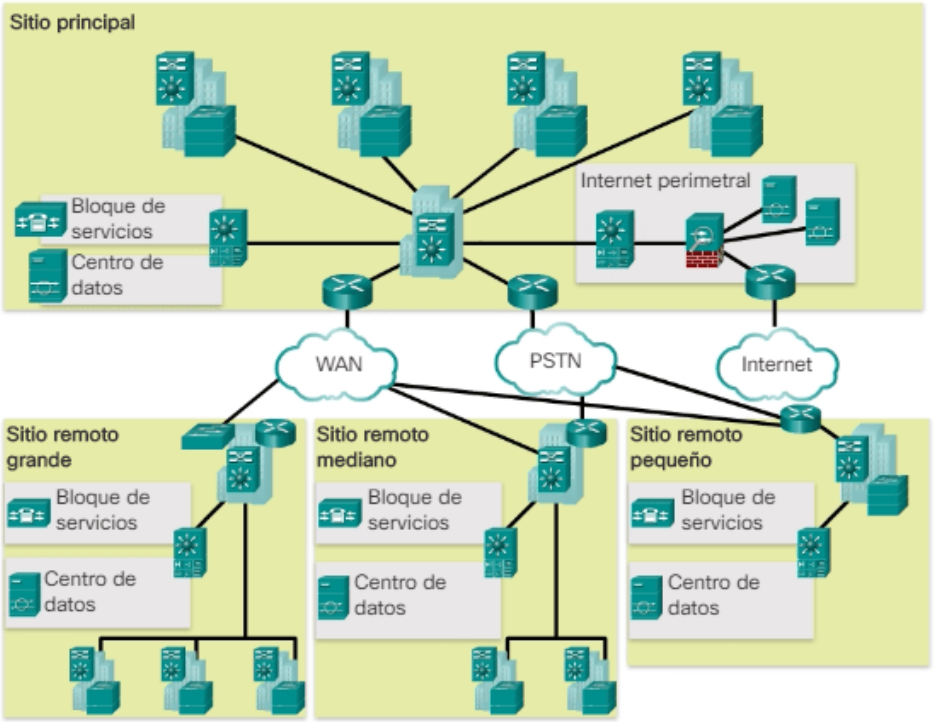
La red de datos es aquel que nos permite establecer comunicación en diferentes áreas o lugares distanciados geográficamente de una organización de forma rápida y sencilla, la red de datos se diferencia de los siguientes elementos (data, 2021):

- **Acceso con su respectivo caudal:** Este tipo de elemento se usa por medio de un cable de fibra o cobre el cual ofrece un ISP para poder establecer las conexiones ya sea inalámbrica o por GPRS. A cada uno de ellos les pertenece un camino que depende de la tecnología de acceso el cual se mide con la cantidad de datos que pude recibir una red por segundos.
- **Router:** Es un dispositivo hardware que permite implementar los mejores caminos en una red para que pueda enviar los paquetes a través de ella, este dispositivo tiene establecida una dirección ip el cual se identifica en una red interna para poder ser controlada desde cualquier lugar para poder hacer las respectivas configuraciones.

- **Respaldos:** Se implementa para evitar la interrupción del servicio en el caso que haiga una pérdida de señal.
- **Red de acceso del operador:** El ISP se encarga de enlazar los servicios en red a una central el cual se encarga de conectar otras centrales de la misma zona para que se puedan comunicar entre si y poder compartir y ver diversos tipos de información que lo requieran.

Ilustración 12

Red de Datos



Nota. El gráfico representa como es una interconexión de redes para la comunicación entre equipos informático,

Fuente: (CSICO, 2021)

D. Vulnerabilidad

La vulnerabilidad es una falla o debilidad de un sistema de información que afecta la seguridad de la data almacenada de una organización permitiendo que un atacante comprometa la disponibilidad, confidencialidad o integridad del mismo, por lo que se requiere hallarlas y eliminarlas lo más pronto posible. Estas vulnerabilidades pueden

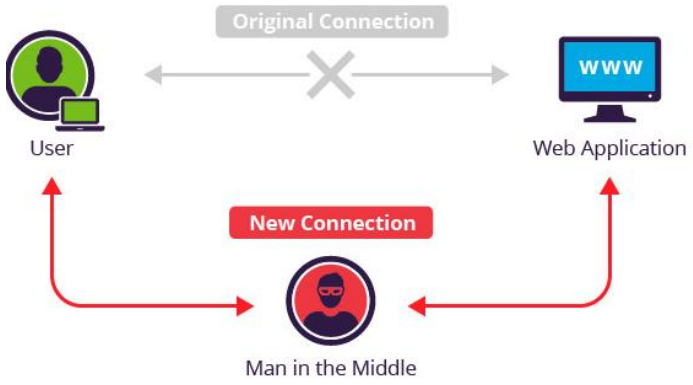
aparecer de diferentes maneras, por ejemplo: errores de configuración, carencias de procedimientos o fallos de diseño (Angel, 2020).

Existen tres tipos de vulnerabilidades (ambit, 2020):

- Vulnerabilidades ya conocidas sobre aplicaciones o sistemas instalados. Son aquellas que ya conocen las organizaciones que desarrollan la aplicación al que afecta y el cual ya cuenta con una solución, que se presenta en forma de parche.
- Vulnerabilidades conocidas sobre aplicaciones no instaladas. Estos tipos de fallas son conocidas también por las organizaciones desarrolladoras de la aplicación, como no contamos con dicho programa instalada no tendremos que actuar.
- Vulnerabilidades aún no conocidas. Son aquellas fallas que aún no han sido detectadas por la organización que desarrolla la aplicación, por lo que, si una persona desconocida a dicha empresa encontrara alguna, podría utilizarla contra todos los equipos que tienen instalado este programa.

Ilustración 13

Vulnerabilidad de servicios en red



Nota. El gráfico representa como los usuarios están expuestos ante cualquier ataque informático.

Fuente: (Hernández, 2020)

Explosión de amenazas informáticas (solarwindsmsp, 2019)

Los errores críticos en el software de la computadora de sus clientes pueden hacer que los datos de toda la red sean vulnerables a una serie de amenazas maliciosas, que incluyen:

- Malware
- Suplantación de identidad
- Proxies
- Spyware
- Adware
- Botnets
- Correo no deseado

E. Políticas de Seguridad

Una política de seguridad es un documento de plan de acción de alto nivel para combatir riesgos de seguridad, o un grupo de reglas para la conservación de cierto nivel de seguridad. Pueden contener diversas cosas desde buenas prácticas para la seguridad en un solo dispositivo, normas de una organización o área, hasta las normativas de seguridad de un país (Wikipedia, 2019).

Estas normativas deben caracterizar cuáles son los aspectos de la organización más relevantes que tienen que estar bajo mayor cuidado. De esta manera se describen una lista de procesos internos de la organización que se tienen que llevar a cabo de forma constante para no estar vulnerables. Las políticas de seguridad no solamente están dirigidas a los dispositivos informáticos y técnicos de una organización, sino a todas áreas de trabajo que estén susceptibles de ocasionar algún descuido o error de seguridad. Es útil organizar cuáles serán los mecanismos de seguridad que se implementarán en nuestra organización. Los cuales están planteados en tres ámbitos diferentes (EmprendePyme, 2020):

- Prevención: Es la primera fase imprescindible para evitar problemas.
- Detección: Al contar con alguna amenaza será necesario cómo realizar y detectar diagnósticos correctos sobre los problemas recibidos.

- Actuación: Por último, si se llega a contar con alguna inviolabilidad en nuestro sistema informático será necesario establecer normas de actuación que nos ayuden a solucionar diversos tipos de amenaza de manera más efectiva y rápida posible.

Ilustración 14

Políticas de Seguridad

Nota. El gráfico representa los pasos a seguir para mantener una red segura.

Fuente: (Wills, 2019)

Evaluación de riesgos

Analizar los riesgos se considera más el hecho de evaluar la posibilidad que se produzcan cosas negativas.

Se tiene que obtener una apreciación económica del impacto de dichos acontecimientos. Los valores obtenidos se podrán usar para reflejar el costo de cierta protección del análisis de la información, contra el costo de volver a suceder. Se tiene que tomar en cuenta la probabilidad que estos hechos sucedan cada uno de estos inconvenientes posibles. De esta manera puedan priorizar dichos inconvenientes y el costo potencial implementando un plan adecuado de acción. Se tiene que saber qué se quiere resguardar, cómo y dónde, cuidando que los costos que se incidan se consigan provechos efectivos. Para todo esto se tiene que identificar cuáles son los recursos (software, hardware, accesorios, información personal, etc.) que se tienen a la mano y las amenazas que estamos expuesto (Rodriguez, 2020).

Tabla 4: Tipo de Riesgo-Factor *(Rodriguez, 2020)*

Tipo de riesgo	Factor
Robo de hardware	Alto
Robo de información	Alto
Vandalismo	Medio
Fallas en los equipos	Medio
Virus Informáticos	Medio
Equivocaciones	Medio
Accesos no autorizados	Medio
Fraude	Bajo
Fuego	Muy Bajo
Terremotos	Muy Bajo

Niveles de riesgo

Como observar en la Tabla 3, los niveles de riesgos se dividen según su impacto de importancia y severidad en la pérdida:

- Consideración de inseguridad de pérdida del recurso (R i)
- Aprecio de importancia del recurso (I i)

Para medir el riesgo de pérdida de un recurso, se le puede conceder una unidad numérico del 0 al 10, empezando por la importancia del recurso (10 es la unidad de mayor importancia) como el peligro de desperdiciar (10 considerado como el riesgo más alto). El peligro de un bien será considerado como el producto importante por el riesgo de extraviarlo (1) (Rodriguez, 2020):

$$WR_i = R_i * I_i$$

Política de seguridad en los protocolos (tutorialspoint, 2019)

Considerando que, las políticas de TI están diseñadas para el departamento de TI, para asegurar los procedimientos y funciones de los campos de TI.

- **Políticas generales:** esta es la política que define los derechos del personal y el nivel de acceso a los sistemas. En general, se incluye incluso en el protocolo de comunicación como una medida preventiva en caso de que haya algún desastre.
- **Políticas del servidor:** esto define quién debe tener acceso al servidor específico y con qué derechos. Qué software se debe instalar, el nivel de acceso a Internet, cómo deben actualizarse.
- **Políticas de acceso y configuración del cortafuego:** define quién debe tener acceso al cortafuego y qué tipo de acceso, como la supervisión, las reglas cambian. Qué puertos y servicios deben permitirse y si deben ser entrantes o salientes.
- **Políticas de copia de seguridad:** define quién es la persona responsable de la copia de seguridad, cuál debe ser la copia de seguridad, dónde debe realizarse la copia de seguridad, cuánto tiempo se debe conservar y la frecuencia de la copia de seguridad.
- **Políticas de VPN:** estas políticas generalmente van con la política de firewall, define a aquellos usuarios que deberían tener acceso a una VPN y con qué derechos. Para las conexiones de sitio a sitio con los socios, define el nivel de acceso del socio a su red, el tipo de cifrado que se debe establecer.

F. Top Down

La metodología Top-Down se aplica para solucionar el problema comenzando por un diseño inicial en cómo se diseñará una red. Nos permite conocer de cómo debería reestructurarse el entorno lógico y físico de la red, es decir, que módulos se podrían aplicar para dar solución al problema. Al desarrollarse los módulos deben contar con una alta cohesión de los inconvenientes que buscan implementar, sin importar que cuenten con una interacción baja con los demás módulos con la finalidad que sean lo más independientes posibles (asana, 2021).

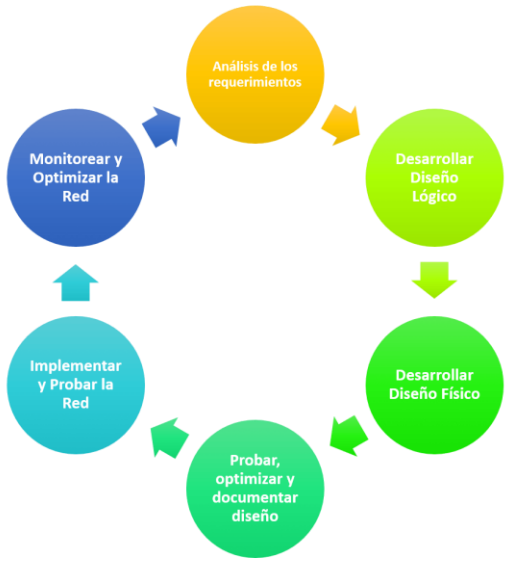
La Metodología Top-Down se utiliza también para diversas disciplinas como la gestión de proyectos o el desarrollo. Para implementarlo en redes de datos sería (Saavedra, juancarlossaavedra.me, 2019):

1. Analizar requerimientos esenciales para seleccionar la topología y los protocolos de red a usar,

2. Seleccionar el hardware para comenzar con las fases de implementación y documentación de la propuesta para llegar a la ejecución
3. optimización y monitoreo de la red de datos propuesta en un ciclo sin final.

Ilustración 15

Diseño de red con metodología



Nota. El gráfico representa el ciclo de vida que tiene una metodología para implementar una solución.

Fuente: (Saavedra, juancarlossaavedra, 2019)

Las fases de la metodología Top-Down se componen de la siguiente manera:

Fase 1: Analizar Requerimientos

- Analizar metas del negocio
- Analizar metas técnicas
- Analizar red existente
- Analizar tráfico existente

Fase 2: Desarrollar Diseño Lógico

- Diseñar topología de red
- Diseñar modelos de direccionamiento y hostnames
- Seleccionar protocolos para Switching y Routing

- Desarrollar estrategias de seguridad
- Desarrollar estrategias de administración de red

Fase 3: Desarrollar Diseño Físico

- Seleccionar tecnologías y dispositivos para redes de campus
- Seleccionar tecnologías y dispositivos para redes empresariales

Fase 4: Probar, optimizar y documentar diseño

- Probar el diseño de red
- Optimizar el diseño de red
- Documentar el diseño

Fase 5: Implementar y probar la red

- Realizar cronograma de implementación
- Implementación del diseño de red (final)
- Realizar pila de pruebas

Fase 6: Monitorear y Optimizar la Red

- Operación de la red en producción
- Monitoreo de la red
- Optimización de la red

2.3. Justificación del Estudio

2.3.1. Conveniencia

Permitirá reducir gastos en cuanto a licenciamiento de terceros para la restructuración de la infraestructura de red de datos y en beneficio, generará una gran cantidad de ahorro para la Municipalidad Provincial de Trujillo en un corto, mediano y largo plazo.

2.3.2. Relevancia Social

Servirá como una ayuda referencial para diversas organizaciones que pasarán o estén pasando por problemas similares y encuentren en este proyecto de investigación una base de cómo implementar y aplicar un servidor firewall perimetral para que administren y aseguren su entorno de red de datos de una manera más útil con información precisa y así poder mitigar posibles problemas.

2.3.3. Aporte Tecnológico

Permitirá a la Gerencia de Sistemas trabajar con un firewall de seguridad perimetral que le proporcionará resguardo en la red corporativa monitoreando el trafico éntrate y saliente además de controlar los accesos con políticas de seguridad reduciendo cualquier vulnerabilidad que pueda comprometer la información de la institución.

2.3.4. Implicaciones Practicas

Servirá como una ayuda referencial para diversas organizaciones que pasarán o estén pasando por problemas similares y encuentren en este proyecto de investigación una base de cómo implementar y aplicar un servidor firewall perimetral para que administren y aseguren su entorno de red de datos de una manera más útil con información precisa y así poder mitigar posibles problemas.

2.3.5. Valor Teórico

Se aplicará los conocimientos que brindaron los docentes a lo largo de la formación académica y además de la experiencia adquirida en el trabajo, y con esto se planteara una solución a un problema encontrado.

2.3.6. Utilidad Metodológica

Este proyecto de investigación se presenta para dar a conocer a la comunidad la importancia que tiene la seguridad en las diversas áreas de Tecnologías de Información en una organización, se aborda con precisión cuales son las vulnerabilidades que se presentan actualmente en un entorno de red empresarial, para la aplicación de un sistema de seguridad perimetral. Un aporte adicional a dicha investigación es que muestra cómo se debe armar una arquitectura de red lógica y física para el mejoramiento de los procesos de control de acceso. Una vez que sean demostrados su validez y confiabilidad podrán ser utilizados en otros trabajos de investigación y en otras instituciones educativas.

2.4. Objetivos

2.4.1. Objetivo General

Implementar solución firewall para medir nivel de confianza en la seguridad perimetral de la red de datos en la Municipalidad Provincial de Trujillo.

2.4.2. Objetivos específicos

- Analizar el estado de seguridad perimetral en la red de datos de la Municipalidad Provincial de Trujillo.
- Configurar la solución firewall perimetral en la red de datos de la Municipalidad Provincial de Trujillo.
- Aplicar la solución firewall para la seguridad perimetral de la red de datos.
- Medir la influencia alcanzado mediante la aplicación de una solución firewall para la seguridad perimetral de la red de datos.

CAPITULO III:

Material y Métodos

3.1. Diseño del estudio

Tipo de Estudio:

Correlacional

Diseño del estudio:

No experimental con finalidad aplicada debido a que permitirá a que un problema mejore, con observación pre-test y post-test.

3.2. Población

La población estará conformada por todos los sistemas que brinda la Municipalidad Provincial de Trujillo tanto interno como externo y los usuarios finales los cuales se desea proteger de los intrusos informáticos, debido a que dichos servicios son utilizados todo el año y los ataques mal intencionados se producen indeterminadamente.

3.3. Muestra, muestreo

Tipo de Muestreo: Por conveniencia (No probabilístico)

Tamaño de la Muestra:

Estará conformado por los 5 sistemas más usados en la red municipal que son SIAF, SIGA, SISTRAM, SIT y PORTAL WEB, y el número de intentos de intrusos a los servicios son altos a lo largo del tiempo, se usa la fórmula de población infinita (Mate316, 2020) para obtener el tamaño de la muestra que se toma como el número de ingresos.

Formula:

$$n = \frac{Z^2 x\ p\ x\ q}{d^2}$$

En donde

Z = nivel de confianza,

P = probabilidad de éxito, o proporción esperada

Q = probabilidad de fracaso

D = precisión (error máximo admisible en términos de proporción).

Como no se tiene conocimiento de la población de fracaso y de éxito se considera a ambos un 50%.

Tabla 5: Nivel de confianza (Elaboración propia)

Z	nivel de confianza		
	92%	96%	98%
	1,93	1,96	1,98

Tomando en cuenta un margen de error de 4% y un nivel de confianza 96% tendremos:

$$n = \frac{1.96^2 x\ 0.5\ x\ 0.5}{0.04^2} = 600$$

Se obtuvo como resultado 600 ataques de intrusos como tamaño de la muestra que serán dividíos entre los 5 servicios que cuenta la red de la Municipalidad.

3.4. Operacionalización de variables

Tabla 6: Variable independiente (Fuente Propia)

Variable	Definición Conceptual	Dimensión	Indicador	Unidad de medida	Técnica
V. Independiente Solución firewall para la seguridad perimetral basado en freebsd pfsense	Sistema firewall implementado por un conjunto de reglas en específico para asegurar la red de datos de la Municipalidad Provincial de Trujillo aplicando un nivel perimetral	Implementación	Escala	0-100%	Encuesta
		Evaluación	Nivel de calidad	0-100%	Cheklist

Tabla 7: Variable dependiente (Fuente Propia)

	Definición Conceptual	Dimensión	Indicador	Unidad de medida	Técnica
V. Dependiente Seguridad perimetral de la red de datos en la Municipalidad Provincial de Trujillo.	Cubre sobre la protección de la red de datos de la Municipalidad Provincial de Trujillo mejorando los servicios	Vulnerabilidades	Cantidad de intentos de acceso de intrusos	0-120	Ficha de incidencia
		Evaluación	Nivel de seguridad	0 - 120	Ficha de incidencia
		Confianza	Nivel de confianza del usuario	1 - 10	Encuesta

3.5. Procedimientos y técnicas

3.5.1 Procedimientos

a. **Análisis de los requerimientos:** Se procede a ordenar todo tipo de información recolectada en las entrevistas, observaciones, revisiones y evaluaciones.
b. **Desarrollar diseño lógico:** La información ordenada y documentada es revisada, editada (de ser necesario) y eliminada si es irrelevante o redundante, y procederá armar la topología lógica.
c. **Desarrollar diseño físico:** Se procederá a escoger la tecnología y equipo para la red empresarial.
d. **Probar, optimizar y documentar diseño:** Se verificará la estabilidad de la red con pruebas respectivas.
e. **Implementar y probar la red:** Se implementará del diseño de la red.
f. **Monitorear y optimizar la red:** Se procede a poner en producción la red implementada.

3.5.2 Técnicas

Técnicas de recolección: Se utilizará como técnica la encuesta que se les aplicara a las personas encargadas de las diversas áreas que interactúan en la red empresarial interna y a la gerencia de sistemas para saber cuáles son las necesidades críticas.

Instrumentos: Se empleará un cuestionario para saber cuáles son los puntos necesarios a conocer y saber cuáles son los requerimientos que tienen las áreas en general.

3.6. Plan de análisis de datos

El análisis de los datos se llevará a cabo por medio de cuadros estadísticos descriptivos (Pruebas hipótesis nula y alternativa y las Pruebas t de Student), ya que la información obtenida será analizada y mostrada por medio de cuadros y gráficos.

CAPITULO IV:

Resultados

Objetivo I: Analizar el estado de seguridad perimetral en la red de datos de la Municipalidad Provincial de Trujillo.

4.1. Analizar la arquitectura de red física y lógica actual de la red de datos

Todo este análisis se realizó por la información aportada del Anexo 2 y Anexo 3.

4.1.1. Analizar requerimientos

a. Descripción de la organización

- **Razón Social:** Municipalidad Provincial de Trujillo
- **Dirección:** Jirón Diego De Almagro 525
- **Rubro:** Promover y planificar el desarrollo urbano

La Municipalidad Provincial está facultada para regular, promover y asegurar la conservación del patrimonio cultural de la ciudad y planificar el desarrollo urbano de la misma, con capacidad para realizar acciones específicas como: formulación y ejecución de planes, definición de las zonas y usos del suelo, cuidado y mantenimiento de los ambientes y edificios históricos monumentales.

b. Visión

"La Visión de Trujillo constituye la imagen de la ciudad posible y deseada, como metrópoli líder, cultural, turística y agroindustrial que democráticamente impulsa la vida, el trabajo, la recreación y promoviendo una cultura de prevención a sus ciudadanos, en su espacio urbano y rural, seguro con un desarrollo sostenible en el tiempo".

c. Misión

"La Municipalidad Provincial de Trujillo, orienta sus recursos y acciones a promover y consolidar el desarrollo local, con el apoyo y participación activa de la población organizada, dotándolos de capacidad para analizar las condiciones del riesgo de desastre, sensibilizando y concientizándoles para la búsqueda de usos productivos alternativos para terrenos peligrosos; creando las condiciones necesarias para concertar la puesta en marcha de los procesos productivos que generan riquezas, empleo y bienestar de su población,

incorporando la Gestión del Riesgo. Propiciar el fortalecimiento institucional y la modernización de la administración municipal a fin de que cumpla la función promotora, promoviendo la creación de condiciones favorables para el financiamiento de proyectos de inversión pública imponiendo el rigor técnico y el uso eficiente de los recursos públicos aplicados a la inversión, que demuestra el espíritu de servicio a la comunidad y al desarrollo de la ciudad".

d. Cronograma de actividades

Ilustración 16

Cronograma de Actividades

Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin
	Solución Firewall para la Seguridad Perimetral de la Red de Datos en la Municipalidad Provincial De Trujillo usando Freebsd Pfsense	**116 días**	**vie 07/12/18**	**vie 17/05/19**
	Analisis de requerimientos	**16 días**	**vie 07/12/18**	**vie 28/12/18**
	Análisis de los objetivos y restricciones del negocio	3 días	vie 07/12/18	mar 11/12/18
	Análisis de los objetivos tecnicos y restricciones	3 días	mié 12/12/18	vie 14/12/18
	Caracterizacion de la red existente	5 días	lun 17/12/18	vie 21/12/18
	Caracterizacion del trafico de red	5 días	lun 24/12/18	vie 28/12/18
	Desarrollar diseño logico	**40 días**	**lun 31/12/18**	**vie 22/02/19**
	Diseño de la topologia de red	7 días	lun 31/12/18	mar 08/01/19
	Diseño de modelo de direccionamiento	10 días	mié 09/01/19	mar 22/01/19
	Desarrollo de estrategia de seguridad de la red	10 días	mié 23/01/19	mar 05/02/19
	Desarrollo de estrategia de gestión de la red	13 días	mié 06/02/19	vie 22/02/19
	Desarrollar diseño físico	**10 días**	**lun 25/02/19**	**vie 08/03/19**
	Selección de Tecnologias y dispositivos para la red empresarial	10 días	lun 25/02/19	vie 08/03/19
	Probar, optimizar y documentar diseño	**20 días**	**lun 11/03/19**	**vie 05/04/19**
	Prueba del diseño de red	4 días	lun 11/03/19	jue 14/03/19
	Optimizacion del diseño de red	8 días	vie 15/03/19	mar 26/03/19
	Documentación de la red	8 días	mié 27/03/19	vie 05/04/19
	Implementar y probar la red	**15 días**	**lun 08/04/19**	**vie 26/04/19**
	Implementacion y prueba de la arquitectura de red	15 días	lun 08/04/19	vie 26/04/19
	Monitorear y optimizar la red	**10 días**	**lun 29/04/19**	**vie 10/05/19**
	Monitorización de la red	7 días	lun 29/04/19	mar 07/05/19
	Optimizacion de la red	3 días	mié 08/05/19	vie 10/05/19

Nota. El gráfico muestra cómo se establecieron los tiempos para la elaboración de la tesis.

Fuente: (Elaboración propia)

e. Presupuesto

RECURSOS HUMANOS

N°	Personal	Descripción	Cantidad	Costo S/.
1	Investigador	Bach. Dionicio Guzmán Antonio Isaac	01	2000
2	Asesor	Mg. Ing. José Vásquez Pereyra	01	1000
			TOTAL	**3000.00**

BIENES: MATERIALES – EQUIPOS – SOFTWARE

N°	Descripción	Precio Unitario S/.	Unidad De Medida	Cantidad	Costo S/.
01	Fotocopias	0.05	Unidad	200	10.00
02	Pasajes	3.00	Unidad	50	150.00
03	Telefonía Móvil	15.00	Unidad	2	30.00
04	Internet fijo	100.00	Unidad	1	100.00
				TOTAL	**290.00**

SERVICIOS

HARDWARE					
N°	**Descripción**	**Precio Unitario S/.**	**Unidad De Medida**	**Cantidad**	**Costo S/.**
1	Laptop HP Core i3.	2500.00	Unidad	1	2500.00
3	Impresora Epson	350.00	Unidad	1	350.00
4	Memoria USB HP 16GB	20.00	Unidad	1	20.00
SUB-TOTAL					**2870.00**
SOFTWARE					
N°	**Descripción**	**Precio Unitario S/.**	**Unidad De Medida**	**Cantidad**	**Costo S/.**
1	Microsoft Office 2016	430.00	Unidad	1	430.00
2	Windows 10 Pro	900.00	Unidad	1	900.00
SUB-TOTAL					**1330.00**
INSUMOS					
N°	**Descripción**	**Precio Unitario S/.**	**Unidad De Medida**	**Cantidad**	**Costo S/.**
1	Papel Bond	15.00	Millar	1	15.00
2	Lapiceros	0.70	Unidad	5	3.50
3	Folder Manila A4	0.50	Unidad	5	2.50

4	Cartucho de tinta Negro	70.00	Unidad	1	70.00
5	Cartucho de tinta Colores	85.00	Unidad	1	85.00
6	CD-ROM	1.00	Unidad	5	5.00
SUB-TOTAL					**181.00**
				TOTAL	**4381.00**

PRESUPUESTO TOTAL

N°	**Descripción**	**Costo S/.**
1	Personal	3,000.00
2	Bienes	4,381.00
3	Servicios	2,90.00
TOTAL		**7,671.00**

PRESUPUESTO DE IMPLEMENTACIÓN DEL PROYECTO

Hardware

EQUIPO	CANTIDAD	PRECIO UNI.	TOTAL
SERVIDORES	3	S/ 45.000,00	S/ 135.000,00
SWITCH CAPA 3 24 PUERTOS DE COBRE	30	S/ 5.000,00	S/ 150.000,00
SWITCH CAPA 3 16 PUERTOS DE FIBRA	2	S/ 12.000,00	S/ 24.000,00
			S/ 309.000,00

Software

SOFTWARE	CANTIDAD	PRECIO	TOTAL
PFSENSE	1	S/ 0	S/ 0
VIRTUALBOX	1	S/ 0	S/ 0
KALI LINUX	1	S/ 0	S/ 0
			S/ 0

f. Estructura organizacional general

La Municipalidad Provincial de Trujillo está establecida por una estructura organizacional jerárquica como podemos ver en la siguiente imagen. Podemos observar que se cuenta con un área especializada, para llevar acabo la implementación del proyecto.

Ilustración 17

Organigrama de la Municipalidad Provincial de Trujillo

Nota. El gráfico representa como está distribuido la jerarquía de toda la organización.

Fuente: (Municipalidad Provincial de Trujillo, 2019)

g. Selección de la estrategia de implementación

La estrategia de implementación del proyecto contiene las siguientes tareas:

Comprender la realidad, actuación de la organización y adaptarnos con la cultura organizacional a través del uso de herramientas como encuestas, entrevistas o check list,

con la finalidad de facilitarnos a desarrollar una visión más cercana de las labores cotidianas de dicho tipo de negocio.

1. Analizar la documentación, políticas y procedimientos de seguridad en el área de sistemas.
2. Analizar el diseño físico y lógico de la red utilizados con sus diversos servicios.
3. Reunir los requerimientos necesarios de la organización.
4. Analizar los requerimientos obtenidos.
5. Realizar el diseño y la arquitectura de la red.
6. Implementar Firewall PfSense.

h. Seleccionar la metodología de desarrollo

La implementación de una solución de un firewall de seguridad perimetral es un desarrollo complejo, debido a que esta aplicación está centrada en la seguridad de los servicios internos y externos de un área específica de una empresa la cual continuamente cambia por las diversas exigencias de los clientes a través del tiempo; permitiendo así ayudar a los altos directivos a tomar mejores decisiones para el beneficio y crecimiento de la organización, debido a eso se tiene que usar las mejores prácticas existentes tal como el método que propone en la metodología top down, la cual consiste en un diseño físico y lógico en la que nos apoyaremos y con la cual se ha planteado objetivos dentro de su marco de trabajo estándar para permitir un acceso con un gran rendimiento.

i. Desarrollar el escenario de uso empresarial

Para este proyecto, el escenario de uso empresarial es el que se muestra a continuación con sus respectivos componentes:

A. Descripción de los Stakeholders

- **Personal Involucrado en el Proyecto:**

Tabla 8: Personal involucrado en el Proyecto

Nombre	Representa	Rol
Gerente de Sistemas	Personal encargado de planificar, dirigir y coordinar las actividades técnico administrativas de los programas de su competencia.	▪ Diseñar un plan estratégico del uso de las tecnologías de información sostenible en función de las potencialidades, de los recursos disponibles y de las necesidades básicas que el resto de áreas las requiera. ▪ Promover el uso de las tecnologías de información dentro y fuera de la institución. ▪ Formular, proponer y monitorear la ejecución del plan operativo anual
Administrador de Redes y Servidores	Personal encargo de implementar nuevas tecnologías y administrar los sistemas informáticos para velar por la	▪ Velar por el buen funcionamiento de todos los sistemas informáticos que se encuentra dentro de la institución.

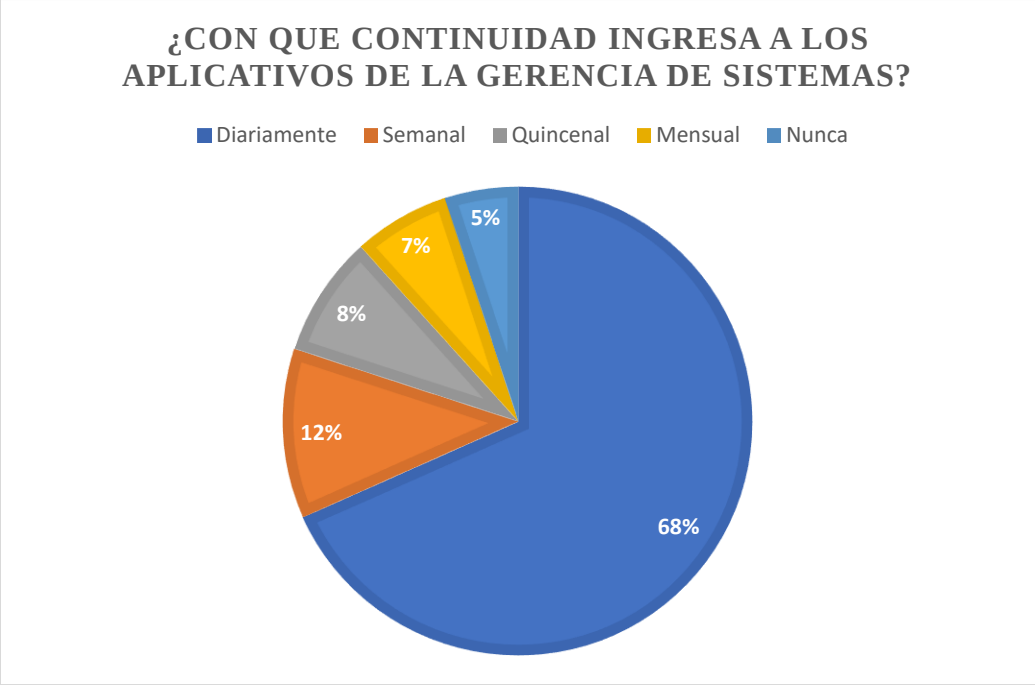
	seguridad de la información de la organización.	▪ Controlar el uso adecuado de la red hacia los usuarios con los sistemas que se encuentran dentro de organización.
Usuarios finales	Personas que usan a diarios las tecnologías dentro de la red interna de la organización.	▪ Utilizar los sistemas informáticos para su trabajo cotidiano
Alcalde y Regidores	Persona responsable de ejecutar todos los acuerdos que se realicen frente al consejo municipal.	▪ Debe proporcionar distintos proyectos de ordenanzas y acuerdos para el mejoramiento de la ciudad

En mención al primer objetivo se aplicó una encuesta a 20 usuarios finales, 10 gerentes, 10 subgerentes, 15 jefes de unidad y 5 regidores.

De acuerdo a la ilustración 18 podemos apreciar que un 68% de los encuestados acceden diariamente a los aplicativos ofrecidos por la gerencia de sistemas, un 12% acceden de manera semanal, un 8% ingresan de manera quincenal, 7% de manera mensual y un 5% afirman que nunca accedieron a los sistemas.

Ilustración 18

Resultados de la primera pregunta encuestada a usuarios finales, gerentes, subgerentes, jefes de unidad y regidores.



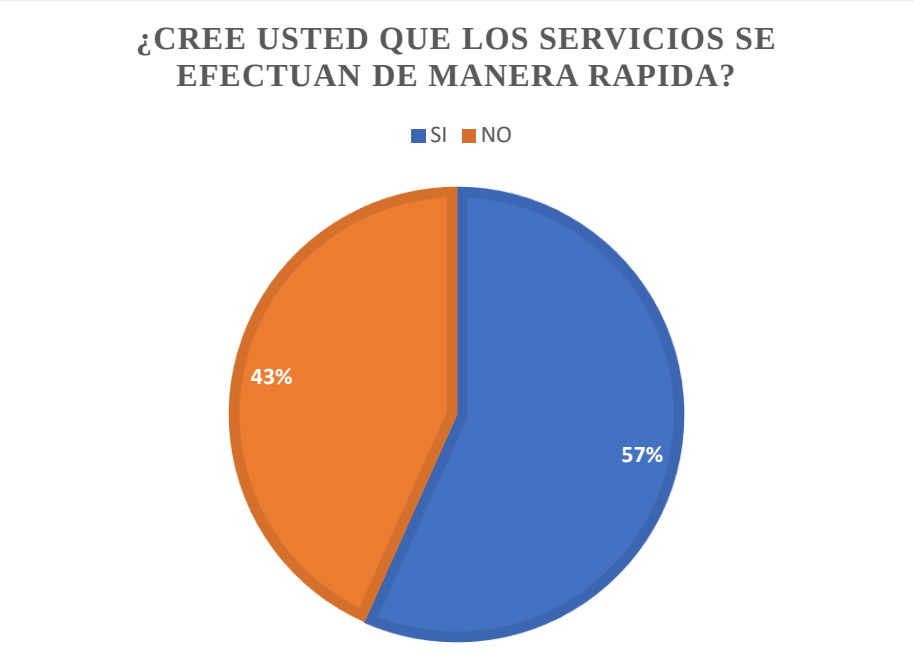
Nota. El gráfico muestra los resultados de la encuesta sobre el ingreso a los aplicativos de la entidad. Resultados obtenidos en la aplicación Google Forms.

Fuente: (Elaboración propia)

De acuerdo a la ilustración 19 un 57% confirma que los servicios ofrecidos por la Gerencia de Sistemas se efectúan de manera rápida mientras que un 43% nos dice que se presentan inconvenientes en los sistemas.

Ilustración 19

Resultados de la segunda pregunta encuestada a usuarios finales, gerentes, subgerentes, jefes de unidad y regidores.



Nota. El gráfico muestra los resultados de la encuesta sobre la efectividad de los servicios. Resultados obtenidos en la aplicación Google Forms.

Fuente: (Elaboración propia)

De acuerdo a la ilustración 20 nos comenta un 58% de los usuarios se sienten seguros con las aplicaciones ofrecidas por la Gerencia de Sistemas mientras que un 42% no se sienten seguros en dichas aplicaciones.

Ilustración 20

Resultados de la tercera pregunta encuestada a usuarios finales, gerentes, subgerentes, jefes de unidad y regidores.

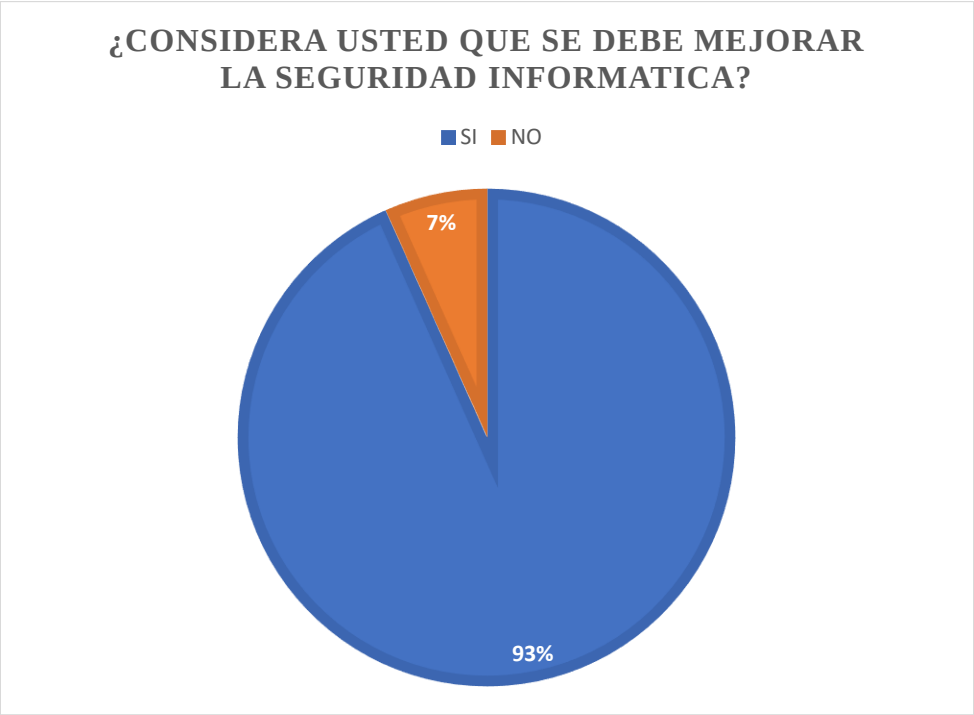
Nota. El gráfico muestra los resultados de la encuesta sobre la seguridad de los aplicativos de la oficina de sistemas de la MPT. Resultados obtenidos en la aplicación Google Forms.

Fuente: (Elaboración propia)

De acuerdo a la ilustración 21 un 93% de los encuestados nos afirma que la seguridad informática debe mejorar mientras un 7% no está de acuerdo.

Ilustración 21

Resultados de la cuarta pregunta encuestada a usuarios finales, gerentes, subgerentes, jefes de unidad y regidores.



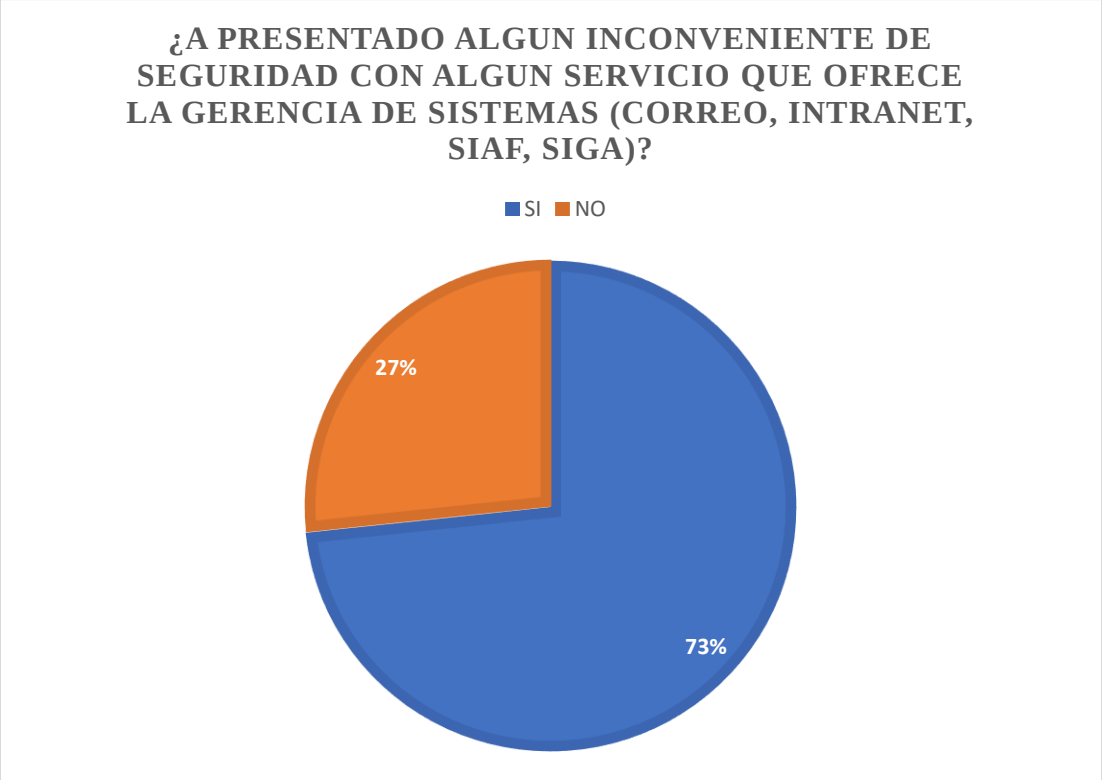
Nota. El gráfico muestra los resultados de la encuesta sobre la mejorar de seguridad informática dentro de la entidad municipal. Resultados obtenidos en la aplicación Google Forms.

Fuente: (Elaboración propia)

De acuerdo a la ilustración 22 un 73% afirma a ver tenido inconvenientes de seguridad al acceder a sus cuentas institucionales mientras que un 27% afirma que no ha presentado ningún problema.

Ilustración 22

Resultados de la quinta pregunta encuestada a usuarios finales, gerentes, subgerentes, jefes de unidad y regidores.



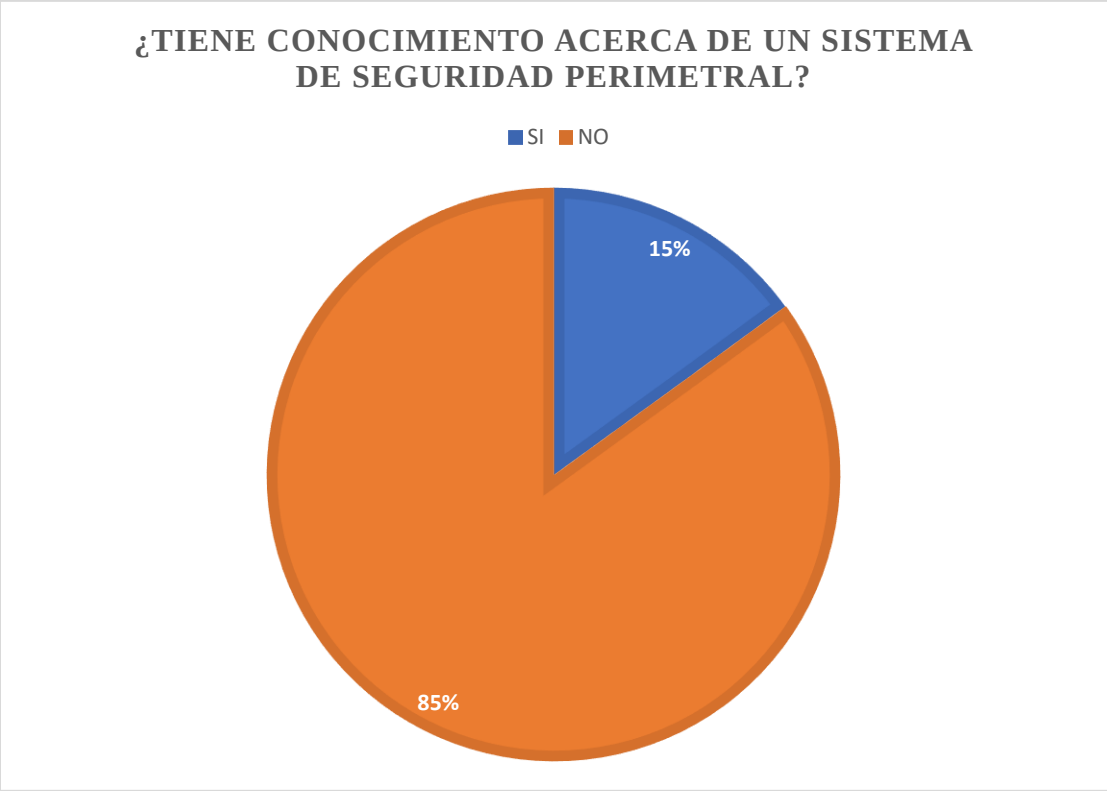
Nota. El gráfico muestra los resultados sobre los inconvenientes de seguridad dentro de la red de datos de la MPT. Resultados obtenidos en la aplicación Google Forms.

Fuente: (Elaboración propia)

De acuerdo a la ilustración 23 un 85% de los encuestados no tiene idea de que se tarta un sistema de seguridad perimetral, mientras que un 15% afirma tener conocimiento sobre que se trata dicho sistema.

Ilustración 23

Resultados de la sexta pregunta encuestada a usuarios finales, gerentes, subgerentes, jefes de unidad y regidores.



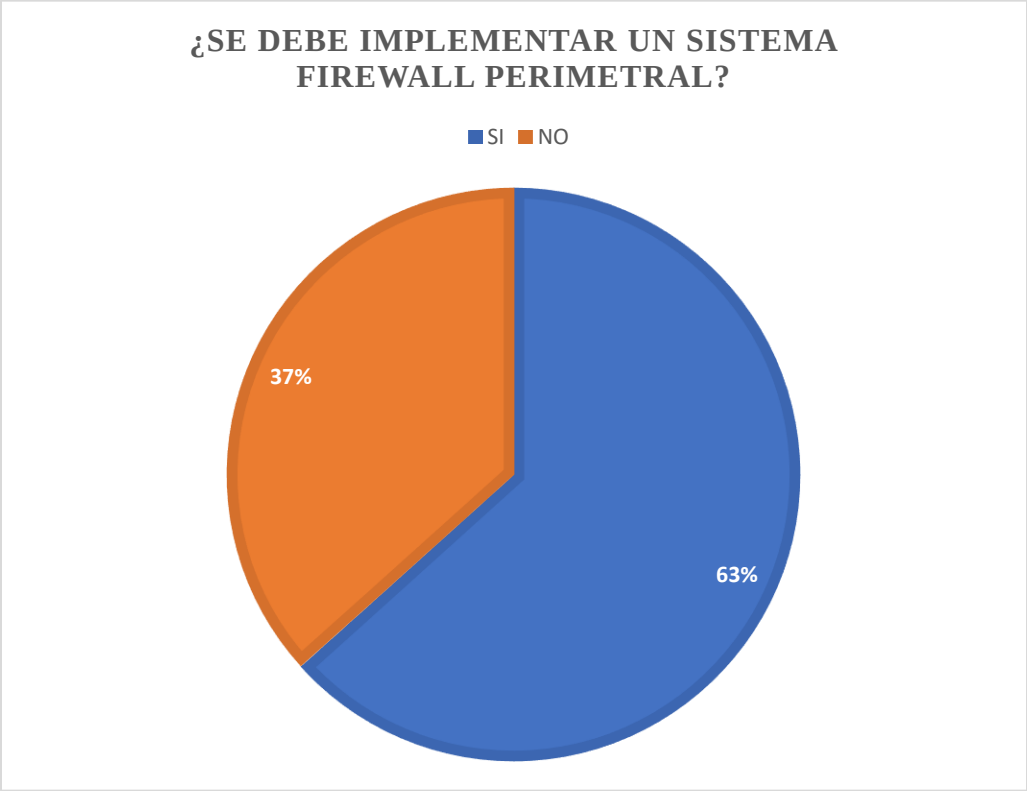
Nota. El gráfico muestra los resultados de la encuesta sobre los conocimientos de los usuarios respecto a la seguridad perimetral. Resultados obtenidos en la aplicación Google Forms.

Fuente: (Elaboración propia)

De acuerdo a la ilustración 24 un 63% nos afirma que se debe implementar un sistema de seguridad perimetral mientras que un 37% no está de acuerdo a dicho sistema.

Ilustración 24

Resultados de la séptima pregunta encuestada a usuarios finales, gerentes, subgerentes, jefes de unidad y regidores.



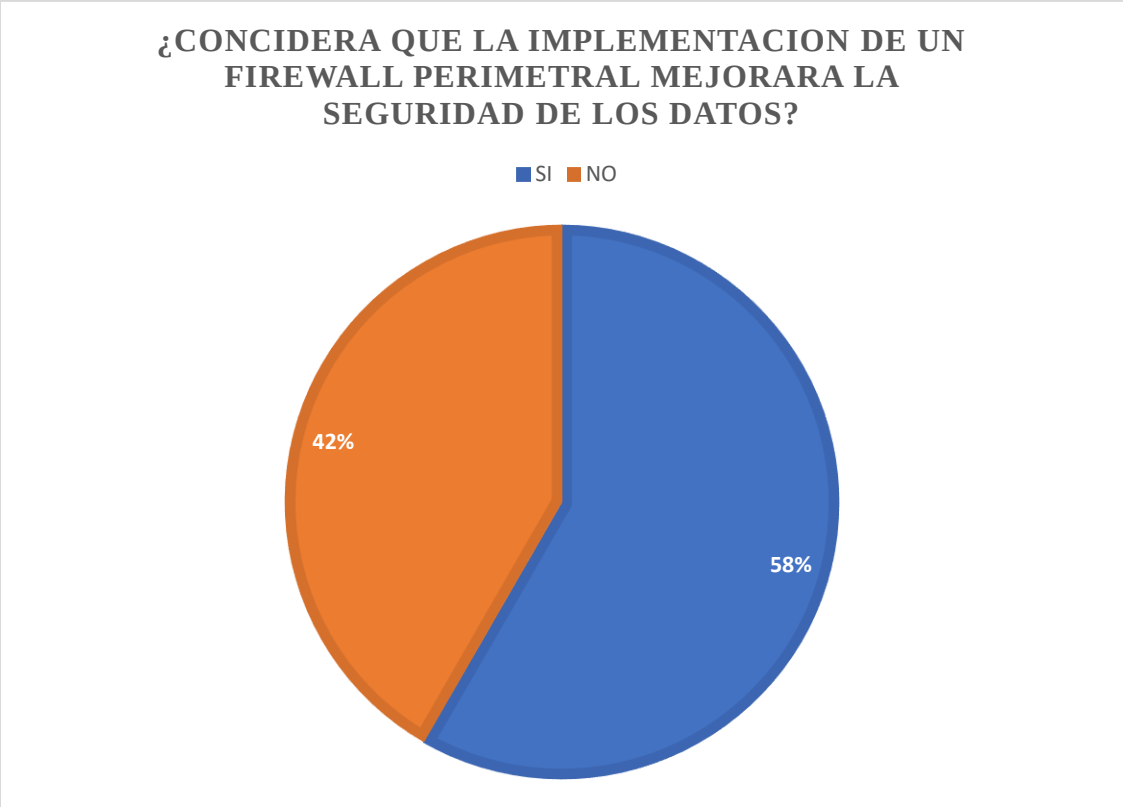
Nota. El gráfico muestra los resultados de la encuesta sobre la importancia de implementar un sistema de seguridad perimetral. Resultados obtenidos en la aplicación Google Forms.

Fuente: (Elaboración propia)

De acuerdo a la ilustración 25 nos muestra que un 58% de los encuestados piensan que un firewall si lograra mejorar la seguridad de la red de datos de la institución mientras que un 42% piensan que no funcionara dicha solución.

Ilustración 25

Resultados de la octava pregunta encuestada a usuarios finales, gerentes, subgerentes, jefes de unidad y regidores.



Nota. El gráfico muestra los resultados de la encuesta sobre mejora de seguridad perimetral cuando se implemente un sistema de seguridad. Resultados obtenidos en la aplicación Google Forms.

Fuente: (Elaboración propia)

j. Análisis técnico

La infraestructura de red actual de la organización de la Municipalidad Provincial de Trujillo no está implementada para segmentar y proteger la red de datos de servicios internos de los servicios externos sobre su misma plataforma.

Con el nuevo diseño que se pretende mejorar la seguridad de los aplicativos y servicios internos y externos con la finalidad de beneficiar al usuario final y la organización. Se logró realizar el levantamiento de requerimientos a través de la observación directa de la infraestructura de red, encuestando al gerente de sistemas, administrador de red y ciertos usuarios finales de la organización, en donde se enfatizaron y persiguieron los siguientes requerimientos:

- Contar con un nuevo servicio hacia los usuarios finales.
- Contar con mayor seguridad en la información.
- Implementar una red LAN por la cual fluyan varios servicios internos.
- Natear las direcciones de ip publica de los servidores que proveen servicios a internet por direcciones ip privadas.

  Para el nateo de direcciones publicas también se realizó una segmentación de red en cada uno de los servidores de la municipalidad dentro del firewall que dan servicio a la red externa como podemos apreciar a continuación:
- Reducir la cantidad de spam generado por el servidor de correos
- Reducir gastos de operación.
- Tener una administración centralizada.
- Implementar una red inalámbrica para conexión a internet para visitantes.

Se tiene en cuenta los siguientes requerimientos técnicos que se pretende realizar los servicios de red:

- Seguridad: Contar con una seguridad lógica y física de la red.
- Disponibilidad: Tener enlaces redundantes con dispositivos de comunicaciones para no interumpir el trabajo diario de los usuarios.
- Calidad de servicios: Permitir que la red priorice cualquier aplicación o servicio que se desee.

- Escalabilidad: Con el diseño de la red, el crecimiento o disminución de usuarios, aplicaciones y servicios se deben adaptar a cualquier cambio.
- Administración: Centralizar el manejo de la red.

k. Análisis de red existente

Actualmente la red de la organización cuenta con una línea dedicada de internet con un pool de 8 ips públicos, el cual son utilizables 5 ips, los servicios de la parte cliente vienen trabajando de forma paralela con los servidores en una misma red, ocasionando que los servidores que brindan servicios a internet se queden sin funcionamiento por problemas que se presentaran en la red cliente o viceversa que se cayera los servicios de los servidores hace que la red cliente deje de funcionar haciendo que los usuarios en la entidad no pudieran trabajar, además de ocasionar un riesgo para la institución, ya que estamos expuesto ante posibles ataques informáticos que podían llevarse información confidencial ver ilustración 1.

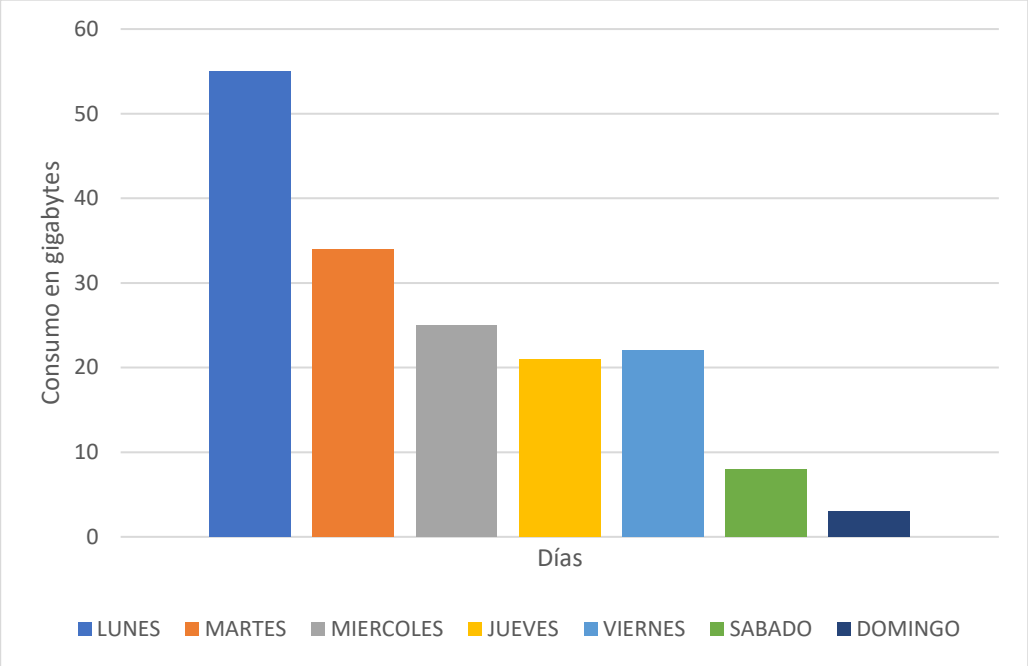
l. Análisis de tráfico existente

Se llevó a cabo un análisis previo para el monitoreo de red donde se escogió el horario en base a la cantidad de usuarios que se encuentran laborando en la organización en diversas horas del día. Se verificó la cantidad de usuarios, también se definió 5 días de monitoreo de la red para ver el consumo total.

Con esta prueba se consideró que el horario más acorde para llevar a cabo el monitoreo de la red fue en el horario de trabajo de 7:00 a.m. a 15:00 p.m. debido a que a estas horas se logra visualizar la mayor fluidez de personal en la organización ya que en ese tiempo todo el personal comienza a enviar y descargar información.

Ilustración 26

Cantidad de consumo diario actual

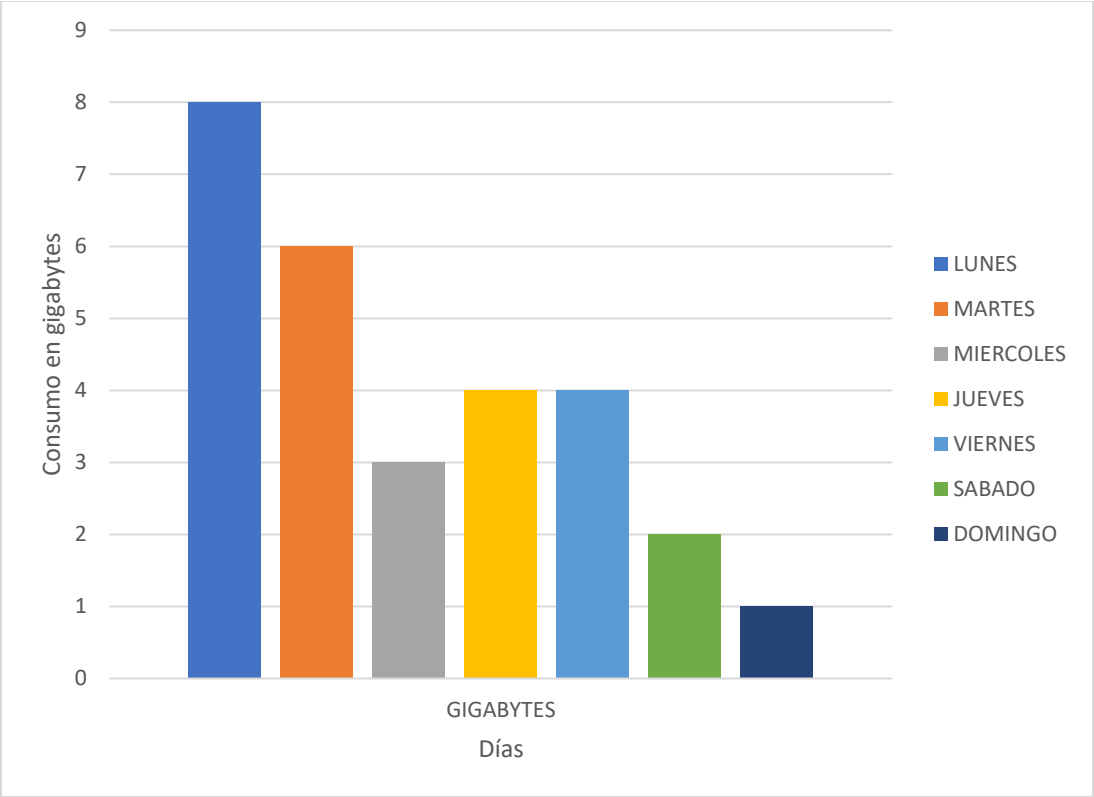


Nota. El gráfico muestra una comparativa de consumo de red diario al utilizar el firewall pfsense. Resultados obtenidos en el Sistema Operativo Kali Linux y la aplicación Google Forms.

Fuente: (Elaboración propia)

Ilustración 27

Cantidad de consumo diario anterior



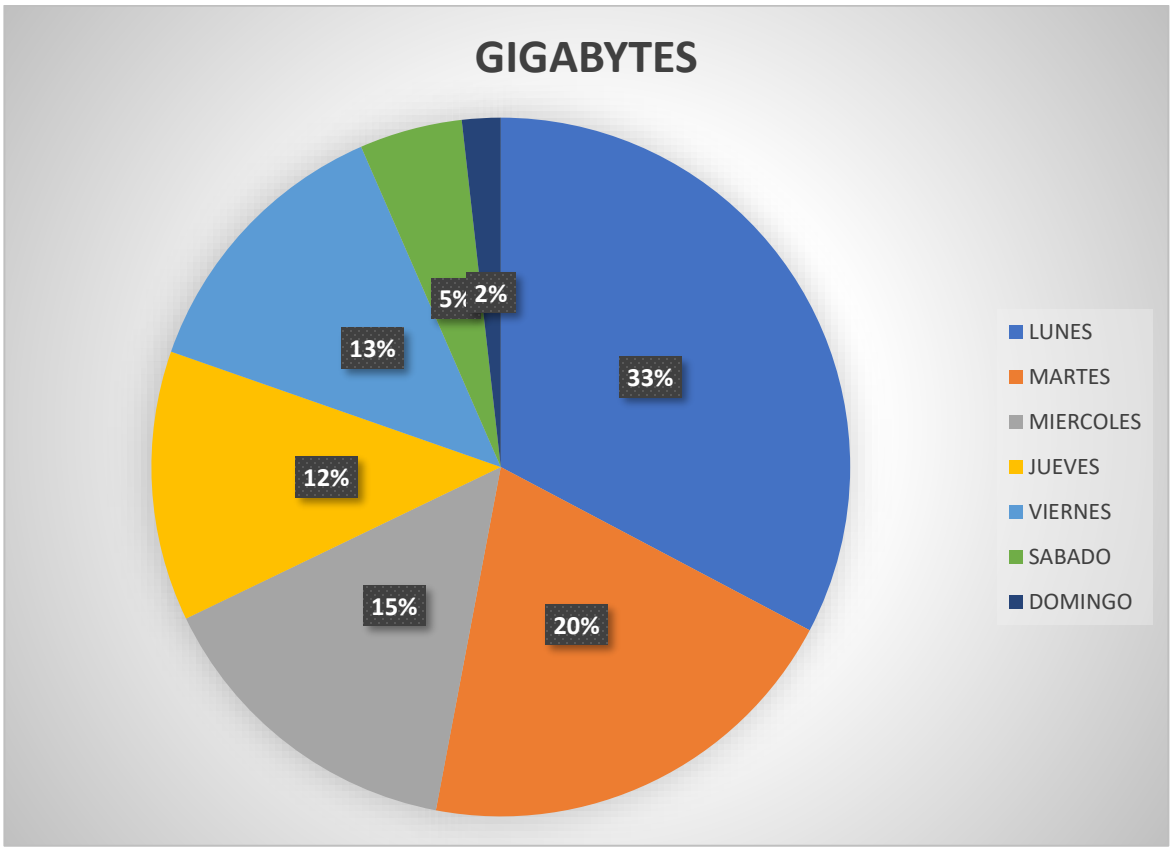
Nota. El gráfico muestra una comparativa de consumo de red diario antes de utilizar el firewall pfsense. Resultados obtenidos en el Sistema Operativo Kali Linux y la aplicación Google Forms.

Fuente: (Elaboración propia)

Al realizar el test de la red en el horario establecido, se pudo verificar que la velocidad de internet no presenta ningún tipo de inconveniente cuando la gran parte de los usuarios se encuentran conectados a la vez, por consecuencia el plan contratado de línea dedicada funciona correctamente. Se puede evidenciar en el porcentaje de uso de la red.

Ilustración 28

Porcentaje de uso de red diario actual

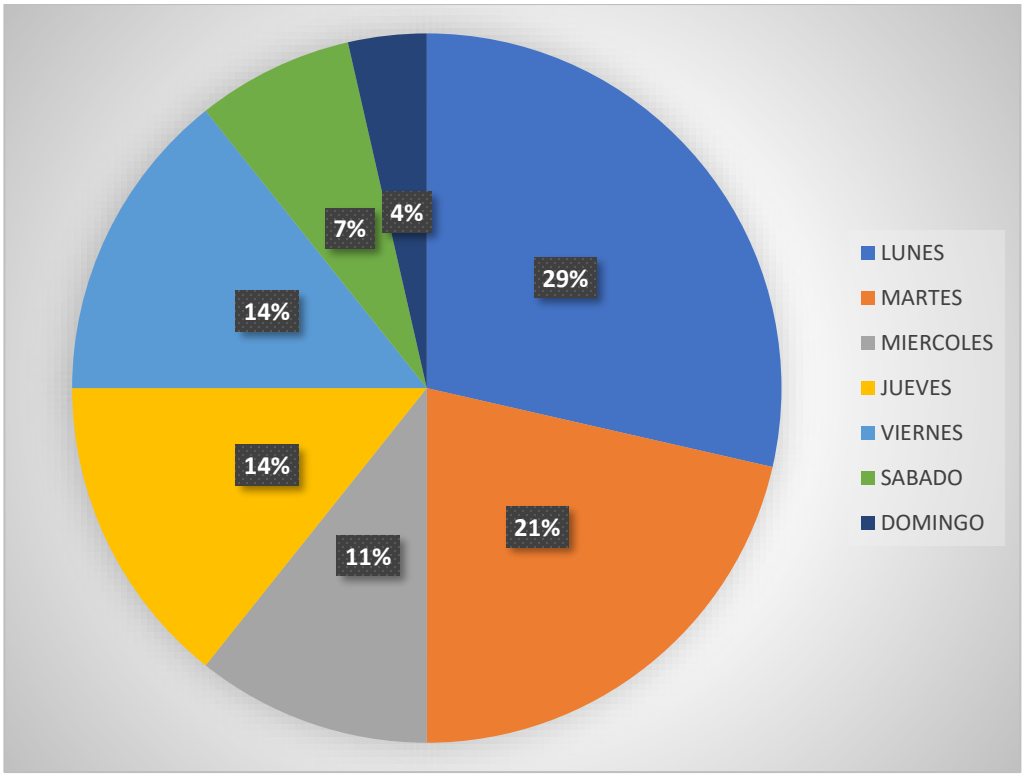


Nota. El gráfico muestra una comparativa de consumo de red en porcentaje al utilizar el firewall pfsense. Resultados obtenidos en el Sistema Operativo Kali Linux y la aplicación Google Forms.

Fuente: (Elaboración propia)

Ilustración 29

Porcentaje de uso de red diario anterior



Nota. El gráfico muestra una comparativa de consumo de red en porcentaje antes de utilizar el firewall pfsense. Resultados obtenidos en el Sistema Operativo Kali Linux y la aplicación Google Forms.

Fuente: (Elaboración propia)

m. Herramientas para la simulación

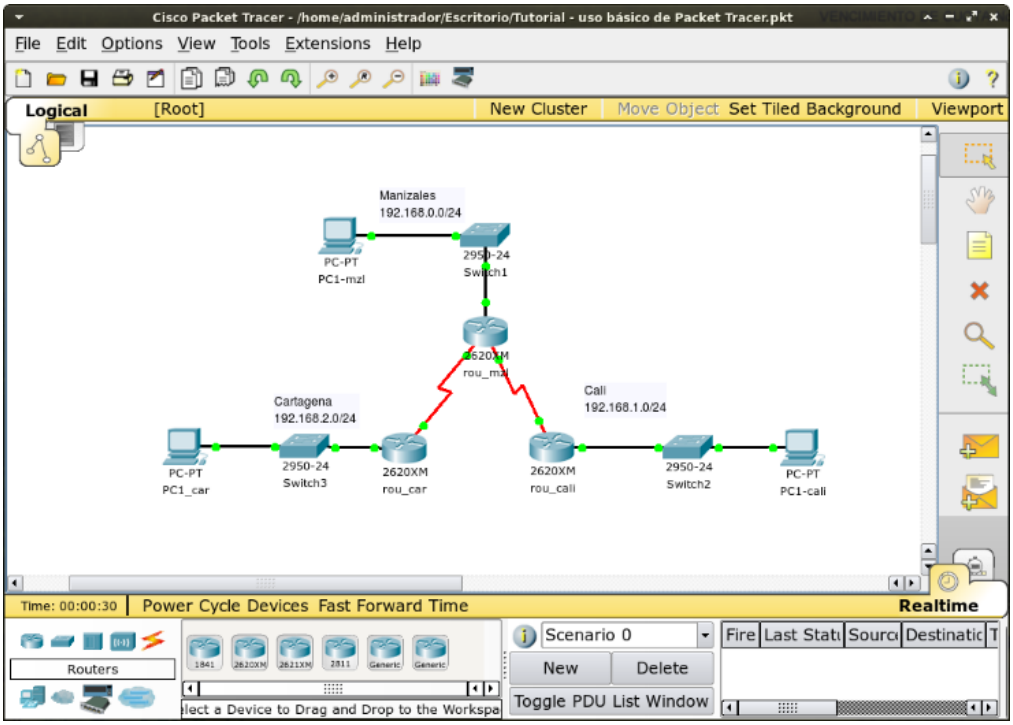
I. Packet Tracer

La aplicación de Packet Tracer permite dar una simulación de la red debido a que tiene los servicios, equipos y protocolos necesarios para simular un entorno de red de todo tipo en cisco, con la facilidad de realizar dichas pruebas sin tener que adquirir los dispositivos físicos para dicha simulación.

Para este tipo de proyecto se utilizó dicho simulador para llevar a cabo la configuración de los equipos simulación de la red y topología de la red para dar a conocer lo propuesto del proyecto.

Ilustración 30

Software Packet Tracer



Nota. Cisco Packet Tracer.

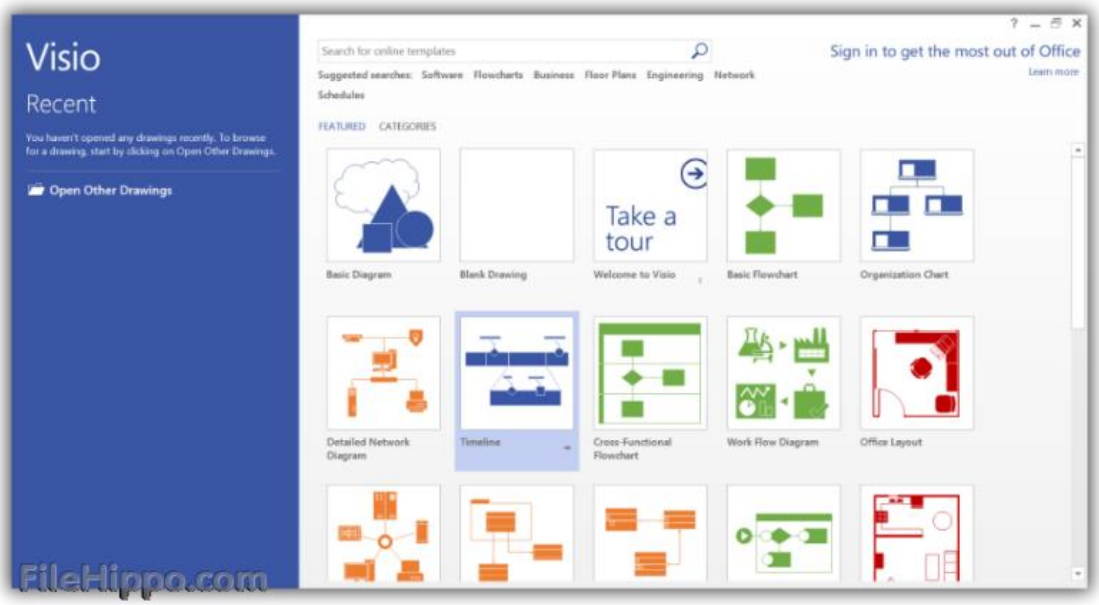
Fuente: (Cisco Networking Academy, 2019)

II. Visio

La aplicación Visio es una herramienta de la compañía Microsoft el cual se usa para crear cualquier tipo de diagramas y procesos a partir de planos de redes de datos a planos estructurales entre otros, dicha aplicación se utilizó para diseñar del plano de red de la Municipalidad Provincial de Trujillo.

Ilustración 31

Software Visio



Nota. Visio, por Microsoft, 2016.

Fuente: (Microsoft, 2017)

III. Kali Linux

Kali Linux es un Sistema Operativo open source basado en Debian que se utiliza para realizar auditorías y seguridad informática en cualquier red de datos y ordenadores nos permite conocer las brechas de seguridad en los equipos informáticos ayudando a mejorar la seguridad en el entorno tecnológico.

Ilustración 32

Kali Linux

Nota. Sistema Operativo Kali-Linux.

Fuente: (Kali, 2021)

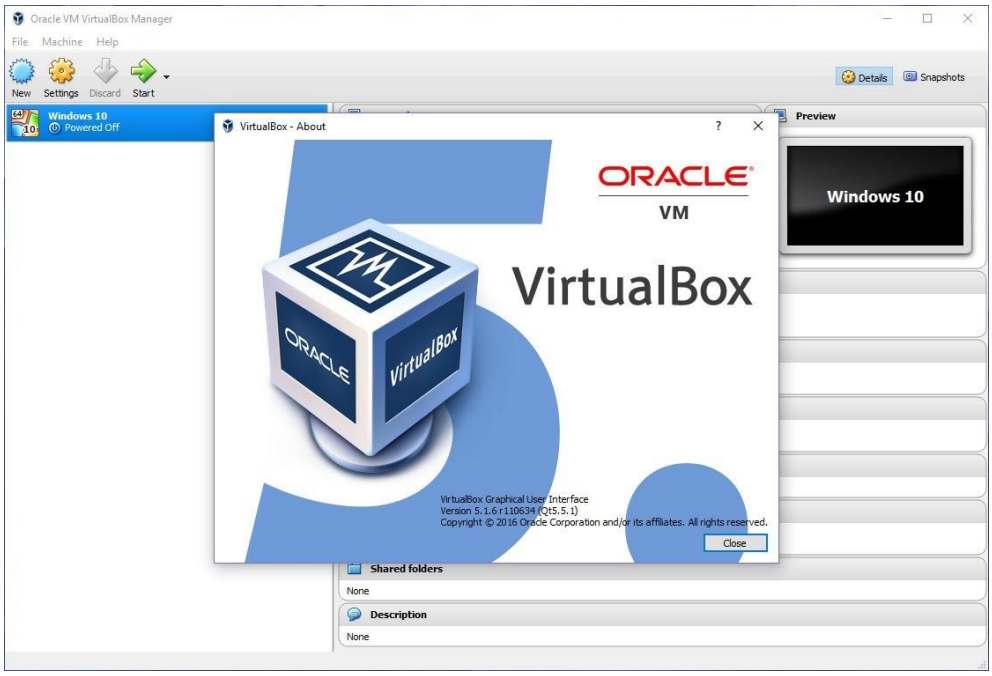
IV. Virtual Box

El software Virtual Box es una aplicación de gran apoyo para todos aquellos que quieran simular sistemas operativos para cualquier tipo de pruebas o de gran utilidad para levantar servicios adicionales en sistemas apartes sin necesidad de adquirir un nuevo equipo, es decir, crear una máquina virtual en el que podemos instalar otro tipo sistema.

Para la implementación de este proyecto se usó el software Virtual Box para levantar los servicios que ofrece PfSense y así poder llevar a cabo el inicio y fin del proyecto realizando pruebas e implementación en entorno real.

Ilustración 33

Software VirtualBox



Nota. Virtual Box software para virtualización.

Fuente: (Oracle, 2019)

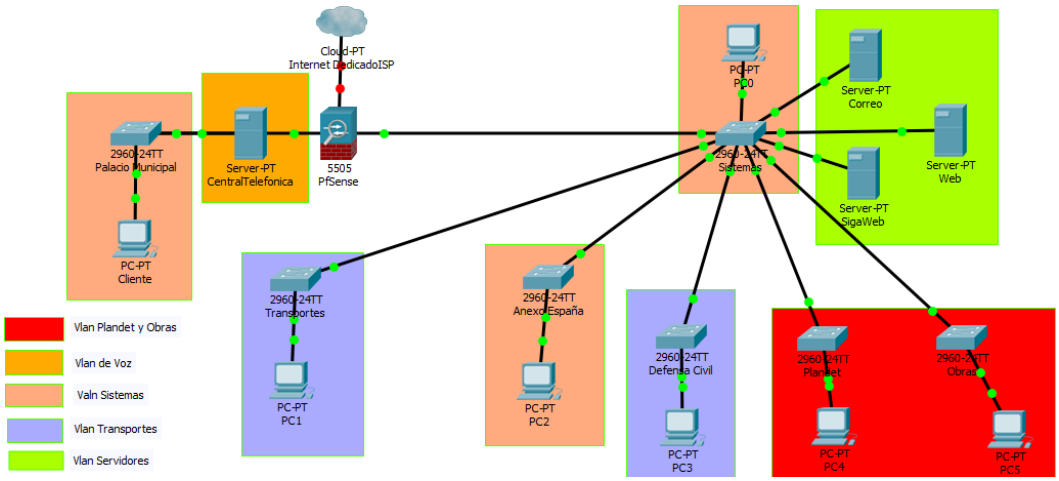
n. Implementación

I. Diseño Lógico

Como se planteó al inicio del proyecto la red lógica estará dividida por distintas VLANs de acuerda a las áreas que permitirán que los equipos puedan conectarse entre ellos mismos para que puedan acceder a los distintos servicios que se plantearon en el proyecto, adicionalmente se estableció reglas de listas de acceso propuestas por el Gerente de Sistemas para que las distintas áreas contengan restricciones y accesos en el diseño lógico. Se muestra a continuación la distribución de los equipos.

Ilustración 34

Diseño de red lógica



Nota. El gráfico muestra de cómo se segmentará la red dentro de la organización para una mejor distribución del servicio estableciendo reglas de seguridad.

Fuente: (Elaboración propia)

II. Switch Core

El switch core se logró configurar las funcionalidades siguientes:

- Los equipos se nombraron de acuerdo a los establecimientos.
- En caso de la falla de un switch se cuenta con el respaldo de uno adicional.
- Se crearon las vlans correspondientes para el entorno de trabajo.
- Los equipos de red que se encuentren dentro del entorno LAN pueden comunicarse entre ellos.

- A ciertas interfaces se ha configurado el tipo de encapsulación dot1q y en modo troncal.

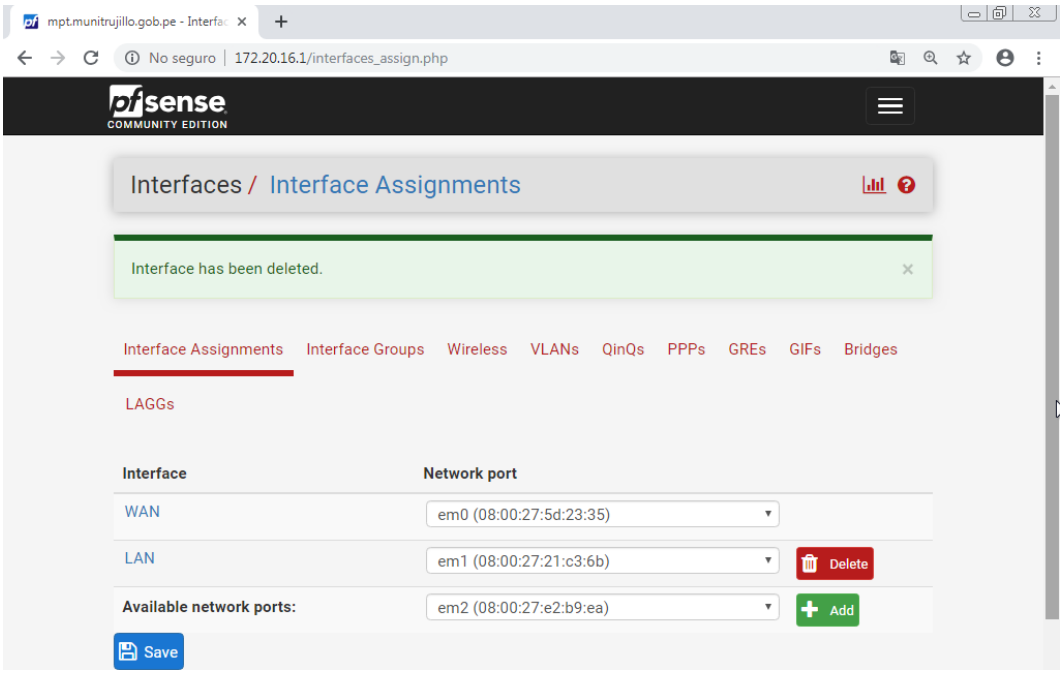
III. Firewall

El firewall se logró configurar las funcionalidades siguientes:

- Se estableció la instalación y configuración de inicio del firewall en Oracle VirtualBox
- Se configura el Nat inside y outside para permitir la comunicación interna además para que tengan salida a internet por una misma IP pública.

Ilustración 35

Configuración NAT en firewall



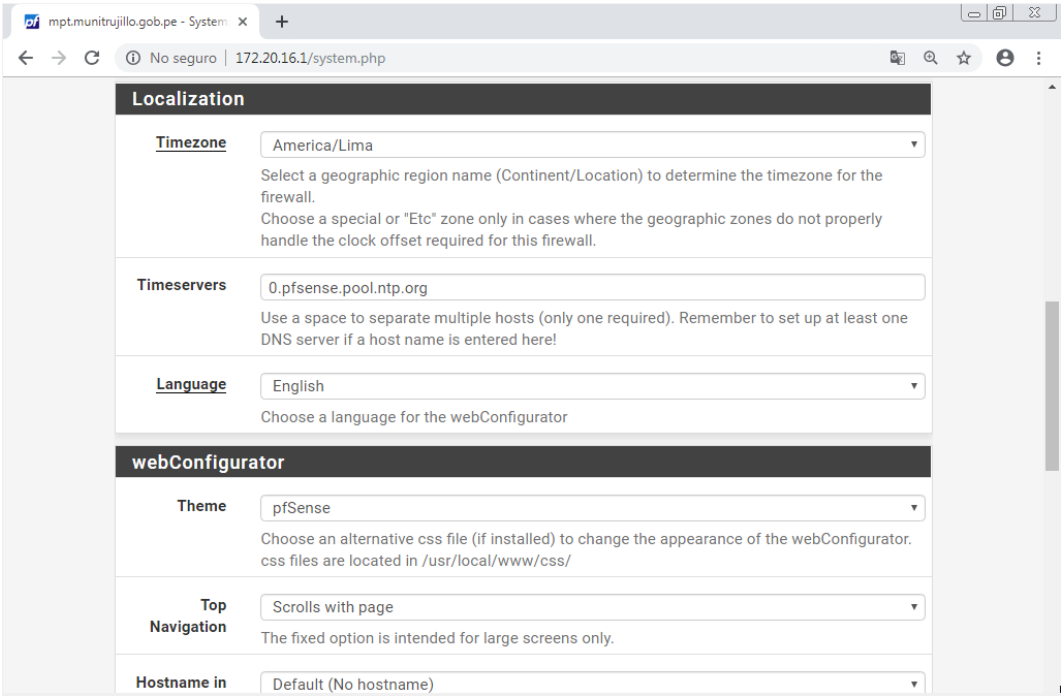
Nota. El grafico muestra como se esta llevando a cabo la configuración de un NAT en el firewall.

Fuente: (Elaboración propia)

- Se configuro el servicio NTP para que los equipos se encuentren sincronizados con el reloj.

Ilustración 36

Configuración NTP



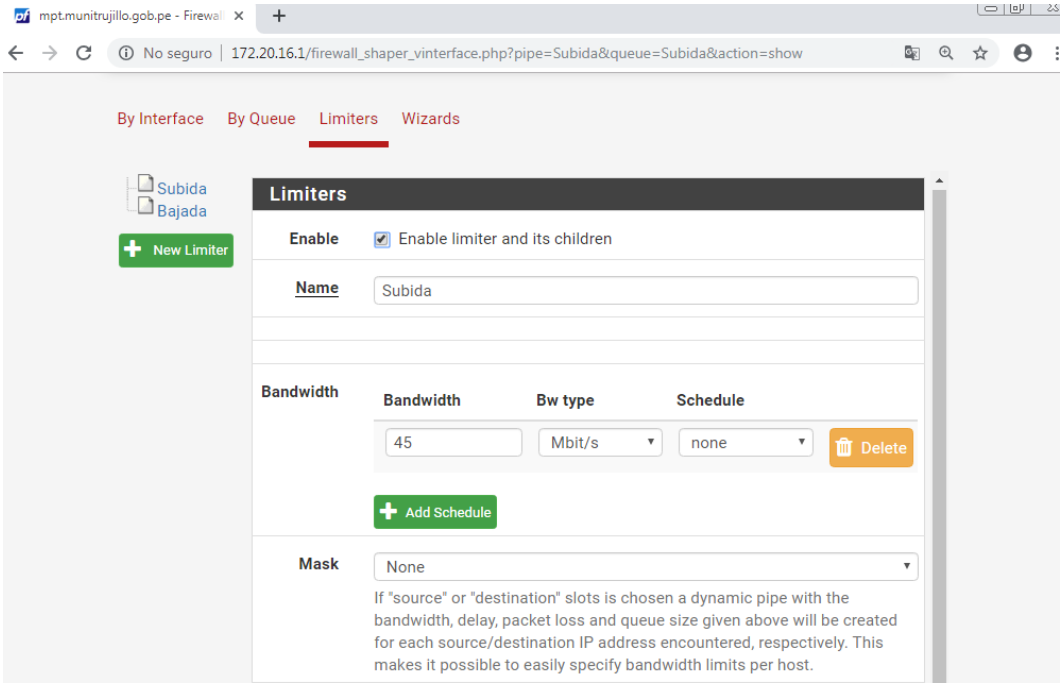
Nota. El grafico muestra cómo se está configurando el servicio de NTP.

Fuente: (Elaboración propia)

- Se configuro el límite de trafico de ancho de banda para los usuarios de acuerdo a las necesidades de sus áreas respectivas y servidores.

Ilustración 37

Configuración WAN



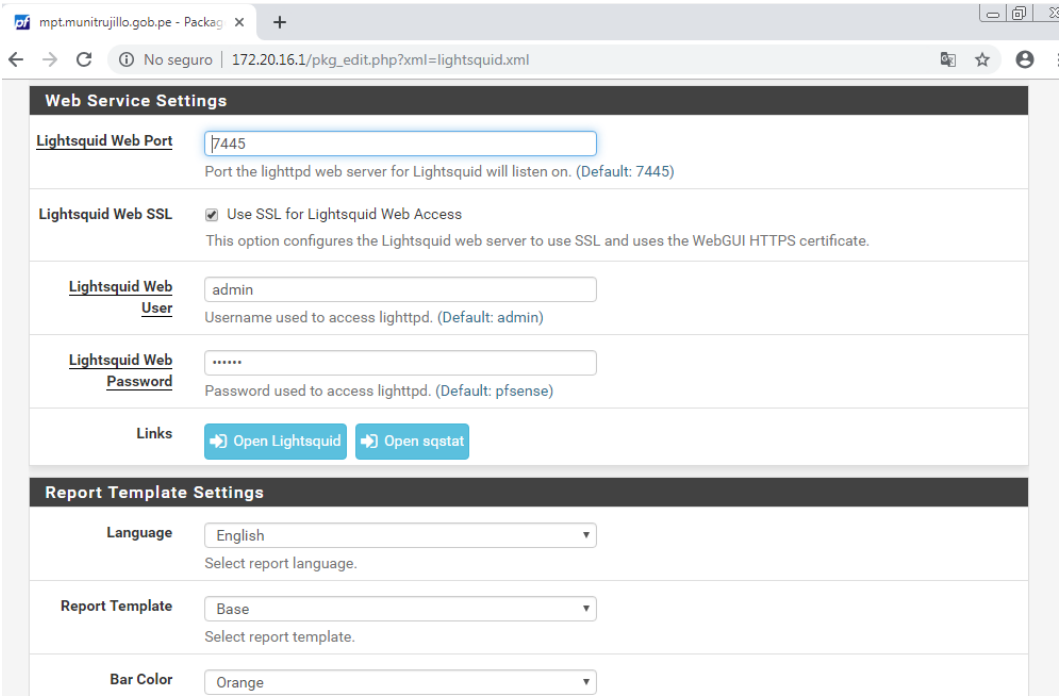
Nota. El grafico muestra cómo se realiza la configuración en la red WAN.

Fuente: (Elaboración propia)

- Se configuro el registro de actividad de navegación de los usuarios y servidores.

Ilustración 38

Configuración de registros



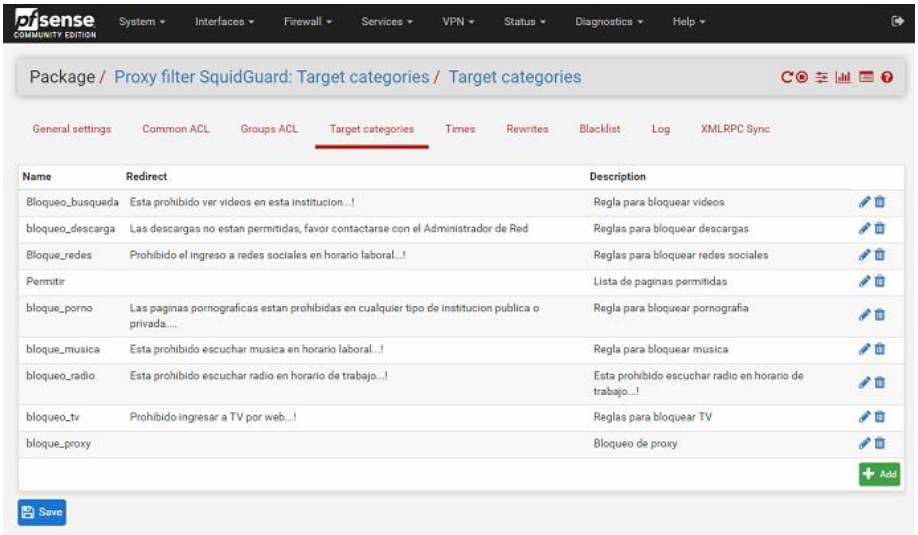
Nota. El grafico muestra cómo se registra la actividad de los usuarios.

Fuente: (Elaboración propia)

- Se configuro restricciones de navegación web para los usuarios

Ilustración 39

Configuración de restricción a usuarios



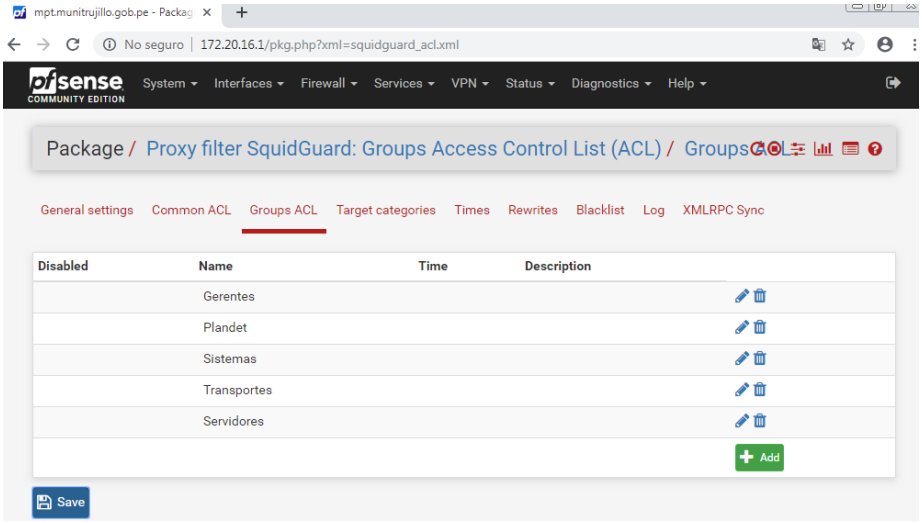
Nota. El grafico muestra cómo se está realizando la restricción de los servicios a los usuarios.

Fuente: (Elaboración propia)

- Se configuro grupo de restricciones de accesos de acuerdo a las necesidades de cada área y servidores.

Ilustración 40

Creación de Grupos



Nota. El grafico muestra cómo se está clasificando los grupos de trabajo.

Fuente: (Elaboración propia)

IV. Servidores

- La página web de la organización se encuentra alojada en un servidor propio con una dirección IP publica diferente.
- Los aplicativos internos de la organización se encuentran alojados en un servidor distinto al servidor web en donde se establecen reglas para que cierto grupo de usuarios puedan acceder a ello
- Se levanta el servicio de GPO para tener un mayor control de los usuarios.
- Se configuro NTP y syslog en los servidores para que tener a los equipos con las fechas actualizadas y logren llevar un registro de cualquier tipo de cambio en los switches.

V. Documentación

El documento debe tener las características técnicas de las fases del diseño de red. Dicha información es sumamente importante para que un administrador de red pueda evidenciar como está distribuida la red tanto lógica como físicamente. La documentación debe está bien elaborada para facilitar las tareas de cambio, mantenimiento o actualización de la topología de la red.

Luego de analizar el diseño lógico en simulación de la red se tomaron en cuenta 3 firewalls para su respectiva comparación las cuales fueron: Endian, IpFire y Pfsense, el cual se realizó un análisis comparativo con la herramienta checklist que ayudo a tomar el mejor firewall para la organización.

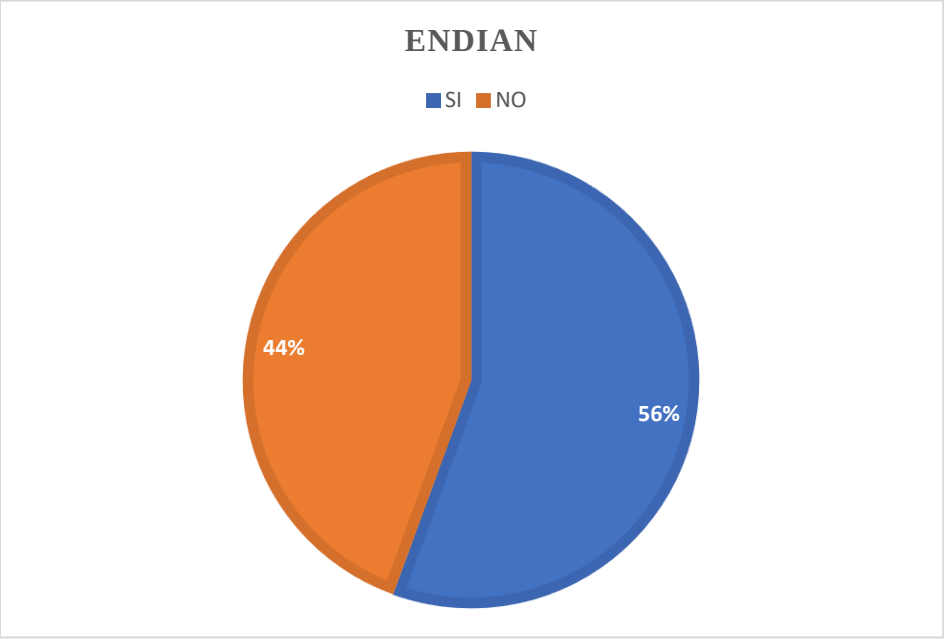
Tabla 9: Resultado del checklist aplicado al firewall Endian

CHECKLIST		
Propósito: Estudio de Firewall Endian		
Proyecto: INFLUENCIA DE LA SOLUCIÓN FIREWALL PARA LA SEGURIDAD PERIMETRAL DE LA RED DE DATOS EN LA MUNICIPALIDAD PROVINCIAL DE TRUJILLO USANDO FREEBSD PFSENSE	**SOFTWARE: Endian**	
Autor		
Nombre: Antonio Isaac Dionicio Guzmán		
Checklist	**SI**	**NO**
¿EL FIREWALL SE PUEDE CONFIGURAR DE MANERA PERSONALIZADA?	X	
¿EL FIREWALL PUEDE INSTALARSE EN UN EQUIPO INDPENDIENTE?	X	
¿EL FIREWALL PUEDE SER INSTALADO COMO UN SERVICIO VIRTUAL?	X	
¿EL FIREWALL NECESITA ALTOS RECURSOS DE HARDWARE?		X
COMPATIBLE CON VIRTUALBOX	X	
ADMINISTRACIÓN WEB	X	
FILTRADO WEB	X	
INTERFAZ GRÁFICA AMIGABLE	X	
ANTISPAM		X
CONTROL DE INTRUSOS		X
ANTIPHISHING		X
ANTIVIRUS		X
CONTROL DE USUARIOS	X	
PERMITE REDUNDANCIA		X
PERMITE REALIZAR BALANCEO DE CARGA	X	
TABAL DE ESTADOS DE CONEXIONES ABIERTAS		X
SERVIDOR GRABADOR DE VIDEO		X
SERVIDOR VPN	X	
SERVIDOR DHCP	X	
SERVIDOR PPPoE		X
SERVIDOR STREAMING		X
SERVIDOR PROXY	X	
SERVIDOR DNS	X	
SERVIDOR PARA CENTRAL VOIP		X
PORTAL CAUTIVO		X
CACHÉ DE NOMBRES DE DOMINIOS	X	
ENRUTAMIENTO ESTÁTICO	X	

De acuerdo a la ilustración 41 nos muestra que el firewall Endian cumple con las reglas de seguridad en un 44% teniendo una aceptación media ya que su incumplimiento de seguridad es elevado a un 56% dando como resultado que no es un sistema seguro.

Ilustración 41

Resultado del checklist aplicado al firewall Endian



Nota. El gráfico muestra el resultado obtenido sobre la aplicación del firewall Endian. Resultados obtenidos en la aplicación Google Forms.

Fuente: (Elaboración propia)

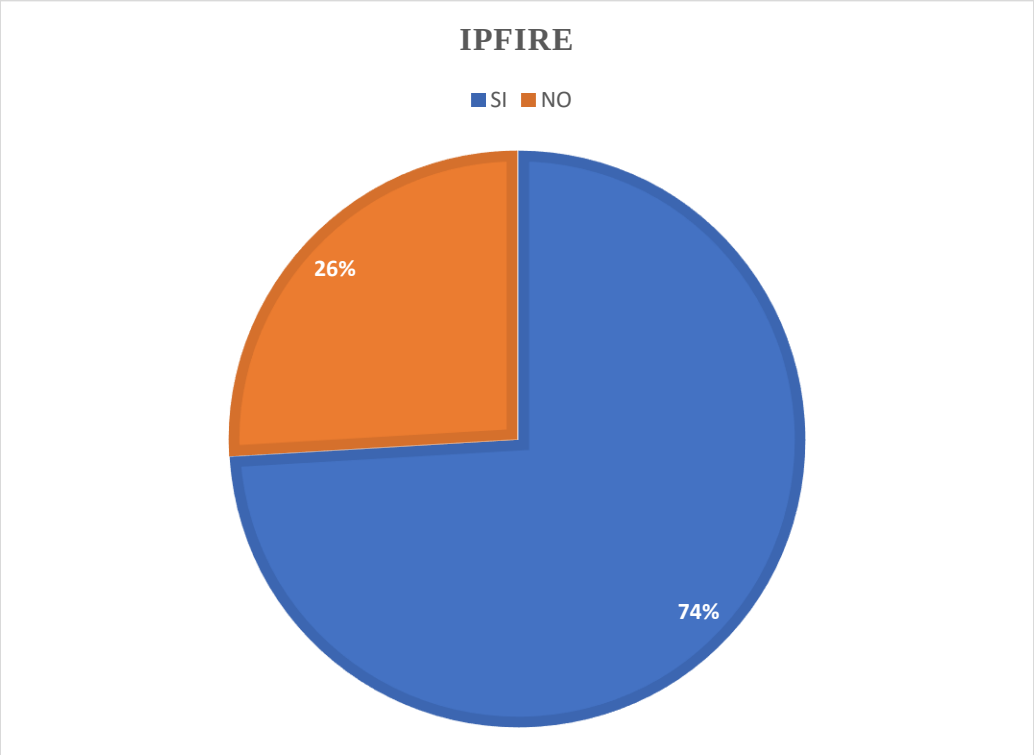
Tabla 10: Resultado del checklist aplicado al firewall IpFire

CHECKLIST		
Proposito: Estudio de Firewall IpFire		
Proyecto: INFLUENCIA DE LA SOLUCIÓN FIREWALL PARA LA SEGURIDAD PERIMETRAL DE LA RED DE DATOS EN LA MUNICIPALIDAD PROVINCIAL DE TRUJILLO USANDO FREEBSD PFSENSE	**SOFTWARE: IpFire**	
Autor		
Nombre: Antonio Isaac Dionicio Guzmán		
Checklist	**SI**	**NO**
¿EL FIREWALL SE PUEDE CONFIGURAR DE MANERA PERSONALIZADA?	X	
¿EL FIREWALL PUEDE INSTALARSE EN UN EQUIPO INDPENDIENTE?	X	
¿EL FIREWALL PUEDE SER INSTALADO COMO UN SERVICIO VIRTUAL?	X	
¿EL FIREWALL NECESITA ALTOS RECURSOS DE HARDWARE?		X
COMPATIBLE CON VIRTUALBOX	X	
ADMINISTRACIÓN WEB	X	
FILTRADO WEB	X	
INTERFAZ GRÁFICA AMIGABLE	X	
ANTISPAM	X	
CONTROL DE INTRUSOS	X	
ANTIPHISHING		X
ANTIVIRUS	X	
CONTROL DE USUARIOS		X
PERMITE REDUNDANCIA		X
PERMITE REALIZAR BALANCEO DE CARGA		X
TABAL DE ESTADOS DE CONEXIONES ABIERTAS	X	
SERVIDOR GRABADOR DE VIDEO	X	
SERVIDOR VPN	X	
SERVIDOR DHCP	X	
SERVIDOR PPPoE	X	
SERVIDOR STREAMING	X	
SERVIDOR PROXY	X	
SERVIDOR DNS	X	
SERVIDOR PARA CENTRAL VOIP	X	
PORTAL CAUTIVO		X
CACHÉ DE NOMBRES DE DOMINIOS	X	
ENRUTAMIENTO ESTÁTICO		X

De acuerdo a la ilustración 42 nos indica que el firewall IpFire cumple un 74% de las características establecidas en cuanto a las necesidades de seguridad de la organización y tan solo con 26% no cumple con ciertos requerimientos, quedando así un poco elevado los niveles de inseguridad.

Ilustración 42

Resultado del checklist aplicado al firewall IpFire



Nota. El gráfico muestra el resultado obtenido sobre la aplicación del firewall IPFire. Resultados obtenidos en la aplicación Google Forms.

Fuente: (Elaboración propia)

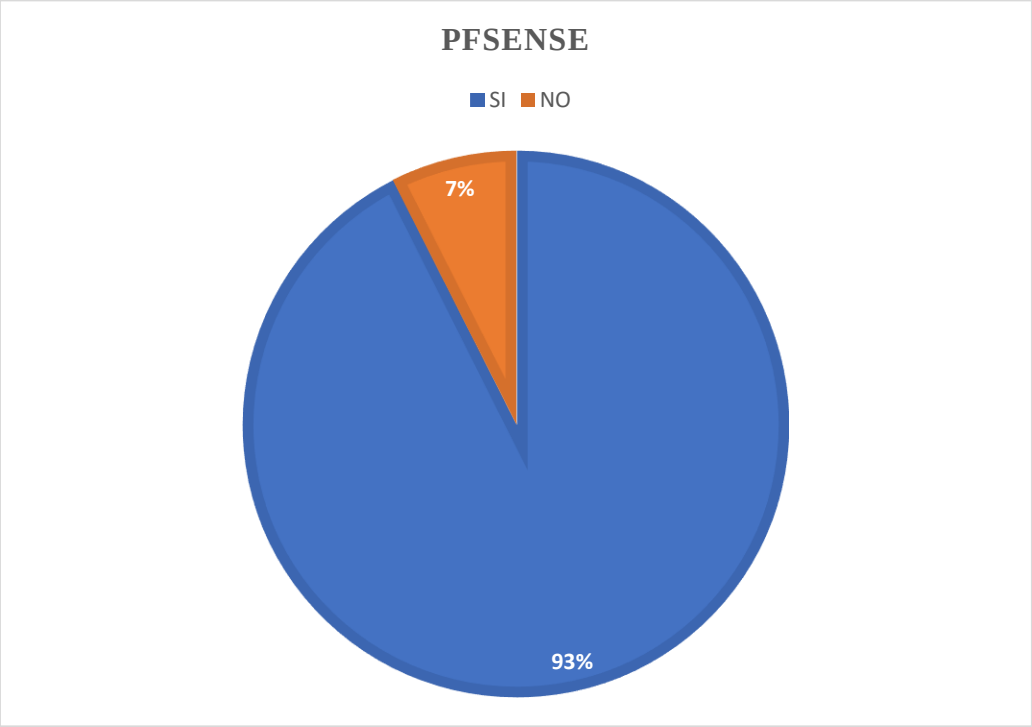
Tabla 11: Resultado del checklist aplicado al firewall PfSense

CHECKLIST		
Proposito: Estudio de Firewall PfSense		
Proyecto: INFLUENCIA DE LA SOLUCIÓN FIREWALL PARA LA SEGURIDAD PERIMETRAL DE LA RED DE DATOS EN LA MUNICIPALIDAD PROVINCIAL DE TRUJILLO USANDO FREEBSD PFSENSE	**SOFTWARE: PfSense**	
Autor		
Nombre: Antonio Isaac Dionicio Guzmán		
Checklist	**SI**	**NO**
¿EL FIREWALL SE PUEDE CONFIGURAR DE MANERA PERSONALIZADA?	X	
¿EL FIREWALL PUEDE INSTALARSE EN UN EQUIPO INDPENDIENTE?	X	
¿EL FIREWALL PUEDE SER INSTALADO COMO UN SERVICIO VIRTUAL?	X	
¿EL FIREWALL NECESITA ALTOS RECURSOS DE HARDWARE?		X
COMPATIBLE CON VIRTUALBOX	X	
ADMINISTRACIÓN WEB	X	
FILTRADO WEB	X	
INTERFAZ GRÁFICA AMIGABLE	X	
ANTISPAM	X	
CONTROL DE INTRUSOS	X	
ANTIPHISHING	X	
ANTIVIRUS	X	
CONTROL DE USUARIOS	X	
PERMITE REDUNDANCIA	X	
PERMITE REALIZAR BALANCEO DE CARGA	X	
TABAL DE ESTADOS DE CONEXIONES ABIERTAS	X	
SERVIDOR GRABADOR DE VIDEO		X
SERVIDOR VPN	X	
SERVIDOR DHCP	X	
SERVIDOR PPPoE	X	
SERVIDOR STREAMING	X	
SERVIDOR PROXY	X	
SERVIDOR DNS	X	
SERVIDOR PARA CENTRAL VOIP	X	
PORTAL CAUTIVO	X	
CACHÉ DE NOMBRES DE DOMINIOS	X	
ENRUTAMIENTO ESTÁTICO	X	

De acuerdo con la ilustración 43 nos indica que el firewall PfSense tiene un nivel de aceptación muy bien elevado ya que el nivel de seguridad esta a un 93% de aceptación mientras que un 7% no cumple ciertas características, quedando asi que el firewall PfSense es adecuado para la organización ya que ofrece un nivel de seguridad más sólido.

Ilustración 43

Resultado del checklist aplicado al firewall PfSense



Nota. El gráfico muestra el resultado obtenido sobre la aplicación del firewall PfSense. Resultados obtenidos en la aplicación Google Forms.

Fuente: (Elaboración propia)

4.1.3. Desarrollo de diseño físico

I. Administración

Para la buena administración documentada y estable de la red, se tiene que identificar cada componente del cableado estructurado, lo cual está compuesto por equipos de comunicaciones, cables, patch panel, racks, jacks y área de equipos.

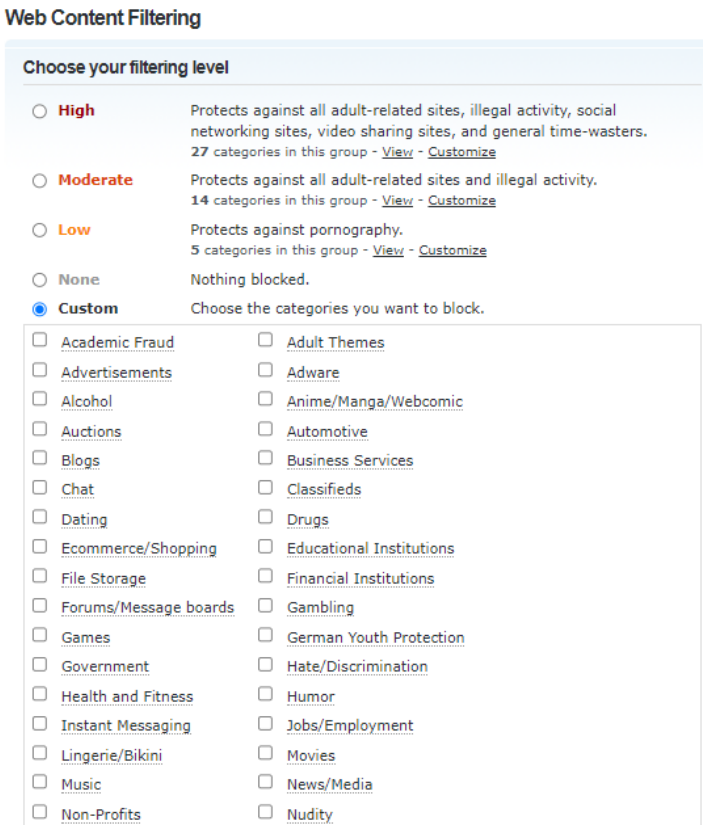
4.2. Identificar y definir las reglas de acceso a los clientes y servidores.

4.2.1. Desarrollo de estrategias de seguridad

De acuerdo a los activos importantes de información que maneja la organización para adecuar la seguridad en la red de datos se encontró que de acuerdo al cuestionario del Anexo 2 y Anexo 3 solo hay información por documentos que establece una agrupación de políticas de seguridad, responsabilidades y cumplimientos técnicos a cada responsable tomando como base la posición de los usuarios en la organización y no es aplicado con políticas en un sistema de seguridad.

Seguridad en los dispositivos informáticos en la red de datos

- Para evitar el acceso no autorizado a software, datos y otros recursos que estén en el servidor se implementara políticas dentro del firewall perimetral que estará asociado al Active Directory.
- Para evitar el acceso a páginas web maliciosas en toda la organización se protegerá con la implementación del firewall perimetral realizando una clasificación de contenidos.

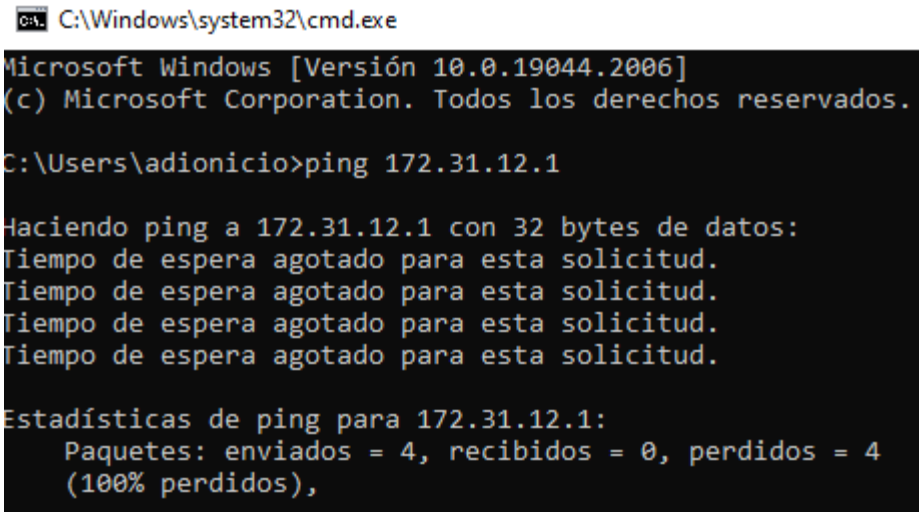


- Los backups de información de los servidores se segmentará en redes distintas a los usuarios.

- Todos los usuarios invitados que acceden por Wi-Fi (172.31.14.1) serán aislados de la red empresarial (172.31.12.1).

```
interface Vlan810
 ip address 172.31.12.1 255.255.254.0
!
interface Vlan830
 ip address 172.31.14.1 255.255.255.0
!
interface Vlan850
 ip address 172.31.15.1 255.255.255.0
!
ip default-gateway 10.10.10.2
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.10.10.2
ip route 172.21.0.0 255.255.0.0 172.21.10.1
ip route 172.23.0.0 255.255.0.0 172.23.10.1
ip ssh version 2
```

Comulación entre red empresarial y wifi



- El monitoreo de la red se centralizará en el firewall perimetral para proteger toda la red en la Municipalidad Provincial de Trujillo.
- Las sedes interconectadas a la Gerencia de Sistemas de Municipalidad Provincial de Trujillo brindan el servicio de internet y demás aplicativos por diferentes VLAN's de acuerdo a la segmentación realizada.

```
interface Vlan10
 ip address 172.22.12.1 255.255.254.0
!
interface Vlan30
 ip address 172.22.14.1 255.255.255.0
!
interface Vlan50
 ip address 172.22.15.1 255.255.255.0
!
interface Vlan60
 ip address 172.22.16.1 255.255.255.0
!
interface Vlan70
 ip address 172.22.17.1 255.255.255.0
!
interface Vlan80
 ip address 172.22.18.1 255.255.254.0
!
interface Vlan90
 ip address 172.22.20.1 255.255.255.0
!
interface Vlan110
 ip address 172.24.12.1 255.255.254.0
!
interface Vlan130
 ip address 172.24.14.1 255.255.255.0
!
interface Vlan150
 ip address 172.24.15.1 255.255.255.0
!
interface Vlan170
 no ip address
!
interface Vlan200
 ip address 172.22.10.1 255.255.255.0
```

II. **Responsabilidad de los usuarios**

Personal	Responsabilidad
Administrador de la red	Personal responsable de la estabilidad de la red, el administrador elabora las configuraciones en el entorno LAN de manera correcta, además del mapeo de software, hardware, funcionalidad y datos, incluso de los impactos inmediatos que pueden suceder en una amenaza y además garantizara las políticas de seguridad de la empresa.
Administrador de la organización	Personal responsable de resguardar la política de seguridad en la red de datos al brindar fondos para armar servicios de seguridad y garantizar el cumplimiento de las políticas, dicho usuario elaborara la perspectiva necesaria para evaluar las consecuencias a largo plazo para la empresa si se presenta una amenaza.
Propietarios de datos y aplicaciones	Personal responsable de acreditar que sus aplicaciones y datos estén correctamente disponibles y protegidos solo a usuarios autorizados.
Usuarios	Personal responsable de brindar información precisa sobre sus datos y aplicaciones.

III. Elementos de seguridad en la red de datos

NAT

El nateo permitirá proteger a los servidores que cuentan con servicios públicos que tienes asignados una IP pública a través de direcciones IPs privadas para que puedan salir a internet y no puedan ser visibles desde el exterior fácilmente, de esta forma se evitara cualquier tipo de ataque mal intencionado de una persona cualquiera que no esté dentro de la red no podrá tener información sobre los servicios internos de la red de la organización.

VLAN

- Configuración de VLANS separadas para voz, datos y video.
- Restringir VLAN a un solo switch.
- Deshabilitación de puertos que no estén siendo utilizados.
- Configuración de los puertos orientados al usuario como no troncales.
- Usar el modo tagged para las VLAN nativas en troncales.
- Desactivar la VLAN 1.

4.2.2. Desarrollo de estrategia de administración de red

Para la administración de red concisa se tiene que tener documentada de la red de datos identificando cada elemento del sistema como es el cableado estructurado, lo cual está conformado por racks, cables, jacks, patch panel, cuartos y equipos de conectividad.

Objetivo II: Aplicar la solución firewall para la seguridad perimetral de la red de datos

4.3. Implementar Solución Firewall

El presente trabajo se llegó a implementar la solución firewall perimetral basado en pfsense utilizando como herramienta un simulador de red como packet tracer utilizando la técnica de sub-divir la red por VLANS para la seguridad perimetral con equipos de red que son los switch y servidores que se mencionan en el presupuesto del proyecto y se muestra en el Anexo 4 el acta instalación y puesta en marcha el proyecto.

4.3.1. Desarrollo de estrategias de seguridad

De acuerdo a los activos importantes de información que maneja la organización para adecuar la seguridad en la red de datos se establece una agrupación de políticas de seguridad, responsabilidades y cumplimientos técnicos a cada responsable tomando como base la posición de los usuarios en la organización.

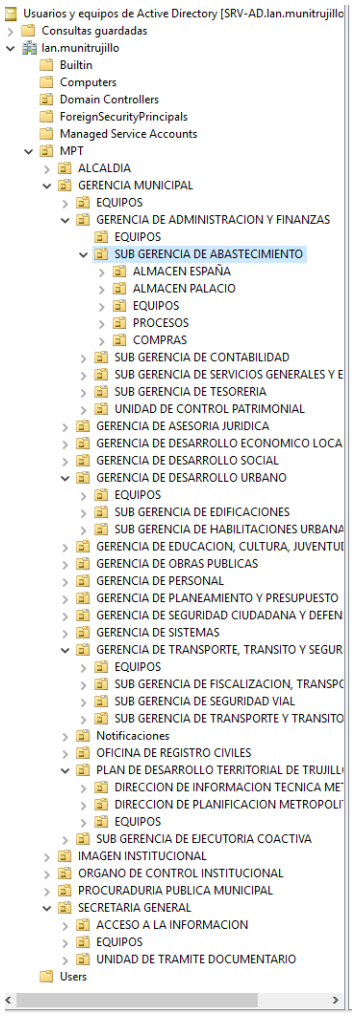
I. Implementación de seguridad

A continuación, se muestra la relación de políticas de seguridad para la organización:

- Para evitar el uso de software malicioso, todos los ordenadores de la institución tendrán un usuario administrador que solo estará autorizado en realizar dichas instalaciones en los equipos informáticos evitando así la propagación de algún tipo de virus.
- Se implementa un servidor de Active Directory para la creación de usuarios y políticas para establecer ciertos permisos.

Ilustración 44

Active Directory



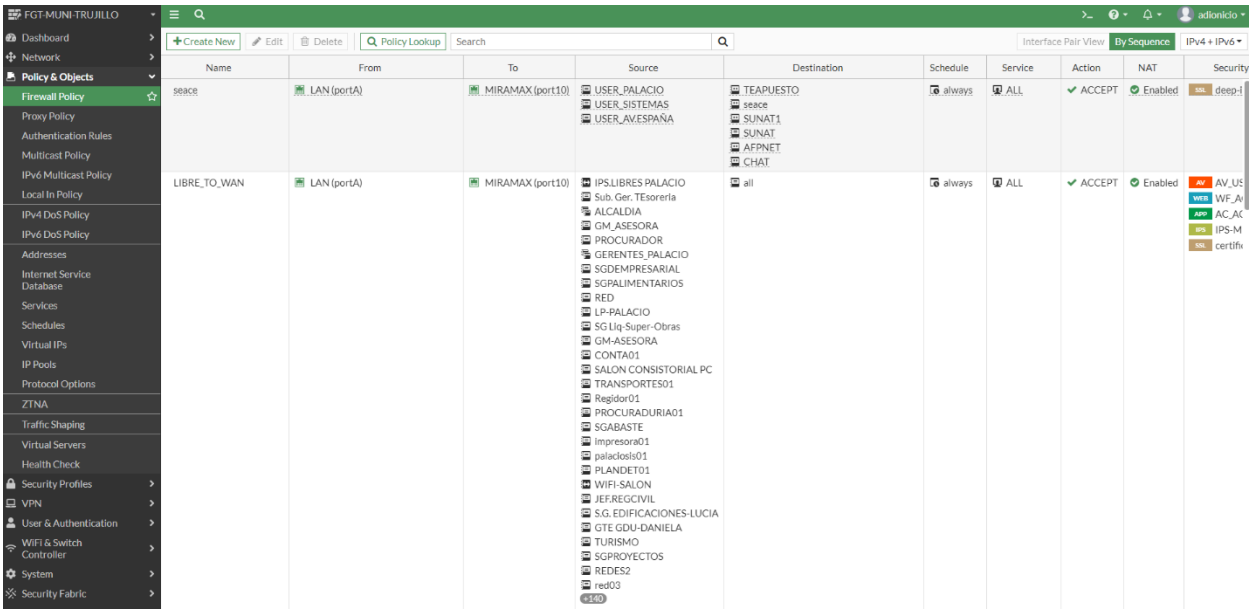
Nota. El grafico muestra cómo está la jerarquía de trabajo dentro del servidor.

Fuente: (Elaboración propia)

Dicho servidor de dominio se interconecto con el firewall de seguridad para realizar diversas políticas de seguridad y brindar un mejor resguardo a todos los usuarios que se encuentran dentro de la red empresarial.

Ilustración 45

Vinculación del Servidor Active Directory con el Firewall



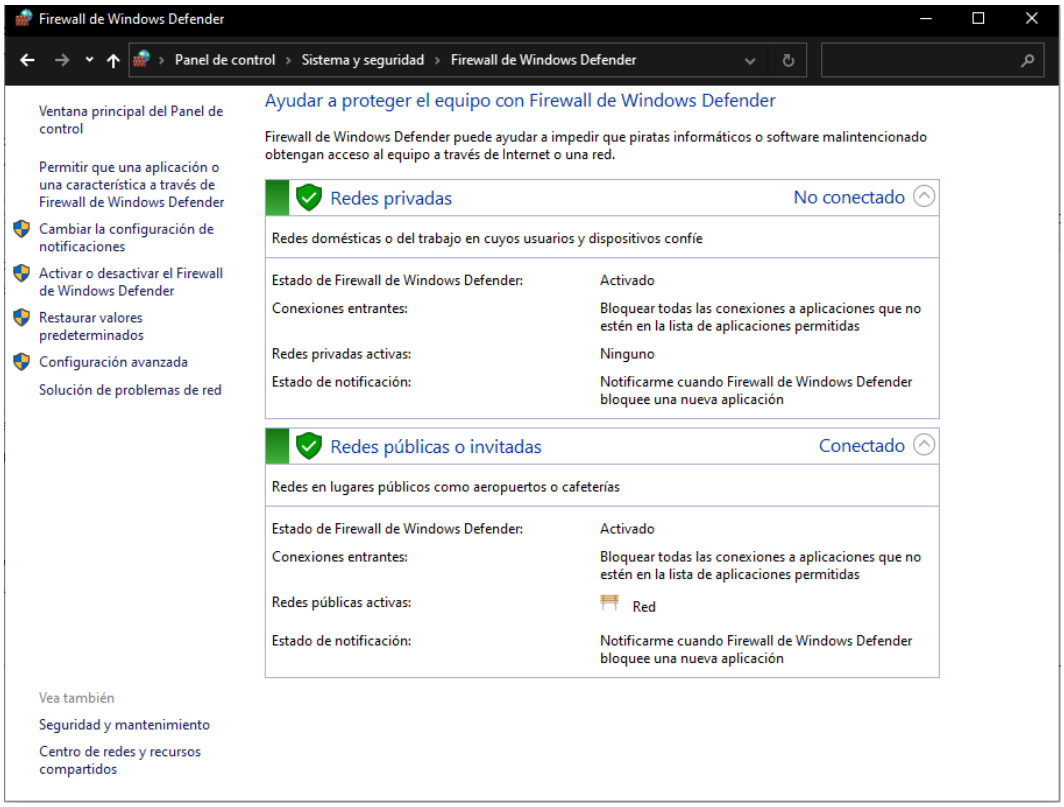
Nota. El grafico muestra como el servidor de Active Directory se enlaza con el firewall

Fuente: (Elaboración propia)

- Se establecieron políticas de seguridad en los ordenadores clientes de los usuarios para tener una protección adicional al firewall perimetral, en donde podemos apreciar que el firewall del sistema operativo de una computadora ahora se encuentra habilitada ya que anteriormente se deshabilitaba para solucionar problemas del momento sin medir los riesgos que podría llevar.

Ilustración 46

Políticas de Seguridad en los Clientes



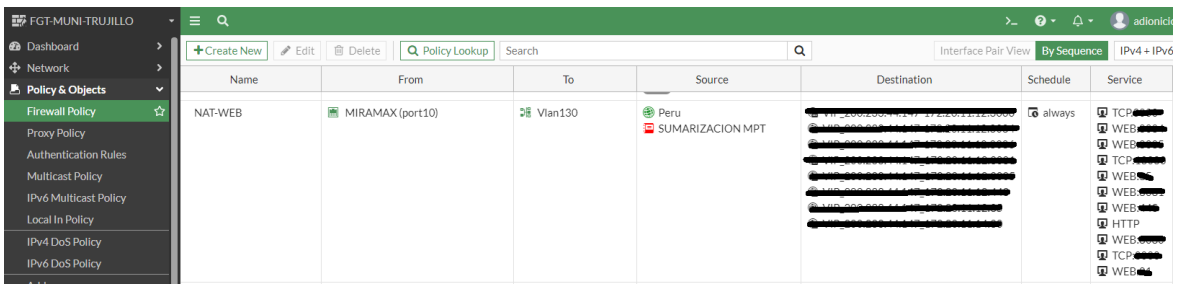
Nota. El grafico muestra cómo se está protegiendo los ordenadores por la parte usuario.

Fuente: (Elaboración propia)

Por parte de la seguridad del firewall de la red empresarial solo se habilitaron puertos que son necesariamente utilizados por los distintos aplicativos y los demás se encuentran deshabilitados para evitar cualquier mal uso de ellos.

Ilustración 47

Habilitación de puertos



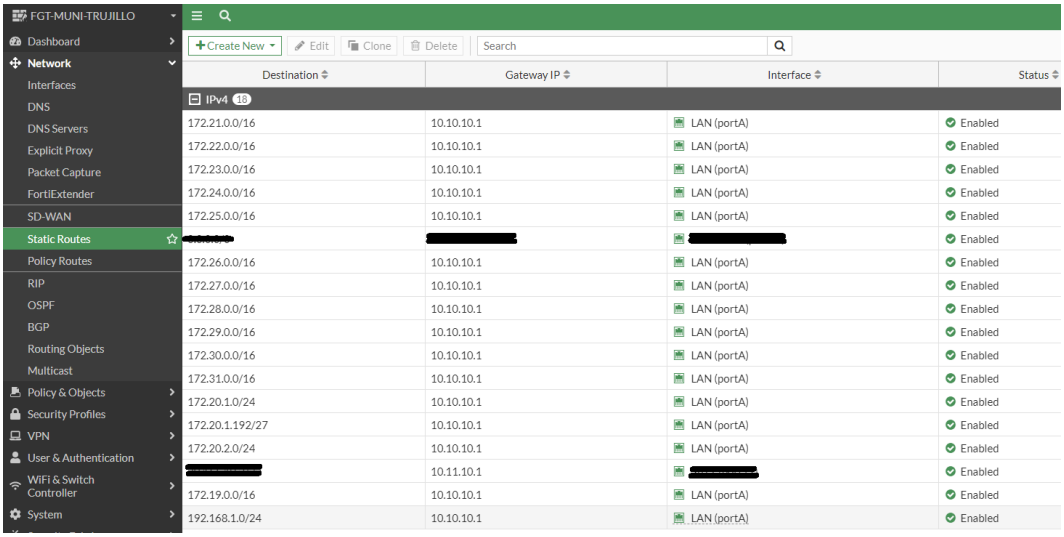
Nota. El grafico muestra cómo se está realizando la habilitación de puertos en la red de la MPT en el firewall.

Fuente: (Elaboración propia)

- Se implemento 12 redes LAN en VLAN'S para la interconexión de sedes con la finalidad de evitar mezclar su comunicación entre ellos como podemos apreciar a continuación:

  Ilustración 48

  Vlans Clientes



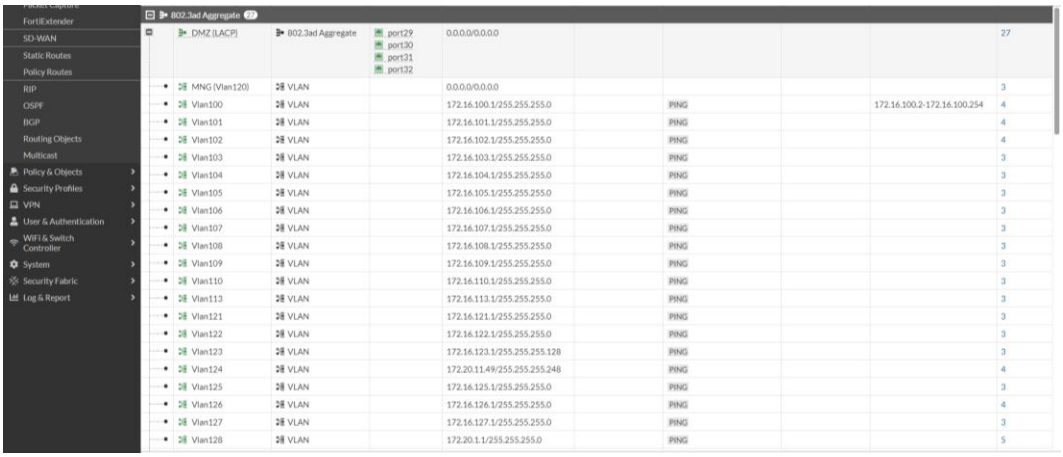
Nota. El grafico muestra cómo se está segmentando la red interna de los clientes en el firewall.

Fuente: (Elaboración propia)

- El nateo de direcciones públicas se realizó una segmentación de red en cada uno de los servidores de la municipalidad dentro del firewall que dan servicio a la red externa como podemos apreciar a continuación:

Ilustración 49

Nateo de IP Publico



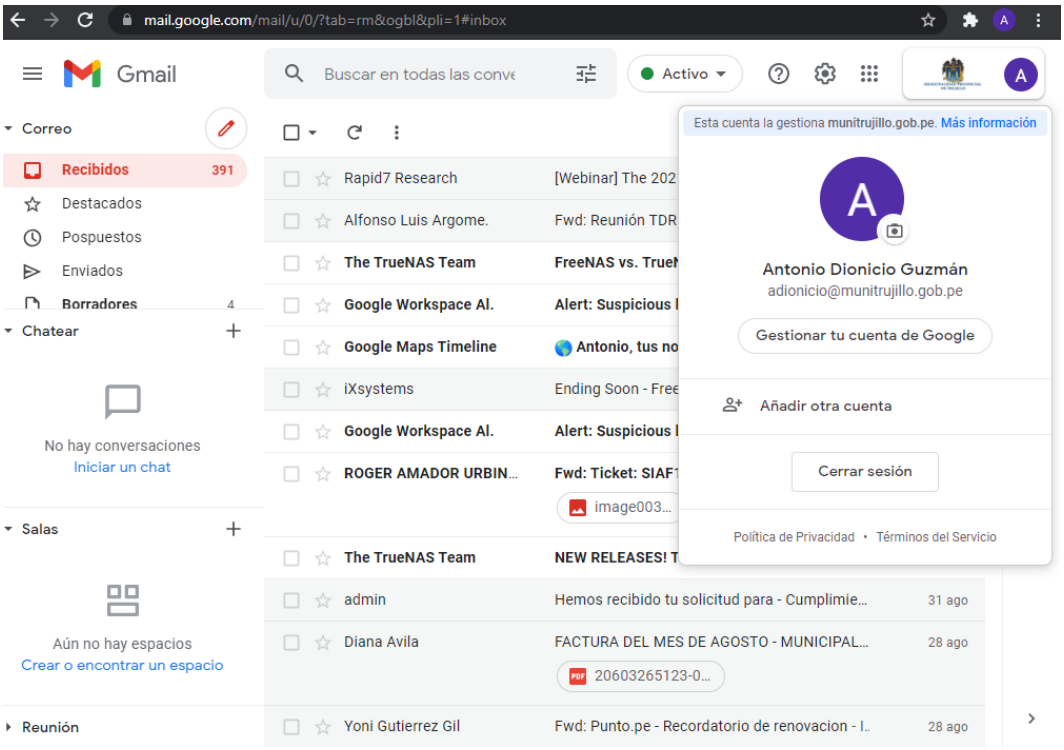
Nota. El grafico muestra cómo se esta realizando el nateo de las direcciones IPs públicas en el firewall.

Fuente: (Elaboración propia)

- Para la reducción de spam la entidad prefirió optar en contratar el servicio de correo electrónico de GMAIL.

Ilustración 50

Correo Institucional



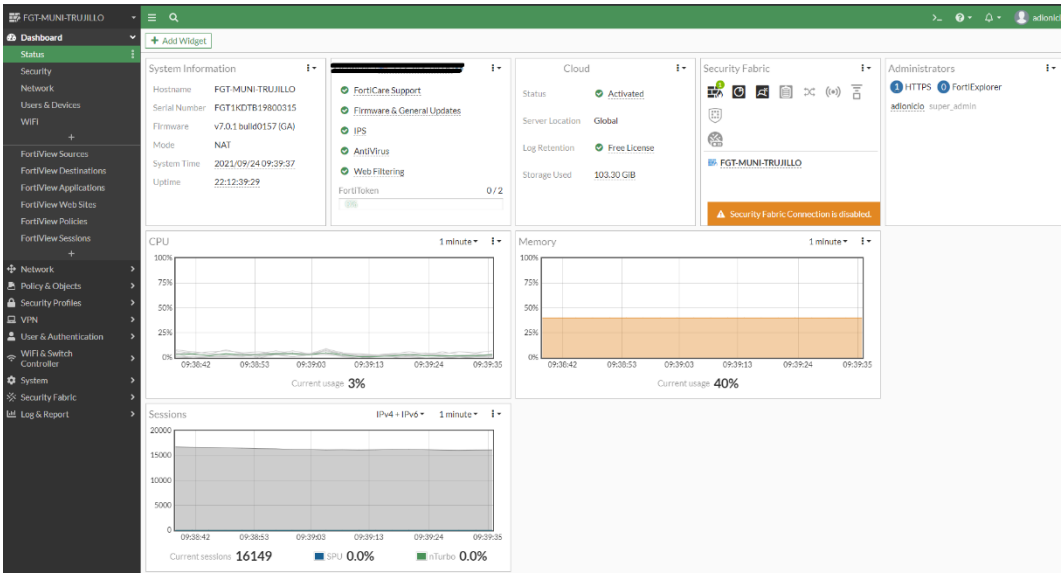
Nota. El grafico muestra el servicio de correo que usa la organización.

Fuente: (Google, 2021)

- La implementación del firewall beneficio a la entidad debido que es un software de libre uso.
- Como se puede apreciar ahora todo se encentra administrable en una sola plataforma donde se puede observar todo tipo de movimiento mal intencionado y también verificar al instante ante cualquier caída que pueda tener algún sistema.

Ilustración 51

Monitoreo de red



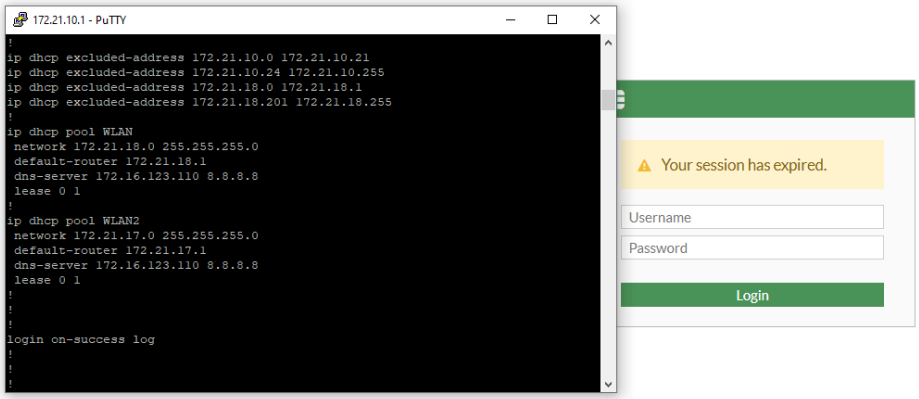
Nota. El grafico muestra cómo se puede monitorear gráficamente la red empresarial.

Fuente: (Elaboración propia)

- Se segmento la red inalámbrica de invitados dentro del firewall para que dicha red no tenga ni un tipo de acceso hacia la red interna de los usuarios y servidores.

Ilustración 52

Creación de red Wi-Fi invitados



Nota. El grafico muestra cómo se lleva a cabo la segmentación de la red de invitados.

Fuente: (Elaboración propia)

- Se tiene en cuenta los siguientes requerimientos técnicos que se pretende realizar los servicios de red:

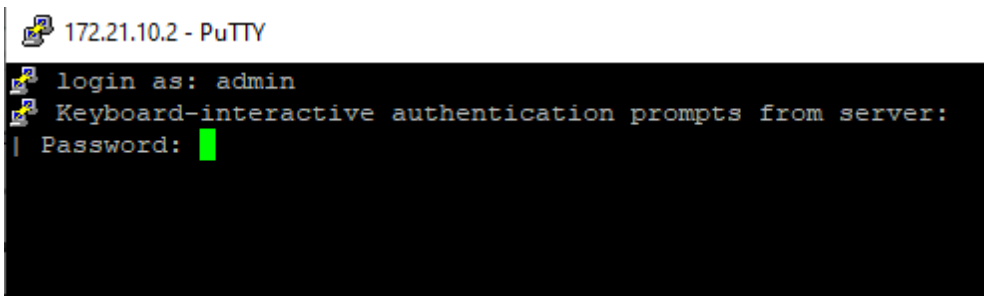
  Seguridad: Contar con una seguridad lógica y física de la red.

  En la seguridad lógica cada acceso a cualquier dispositivo de comunicación (Firewall, Switch, Servidores y computador del administrador) cuenta con un logeo de usuario y clave que debe cumplir con cierto nivel de complejidad.

  Acceso a un switch y router:

Ilustración 53

Autenticación



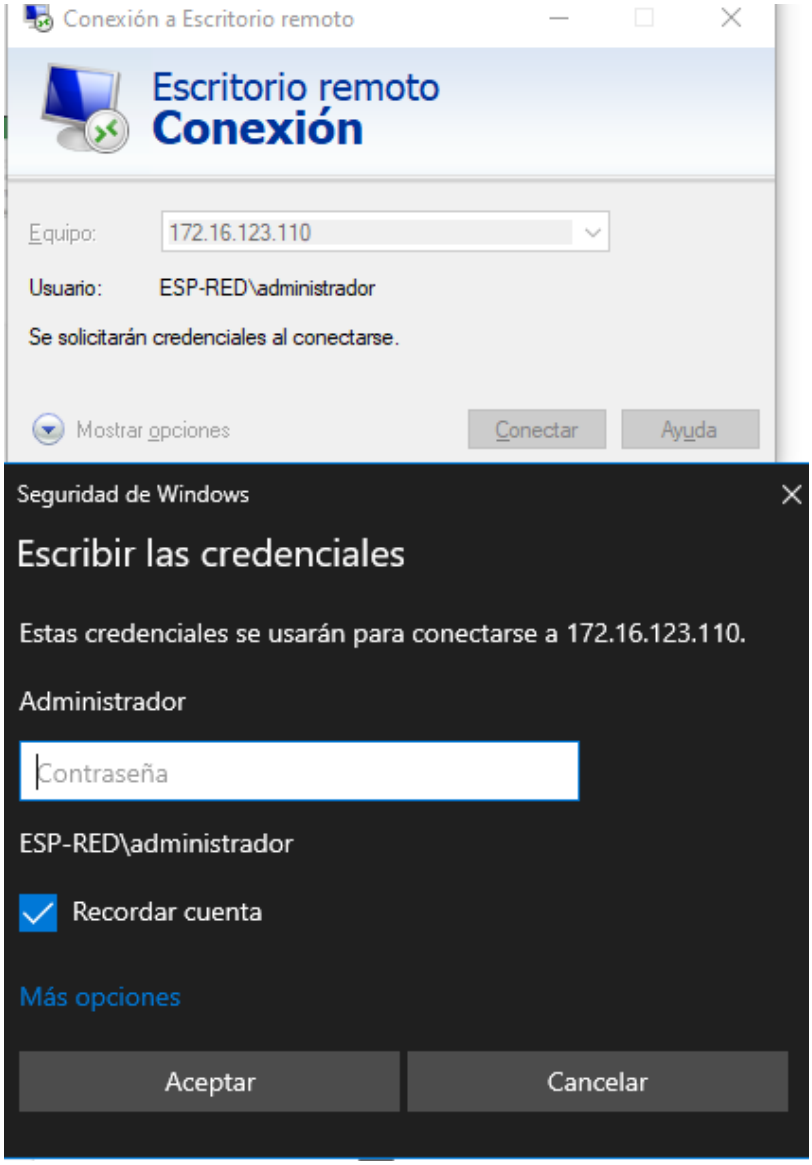
Nota. El grafico muestra cómo se está realizando la conexión a los equipos de comunicación con una autenticación de credenciales.

Fuente: (Elaboración propia)

Acceso a un servidor:

Ilustración 54

Autenticación de servidores



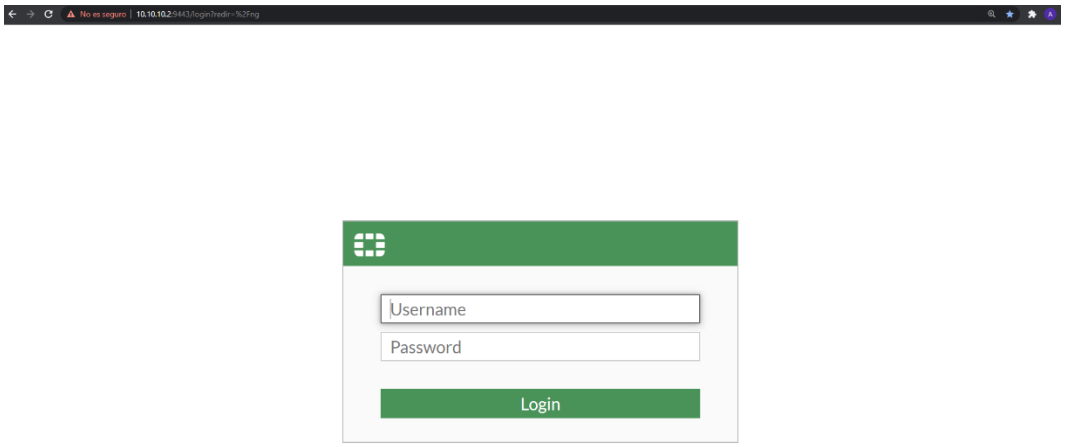
Nota. El grafico muestra cómo se debe ingresar a los servidores con una autenticación de credenciales.

Fuente: (Elaboración propia)

Acceso al firewall:

Ilustración 55

Firewall PfSense



Nota. El grafico muestra cómo se debe ingresar al firewall con una autenticación de credenciales.

Fuente: (Elaboración propia)

- Seguridad física en un data center se debe contar con un acceso limitado de personas que sea registrador por un vigilante, luego que el acceso a los servidores sea con una puerta blindada y sea abierto con una tarjeta de autorización y por último dentro del data center los gabinetes de comunicación deben contar con llave para que solo el personal autorizado pueda acceder a los equipos físicamente.

Acceso al data center:

Ilustración 56

Seguridad Física

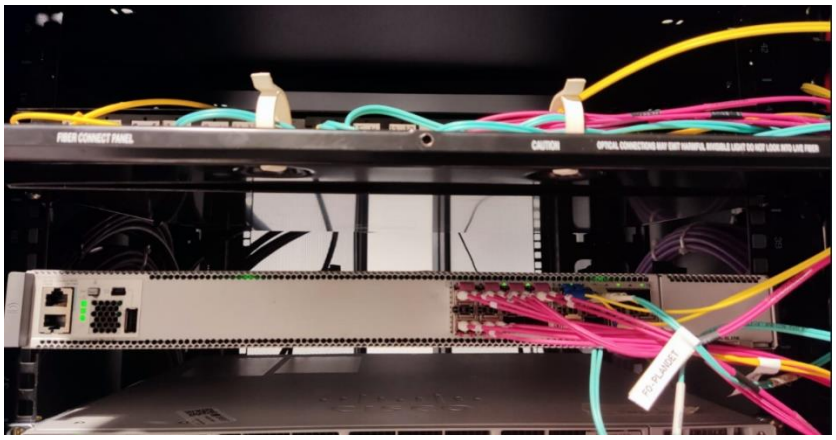
Nota. El grafico muestra cómo se debe proteger los equipos de comunicación en un data center.

Fuente: (Elaboración propia)

- Se implemento la redundancia de datos en la red para evitar cualquier caída para los usuarios finales como para los servidores que brindan servicios a los usuarios internos y ciudadanos en general.

Ilustración 57

Redundancia de servicio



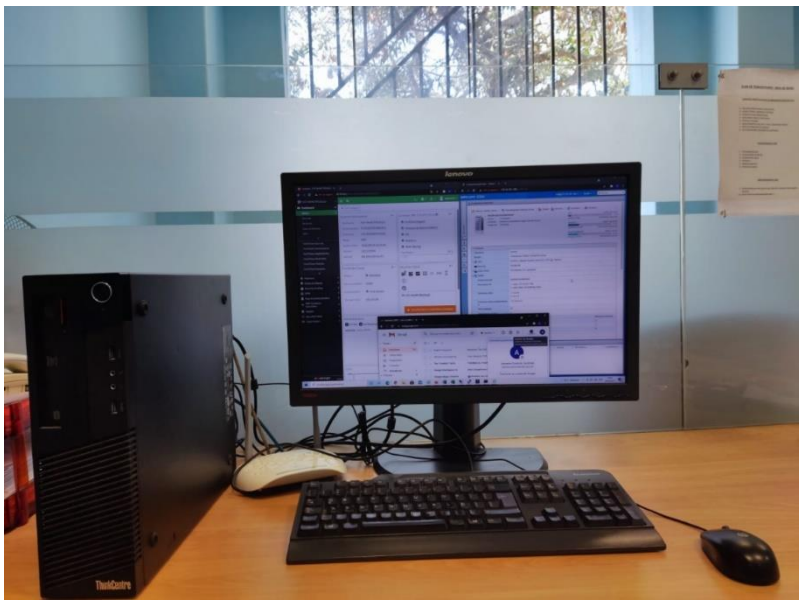
Nota. El grafico muestra cómo se está realizando la redundancia del servicio con el firewall para mantener operativo las aplicaciones.

Fuente: (Elaboración propia)

- Se automatizo con la ayuda del firewall poder administrar todos los servicios de la red en el ordenador del administrador para que lleve un mejor control de todo el equipamiento de la red ante cualquier incidente o amenaza que pueda suceder.

Ilustración 58

Administración de la red con el Firewall Pfsense



Nota. El grafico muestra cómo ahora se está administrando todo desde la pc del Administrador de Red.

Fuente: (Elaboración propia)

II. Informe Técnico

Informe Técnico	Detalle
Autenticación e Identificación	Permitirá asegurar que el ingreso a la red solo sean personas autorizadas.
Control de acceso	Asegura que los recursos de la red estén siendo usadas de manera autorizadas.
Confidencialidad de los datos	Asegura que los datos no sean visibles por personas no autorizadas.
Integridad de los datos	De igual forma de la confidencialidad, en esta parte se refiere a que la modificación de los datos no sea alterada.
Monitoreo y Acceso	Permitirá monitorear la red.

4.3.2. Desarrollo de diseño lógico

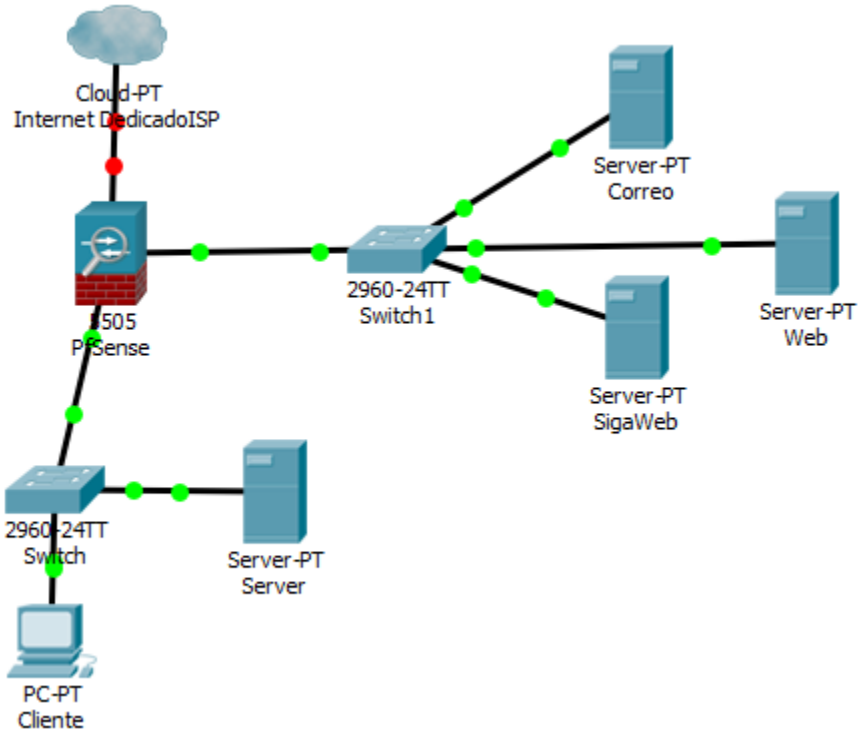
I. Diseño de topología de red

De acuerdo a la metodología Top Down, el diseño de red tiene que estar establecido por tres capas las cuales son: acceso, distribución y Core. Sin embargo, debido al tamaño de la empresa se puede contraer dos capas. Quedando solo las siguientes capas para el diseño:

- Capa distribución y Core: En esta capa encontramos a los equipos que brindaran performance y velocidad a la red. Necesariamente se aplicarán switchs de capa 3 que establecerán políticas de distribución para gestionar.
- Capa de acceso: En esta capa encontramos a los equipos finales, firewalls y switchs administrables. Como podemos apreciar en la siguiente imagen, se propone dividir la red en las dos capas propuestas, a diferencia del modelo actual que tiene la red.

Ilustración 59

Diseño de topología de red



Nota. Se propone implementar VLANs para cada sucursal que esta distancia de la gerencia de sistemas para segmentar y controlar el acceso de los usuarios. Esta segmentación para la sucursal de palacio municipal, plandet, transportes y anexo Av. España.

Fuente: (Elaboración propia)

II. Diseño de direccionamiento

Para la Municipalidad Provincial de Trujillo se establece un modelo basado en VLSM dentro del firewall, lo cual permitirá que la red de la organización tenga la capacidad de manejar diferentes subredes dentro del rango de direcciones IPs privadas establecidas por el administrador de red, dicho modelo de direcciones IPs tienen que ser planeadas, significativas y jerárquicas.

Las direcciones IPs se van a establecer en los siguientes tipos:

- Clase B será segmentada de acuerdo al id de red 172.20.0.0/16 para el entorno de trabajo que serán para los usuarios finales y se distribuye de la siguiente manera:

	VLAN NAME	IP DE VLAN
PALACIO	DATOS	172.21.12.1/23
	VOZ	172.21.14.1/24
	VIDEO	172.21.15.1/24
ANEXO ESPAÑA	DATOS	172.22.12.1/23
	VOZ	172.22.14.1/24
	VIDEO	172.22.15.1/24
OBRAS	DATOS	172.23.12.1/23
	VOZ	172.23.14.1/24
	VIDEO	172.23.15.1/24
SISTEMAS	DATOS	172.24.12.1/23
	VOZ	172.24.14.1/24
	VIDEO	172.24.15.1/24
TRANSORTES	DATOS	172.25.12.1/254
	VOZ	172.25.14.1/24
	VIDEO	172.25.15.1/24
COEP	DATOS	172.26.12.1/24
	VOZ	172.26.14.1/24
	VIDEO	172.26.15.1/24
SALUD	DATOS	172.27.12.1/24
	VOZ	172.27.14.1/24
	VIDEO	172.27.15.1/24
DESARROLLO SOCIAL	DATOS	172.28.12.1/24
	VOZ	172.28.14.1/24
	VIDEO	172.28.15.1/24
SERVICIOS GENERALES	DATOS	172.29.12.1/24
	VOZ	172.29.14.1/24
	VIDEO	172.29.15.1/24
DEFENSA CIVIL	DATOS	172.30.12.1/24
	VOZ	172.30.14.1/24
	VIDEO	172.30.15.1/24
PLANDET	DATOS	172.31.12.1/24
	VOZ	172.31.14.1/24
	VIDEO	172.31.15.1/24
JUVENTUD	DATOS	172.19.12.1/24
	VOZ	172.19.14.1/24

- Clase B DMZ para servidores será segmentada por el id de red 172.16.0.0/16, por políticas de seguridad de la entidad solo menciono el direccionamiento de cada VLAN que se segmentan por 23 VLAN'S sin mencionar a que servicio pertenece.

ITEM	IP
1	172.16.100.1/24
2	172.16.101.1/24
3	172.16.102.1/24
4	172.16.103.1/24
5	172.16.104.1/24
6	172.16.105.1/24
7	172.16.106.1/24
8	172.16.107.1/24
9	172.16.108.1/24
10	172.16.109.1/24
11	172.16.110.1/24
12	ADMINISTRACION
13	172.16.121.1/24
14	172.16.122.1/24
15	172.16.123.1/25
16	172.20.11.49/29
17	172.16.125.1/24
18	172.16.126.1/24
19	172.16.127.1/24
20	172.20.1.1/24
21	172.20.74.1/24
22	172.20.11.9/29
23	172.16.131.1/24

Tomado en cuenta para la red de clase B se calculó crear las 12 subredes a utilizar para los usuarios finales de cada sede. A continuación, se listará las VLANs creadas con su descripción de accesos:

- VLAN Palacio Municipal: Tiene acceso al sistema siaf, sigamef y siganet
- VLAN Anexo España: Tiene acceso a internet, al sistema sigamef y simi.
- VLAN Obras: Tiene acceso a internet y al sistema sigamef.

- VLAN Sistemas: Tiene acceso a todos los sistemas.
- VLAN Transportes: Tiene acceso a internet, al sistema sigamef y taxi
- VLAN COEP: Tiene acceso a internet
- VLAN Salud: Tiene acceso a internet
- VLAN Desarrollo Social: Tiene acceso a internet
- VLAN Servicios Generales: Tiene acceso a internet
- VLAN Defensa Civil: Tiene acceso a internet
- VLAN Plandet: Tiene acceso al sistema sigamef y catastro.
- VLAN Juventud: Tiene acceso a internet.

III. Selección de protocolos

Los protocolos seleccionados se establecen en los requerimientos de la organización y en su diseño que pretende la empresa para la futura implementación del proyecto.

- IMAP
- POP
- UDP
- TCP
- SSL
- IEEE 802.1Q
- VTP
- HTTP/S

Objetivo III: Medir la influencia alcanzado mediante la aplicación de una solución firewall para la seguridad perimetral de la red de datos.

4.4. Firewall en funcionamiento

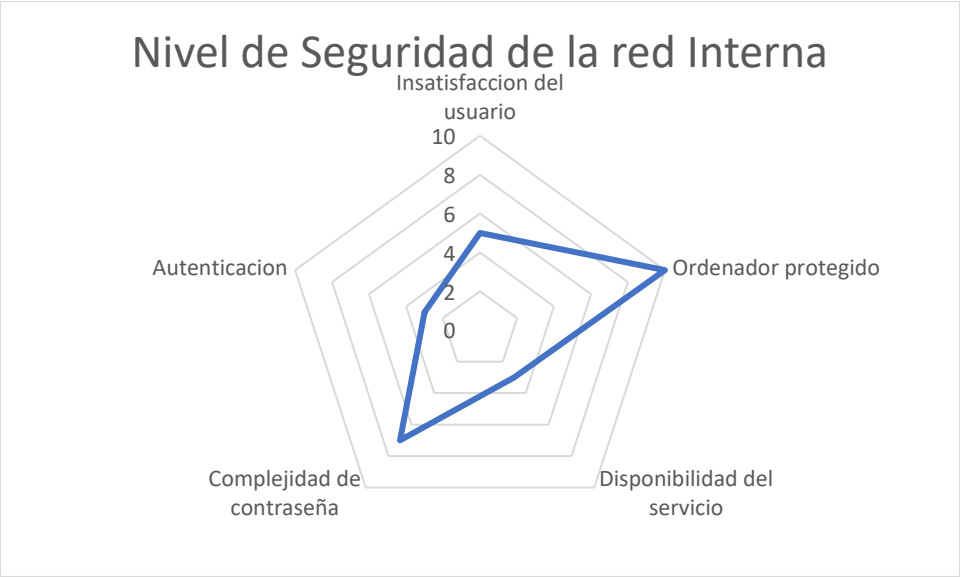
4.4.1. Nivel de seguridad de la red interna

Se evaluó la implantación del rendimiento de firewall para la seguridad perimetral basado en pfsense dentro de la red interna de datos de la Municipalidad Provincial de Trujillo. Para la elaboración de este objetivo, se aplicó el instrumento de recolección de datos (Encuesta).

En cuanto a lo que corresponde respecto a los niveles de confianza en la seguridad perimetral de la red de datos interna podemos observar que la protección de la información tiene un nivel de confianza de un 94% en los servidores, en cuanto a la disponibilidad de servicio para los servidores es de un 97%, luego el administrador de red siente que ahora los servidores están correctamente protegidos dando una calificación del 90%, respecto a los niveles de complejidad de las contraseñas nos da un resultado que un 80% de usuarios está siguiendo lo recomendado, con respecto a la seguridad física luego de lo recomendado el responsable de redes nos indica que se encuentra protegido a un 98%, en cuanto a la autenticación en el firewall el resultado es 95% de protección y por último en cuanto las conexiones externas el nivel de confianza es de un 94%, todo estos resultados son luego de la implementación del firewall perimetral.

Ilustración 60

Nivel de Seguridad de la red Interna



Nota. El grafico muestra cómo a mejorado el servicio de seguridad de la red interna después de utilizar el Firewall Perimetral PfSense.

Fuente: (Elaboración propia)

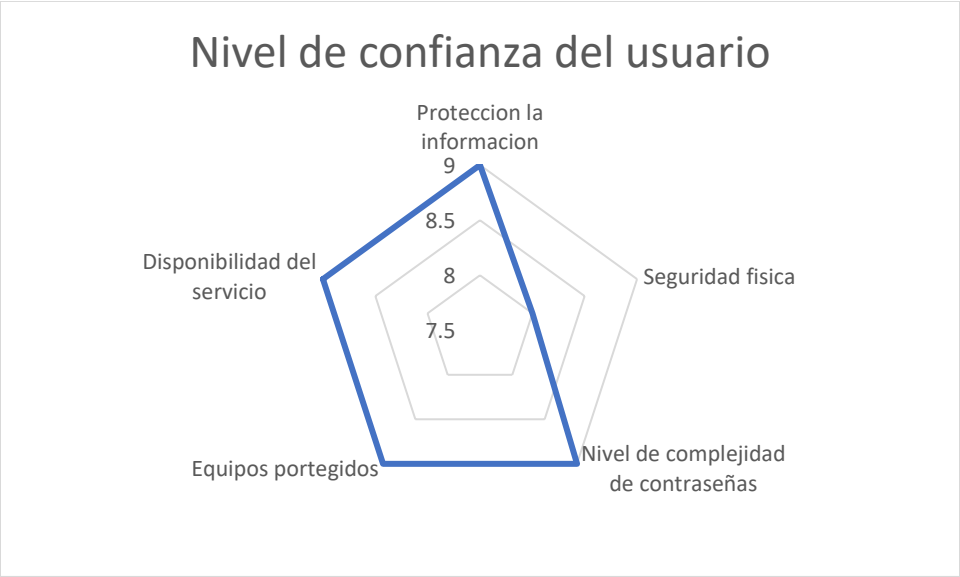
4.4.2. Nivel de confianza del usuario

Se evaluó el nivel de confianza del usuario final respecto a la implementación de la solución firewall perimetral basado en pfsense en la Municipalidad Provincial de Trujillo. Para la elaboración de este objetivo, se aplicó el instrumento de recolección de datos (Encuesta).

En cuanto a lo que corresponde al nivel de confianza del usuario luego de la implementación de la solución firewall perimetral basado en pfsense podemos observar que el usuario se siente seguro con la información que guarda en su ordenador de la municipalidad calificando con un nivel de confianza de un 98%, luego en la disponibilidad del servicio en la red califica satisfactoriamente con un 97% y por ultimo los usuarios ahora sienten que su computador en la red de la municipalidad se encuentra verdaderamente protegido con un 98% de confianza.

Ilustración 61

Nivel de confianza del usuario



Nota. El grafico muestra cómo los usuarios se encuentran satisfechos al ver que la seguridad en la red interna a mejorado dándoles más confianza en su rutina de trabajo.

Fuente: (Elaboración propia)

CAPITULO V:

Discusión

Para la contratación de la hipótesis se ha considerado lo siguiente:

Formulación del problema

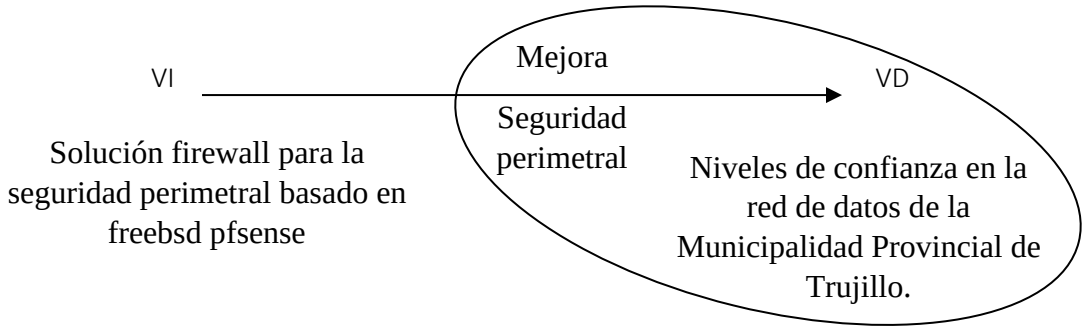
¿Cómo la solución de un firewall con seguridad perimetral permitirá proteger la red de datos de la Municipalidad Provincial de Trujillo?

Hipótesis

La solución de un firewall para la seguridad perimetral basado en freebsd pfsense permitirá definir niveles de confianza en la red de datos de la Municipalidad Provincial de Trujillo.

Luego se definen las variables que intervienen en la veracidad o falsedad de la hipótesis:

- Variable independiente (VI): Solución firewall para la seguridad perimetral basado en freebsd pfsense
- Variable dependiente (VD): Niveles de confianza en la red de datos de la Municipalidad Provincial de Trujillo.



5.1. Diseño Pre experimental pre-prueba y post-prueba

PRE-PRUEBA (O1): Medición para la previa de X a G

POST-PRUEBA (O2): Corresponde a la nueva medición de X a G

Se definió usar el Diseño Pre-experimental Pre-Prueba y Post-Prueba, debido a que la hipótesis se adapta al diseño. Este diseño se experimenta con un solo grupo de sujetos el cual es medido a través de una prueba de vulnerabilidad antes y después de presentar el estímulo (SP). Este diseño se presenta de la siguiente manera:

G O1 X O2

Donde:

X: Seguridad perimetral (SP)

O: Medición a sujetos (Ataques)

G: Grupo de sujetos (Aplicaciones)

El espacio muestral que se tomó para la medición de los indicadores de la hipótesis, correspondió al total de aplicativos que funcionan a través de la red, siendo estos 5: PORTAL WEB, SISTRAM, SIAF, SIGA y SIT a estos cinco aplicativos se le aplicó un cuestionario, antes de interactuar con el SP **(O1)** y después de interactuar con el mismo **(O2)**. Al concluir la investigación se establecen las diferencias entre O1 y O2 para determinar si hay o no incremento en los resultados obtenidos.

5.2. Cálculo de los indicadores de la hipótesis

Ilustración 62

Cálculo de los indicadores de la hipótesis

	KPI: Ataques para analizar el nivel de seguridad (cantidad)		KPI: Ataques a nivel de seguridad de la red interna		KPI: Nivel de confianza del usuario	
APLICACIÓN	PRE-PRUEBA	POST-PRUEBA	PRE-PRUEBA	POST-PRUEBA	PRE-PRUEBA	POST-PRUEBA
1	110	10	95	5	2	9
2	95	5	110	10	1	8
3	85	5	96	3	3	9
4	96	4	98	7	1	9
5	98	6	85	3	2	9

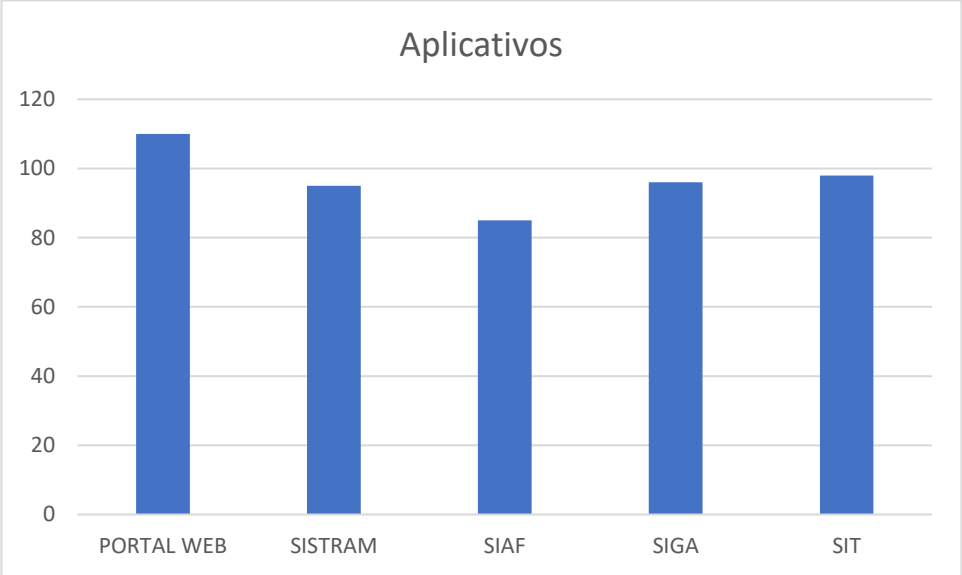
Nota. El gráfico muestra una tabla comparativa de como disminuyo las vulnerabilidades luego de empezar a utilizar un firewall de seguridad perimetral.

A. Indicador: Ataques para analizar el nivel de seguridad.

Se puso a prueba los ataques hacia los servicios de red que se requieren proteger para ello se utilizó el sistema operativo Kali Linux para la medición de la prueba y se tomó en cuenta la muestra con la finalidad de burlar la seguridad perimetral antes de poner en marcha el firewall pfsense para saber luego que tan efectivo es su nivel de seguridad, de la muestra utilizamos 112 ataques de accesos prohibidos para cada servicio de acuerdo a ello confirmamos que el SISTRAM se efectuó con éxito 95 ataques prohibidos, quedando 17 intentos sin éxito a continuación se muestra un gráfico de registros de accesos prohibidos de cada servicio de red, demostrando así la pésima calidad de protección al SISTRAM antes de aplicar el firewall pfsense.

Ilustración 63

Resultado de Pre-Prueba.



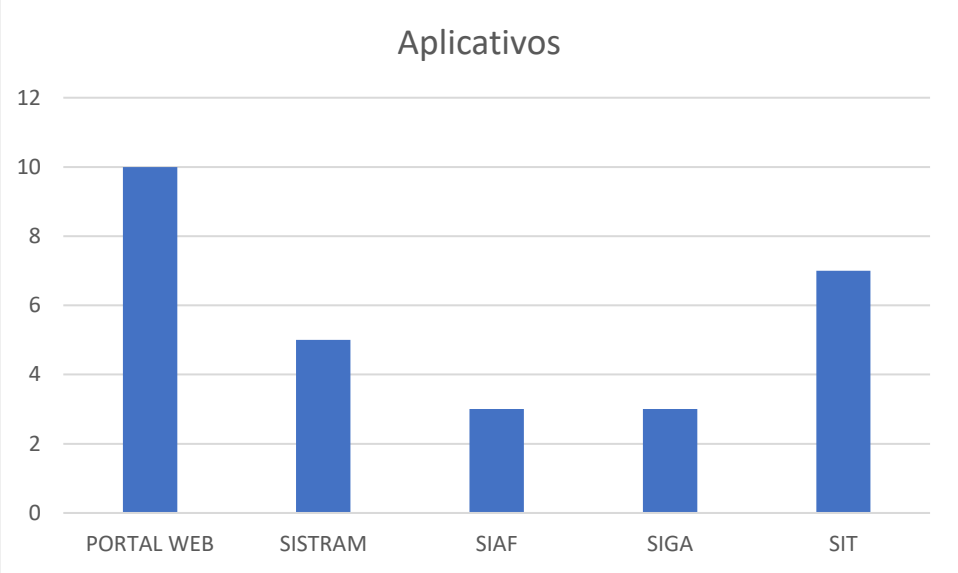
Nota. El gráfico muestra el resultado obtenido sobre los ataques realizados a los distintos aplicativos sin un sistema de seguridad firewall. Resultados obtenidos en la aplicación Kali Linux.

Fuente: (Elaboración propia)

Se puso a prueba los ataques hacia los servicios de red que se requieren proteger utilizando el sistema operativo Kali Linux para la medición de la prueba y para ello se tomó en cuenta la muestra con la finalidad de burlar la seguridad perimetral al poner en marcha el firewall pfsense para saber luego que tan efectivo es su nivel de seguridad, de la muestra utilizamos 112 ataques de accesos prohibidos para cada servicio de acuerdo a ello confirmamos que el SISTRAM se efectuó con éxito 5 ataques prohibidos, quedando 107 intentos sin éxito a continuación se muestra un gráfico de registros de accesos prohibidos de cada servicio de red, demostrando así la calidad de protección al SISTRAM al aplicar el firewall pfsense.

Ilustración 64

Resultado de Post-Prueba

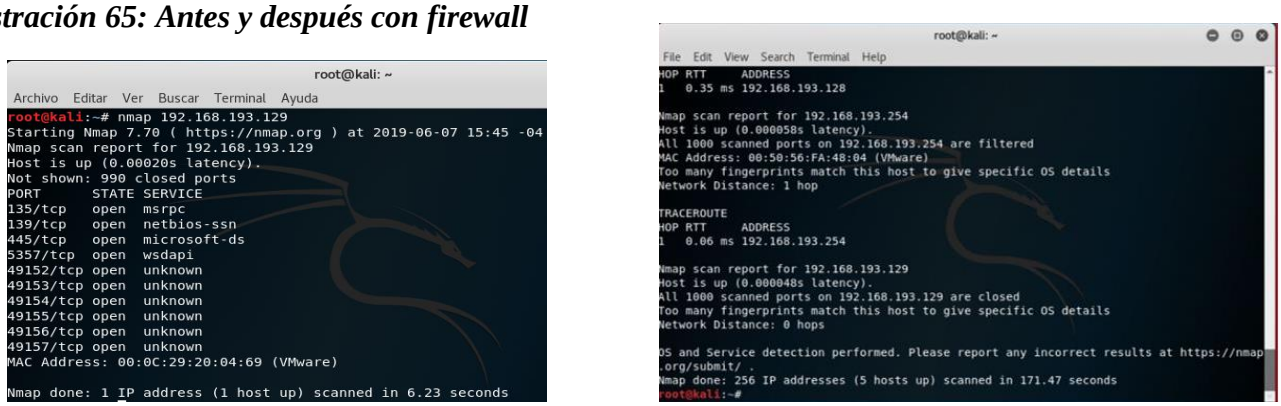


Nota. El gráfico muestra el resultado obtenido sobre los ataques realizados a los distintos aplicativos con un sistema de seguridad firewall. Resultados obtenidos en la aplicación Kali Linux.

Fuente: (Elaboración propia)

Al llevar acabo el diagnóstico de la seguridad perimetral del firewall hacia los aplicativos que se brindan en red de la Municipalidad Provincial de Trujillo se obtuvieron resultados del antes y después de la implantación del firewall con seguridad perimetral, con la ayuda del sistema operativo Kali Linux se logró obtener el promedio de los ataques no deseados exitosos antes que se ponga en marcha dicho sistema y el resultado fue de 98.67 con desviación estándar de 84.67 ingresos, luego de poner en marcha el firewall el promedio fue de 6 con una desviación estándar de 2 ingresos no deseados, podemos apreciar que hay una diferencia de 92.67 de ataques no deseados exitosos dando así el promedio a favor del firewall de seguridad perimetral, podemos apreciar que la cantidad de ingresos mínimos y máximos sin firewall fue de 85 a 110 respectivamente, mientras los ingresos con firewall fue de 4 a 8 respectivamente.

Ilustración 65: Antes y después con firewall



Fuente: (Elaboración Propia)

Tabla 12: Comparación Pre-Prueba y Post-Prueba

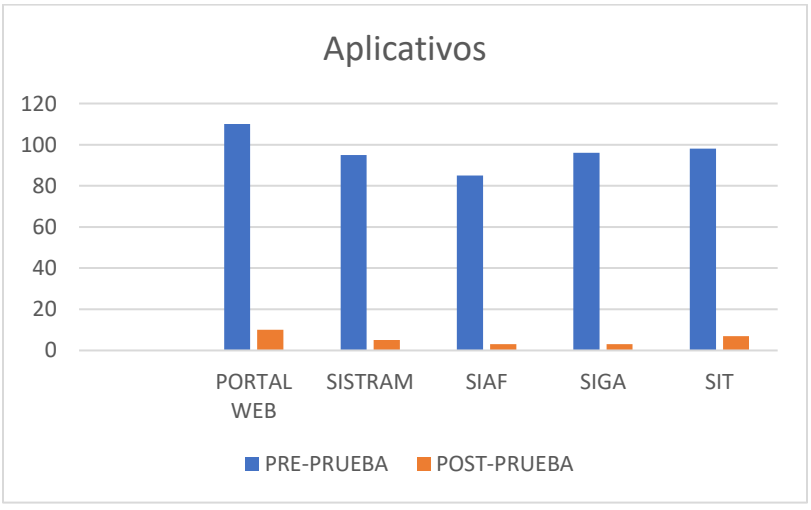


Tabla 13: Resultados de Pre-Prueba y Post-Prueba para indicador

KPI: Ataques para analizar el nivel de seguridad	PRE-PRUEBA	POST-PRUEBA
PORTAL WEB	110	10
SISTRAM	95	5
SIAF	85	5
SIGA	96	4
SIT	98	6
PROMEDIO	96.80	6

Hi: El Servidor firewall para la seguridad perimetral basado en freebsd pfsense **disminuye la cantidad de ataques no deseados determinando** niveles de confianza en la red de datos de la Municipalidad Provincial de Trujillo.

Solución:

a. Planteamiento de la Hipótesis

μ1 = Media de cantidad de vulnerabilidad para determinar niveles de confianza en la red en la Pre-Prueba.
μ2 = Media de cantidad de vulnerabilidad para determinar niveles de confianza en la red en la Post-Prueba.

a.1. Análisis estadístico para la prueba presencial de la hipótesis

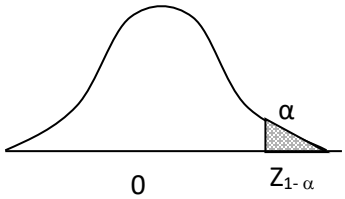
Cálculo de la diferencia de dos medias:

Tabla 14: Cálculo de la diferencia de dos medias

DESCRIPCIÓN	MEDIAS	VARIANZAS
Fórmula	$\mu_i = \frac{\sum X_i}{N}$	$\sigma^2 = \frac{\sum (X_i - \mu_i)^2}{N}$
Cálculo N=5	μ_1= 96.80 μ_2= 6	$\sigma^2{}_1$ = 72.84 $\sigma^2{}_2$ = 2

Cálculo de la Prueba de Hipótesis:

Tabla 15: Cálculo de la Prueba de la Hipótesis

TIPO DE HIPÓTESIS	ESTADÍSTICA DE PRUEBA	REGIONES DE ACEPTACIÓN Y RECHAZO DE Ho	VALOR CRÍTICO
Hipótesis Nula Ho : $\mu_1 - \mu_2 = 0$ Nivel de signif α	$z_0 = \frac{\overline{X_1} - \overline{X_2} - (\mu_1 - \mu_2)}{\sqrt{\sigma^2{}_1 / n + \sigma^2{}_2 / n}}$		α = 0.05 $Z_{1-\alpha}$ = 0.95
Hipótesis Alterna $H_1 : \mu_1 > \mu_2$	**Zo = 84.31**	**Rechazar Ho si, Zo > $Z_{1-\alpha}$**	**84.31>0.95**

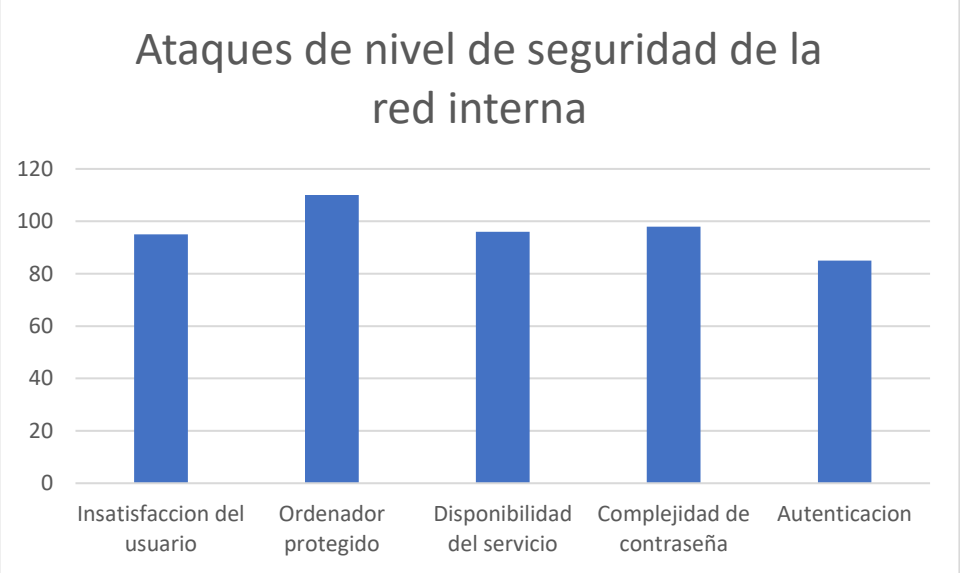
CONCLUSIÓN: La solución firewall para la seguridad perimetral basado en freebsd pfsense **disminuye la cantidad de ataques no deseados determinando** una mejor seguridad perimetral en la red de datos. Se logró reducir de 96.80 ataques no deseados a 6 ataques no deseados logrando una diferencia de 90.80 ataques no deseados logrando determinar niveles de confianza.

B. Indicador: Nivel de seguridad de la red interna.

Se puso a prueba los ataques hacia los servicios de la red interna que se requieren proteger con el sistema operativo Kali Linux, para ello se tomó en cuenta la muestra con la finalidad de burlar la seguridad perimetral antes de poner en marcha el firewall pfsense para saber luego que tan efectivo es su nivel de seguridad, de la muestra utilizamos 112 ataques de accesos prohibidos para cada servicio de acuerdo a ello confirmamos que la falta de confianza del usuario es de 95 mientras su nivel de confianza es de 17 a continuación se muestra un gráfico de registros de accesos prohibidos de cada servicio de red, demostrando así la pésima calidad del nivel de seguridad de la red interna antes de aplicar el firewall pfsense.

Ilustración 66

Resultado de Pre-Prueba.



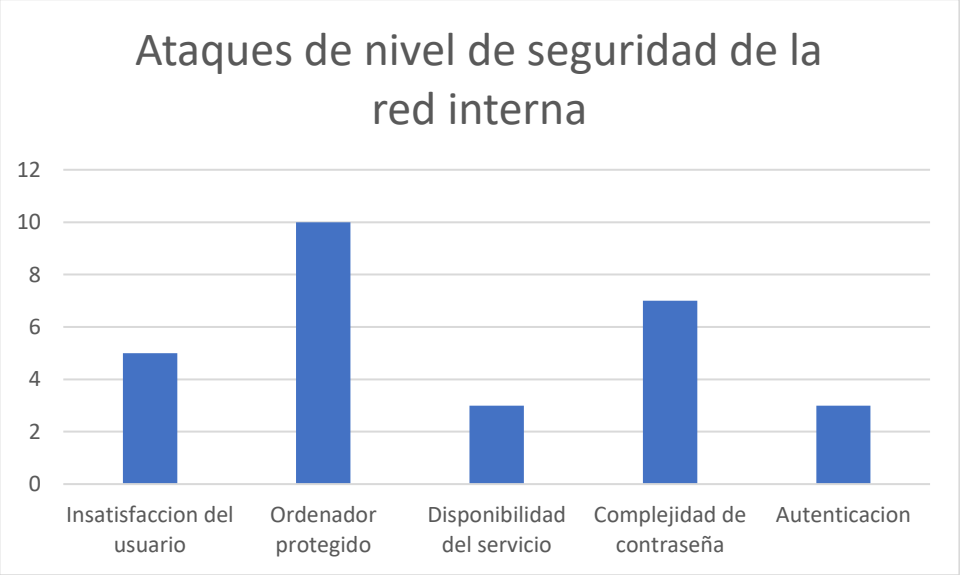
Nota. El gráfico muestra el resultado obtenido sobre los ataques realizados a la red interna de la Municipalidad Provincial de Trujillo sin un sistema de seguridad firewall. Resultados obtenidos en la aplicación Kali Linux.

Fuente: (Elaboración propia)

Se puso a prueba los ataques hacia los servicios de la red interna que se requieren proteger con el sistema operativo Kali Linux, para ello se tomó en cuenta la muestra con la finalidad de burlar la seguridad perimetral al poner en marcha el firewall pfsense para saber luego que tan efectivo es su nivel de seguridad, de la muestra utilizamos 112 ataques de accesos prohibidos para cada servicio de acuerdo a ello confirmamos que la falta de confianza del usuario alcanzo un 5, mientras que el nivel de confianza fue de 107, a continuación se muestra un gráfico de registros de accesos prohibidos de cada servicio de la red interna, demostrando así la calidad de protección al aplicar el firewall pfsense.

Ilustración 67

Resultado de Post-Prueba



Nota. El gráfico muestra el resultado obtenido sobre los ataques realizados a la red interna de la Municipalidad Provincial de Trujillo con un sistema de seguridad firewall. Resultados obtenidos en la aplicación Kali Linux.

Fuente: (Elaboración propia)

Al llevar acabo el diagnóstico de la seguridad perimetral del firewall hacia los aplicativos que se brindan en red de la Municipalidad Provincial de Trujillo con el sistema operativo Kali Linux se obtuvieron resultados del antes y después de la implantación del firewall con seguridad perimetral, se logró obtener el promedio de los ataques no deseados exitosos antes que se ponga en marcha dicho sistema y el resultado fue de 96.8 con desviación estándar de 72.8 ingresos, luego de poner en marcha el firewall el promedio fue de 6 con una desviación estándar de 2 ingresos no deseados, podemos apreciar que hay una diferencia de 90.8 de ataques no deseados exitosos dando así el promedio a favor del firewall de seguridad perimetral, podemos apreciar que la cantidad de ingresos mínimos y máximos sin firewall fue de 82 a 110 respectivamente, mientras los ingresos con firewall fue de 3 a 8 respectivamente.

Tabla 16: Comparación Pre-Prueba y Post-Prueba

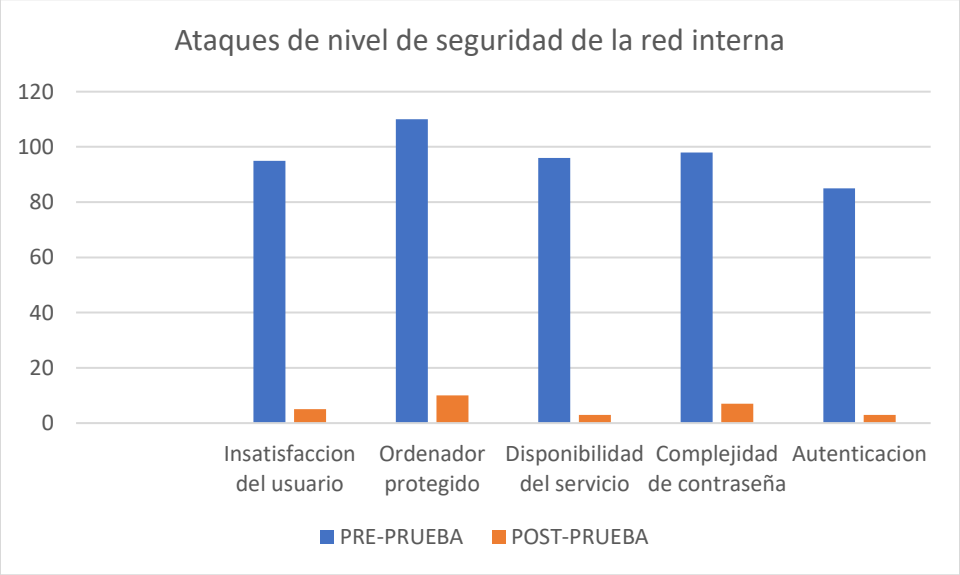


Tabla 17: Resultados de Pre-Prueba y Post-Prueba para indicador

	KPI: Ataques a nivel de seguridad de la red interna	
APLICACIÓN	PRE-PRUEBA	POST-PRUEBA
1	95	5
2	110	10
3	96	3
4	98	7
5	85	3
PROMEDIO	96.8	5.6

Hi: El Servidor firewall para la seguridad perimetral basado en freebsd pfsense **disminuye la cantidad de ataques no deseados determinando** niveles de confianza en la red de datos de la Municipalidad Provincial de Trujillo.

Solución:

a. Planteamiento de la Hipótesis

μ1 = Media de cantidad de vulnerabilidad para determinar niveles de confianza en la red en la Pre-Prueba.
μ2 = Media de cantidad de vulnerabilidad para determinar niveles de confianza en la red en la Post-Prueba.

b.1. Análisis estadístico para la prueba presencial de la hipótesis

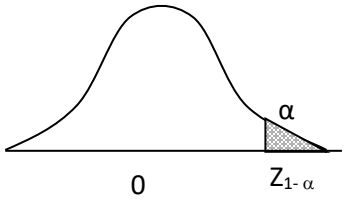
Cálculo de la diferencia de dos medias:

Tabla 18: Cálculo de la diferencia de dos medias

DESCRIPCIÓN	MEDIAS	VARIANZAS
Fórmula	$\mu_i = \frac{\sum X_i}{N}$	$\sigma^2 = \frac{\sum (X_i - \mu_i)^2}{N}$
Cálculo N=5	μ_1= 96.80 μ_2= 5.60	$\sigma^2{}_1$ = 72.8 $\sigma^2{}_2$ = 2

Cálculo de la Prueba de Hipótesis:

Tabla 19: Cálculo de la Prueba de la Hipótesis

TIPO DE HIPÓTESIS	ESTADÍSTICA DE PRUEBA	REGIONES DE ACEPTACIÓN Y RECHAZO DE Ho	VALOR CRÍTICO
Hipótesis Nula Ho : $\mu_1 - \mu_2 = 0$ Nivel de signif α	$z_0 = \frac{\overline{X_1} - \overline{X_2} - (\mu_1 - \mu_2)}{\sqrt{\sigma^2{}_1 / n + \sigma^2{}_2 / n}}$		α = 0.05 $Z_{1-\alpha}$ = 0.95
Hipótesis Alterna $H_1 : \mu_1 > \mu_2$	**Zo = 82.86**	**Rechazar Ho si, Zo > $Z_{1-\alpha}$**	**82.86>0.96**

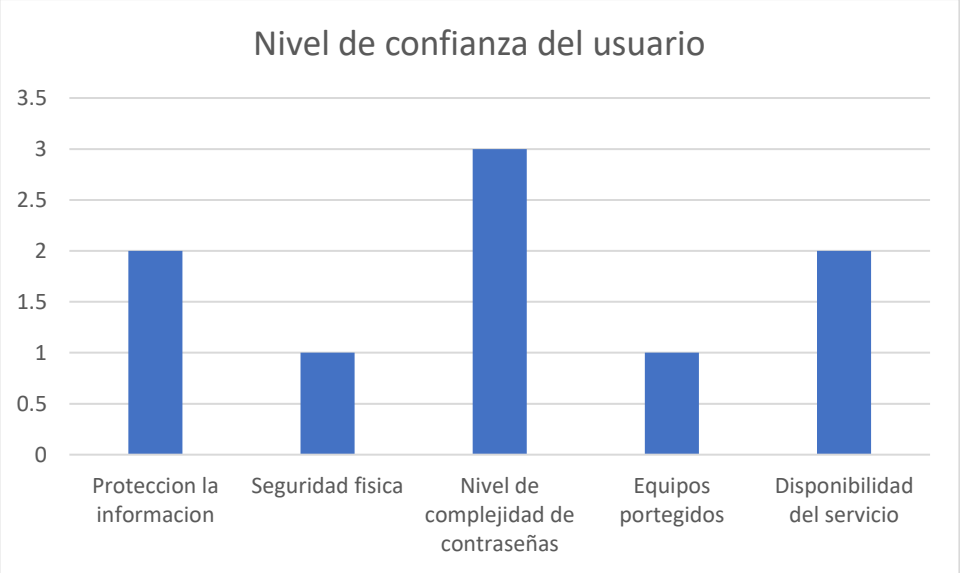
CONCLUSIÓN: El Servidor firewall para la seguridad perimetral basado en freebsd pfsense **disminuye la cantidad de ataques no deseados** determinando una mejor seguridad perimetral en la red de datos. Se logró reducir de 96.80 ataques no deseados a 5.60 ataques no deseados logrando una diferencia de 91.20 ataques no deseados logrando determinar niveles de confianza.

C. Indicador: Nivel de confianza del usuario.

Se puso a prueba el nivel de confianza de los usuarios en general sobre la protección de la red interna de datos en la diferentes sucursales de la Municipalidad Provincial de Trujillo sobre los ataques mal intencionados que se requieren proteger para ello se tomó en cuenta la muestra con la finalidad de encontrar el nivel de confianza de todos los usuarios antes de poner en marcha el firewall pfsense para saber luego que tan efectivo es su nivel de confianza, de la muestra utilizamos calificamos una puntuación de 10 como un nivel de confianza muy alto de acuerdo a ello confirmamos que la confianza del usuario es de 1.8 mientras su falta de confianza es de 8.2 a continuación se muestra un gráfico de registros del nivel de confianza del usuario, demostrando así la pésima calidad del nivel de seguridad de la red interna antes de aplicar el firewall pfsense.

Ilustración 68

Resultado de Pre-Prueba.



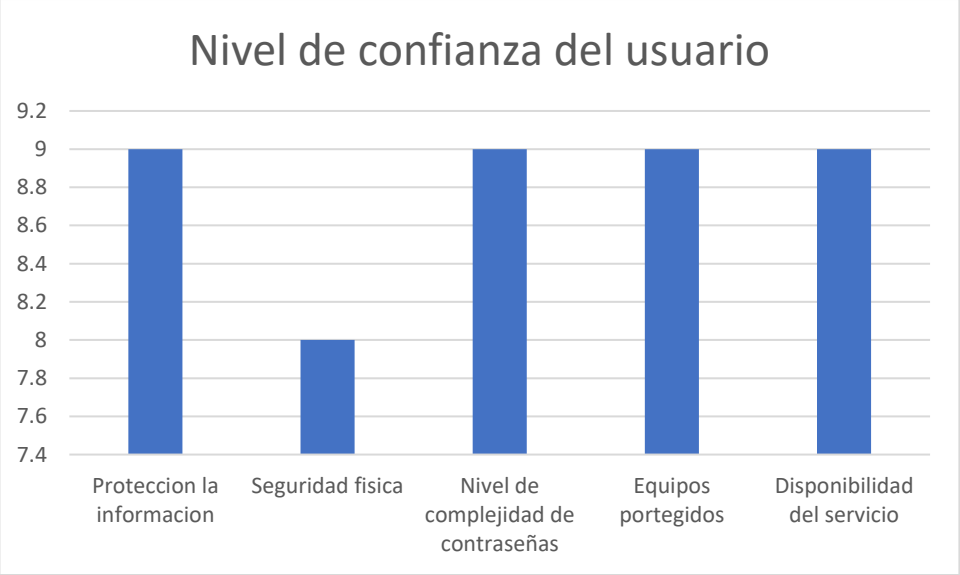
Nota. El gráfico muestra el resultado obtenido sobre el nivel de confianza de los usuarios respecto a la seguridad perimetral de la red interna sin un sistema de seguridad firewall.

Fuente: (Elaboración propia)

Se puso a prueba el nivel de confianza de los usuarios en general sobre la protección de la red interna de datos en las diferentes sucursales de la Municipalidad Provincial de Trujillo para ello se tomó en cuenta la muestra con la finalidad de conocer el nivel de confianza de los usuarios al poner en marcha la seguridad perimetral usando firewall pfsense, de la muestra utilizamos 10 como la puntuación más alta en nivel de confianza para a ello confirmamos que el nivel de confianza del usuario alcanzo una puntuación de 8.80, mientras que la falta de confianza fue de 1.20, a continuación se muestra un gráfico de puntuación del nivel de confianza de los usuarios, demostrando así el nivel de confianza al aplicar el firewall pfsense.

Ilustración 69

Resultado de Post-Prueba



Nota. El gráfico muestra el resultado obtenido sobre los niveles de confianza de los usuarios sobre la red interna de la Municipalidad Provincial de Trujillo con un sistema de seguridad firewall.

Fuente: (Elaboración propia)

Al llevar acabo el diagnóstico de la seguridad perimetral del firewall hacia los aplicativos que se brindan en red de la Municipalidad Provincial de Trujillo se obtuvieron resultados del antes y después de la implantación del firewall con seguridad perimetral, se logró obtener el promedio del nivel de confianza de los usuarios antes que se ponga en marcha dicho sistema y el resultado fue de 1.8 con desviación estándar de 2.3 de confianza, luego de poner en marcha el firewall el promedio fue de 8.80 con una desviación estándar de 2 de falta de confianza de los usuarios, podemos apreciar que hay una diferencia de 1.20 de confianza exitosos dando así el promedio a favor del firewall de seguridad perimetral, podemos apreciar que la cantidad de confianza sin firewall fue de 1 a 3 respectivamente, mientras los ingresos con firewall fue de 8 a 9 respectivamente.

Tabla 20: Comparación Pre-Prueba y Post-Prueba

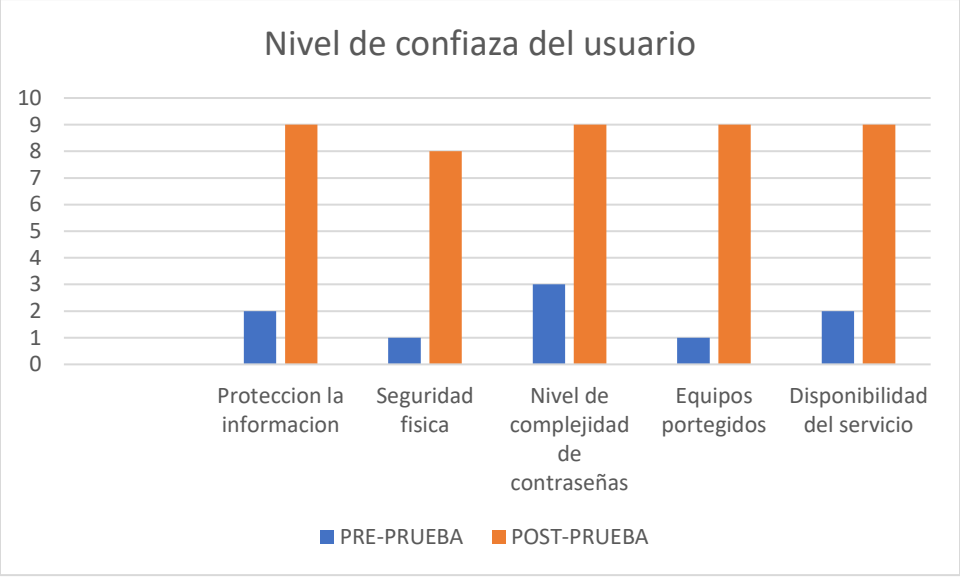


Tabla 21: Resultados de Pre-Prueba y Post-Prueba para indicador

KPI: Nivel de confianza del usuario	PRE-PRUEBA	POST-PRUEBA
Protección la información	2	9
Seguridad física	1	8
Nivel de complejidad de contraseñas	3	9
Equipos protegidos	1	9
Disponibilidad del servicio	2	9
PROMEDIO	1.8	8.80

Hi: El Servidor firewall para la seguridad perimetral basado en freebsd pfsense **disminuye la cantidad de ataques no deseados determinando bajando así los** niveles de falta de confianza a los usuarios de la Municipalidad Provincial de Trujillo.

Solución:

a. Planteamiento de la Hipótesis

μ1 = Media de cantidad de vulnerabilidad para determinar niveles de confianza en la red en la Pre-Prueba.
μ2 = Media de cantidad de vulnerabilidad para determinar niveles de confianza en la red en la Post-Prueba.

b. Análisis estadístico para la prueba presencial de la hipótesis

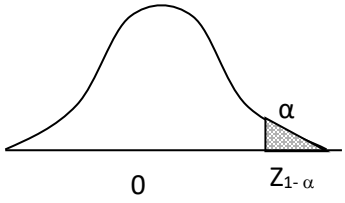
Cálculo de la diferencia de dos medias:

Tabla 22: Cálculo de la diferencia de dos medias

DESCRIPCIÓN	MEDIAS	VARIANZAS
Fórmula	$\mu_i = \frac{\sum X_i}{N}$	$\sigma^2 = \frac{\sum (X_i - \mu_i)^2}{N}$
Cálculo N=5	μ_1= 1.80 μ_2= 8.80	$\sigma^2{}_1$ = 2.3 $\sigma^2{}_2$ = 0.82

Cálculo de la Prueba de Hipótesis:

Tabla 23: Cálculo de la Prueba de la Hipótesis

TIPO DE HIPÓTESIS	ESTADÍSTICA DE PRUEBA	REGIONES DE ACEPTACIÓN Y RECHAZO DE Ho	VALOR CRÍTICO
Hipótesis Nula Ho : $\mu_1 - \mu_2 = 0$ Nivel de signif α	$z_0 = \frac{\overline{X_1} - \overline{X_2} - (\mu_1 - \mu_2)}{\sqrt{\sigma^2{}_1 / n + \sigma^2{}_2 / n}}$		α = 0.05 $Z_{1-\alpha}$ = 0.95
Hipótesis Alterna $H_1 : \mu_1 > \mu_2$	**Zo = 10.93**	**Rechazar Ho si, Zo > $Z_{1-\alpha}$**	**10.93>0.95**

CONCLUSIÓN: El Servidor firewall para la seguridad perimetral basado en freebsd pfsense **disminuye la cantidad de ataques no deseados** determinando una mejor seguridad perimetral en la red de datos. Se logró aumentar el nivel de confianza de los usuarios de 1.80 a 8.80 logrando determinar confianza.

CONCLUSIONES:

- Se logro medir el impacto positivo de la solución firewall al implementarlo debido a que se redujeron los ataques informáticos dentro de los diversos aplicativos que ofrecen servicios a los usuarios internos y externos.

- Se logró presenciar ataques no deseados en los 5 servicios brindados por la red de datos de la Municipalidad Provincial de Trujillo. Se localizaron vulnerabilidades con un promedio de 96.80 por aplicativo y detectando el mayor ataque no deseado al "PORTAL WEB" con 110 y el menor al "SIAF" con 85.

- Se diseñó e implemento el sistema de seguridad open source pfsense para la administración y seguridad perimetral mejorando los niveles de confianza en la red.

- Al finalizar la implementación y ponerla en marcha el firewall pfsense se logró visualizar una gran reducción de los ataques no deseados en la red de datos con un promedio de 6 y el aplicativo con mayores ataques fue "PORTAL WEB" con 10 y los menores fue el "SIGA" con 4.

RECOMENDACIONES:

- Se recomienda a la Municipalidad de Trujillo que en su red de datos considere los resultados obtenidos para un continuo mejoramiento en la seguridad perimetral a sus aplicativos.

- Se recomiendo utilizar el Sistema Operativo Kali Linux para realizar auditorías en la red datos y equipos informáticos para mejorar cualquier tipo de vulnerabilidad informática.

- Las vulnerabilidades y amenazas están en constante mejoramiento y para ello se recomienda que los aplicativos como sistemas operativos, anti virus y demás aplicaciones que trabajen en red sean actualizados constantemente cuando salgan nuevas versiones para evitar estar vulnerables ante cualquier amenaza informática.

- La red de datos interna de la Municipalidad Provincial de Trujillo y de cualquier organización en cuanto a la seguridad informática depende bastante de una adecuada implementación de políticas de seguridad y diseño en el entorno organizacional, estas deben ser constantemente actualizadas ante posibles amenazas nuevas.

- Documentar bien el diseño de la red de datos para futuros proyectos, con la finalidad de acelerar la constante actualización de la seguridad perimetral porque permitirá contar con un historial de todo lo que se ha elaborado además de tener una mejor gestión.

CAPITULO VI:

Referencias Bibliográficas

Bibliografía

Aco-Cas. (25 de agosto de 2015). *infoacocas.blogspot.com*. Obtenido de infoacocas.blogspot.com: http://infoacocas.blogspot.com/2015/08/actividad-4.html

Alegsa, L. (05 de Diciembre de 2010). *www.alegsa.com.ar*. Obtenido de www.alegsa.com.ar: http://www.alegsa.com.ar/Dic/tolerancia_de_fallas.php

areatecnologia. (14 de septiembre de 2017). *areatecnologia*. Obtenido de areatecnologia: http://www.areatecnologia.com/sistemas-operativos.htm

barracuda. (7 de septiembre de 2018). *barracuda.com*. Obtenido de barracuda.com: https://www.barracuda.com/glossary/network-perimeter

Clouding.io. (4 de enero de 2019). *clouding.io*. Obtenido de clouding.io: https://clouding.io/blog/nueva-imagen-pre-instalada-pfsense/

computerworld. (09 de Junio de 2000). *http://www.computerworld.es*. Obtenido de http://www.computerworld.es: http://www.computerworld.es/tendencias/que-es-el-balanceo-de-carga

director-it. (11 de mayo de 2009). *director-it*. Obtenido de director-it: http://director-it.com/index.php/es/ssoluciones/red-de-datos/177-%C2%BFqu%C3%A9-es-un-red-de-datos.html

docusign. (02 de abril de 2020). *docusign*. Obtenido de docusign: https://www.docusign.mx/blog/tipos-de-servidores

EmprendePyme. (19 de octubre de 2016). *EmprendePyme.net*. Obtenido de EmprendePyme.net: https://www.emprendepyme.net/politicas-de-seguridad.html

geeksforgeeks. (14 de diciembre de 2016). *geeksforgeeks.org*. Obtenido de geeksforgeeks.org: https://www.geeksforgeeks.org/operating-systems-need-and-functions/

Gemalto. (10 de septiembre de 2017). *gemalto.com*. Obtenido de gemalto.com: https://www.gemalto.com/press/pages/nuevas-investigaciones-revelan-una-amplia-brecha-entre-la-precepcion-y-la-realidad-en-relacion-con-la-seguridad-perimetral.aspx

Hernandez, S. (5 de marzo de 2017). *sites.google.com/site/seguridadinformaticahernandez*. Obtenido de sites.google.com/site/seguridadinformaticahernandez: https://sites.google.com/site/seguridadinformaticahernandez/conceptos-basicos-de-seguridad-informatica/7-6-vulnerabilidades-de-los-servicios-de-red

Holbrook., J. R.-P. (14 de Julio de 1991). *segu-info.com.ar*. Obtenido de segu-info.com.ar: https://www.segu-info.com.ar/politicas/riesgos.htm

HP. (30 de Agosto de 2021). *HP*. Obtenido de HP: https://www.hp.com/mx-es/shop/tech-takes/que-es-un-firewall-de-red-y-como-

funciona#:~:text=Un%20firewall%20es%20un%20sistema,o%20una%20combinaci%C3%B3n%20de%20ambos.

INCIBE. (20 de marzo de 2017). *www.incibe.es*. Obtenido de www.incibe.es: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

IONOS. (30 de mayo de 2016). *ionos.es*. Obtenido de ionos.es: https://www.ionos.es/digitalguide/servidores/know-how/que-es-un-servidor-un-concepto-dos-definiciones/

Ionos. (15 de septiembre de 2020). *Ionos*. Obtenido de Ionos: https://www.ionos.es/digitalguide/servidores/know-how/que-es-un-servidor-un-concepto-dos-definiciones/

McAfee. (25 de Octubre de 2021). *McAfee*. Obtenido de McAfee: https://www.mcafee.com/es-pe/antivirus/firewall.html#:~:text=Los%20firewall%20son%20programas%20de,de%20su%20conexi%C3%B3n%20a%20Internet.

nginx. (14 de junio de 2016). *nginx.com*. Obtenido de nginx.com: https://www.nginx.com/resources/glossary/load-balancing/

OAS. (19 de febrero de 2014). *OAS*. Obtenido de OAS: http://163.10.22.82/OAS/modularizacion/metodologa_topdown.html

Optical News. (03 de agosto de 2018). *optical.pe*. Obtenido de optical.pe: https://www.optical.pe/alerta-en-las-entidades-publicas-peruanas-por-incremento-de-ciberataques/

PAREDES VASQUEZ, E. E. (2016). *MEJORAMIENTO DE LA SEGURIDAD DE LA INFORMACION EN LA RED DE MICREDITO SAC.* Trujillo: Creative Commons.

Peña, I. S. (17 de Noviembre de 2014). *Loyvan*. Obtenido de Loyvan: https://www.loyvan.com/informatica/cuales-son-los-tipos-de-firewall-que-existen/

PERMALINK. (10 de Noviembre de 2013). *infosegur.wordpress.com*. Obtenido de infosegur.wordpress.com: https://infosegur.wordpress.com/tag/vulnerabilidades/

perulinux. (24 de Septiembre de 2016). *perulinux*. Obtenido de perulinux: http://www.perulinux.pe/service/pfsense/

Quispe, G. H. (13 de Agosto de 2016). *paginaswebencusco*. Obtenido de paginaswebencusco: https://www.paginaswebencusco.com/blog/servidores/hosting-compartido/definicion-servidor-web-compartido.html

rockconten. (14 de junio de 2019). *rockconten*. Obtenido de rockconten: https://rockcontent.com/es/blog/que-es-un-servidor/

Rouse, M. (16 de diciembre de 2016). *searchdisasterrecovery.techtarget.com*. Obtenido de searchdisasterrecovery.techtarget.com: https://searchdisasterrecovery.techtarget.com/definition/fault-tolerant

S Echeverría, J. J. (Abril de 23 de 2002). *researchgate*. Obtenido de researchgate: https://www.researchgate.net/figure/Figura-4-Esquema-generico-de-la-red-de-datos_fig4_228538730

Saavedra, J. C. (30 de enero de 2015). *juancarlossaavedra.me*. Obtenido de juancarlossaavedra.me: https://i2.wp.com/juancarlossaavedra.me/wp-content/uploads/2015/01/ppdioo-1.png

Saavedra, J. C. (18 de junio de 2017). *juancarlossaavedra.me*. Obtenido de juancarlossaavedra.me: http://juancarlossaavedra.me/2017/06/infografia-metodologia-top-down-para-el-diseno-de-redes/

Segu-Info. (11 de agosto de 2017). *evaluandosoftware.com*. Obtenido de evaluandosoftware.com: http://www.evaluandosoftware.com/politicas-de-seguridad/

solarwindsmsp. (26 de julio de 2017). *solarwindsmsp.com*. Obtenido de solarwindsmsp.com: https://www.solarwindsmsp.com/content/computer-security-vulnerabilities

Tecnologia & Informatica. (14 de Mayo de 2015). *tecnologia-informatica*. Obtenido de tecnologia-informatica: https://tecnologia-informatica.com/que-es-firewall-como-funciona-tipos-firewall/

tecnozero. (26 de diciembre de 2018). *tecnozero.com*. Obtenido de tecnozero.com: https://www.tecnozero.com/blog/zona-dmz-zona-segura-contra-intrusos/

tutorialspoint. (29 de junio de 2018). *tutorialspoint.com*. Obtenido de tutorialspoint.com: https://www.tutorialspoint.com/computer_security/computer_security_policies.htm

wikipedia. (29 de noviembre de 2011). *wikipedia*. Obtenido de wikipedia: https://es.wikipedia.org/wiki/Zona_desmilitarizada_(inform%C3%A1tica)

Wikipedia. (17 de Abril de 2017). *wikipedia*. Obtenido de wikipedia: https://es.wikipedia.org/wiki/Zona_desmilitarizada_(inform%C3%A1tica)#/media/File:Demilitarized_Zone_Diagram.png

Wikipedia. (26 de diciembre de 2018). *es.wikipedia.org*. Obtenido de es.wikipedia.org: https://es.wikipedia.org/wiki/Dise%C3%B1o_de_tolerancia_a_fallos

Wikipedia. (17 de agosto de 2018). *Wikipedia*. Obtenido de Wikipedia: https://es.wikipedia.org/wiki/Berkeley_Software_Distribution

Wikipedia. (13 de febrero de 2019). *Wikipedia*. Obtenido de Wikipedia: https://es.wikipedia.org/wiki/Pol%C3%ADtica_de_seguridad_inform%C3%A1tica

Williams, A. (2017 de Octubre de 23). *rizolatti.blogspot.com*. Obtenido de rizolatti.blogspot.com: http://rizolatti.blogspot.com/2017/10/balanceo-de-carga-mikrotik-diferentes.html

Ximena, L. (15 de marzo de 2009). *laurapita.blogspot.com*. Obtenido de laurapita.blogspot.com: http://laurapita.blogspot.com/2009/03/arquitectura-de-red.html

ANEXOS:

ANEXO 1

CARTA DE ACEPTACIÓN PARA REALIZAR INVESTIGACIÓN

MUNICIPALIDAD PROVINCIAL DE TRUJILLO GERENCIA DE SISTEMAS

CARTA DE ACEPTACIÓN PARA REALIZAR INVESTIGACIÓN COMO MOTIVO DE REALIZAR TESIS PARA OBTENER GRADO DE MAESTRO

Trujillo 10 de enero del 2019

Señor
ING. YONY SALOME VERA TOLEDO
Gerente de Sistemas
Municipalidad Provincial de Trujillo

Presente. -

Tengo el agrado de dirigirme a usted, con la finalidad de hacer de su conocimiento que el Bachiller DIONICIO GUZMÁN, ANTONIO ISAAC con su DNI: 72761077, perteneciente a la Escuela de Posgrado de la Universidad Privada Antenor Orrego, ha sido **ACEPTADO** para realizar su investigación en nuestra empresa "Municipalidad Provincial de Trujillo" con RUC: 20175639391, en la Gerencia de Sistemas por una duración de 4 meses desde 10 de enero al 10 de mayo del 2019, para que realice su tesis.

Aprovecho la oportunidad para expresarle mi consideración y estima personal.

Atentamente.

Municipalidad Provincial de Trujillo
GERENCIA DE SISTEMAS
Ing. Yony S. Vera Toledo
GERENTE

Firma del gerente o jefe de área.

ANEXO 2

CUESTIONARIO PARA ENTREVISTA Nº 1: GERENTE DE SISTEMAS Y ADMINISTRADOR DE REDES

MUNICIPALIDAD PROVINCIAL DE TRUJILLO

ENTREVISTA GERENTE DE SISTEMAS Y ADMINISTRADOR DE RED

A. LAS RESPONSABILIDADES

- Describe su organización y su relación al resto de la compañía.
- ¿Cuáles son sus responsabilidades primarias?

B. ANÁLISIS Y REQUISITOS DE LA RED

- ¿Cuál es el proceso actual para hacer llegar (obtener) la información?
- ¿Le piden que realice los análisis rutinarios?
- ¿Usted crea los informes estandarizados?
- ¿Cómo es el mecanismo de apoyo?
- ¿Cuál es el cuello de botella más grande / los problemas con los datos actuales que encuentran en el proceso?

C. ESTABILIDAD DE LA RED Y CALIDAD

- ¿Qué tan estable es la red durante el día?
- ¿Qué tipo de herramientas usa para administrar toda la red?
- ¿Cada que tiempo realiza un mantenimiento lógico y físico a los servidores?
- ¿Cada que tiempo realiza un backup a los sistemas? Describa el mantenimiento de este proceso.
- ¿Lleva el inventario de los equipos y la cantidad de usuarios que maneja en total?, a todo eso como logra mantener estable los sistemas

ANEXO 3

CUESTIONARIO PARA ENTREVISTA Nº 2: ADMINISTRADOR DE REDES

MUNICIPALIDAD PROVINCIAL DE TRUJILLO

ENTREVISTA ADMINISTRADOR DE RED

Nombre: _____ Fecha: ___/___/___

1. ¿Cómo califica la seguridad perimetral actual?

   _____

2. ¿Qué opina de la rapidez de respuesta ante amenazas del firewall actual?

   _____

3. ¿Basado en su experiencia, cree usted que el firewall actual es eficiente?

   _____

4. ¿Con el firewall actual usted puede tener control de la seguridad con rapidez y eficiencia?

   _____

5. ¿Cree usted que todas las organizaciones medianas y grandes con un firewall para su seguridad perimetral? ¿Por qué?

   _____

6. ¿Considera importante que el firewall brinde información puntual y precisa de los ataques y control de tráfico de la red?

   _____

ANEXO 4

Acta de instalación de firewall

MUNICIPALIDAD PROVINCIAL DE TRUJILLO

ACTA DE INSTALACION FIREWALL

Para la conformidad de instalación llenar los siguientes datos que se muestran a continuación

Fecha de instalación:	08/04/19
Responsable:	Ing. Antonio Isaac Dionicio Guzmán

DATOS DE LA INSTITUCION

Organización:	Municipalidad Provincial de Trujillo
Dirección:	Av. España 738
Tipo de institución:	Estatal

DATOS DEL SOFTWARE

Nombre:	PfSense
Versión:	V. 5.0.1

OBSERVACIONES	

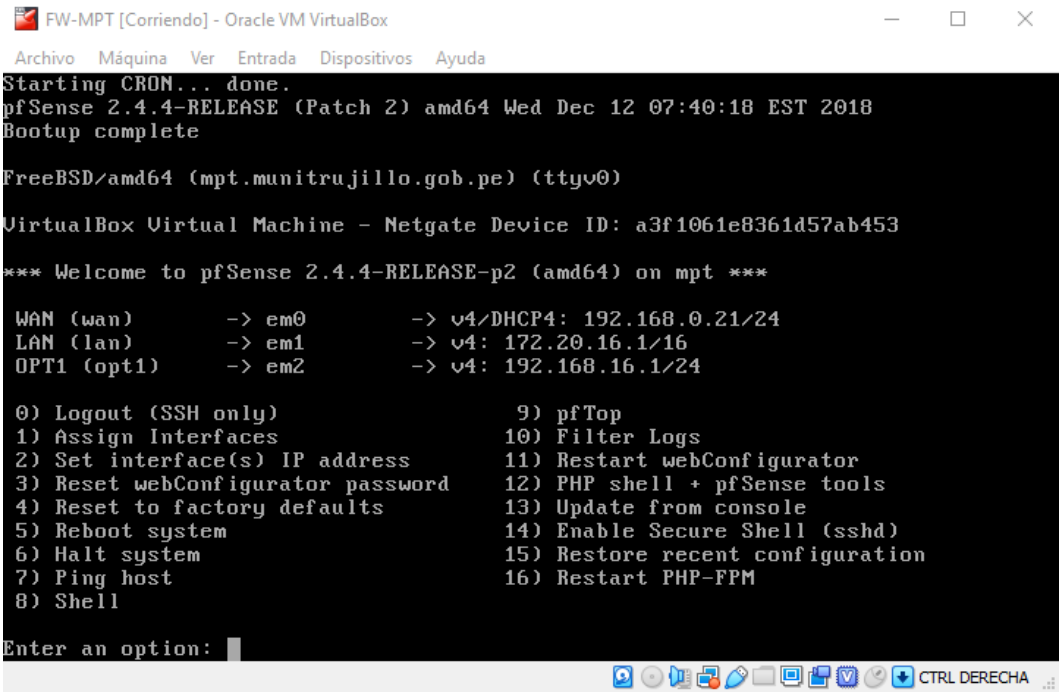
Firma del gerente o jefe de área.

ANEXO 5

Data Center

ANEXO 6

Interface de la consola PfSense



ANEXO 7

Interface web del firewall PfSense