UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO

FACULTAD DE INGENIERÍA

CARRERA PROFESIONAL DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

ANÁLISIS E IMPLEMENTACIÓN DE UN FIREWALL DE SEGURIDAD PARA EL CONTROL DE ACCESOS Y PROTECCIÓN DE LA RED DE DATOS DE LA EMPRESA FERRETERÍA SOTO, 2021.

Autores:

Bach. Bernal Cojal José Neiber.

Bach. Sangay Huaccha Willam Elí.

Asesor:

Dr. Ing. Diana Cruzado Vásquez

Cajamarca – Perú

Octubre – 2022

UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO

FACULTAD DE INGENIERÍA

CARRERA PROFESIONAL DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

ANÁLISIS E IMPLEMENTACIÓN DE UN FIREWALL DE SEGURIDAD PARA EL CONTROL DE ACCESOS Y PROTECCIÓN DE LA RED DE DATOS DE LA EMPRESA FERRETERÍA SOTO, 2021.

TESIS PRESENTADA EN CUMPLIMIENTO PARCIAL DE LOS REQUERIMIENTOS, PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO INFORMÁTICO Y DE SISTEMAS

Autores:

Bach. Bernal Cojal José Neiber.

Bach. Sangay Huaccha Willam Elí.

Asesor:

Dr. Ing. Diana Cruzado Vásquez

Cajamarca – Perú

Octubre – 2022

UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO

FACULTAD DE INGENIERÍA

CARRERA PROFESIONAL DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

APROBACIÓN DE TESIS PARA OPTAR EL TÍTULO PROFESIONAL

ANÁLISIS E IMPLEMENTACIÓN DE UN FIREWALL DE SEGURIDAD PARA EL CONTROL DE ACCESOS Y PROTECCIÓN DE LA RED DE DATOS DE LA EMPRESA FERRETERÍA SOTO, 2021.

Presidente: _____

Secretario: _____

Vocal: _____

Asesor: _____

Dedicatoria

Considerando todo el esfuerzo realizado hacia mi persona y por el apoyo incondicional que jamá dejó mi mano, le dedico este trabajo de investigación a mis padres y hermanos; sus consejos, su apoyo económico y su incondicional motivación que, hizo de mí persona escalar una etapa más en mi vida y conseguir la culminación de mi tesis. Jamás olvidaré este momento, debido a que ha sido una meta muy difícil de alcanzar, solo mi familia sabe lo duro que ha sido llegar hasta este punto y conseguir con todo orgullo la culminación de mi tesis.

BERNAL COJAL JOSÉ NEIBER.

Con el corazón muy en alto y orgulloso de lograr un mérito muy importante en mi vida personal, le dedico este trabajo a mi madre, por ser la persona que me enseñó a dar mis primeros pasos y hoy comparte con mi persona la felicidad de convertirme en un profesional de éxito. En este tiempo comprendo que todo lo que hizo ella por mí tenía una razón de ser, tenía un propósito, tenía un plan y un único objetivo. Ser quien soy ahora y verme convertido en un gran profesional.

SANGAY HUACCHA WILLAM ELÍ.

Agradecimiento

Si de agradecimiento se trata, Dios es el primer centro de agradecimiento universal, su gran poder e inmensa gloria permitió que logre llegar hasta este momento y que me encuentre con vida. En segundo lugar, agradecer de todo corazón a mi familia, por todo lo brindado; gracias a la fuerza que me brindaron pude seguir en el camino que me permite hoy en día la culminación de un trabajo de investigación completo y con grandes perspectivas. De igual modo agradecer a la empresa ferretería SOTO, ya que al abrirme las puertas de sus instalaciones pude conseguir la culminación de mi tesis y seguir dando un paso más en mi vida profesional

BERNAL COJAL JOSÉ NEIBER.

Agradecer, me convierte en alguien que ha comprendido mucho más de la vida, un virus que destruyó muchas personas a nivel mundial. Pero, que gracias a Dios él permitió que siga con vida y con las fuerzas de avanzar en una etapa más de mi desarrollo personal. Agradecer también a mi madre, porque gracias a ella comprendí que una mujer tiene la determinación de lograr y alcanzar todo lo que se proponga. De igual manera, agradecer a la Dr. Ing. Diana Cruzado Vásquez, que fue una guía muy importante en el desarrollo de este trabajo de investigación, gracias a su persona se ha conseguido la culminación de la presente investigación.

SANGAY HUACCHA WILLAM ELÍ

Resumen

La implementación de un firewall de seguridad permite que exista un control de accesos en la red e incrementa la protección de la red de datos. El desarrollo de la presente tesis: "Análisis e implementación de un Firewall de seguridad para el control de accesos y protección de la red de datos de la empresa Ferretería Soto, 2021", ha tenido el objetivo de implementar un firewall de seguridad que mejore el control de accesos y protección de la red de datos de la empresa Ferretería Soto.

La presente tesis presenta un tipo de investigación aplicada – tecnológica, con un enfoque y diseño no experimental. Tomando como población a 7 administrativos de la empresa ferretera, los cuales a través de un cuestionario implementado brindaron datos necesarios para la contratación de la hipótesis, asimismo la implementación del firewall físico fue verificada por tres expertos, quienes a través de una hoja de cotejo validaron la implementación.

Para la investigación se ha tomado en cuenta la siguiente hipótesis: La implementación de un firewall de seguridad influye positivamente en el control de accesos y protección de la red de datos en la empresa Ferretería Soto. Con el fin de contrastar la hipótesis planteada se realizó la prueba estadística de Chi-Cuadrado, prueba estadística que brindó un resultado con una significancia de Pearson de 0.013, significancia de razón de verosimilitud de 0,037 y finalmente una significancia en la asociación lineal por lineal de 0,015. Resultados que permitieron conocer que la influencia de la implementación de firewall es positiva frente al control de accesos y protección de la red de datos. A este resultado se le añade la aceptación del 100% de

expertos quienes realizaron la hoja de cotejo. Finalizando de tal modo la investigación, con la conclusión que, la implementación de un firewall mejora sobre los controles de acceso y protección a la red de datos en la Ferretería Soto.

Palabras Clave: Firewall, Chi-Cuadrado, Acceso a la red, Protección de red, significancia.

Abstract

The implementation of a security firewall allows for access control in the network and increases the protection of the data network. The development of this thesis: "Analysis and implementation of a security firewall for access control and protection of the data network of the company Ferretería Soto, 2021", has had the objective of implementing a security firewall that improves the access control and protection of the data network of the company Ferretería Soto.

This thesis presents a type of applied research - technological, with a non-experimental approach and design. Taking as a population 7 administrators of the hardware company, which through an implemented questionnaire provided the necessary data for the contracting of the hypothesis, likewise the implementation of the physical firewall was verified by three experts, who through a check sheet validated the implementation.

For the investigation, the following hypothesis has been taken into account: The implementation of a security firewall positively influences access control and protection of the data network in the company Ferretería Soto. In order to contrast the proposed hypothesis, the Chi-Square statistical test was performed, a statistical test that provided a result with a Pearson significance of 0.013, a likelihood ratio significance of 0.037 and finally a significance in the linear by linear association of 0.015. Results that allowed to know that the influence of the implementation of firewall is positive against access control and protection of the data network. To this result is added the acceptance of 100% of the experts who carried out the checklist. Thus concluding the

investigation, with the conclusion that the implementation of a firewall improves access controls and protection of the data network at Ferreter Soto.

Keywords: Firewall, Chi-Square, Network access, Network protection, significance.

Índice

LISTA DE TABLAS

LISTA DE FIGURAS

CAPÍTULO I: INTRODUCCIÓN

1. Planteamiento del problema

1.1. Descripción de la realidad problemática

Actualmente, con el desarrollo impulsivo de la tecnología a nivel global, han surgido diversas soluciones que le permiten a las personas comunicarse y desarrollarse en muchos ámbitos y, en cada una de las etapas de su vida. Día a día estas nuevas tecnologías se van actualizando y mejorando sus funcionalidades, dichas tecnológicas poco a poco han ido desarrollándose e imponiéndose sobre las que ya existían, este cambio a su vez da lugar a circunstancias que llevan al mal uso de las tecnologías convergentes, comprometiendo la integridad de la información en el medio personal y corporativo (Castillo, Domínguez y Sulca, 2017, p. 13).

Si hablamos de seguridad, se conoce que el 80% de las Pymes en Latinoamérica les preocupa la seguridad, a pesar de ello, el 98% no considera este aspecto como una prioridad dentro de sus organizaciones. Un estudio elaborado por IDC, menciona que, las empresas no saben el que ni el como se comportan los códigos maliciosos. Las soluciones de seguridad existentes para la infraestructura y dispositivos de las empresas requieren demasiado poder adquisitivo, un ejemplo de esto son los firewalls UTM, usados principalmente para asegurar el área perimetral de la red, que además se encargan de prevenir y proteger los datos y dispositivos. (Chicaiza, 2018, p. 13).

Un incidente de vulnerabilidad informática puede no solo denegar el servicio a los consumidores, sino provocar la pérdida de los datos confidenciales de la empresa que se perjudica ante un robo de información o una maniobra maliciosa de competencia desleal en el ámbito comercial. Peñafiel (2021), indica que la seguridad informática es un conocimiento que toda empresa debe considerar como información básica, siendo el principal objetivo salvaguardar la información de una organización, ya que, este es el

recurso de mayor importancia en una organización (p. 145) … Las amenazas relacionadas a la seguridad informática se dividen en amenazas internas y externas; siendo las amenazas internas las que afectan la información y limitan el acceso a la data que contiene la empresa (p. 147).

Considerando la información de Peñafiel, también se toma en cuenta el principal problema de las empresas es que carecen de un firewall. Martínez, Pacheco y Zúñiga (2017) mencionan que, la mayoría de organizaciones consideran que su información esta salvaguardada, pero, jamás miden los problemas que se presentarían de ser el caso que exista un ataque a su red. Los firewalls son mecanismos de defensa y filtración de información que tienen el fin de evitar ataques externos, que perjudiquen las empresas o busquen robar data (pp. 156-157).

Si se tiene en cuenta lo mencionado, se puede afirmar que la empresa Ferretería Soto S.R.L era ajena a esta situación, ya que no contaba con ningún tipo de cortafuegos, barrera o herramienta que permita restringir el tráfico malicioso desde los equipos que podían ser infectados. La mayoría de infecciones computarizadas se pueden dar visitando sitios web maliciosos, correos electrónicos con virus o simplemente al conectar un pendrive. Al existir una infección se crean brechas en la seguridad y ponen en riesgo la infraestructura de redes, la vulnerabilidad de la información y de las tecnologías de información primordiales de la empresa.

La problemática de la empresa se formó, desde que se inició a trabajar con equipos tecnológicos: internet, computadoras y softwares. Esto generaba una gran problemática para la empresa, debido que los empleados y personal que tienen contacto con los programas, internet y equipo tecnológico; no tenían ninguna filtración de información ni control alguno sobre la manipulación en los equipos.

Por lo expuesto, es que la Ferretería Soto solicitó la implementación de algún

instrumento que restrinja, filtre y proteja la información, con el fin de que ya no se ponga en alto riego la confidencialidad de la data que se maneja dentro de la empresa. En el contexto planteado fue de mucha importancia encontrar una solución al problema de la seguridad; lográndose la implementación de tecnologías Firewall de hardware y cumplir con los requerimiento y problemas con los que contaba la ferretería Soto.

1.2. Definición del problema

¿Cómo influirá la implementación de un firewall de seguridad en el control de accesos y protección de la red de datos de la empresa Ferretería Soto?

1.3. Objetivos

1.3.1. Objetivo general

Implementar un firewall de seguridad para mejorar el control de accesos y protección de la red de datos de la empresa Ferretería Soto, 2021.

1.3.2. Objetivos específicos

- Evaluar los problemas de seguridad y de vulnerabilidad en la información de la red con el fin de identificar los requerimientos funcionales y operativos del sistema.
- Analizar el comportamiento de la red antes y después de aplicar políticas de firewall.
- Establecer lineamientos y políticas de seguridad necesarios para la administración en la red de datos.
- Medir y describir los resultados obtenidos al implementar el sistema firewall para conocer el impacto en el control de acceso y la seguridad de la red de datos.

1.4. Justificación e importancia.

En la actualidad las organizaciones, instituciones y empresas sufren ataques informáticos; esto genera pérdidas millonarias, siendo necesario invertir en la seguridad de la información y en los servicios que se brinda. Con la implementación de un sistema de seguridad perimetral se consigue el control de los accesos en la información, sobre todo en los servicios que se oferta y la seguridad en la información confidencial de la empresa, generando un monitoreo continuo y con el registro constante de todo servicio que se utiliza en una empresa (Díaz y Silva, 2016, p.14).

Estrada, Unás y Flores (2021) indican que, un estudio realizado por la universidad del valle sobre las prácticas de seguridad de información, en donde se realizó un cuestionario a un determinado grupo de organizaciones. El estudio arrojó que el 34,1% de organizaciones no conoce en lo absoluto la práctica de seguridad a través de firewall y, un 27,3% ni siquiera conoce si lo utilizan en sus organizaciones. Solamente el 33.6% considera la utilización del firewall en sus organizaciones, haciendo de este tema uno con grandes campos de investigación (p. 104).

En los últimos años los ataques de denegación de servicios generan un gran problema en las organizaciones y empresas que no cuentan con un cortafuegos o firewall; el ataque DDoS se potencia con el volumen de información inhabilitando, los servicios personales, dispositivos móviles, servidores, computadores y todo equipo tecnológico conectado a la red. Este problema tiene una principal causa y es la carencia de un programa hardware o firewall físico que evite un ataque a través de denegación de servicios, permitiendo la infiltración de malware hacia los servicios de una organización (Márquez, 2019, p. 97)

Es de mucha importancia considerar la presencia de un firewall y el gran aporte

que le genera a una organización, toda organización debe considerar la implementación de un firewall como medida preventiva ante ataques de diversos tipos, filtración de servicios y sobre todo la manipulación correcta de los usuarios propios del sistema, restringiendo toda usabilidad externa o ajena a la organización que busque dañar toda operatividad propia de la empresa (Romero, Pineda y López, 2016, p. 478).

Entonces, considerando lo expuesto se tiene una justificación práctica, teórica y metodológica. A nivel práctico la investigación se justifica mediante la implementación correcta de un firewall, ya que la nueva tecnología plantea utilizar instrumentos que estén a la vanguardia de la seguridad, además de brindar aspectos favorables en el desarrollo investigativo. Con la implementación del firewall, se permite tener resultados que mejoran el control de seguridad en la Ferretería Soto, ya que esto le permitirá a la empresa lograr plantear metodologías y políticas de seguridad para salvaguardar su información. En tal sentido, la Ferretería Soto logrará tener un control interno y externo de su información.

Por el lado teórico, la investigación se justifica debido a las diversas teorías, enfoques y modelos que se presentan actualmente en la implementación de un firewall, realizando una sistematización correcta con el control de accesos para la protección de datos en la red, esto con el propósito de consolidar la información y mejorar el manejo de los paquetes en red, todo en una realidad contundente.

Con el desarrollo del aporte teórico se logró realizar una prueba estadística denominada Chi-Cuadrado, dicha prueba estadística logra para conocer el porcentaje de influencia que presenta una variable sobre la otra, generando que exista una comprobación estadística en torno a la asociación y mejora entre las variables, ya que se realizan mediciones del control de accesos para que exista una protección en la red más adecuada

y confiable; además que la tabla cruzada realizada por Chi-cuadrado muestra los valores de significancia en la mejora. Asimismo, se realizó un análisis de un juicio de expertos el cual aporta el conocimiento necesario para la afirmación acerca de la implementación de un firewall en el control de accesos y la protección de datos en red de datos.

Finalmente, se tiene una justificación metodológica, ya que, si se ha dispuesto alcanzar objetivos, estos se logran únicamente en un proceso de implementación de un firewall denominado Button Up, el cual faculta de pautas y métricas estrictas en la implementación de un firewall. Además, de utilizarse técnicas de análisis y desarrollo de la implementación de un Firewall para incrementar el control de accesos y la protección de red en la Ferretería Soto.

CAPÍTULO II: MARCO TEÓRICO

2. Fundamentos teóricos de la investigación

2.1. Antecedentes teóricos

Chicaiza (2018) en su proyecto “Implementación de un firewall construido a partir de software y una placa de circuitos compacta o SBC (single Board Computer)”, la investigación se planteó como objetivo general, el mejorar la seguridad perimetral mediante appliance de seguridad de bajo costo, construido a partir de software libre y una placa de circuitos. Para el desarrollo del software se utilizó la metodología de carácter descriptivo, con enfoque cuantitativo y cualitativo para poder probar la hipótesis.

Los resultados que se obtuvieron de la implementación del firewall se dividieron en dos resultados: de usabilidad y de operatividad. Con los resultados de usabilidad se logró controlar la amenaza de virus o problemas con softwares parchados o actualizados; mientras que, por la parte operativa se logró mitigar los riesgos referentes a la infraestructura tecnológica. Con el firewall instalado se puede evidenciar que el 100% todos los ataques realizados a los diferentes servicios no pudieron ser afectados, ya que el firewall logró bloquear y registrar las conexiones que pueden interferir con el correcto funcionamiento del servicio atacado. Dentro de las debilidades evidenciadas en la implementación del appliance se destaca que, al ser un hardware limitado por sus componentes, solamente realiza una protección en capa transporte, esto se debe a que al no ser un firewall físico, presenta limitantes para la cantidad de equipos conectados, por esta razón se recomienda realizar un monitoreo más exhaustivo, ya que se presenció que el 10% de paquetes filtrados en el software no eran restringidos, debiéndose a que los dispositivos conectados sobrepasan los diez dispositivos.

Roba, Vento y García (2016) realizaron un proyecto de investigación denominado: “Metodología para la detección de vulnerabilidades en las redes de datos utilizando Kali-Linux”; su objetivo principal de este trabajo fue diseñar una metodología para la detección de vulnerabilidades en redes de datos. Para esto se desarrollaron diferentes etapas: valoración, ejecución e informe; cada una de las cuales es soportada por diferentes herramientas incluyendo los softwares(s) utilizados.

El desarrollo de la metodología proporcionó resultados por etapas, cada resultado es de mucha importancia debido a que cada etapa suministra datos necesarios para la ejecución de la investigación. Con el fin de validar la utilidad de la metodología propuesta, se llevó a cabo la implementación en la red de datos perteneciente a la Unidad Empresarial de Base Logística de la empresa de Construcción y Montaje de Pinar del Río, encontrando diferentes tipos de vulnerabilidades, en relación a los servidores el 100% de los servidores presentaba vulnerabilidades, los equipos no presentaban contraseñas modificadas, lo que generaba que cualquier persona pudiere conectarse a la red y vulnerar los datos de la empresa. Con el cuestionario realizado a los trabajadores de la empresa, se encontró que el 47% del personal no presentaba la capacidad necesaria para administrar los datos de la red, lo que genera que la red quede vulnerable por falta de conocimiento en seguridad informática. Finalmente, apoyándose en los resultados obtenidos se demostró que la metodología propuesta es de gran utilidad para detectar vulnerabilidades en redes de datos, lo que demuestra su importancia para el área de la seguridad informática.

Esparza (2013), en su tesis: “Implementación de un firewall sobre la plataforma LINUX en la empresa de contabilidad y finanzas Armas & Asociados”, el objetivo de la implementación se desarrolló por la gran cantidad de servicios que no son utilizados

por los usuarios y a la ves que, el internet no presentaba ninguna restricción para evitar cualquier ataque por virus o softwares malintencionados que, busquen robar la información. Armas & Asociados al ser una empresa de contabilidad cuenta con información de mucho valor, por esta razón que con la implementación de un firewall se tendría un mejor resguardo de la red y de la información con la que cuenta la empresa de contabilidad.

La implementación del firewall se basó en un software, este se desarrolló a medida con el propósito de salvaguardar los puntos que la empresa de contabilidad requería, una vez implementado el software, se consideró que la usabilidad del software es muy sencilla, pero que, internamente es muy potente para salvaguardar la información. De igual manera, la implementación del firewall brindó resultados relacionados a la búsqueda de amenazas, control de módulos, búsqueda de errores y detección de fallas en el sistema. Entre los resultados cuantitativos de la investigación solamente se realizó una demostración de la ejecución del firewall, lo que mostró que el firewall realizaba una protección del protocolo http del 20%, esto es algo muy bajo hablándose de un protocolo de mucha importancia, como el protocolo encargado de la salida para conexión con páginas WAN.

Pacheco y Martínez (2009) en su tesis: “Diseño e implementación de un servidor firewall en LINUX”, el desarrollo investigativo se realizó con el propósito de efectuar la implementación de un servidor GNU/Linux que tenga la funcionalidad de actuar como una herramienta capaz de brindar la seguridad necesaria para una red de tipo institucional o de tipo organizacional; el desarrollo de la investigación consiguió a detalle conocer el procedimiento de la implementación de un firewall hardware con la herramientas Iptraf e Iptables.

Los resultados que se obtuvieron de la implementación del firewall se relacionaron estrechamente con el aspecto de la funcionalidad, el producto final logró el análisis de las comunicaciones de red, establecer conexión con las peticiones que se generaban en el host hacia una red externa, filtrar paquetes en la capa de red y análisis de las direcciones IP que salían y entraban a la red. Además, a nivel de conocimiento se logró comprender que no solo es suficiente con la utilización de una herramienta software para la implementación de un firewall físico, ya que la utilización de las herramientas software permitieron que se realizara una red segura y con el tráfico controlado.

Joaquin, (2020) en su tesis “Implementación de firewall para el control de servicio de internet en la filial Chanchamayo de la universidad Peruana los Andes” se plantea como objetivo implementar un Firewall para controlar el uso del internet, gestionando los accesos de acuerdo al uso o labor de cada personal administrativo, gestionando en los laboratorios de cómputo el control del servicio de internet de acuerdo las demandas tecnológicas que cada curso desarrollado por el docente requería. Asimismo, Joaquin realizó un servicio de internet controlado en horarios en los que los laboratorios no se encuentren laborando, con el fin de no saturar los servicios relacionados con la red de computadoras internas.

La implementación del firewall se realizó mediante la metodología Top Down con un tipo de investigación aplicada-tecnológica y con un diseño pre-experimental. Se obtuvo como resultados que al implementar reglas para habilitar protocolos mediante la metodología Top Down Network Design, existen mejoras en el control de accesos al servicio de internet en la Filial Chanchamayo, estas reglas definen las páginas necesarias a las que el personal administrativo y el personal de los laboratorios de cómputo tendrán acceso.

Entre los resultados más importantes de la investigación, son los datos obtenidos en relación a los términos de vulnerabilidad y la estadística de Wilcoxon ya que se obtuvo que luego de la implementación del firewall se consiguiera una mejora en la seguridad del sistema del 91,83%. Además, el 100% de quejas que realizan los trabajadores de la empresa, desparecieron en su totalidad, ya que el firewall realizaba una protección correcta para el filtrado de paquetes. Por la parte estadística luego de la implementación se realizó un análisis de 1000 paquetes los cuales en la prueba estadística arrojaron una significancia del 0,000, lo cual permite afirmar su hipótesis ya que está bajo el 0,05 de la significancia correspondiente. En relación a la velocidad de transferencia de paquetes, se consiguió una mejora del 66%, mejorando aquellas zonas donde difícilmente llegaba la conexión de red.

Villanueva y Riveros (2014) en su tesis “Diseño de un esquema lógico para la seguridad perimetral de una red de comunicaciones” se planteó como objetivo diseñar un esquema lógico para mejorar la seguridad perimetral de la red de comunicaciones. Para el diseño lógico se utilizó la metodología Top Down de Cisco, presentando resultados de gran importancia, esto se debió a que se logró diseñar un nuevo esquema lógico de seguridad perimetral, el cual permitirá mejorar enormemente la seguridad de datos en la entidad. Por lo tanto, los funcionarios podrán realizar sus labores con normalidad sin preocuparse en la información, ya que su información tendrá un grado de seguridad superior en contra de ataques por intrusos. La investigación concluyó con la idea que por más seguridad que se pueda instalar en una empresa, jamás se podrá mantener una seguridad al 100%, principalmente porque en la actualidad la gran mayoría de amenazas van surgiendo continuamente, muchas de estas controlables, pero algunas con futuros inciertos.

Entre los resultados cuantitativos de mayor importancia se tiene la prueba estadística Z-Teórica, la que se utiliza para realizar una medición pre con una medición post hipotética, ya no existe la implementación como tal. En el desarrollo de esta prueba se encontró con un valor inicial del 28%, y con la medición hipotética se tiene un valor de 88%, esto quiere decir que el grado de seguridad perimetral mejora en un 60% la red de comunicación, esta misma prueba realizó un valor de significancia, la cual obtuvo un valor de 0.05, demostrando que el diseño lógico planteado tiene un 5% de aceptar una hipótesis nula y un 95% de rechazala. Por lo tanto, debemos confiarnos de una seguridad perimetral desarrollada, confiando en el desarrollo de una seguridad estructural y notoria que esta misma crea, informándose constantemente de los nuevos ataques y herramientas de seguridad existentes.

Vila (2019) en su tesis titulada: “Implementación de Firewall que permita optimizar la seguridad y los servicios de red en Cineplanet” menciona que la implementación de equipos Firewall dentro en la empresa Cineplanet permitirán reforzar la seguridad y la prestación de servicios dentro de la red corporativa. Se utilizó la metodología PPDIOO, que fue dividido en 6 fases para llevar a cabo la implementación adecuada según los requerimientos establecidos.

Una vez implementado el firewall se demostró el control de los servicios y control de páginas y aplicaciones que acceden los usuarios en la red de la empresa, esto era de una importancia muy alta, debido a que el control de las páginas web no se encontraba limitado, facilitando la usabilidad de la internet según los usuarios quisieren, por lo que dañaba la conexión de red y dificultaba la conexión de red fluida. Por lo tanto, se concluye que la implementación de firewall en la empresa tiene una influencia positiva en el entorno a red y logra mejorar el ancho de banda en relación al servicio de internet.

Con relación a sus resultados cuantitativos no muestra datos de dicha índole, debido a que fundamenta su investigación solamente en el desarrollo de un dispositivo que optimice la seguridad y mejore los servicios, lo que se consigue únicamente con la implementación del Firewall.

2.2. Marco conceptual.

2.2.1. Redes de computadores.

Las redes de computadores presentan una orientación directa con la comunicación de datos entre los ordenadores, involucrando aspectos relacionados a la seguridad de la transmisión de paquetes, el enrutamiento de datos, protocolos de comunicación, capas de transporte, red y aplicación.

Tanenbaum y Wetherall (2012) indican que las redes de computadoras tienen la finalidad de realizar la comunicación de los equipos y programas de una determinada red, con la finalidad que exista equidad entre los servicios, mejorando la comunicación de recursos entre los equipos y logrando la seguridad de la comunicación (p. 2) (…) Toda red de comunicación tiene la facilidad de tener una aplicación en diversos ambientes de usabilidad; la aplicación en negocios tiene la finalidad de realizar comunicación entre los equipos de una empresa y generar la seguridad de la información con la que cuenta el negocio. Por otro lado, la aplicación de uso doméstico busca una comunicación de datos no muy especializada, pero que genere una confianza al momento de utilizar los servicios con que se cuenta (pp. 3-5).

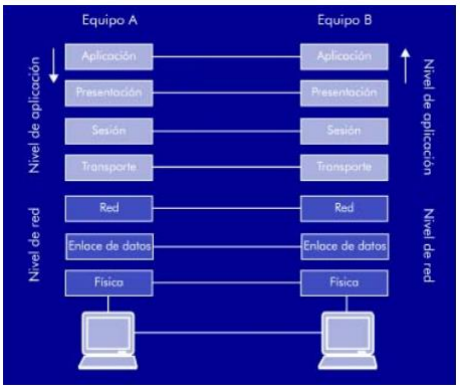
2.2.1.1. Arquitectura de protocolos: OSI

La gran cantidad de arquitecturas de protocolos, algunas abiertas y otras propietarias realizó que se desarrolle una arquitectura de uso flexible y sencillo, teniendo la facilidad de poder conectar los servicios y protocolos de diversas marcas y que juntas trabajen sin generar problemas. Este modelo se conoció como el modelo OSI, Barceló

et. al. (2004) mencionan que el principal problema del modelo era la comunicación de datos entre diversas redes informáticas, por tal razón, se realizó la división de niveles. Donde cada participante del modelo incorpora uno de los niveles, pero el equipo final contiene todos los niveles (p. 39).

Figura 1

Niveles del modelo OSI en comunicación de equipos



Tomado de *Redes de computadoras* (p. 40), por Barceló Et. al., 2004. Eureca Media

Capas del modelo OSI.

El modelo OSI está conformado de 7 capas, cada una con propias características y descripciones (Stallings, 2004, pp. 36-40).

Tabla 1

Capas de la arquitectura OSI

Capa	Funcionalidad
Capa Física	Tiene la funcionalidad de buscar la compatibilidad entre los equipos físicos de la red, además de regir la transmisión de bits. Sus características básicas son de tipo mecánicas, eléctricas, funcionales y de procedimiento.
Capa de enlace de datos	Si bien la capa física supervisa la parte de comunicación de datos, la capa de enlace busca la filtración de lo que se está comunicando. Supervisando detenidamente la detección y el control de errores que puedan surgir en la red.

Capa de datos.	En esta capa se gestiona las prioridades principales de la comunicación, donde el computador le solicita a la red algunos servicios y además le muestra la dirección de destino.
Capa de transporte	Tiene el mecanismo para la comunicación entre sistemas finales, esta capa es la encargada de realizar la entrega de los paquetes según sean enviados y evitar la duplicidad de paquetes; en esta capa se evidencia los protocolos de transporte, cada protocolo tiene una finalidad específica de uso.
Capa de Sesión	Busca la comunicación entre sistemas finales, pero con la posibilidad de realizar un diálogo seguro entre los sistemas finales. Entre sus principales servicios ofrecidos se tiene: Control de diálogo para realizar una comunicación simultánea en dos sentidos *(full-duplex*) o de manera alternada (*half-duplex*); el agrupamiento para definir el grupo de los datos y, por último, la recuperación para obtener la información donde se quedó en el último momento de la comprobación.
Capa de presentación	Define exclusivamente los diferentes tipos de datos que se van a intercambiar, redefiniendo y utilizando la presentación a utilizar.
Capa de aplicación	Brinda el medio por el que las aplicaciones van a poder tener comunicación con el modelo OSI. Esta capa cuenta con servicios exclusivos relacionados a las funciones administrativas y mecanismos para la implementación de sistemas distribuidos.

2.2.1.2. Arquitectura de protocolos: TCP/IP

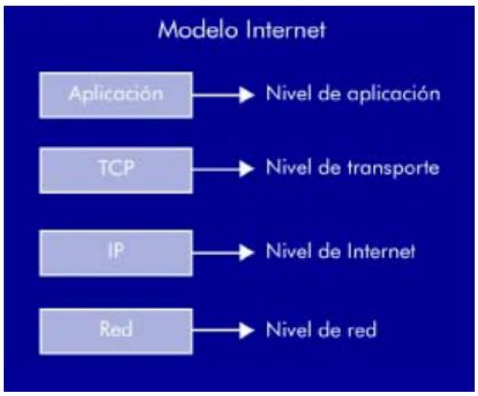
Esta arquitectura se desarrolló específicamente luego de la investigación realizada en la red experimental de ARPANERT. Conocido generalmente como la familia de protocolos TCP/IP. Este grupo de protocolos tiene la función específica de ser estándares de internet.

Barceló Et. al. (2004) mencionan que más que una arquitectura de protocolos, TCP/IP divide sus funcionalidades por niveles, estas partes se dividen en todo lo que hay por debajo de la IP, el IP, el TCP y lo que hay por encima del TCP (pp. 71-73).

- **Por debajo de IP:** Sencillamente este nivel está conformado por todos los equipos que tienen conexión a internet. Generalmente formado por una red WAN o LAN y comúnmente conocido cono nivel de red.
- **El IP:** Tienen la funcionalidad de direccionar y asignar cada dirección según corresponda su funcionabilidad. En este nivel se le asigna a cada equipo la unidad y la interconexión de las redes.
- **El TCP:** Este nivel tiene la función de brindar confiabilidad a la red, controlando el flujo de comunicación y evitando los errores que puedan presentarse. Únicamente este servicio solo se da a equipos que tienen conexión con internet, a razón que los equipos de conmutación como routers o switchs no presentan este nivel.
- **Por encima del TCP:** Corresponde a todas las aplicaciones que tiene la facultad de poder utilizar internet. Al ser un nivel de aplicación, solamente está enfocado en los usuarios de la red como son: FTP, correo electrónico, servidor www y clientes.

Figura 2

Niveles de arquitectura TCP/IP



Tomado de *Redes de computadoras* (p. 40), por Barceló Et. al., 2004. Eureca Media

Protocolos de transporte en la arquitectura TCP/IP.

Para la comunicación de redes de datos y la transmisión de paquetes en la red existen protocolos encargados de la comunicación en la red, entre los protocolos encargados de la comunicación y transporte de paquetes se tiene:

Tabla 2

Protocolos pertenecientes a la arquitectura TCP/IP.

Protocolo	Funcionalidad
ICMP	Encargado de enviar la información en datagramas (paquete de datos comprimido en un solo bloque), permitiendo a la familia de protocolos del TCP/IP realizar funciones como: control de flujos, detección de destinos lejanos, redireccionamiento de las rutas y realizar pruebas de conectividad con el punto que se busca comunicar (Crespo y Candelas, 1998, p. 75)
UDP	Brinda la posibilidad de enviar mensajes con facilidad y tiene una complejidad mínima. Algunas de las aplicaciones que son de transacciones utilizan este protocolo, principalmente la función que tiene es brindarle al IP la capacidad de identificar los puertos.
SMTP	Brinda los mecanismos necesarios para el envío de mensajes entre computadores, sus principales funciones están relacionadas a la lista de mensajerías, reenvío de un mensaje y gestión de recepciones.
FTP	Encargado del control de envío de archivos bajo la supervisión del usuario, pero verificando que la autenticidad del usuario sea la verídica. Con este protocolo se tiene control de mensajes en salida y en ingreso al sistema.

2.2.2. Direccionamiento IPv4 e IPv6

2.2.2.1. Concepto

Un direccionamiento o también conocido como camino de la red se compone de 32 bits, estos se dividen estrechamente en forma decimal, divididos en 4 grupos de tres

dígitos por grupo y separados por un punto, cada grupo lo conforma un número que puede iniciar en 0 y terminar en 255. Se debe dejar en claro que cada grupo se compone de 8 dígitos binarios (00000000 a 11111111), esto se realiza a razón que la red solo comprende dígitos binarios (Federación CC.OO., 2010, p.1).

2.2.2.2. Clases de direccionamiento IP

La comunidad internacional de internet determinó que la división de clases en direccionamiento IP se distribuya en 5 clases, solamente la arquitectura de protocolos TCP/IP soporta las clases A, B Y C que son asignadas directamente a servidores. Una clase tiene la funcionalidad de determinar la cantidad de bits que se van a asignar por red y a la ves la cantidad de bits que son asignados al servidor (Agramunt, s.f., p.6).

- **Clase A:** Se asignan preferentemente a redes que presentan un número grande de servidores. En este caso el bit de rango alto siempre debe presentar el valor de 0, mientras que el resto del primer octeto completan el identificador de la red. Por otra parte, los restantes 24 bits completan el identificador del servidor con quien se está comunicando.
- **Clase B:** Se asignan preferentemente a redes de tamaño mediano. En este caso el par de bits de rango alto siempre debe presentar el valor de 10, mientras que el resto de los dos primeros octetos se completan para representar el identificador de la red. Por otra parte, los restantes 16 bits completan el identificador del servidor con quien se está comunicando.
- **Clase C:** Se asignan preferentemente a redes de tamaño pequeño. En este caso, los tres bits de rango alto, siempre debe presentar el valor de 110, mientras que el resto de los tres primeros octetos se completan para representar el identificador de la red. Por otra parte, los restantes 8 bits completan el identificador del servidor con quien se está comunicando.

- **Clase D:** Conformado por el tipo de red multicast. En este caso, los cuatro bits de rango alto siempre deben presentar el valor de 1110, mientras que el resto de los bits son destinados para servidores que se consideren interesantes de reconocer.
- **Clase E:** Conformado por todas las direcciones experimentales, estas pueden ser utilizadas posteriormente. En este caso, los cuatro bits de rango alto siempre deben presentar el valor de 1111.

Figura 3

Direcciones IP reservadas.

Clase	Rango inicial	Rango Final	Mascara
Clase A	1.0.0.0	126.0.0.0	255.0.0.0
Clase B	128.0.0.0	191.255.0.0	255.255.0.0
Clase C	192.0.0.0	223.255.255.0	255.255.255.0

Tomado de *Direccionamiento IP cálculo de redes TCP/IP* (p. 7), por Agramunt, V. s.f.

2.2.2.3. Direccionamiento IPv4.

Bejarano, Miranda y Henríquez (2008) la arquitectura de protocolos TCP/IP trajo consigo en los años 80 el elemento de mayor importancia actualmente, el direccionamiento de host, conocido comúnmente como direccionamiento IP, constando de 32 bits divididos en 4 grupos de 8 bits por grupo. El desarrollo de este esquema presenta características específicas como la utilización de las clases, de las cuales solo se utilizan las tres primeras; la división de los dos grupos, el primero dirigido a la red o subred, mientras que el otro grupo se dirige para el host o servidor (p. 3).

La limitante de este direccionamiento surgió por el número de bloques de divisiones, muchas de las direcciones se desperdiciaron en direcciones públicas, disminuyendo exponencialmente el crecimiento de la internet, a razón de las direcciones destinadas a computadores, fax, impresoras, móviles, etc. Por otra parte, se sumaba a ello, los servicios múltiples de vos, video, datos, etc. Generando que la cantidad de direcciones

IP públicas comiencen a limitarse y la falta de disponibilidad sea muy abismal.

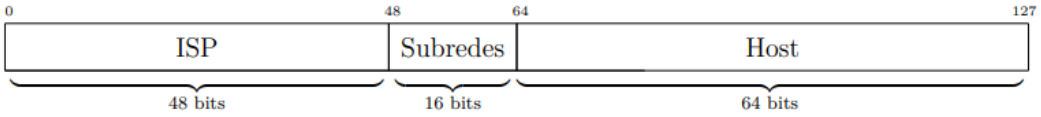
2.2.2.4. Direccionamiento IPv6.

Luke (2019) la principal característica de cambio que se realizó de versión de ipv4 a ipv6 se fundamenta en el número de bits, pasando de 32 a 128. Un cambio que ha generado que el direccionamiento pareciera alterarse, pero con la facilidad de generar múltiples rutas disponibles. Otro paso importante se da por la división de los grupos de cuatro dígitos con números hexadecimales y ya no usando números decimales, quedando finalmente 8 grupos de 4 dígitos (p. 21).

Luke (2019) con el desarrollo del direccionamiento IPv6 se consiguió liberar la cantidad de rutas restringidas por la versión 4, pero en el caso de la máscara de red esta guarda la funcionalidad de la versión 4, con ciertos cambios como la distribución de bits destinados a la red y destinados al host. En este caso 48 bits del nivel más alto se reservan para el enrutamiento de la red, luego los 16 bits que continúan les pertenecen a las subredes. Por último, los 64 bits restantes están destinados al enrutamiento del host o direccionamiento del servidor (p. 21).

Figura 4

Distribución de bits relacionados a IPv6



Tomado de *Guía sobre direccionamiento IP, subredes y enrutamiento.* (p. 22), por Luke, J.P., 2019. Creative Commons

2.2.3. Firewall.

2.2.3.1. Conceptos

Cisco (s.f.) afirma lo siguiente: Un firewall es un dispositivo de seguridad de la red que monitoriza el tráfico entrante y saliente, este decide si debe permitir o bloquear un tráfico específico en función de un conjunto de restricciones de seguridad ya

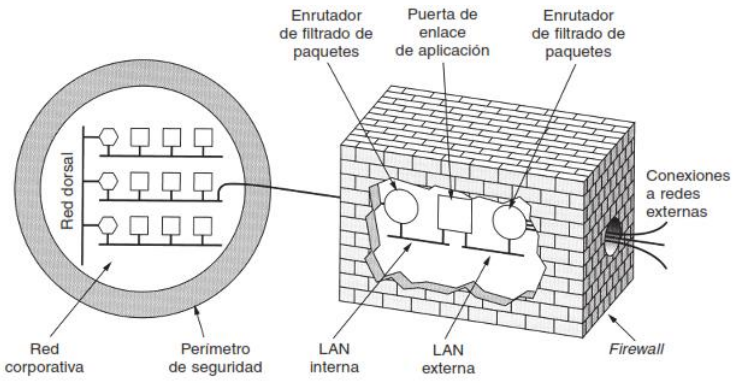
definidas.

UIT (2005) indica que un firewall o cortafuegos, es un dispositivo de hardware o un software que nos permite gestionar y filtrar la totalidad de tráfico entrante y saliente entre 2 redes u ordenadores de una misma red. Si el tráfico entrante o saliente cumple con una serie de reglas que nosotros podemos especificar, entonces el tráfico podrá acceder o salir de nuestra red u ordenador sin restricción alguna. En caso de no cumplir las reglas, el tráfico entrante o saliente será bloqueado.

De igual manera Pacotaype (2018) afirma de manera similar que: *“Firewall es una herramienta de software o hardware que filtran todas las conexiones que ingresan a la red interna de la organización o que se dirigen hacia el exterior de la misma*”. (p.25)

Figura 5

Firewall como filtrador de paquetes



Tomado de *Redes de computadoras.* (p. 777), por Tanenbaum, A, 2003. PearsonEducación.

2.2.3.2. Tipos de Firewall.

Firewall por software.

Un firewall gratuito es un software que se puede instalar y utilizar libremente, en la computadora. Son también llamados “Desktop firewall” o “Software firewall”.

Son firewalls básicos para pequeñas instalaciones hogareñas o de oficina

que monitorean y bloquean, siempre que sea necesario el tráfico de internet.

Los programas de firewall se usan ampliamente en los hogares, aunque muchas veces son utilizados en organizaciones, pero, su uso está limitado a ciertas características de los computadores, muchos están restringidos al tipo de sistema operativo y el tipo de red. Muchos de estos softwares también presentan cierta incomodidad porque consumen recursos adicionales de los computadores, otros tienen la dificultad de ejecutarse (Roca y Pereira, s.f., p.7).

Características de un firewall por software son:

- Los firewalls gratuitos se incluyen con el sistema operativo y normalmente son para uso personal.
- Pueden ser fácilmente integrados con otros productos de seguridad.
- No necesitan de hardware para instalarlo en la computadora.
- Un firewall por software es lo más básico en materia de seguridad que debe existir en una computadora y no hay razones que justifiquen la no utilización de por lo menos un desktop firewall.

Figura 6

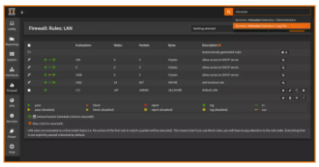
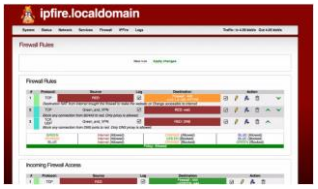
Firewall por software

Principales firewalls por software.

Fernández (2020), considerando que el cortafuego y protector de información de mayor importancia es un firewall, se debería considerar la utilización de un firewall como mínimo, tanto a nivel de hogar como a nivel empresarial. Por ello, se mencionan los principales firewalls por software según el tipo de producto y la seguridad registrada en los últimos años.

Tabla 3

Principales firewalls de software

Firewall	Características	Imagen
Pfsence	- Funcionalidades de routing y avanzado. - Disponibilidad de cliente servidor con VPN. - Monitoreo de red con gráficos y logs - Servidor DNS - Servicios DHCP.	
OPNSence	- Utilización de servicios routing con NAT. - Balanceador de carga. - Sistema IDS/IPS Suricata	
IpFire	- Modularidad y flexibilidad. - Sirve como servidor proxy - DNS dinámico - Servicios DHCP.	

Firewall por Hardware.

Los dispositivos firewalls son utilizados generalmente en organizaciones grandes o empresas que requieren la seguridad de información o el control de sus

usuarios, cortafuegos de la internet, etc. Su costo es muy grande y su efectividad es mucho más amplia. Cuando una organización requiere el servicio instala el dispositivo entre el router y la salida a la internet, generando la interferencia de la red filtrando todos los paquetes, por otra parte, no cualquiera puede configurar un firewall físico, debido a que se necesita de códigos necesarios o herramientas adicionales para la configuración pertinente (Roca y Pereira, s.f., p.7).

Existen ciertos firewalls por hardware que vienen normalmente instalado en los routers que utilizamos para acceder a internet, lo que significa que todas las computadoras que estén detrás del router estarán protegidas por un firewall que está incluido en el dispositivo. La configuración de un firewall por hardware es más compleja que una instalación de un firewall por software y, es normalmente realizada a través del navegador que se utiliza para acceder a internet (RedFibra, 2020).

Figura 7

Representación de un firewall por hardware

Principales firewalls de hardware.

TotalPlay (2019), la página de total play realiza una recopilación de los principales firewalls que son utilizados por las compañías para proteger la seguridad de sus organizaciones y mantener el control de la gestión en su red, dicha página realizó una lista de los principales firewalls de este tipo.

Tabla 4

Principales firewalls de hardware.

Firewall	Características	Imagen
CISCO	- Monitoreo de tráfico antes de que ingrese a la red local. - Control remoto de la aplicación. - Ancho de banda de un GBIT. - Admite detecciones IDS/IPS.	
Firewalla	- Fácil instalación - Interfaz de usabilidad sencilla. - Protección de la seguridad cibernética.	
Zyxel Cortafuegos VPN	- Posibilidad de configurar 10 VPNs - Servicio Zyxel para actualizaciones gratuitas. - Instalación guiada.	

2.2.4. Vulnerabilidades y amenazas en la red.

2.2.4.1. Vulnerabilidades.

Una vulnerabilidad es un fallo o debilidad de un sistema de información que pone en riesgo la seguridad de la misma. Se trata de un “agujero” que puede ser producido por un error de configuración, una carencia de procedimientos o un fallo de diseño. Los ciberdelincuentes aprovechan las vulnerabilidades de los sistemas informáticos (por ejemplo, los sistemas operativos) para poder entrar en los mismos y realizar actividades ilegales, robar información sensible o interrumpir su funcionamiento. Las vulnerabilidades son una de las principales causas por las que

una empresa puede sufrir un ataque informático contra sus sistemas (Ambit, 2020).

Tipos de vulnerabilidades

- **Vulnerabilidades físicas**

  Las vulnerabilidades físicas son las que van a afectar a la infraestructura de la organización de manera física y se pueden mencionar en este tipo de clasificación a los desastres naturales.

- **Vulnerabilidades lógicas**

  Las vulnerabilidades lógicas son las que van a afectar directamente la infraestructura y el desarrollo de la operación de estos, estas pueden ser de:

  - Configuración
  - Actualización
  - Desarrollo

  Existen algunos tipos de vulnerabilidades que son mecanismos aprovechados por los atacantes para infectar una red o robar información entre los cuales se puede mencionar a los siguientes tipos:

- **Errores de configuración**

  Otra de las principales vulnerabilidades, son los errores de configuración, se puede mencionar, por ejemplo, los password por default, password débiles, usuarios con demasiados privilegios e inclusive la utilización de protocolos de encriptación obsoletos.

- **Errores web**

  Otros tipos de vulnerabilidades son las WEB, aquí simple y sencillamente se tiene errores de validación de input, Scripts inseguros, errores de configuración de aplicaciones web, entre algunas otras situaciones, que a final de cuenta todos y cada uno de esos errores son los medios para algún ataque de XSS (Cross Site Scripting) o inyección SQL.

- **Errores de protocolo**

  En las vulnerabilidades de protocolos, existen diversas cantidades de protocolos que normalmente fueron definidos sin la necesidad o sin tener en cuenta precisamente la parte de la seguridad y en muchas veces no se previó el crecimiento que estos iban a tener y, como el internet no estaba preparado para ser tan grande, no se pensó en la parte de la seguridad (Romero Et. al., 2018).

2.2.4.2. Amenazas.

Las organizaciones, sus redes y sistemas de información enfrentan crecientes amenazas a su seguridad entre las cuales se incluyen: fraude asistido por computadora, actos de espionaje, sabotaje, vandalismo y hasta incendios e inundaciones. En este contexto, amenaza puede ser definido como todo aquel evento cuya ocurrencia podría impactar en forma negativa en la organización (Caballa y torres, 2010).

Tipos de amenazas.

Techclub (2017) cataloga los tipos de amenazas según varias características:

- **Naturales**

  Son todas aquellas vulnerabilidades que están relacionados con las condiciones de la naturaleza ya que no es constante y pueden poner en riesgo la información. Estas amenazas naturales son principalmente determinantes por la elección del lugar y montaje de un sistema. Por lo cual, se deberán tomar cuidados especiales con el local, un ejemplo: Ambientes sin protección contra incendios, prevención de los mismos, infraestructura incapaz de resistir a las manifestaciones de la naturaleza como: terremotos, maremotos, huracanes, etc.

- **Hardware**

  En este tipo de vulnerabilidad es causado por los posibles defectos de fabricación

o configuración de los equipos que utilice un sistema, los cuales puedan permitir el ataque o alteración de los mismos. Por ello, la seguridad de la información busca evaluar: si el hardware utilizado está dimensionado correctamente para sus funciones. Si posee área de almacenamiento suficiente, procesamiento y velocidad adecuada.

- **Almacenamiento**

  Los medios de almacenamiento son principalmente los soportes físicos o magnéticos que se utilizan para almacenar la información. Si los soportes que almacenan información, no se utilizan de forma adecuada, el contenido en los mismos podrá estar vulnerable a una serie de factores que podrán afectar la integridad, disponibilidad y confidencialidad de la información.

- **Software**

  Considerados como puntos débiles en aplicaciones o programas que permiten que ocurran accesos indebidos a sistemas informáticos, normalmente sin el conocimiento de un usuario o administrador de red. Una de las causas principales de este tipo de vulnerabilidad es la descarga de programas de sitios no confiables, configuración e instalaciones indebidas de estos u otros programas no testados en un PC, que podrán llevar al uso abusivo de los recursos por parte de usuarios mal intencionados. A veces la libertad de uso implica el aumento del riesgo.

- **Humanas**

  Este tipo de vulnerabilidad está relacionada con los daños que las personas pueden causarle a la información y al ambiente tecnológico que la soporta. Este tipo de vulnerabilidades de tipo humana pueden ser intencionales o no. La mayor vulnerabilidad es el desconocimiento de las medidas de seguridad adecuadas para ser adoptadas por cada elemento constituyente, principalmente los

miembros internos de una empresa. Entre los puntos débiles humanos por su grado de frecuencia están: la falta de capacitación específica para la ejecución de las actividades o funciones de cada uno y la falta de conciencia de seguridad para las actividades de rutina.

- **Comunicación**

  La información se puede transmitir por distintos medios físicos, ya sea vía cable, satélite, fibra óptica y ondas de radio. El éxito en el tránsito de los datos es un aspecto crucial en la implementación de la seguridad de la información. En un sistema de una empresa, puede haber un gran intercambio de datos a través de medios de comunicación que rompen barreras físicas tales como teléfono, internet, WAP, fax, télex etc. Siendo estos medios considerados los más vulnerables en la comunicación de la información, por lo que deberán recibir tratamiento de seguridad adecuado con el propósito de evitar que: cualquier falla en la comunicación haga que una información quede no disponible para sus usuarios, por el contrario, deben estar disponible para quien no posee derechos de acceso.

2.2.5. Seguridad de la información.

Vega (2021) menciona que, existe una gran cantidad de definiciones relacionadas a la seguridad de la información, actualmente los tiempos son difíciles y la información esta que juega un papel muy importante en nuestra sociedad, tanto las empresas como las personas buscan realizar la mayoría de sus actividades al frente de un ordenador y, toda la información que guardan la almacenan en dispositivos móviles, PCs, laptops, etc. Esto ha generado que se tenga una gran cantidad de amenazas contra la información; si bien la internet es el medio por el cual se obtiene mucha información, no se le quita la gran cantidad de amenazas que produce en una empresa, un solo click

sobre un acceso de riesgo, puede generar la filtración de muchos virus sobre la red y terminar robando la información de vital importancia (p.9).

ISO 27001 (2016) considera que la seguridad de la información está conformada por el grupo de buenas prácticas y métodos relacionados a evitar todo riesgo que puede generar la pérdida, destrucción y uso indebido de la información.

2.2.5.1. Seguridad informática.

La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sea utilizado de la manera en que decidió, además, que el acceso a la información sea la que este allí contenida. Teniendo la capacidad de realizar modificación solo a las personas que se encuentren acreditadas y dentro de los límites de su autorización. Para que un sistema se pueda definir como seguro debe tener estas cuatro características:

- **Integridad:** La información solo puede ser modificada por quien está autorizado y de manera controlada.
- **Confidencialidad:** La información solo debe ser legible para los autorizados.
- **Disponibilidad:** Debe estar disponible cuando se necesita.
- **Seguridad:** Mostrá protección para manipulación.
- **Irrefutabilidad (No repudio):** El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción (Grajales, 2011, p. 20).

2.2.5.2. Políticas de seguridad de la información:

Vega (2021) todo lineamiento relacionado con la seguridad de la información,

norma que establezca las dimensiones relacionadas a la seguridad y procedimientos que garanticen una seguridad eficiente, se consideran como políticas de seguridad (p. 87).

La norma que establece la seguridad de la información o data es la ISO 27001, indicando las métricas necesarias al momento de realizar cualquier procedimiento o instalación de equipos relacionados con la información.

ISO 27001 (2016) indica que con el fin de una organización es la preservación, cuidad y protección de la información, si bien es un recurso intangible, se considera el activo de mayor importancia en una organización. Por tal razón, la ISO 27001 busca medir las dimensiones principales en la instalación de cualquier equipo tecnológico que busque el cuidado, protección o preservación de la información.

2.2.5.3. Dimensiones relacionadas a la ISO 27001.

- **Confidencialidad:** Acceso a la información únicamente por el personal que tenga los permisos para la manipulación de la data.
- **Verificación y la autorización:** Mecanismos para realizar la verificación del usuario quien ingresa y autorización de realizar actividades permitidas según sea el usuario.
- **Disponibilidad:** Se refiere a la información solicitada por los usuarios, esta debe estar siempre cuando lo solicite el usuario con los permisos respectivos, además que el tratamiento de los datos siempre debe estar autorizado al usuario que lo requiera y cuente con los permisos necesarios.

Figura 8

Secuencia de las políticas de seguridad

Tomado de *Gestión de la seguridad de la información* (p. 88), por Silva, Segadas y Kowask, 2010. RedCedia

2.2.6. Ataques informáticos.

Mieres (2009) habla de ataque informático, a todo hecho o acto que atenta contra la seguridad y las vulnerabilidades de una red de datos o un software, en su mayoría estos ataques están orientados en buscar el beneficio económico, buscando la vulnerabilidad de la información en una empresa. Es de mucha importancia conocer cuáles son los diversos tipos de ataques informáticos que existen, esto ayudará a una organización a comprender cuales son los puntos de mejora a tener en cuenta y evitar posibles ataques que perjudiquen su organización (p. 4).

2.2.6.1. Etapas de un ataque informático

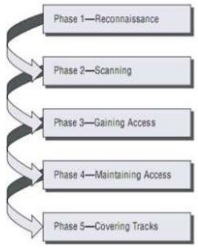
Mieres (2009) también menciona que es de vital importancia conocer las etapas de un ataque informático, brindando la posibilidad de adelantarse a los hechos y cerrando las vulnerabilidades que busquen perjudicar una organización, entidad o empresa (p. 5).

- **Reconocimiento:** Es la etapa inicial de un ataque, donde el atacante busca conocer o sacar información de una organización o persona. La mayoría busca la información de servicios como google o utiliza ataques relacionados al Diving, Sniffing, ingeniería social, etc.

- **Exploración:** Una vez la información se encuentre en manos del ataque, este procederá a obtener información sobre los accesos al software o hardware que busca vulnerar, obteniendo información relacionada a las direcciones IP, direcciones de enrutamientos de paquetes, direcciones de hosts, información sobre autenticación, etc. Algunas de las herramientas utilizadas en este proceso son: port scanner, network mappers, vulnerability scanner, etc.
- **Obtención de accesos:** Se materializa el ataque en relación a los equipos físicos de la organización, buscando toda vulnerabilidad que este al descubierto o que no cuente con la seguridad necesaria para poder realizar el ataque. Algunos de los softwares utilizados en este proceso son: Denial of Service, Password filtering, Session hijacking, etc.
- **Mantener el acceso:** Cuando el ataque está completado, este buscará de cualquier otro modo nuevamente ingresar al sistema, dejando utilidades que servirán para ingresos futuros, entre las principales utilidades se tiene: troyanos, backdoors, rootkits, etc.
- **Borrar las huellas:** Al momento que el atacante consiguió su cometido buscará la manera de dejar todo en orden y borrar toda huella que ha dejado. El fin del borrado de huellas es seguir ingresando al sistema o red, pero sin ser detectado.

Figura 9

Fases de un ataque informático



Tomado de *Ataques informáticos. debilidades de seguridad comúnmente exploradas.* (p. 5), por Mieres, J., 2009. EvilFingers

2.2.6.2. Tipos de ataques informáticos.

INCIBE (2020) menciona sobre los principales ataques cibernéticos que existen actualmente en esta sociedad, ayudando en tal sentido a que las organizaciones, empresas y personas tengan mayor cuidado con la protección de su información y recursos que son de mucha importancia.

1. **Ataques a contraseñas**

   Directamente relacionado con el uso de contraseñas similares, muchos usuarios consideran que la usabilidad de la misma contraseña para diversas cuentas beneficia recordar su información, pero lo que hace es perjudicar su seguridad.

   - **Fuerza Bruta:** Adivina la contraseña en un ensayo y error, solicitando peticiones, busca vulnerar la contraseña y obtener la información.
   - **Ataque por diccionario:** Utilización de un software que a través de las constantes peticiones de búsquedas obtiene la información.

2. **Ataques por ingeniera social**

   La relación de los ataques de ingeniera social con el uso de la palabra y manejo del lenguaje tienen una relación muy estrecha.

   - **Phishing, Vishing y Smishing:** Envío de mensajes con información de mucha importancia y con el logo de una página que es una entidad conocida.
   - **Baiting o Gancho:** La utilización de un recurso denominado cebo, para poder llegar a la información que se trata robar.
   - **Shoulder surfing:** Se utiliza un conocido para la manipulación de la víctima.
   - **Dumpster Diving:** Conocido como la búsqueda de la basura. Encontrar recursos desechados pero que contienen información importante.
   - **Spam:** Anuncios publicitarios relacionados con información interesante que

busca conocer tus cuentas principales.

3. **Ataques a las conexiones.**

Un ataque de mucho poder tecnológico, buscan infiltrarse en la información de la empresa y conseguir de cualquier manera su objetivo. Este ataque está relacionado con ataques a los servidores de reconexiones, puntos de acceso, nodos, etc.

- **Redes trampa:** Se crea una red wifi de igual nombre, pero de uso libre, en esta red los usuarios ingresarán y colocarán sus datos.
- **Spoofing:** Técnicas de utilización de hacking para suplantar la identidad de otra persona.
- **IP Spoofing:** Altera la dirección IP que se comunica con el router y se salta la protección.
- **Web Spoofing:** Suplantar una página web que contiene información de mucha importancia.

4. **Ataques a las cookies**

La especialidad de estos ataques está relacionada con la información de las páginas visitadas, historiales de navegación, idioma, anuncios vistos, etc.

5. **Ataques DDoS**

Conocido comúnmente cono ataque de denegación de servicios, consiste en un ataque simultáneo de diversos equipos con el fin de detener un servidor o la red en donde se ejecuta el ataque.

- **Inyección SQL:** Un gran número de páginas web tiene una conexión a una base de datos, algunas de estas son de SQL, el ataque consiste en alterar las líneas de código para ocasionar una caída en el servidor.
- **Escaneo de puertos:** El portscan es una técnica relacionada al análisis de las puertas de ingreso en la red, analizando que puertas de acceso se tienen

abiertas y cuáles no.

- **Man in the middle:** La interferencia se genera al momento en que el atacante se posiciona entre los usuarios y el servidor.
- **Sniffing:** Realiza el monitoreo de una red, comprendiendo el flujo de la información y captando la data.

6. Ataques por malware

Este tipo de ataques lo conforman los programas encargados del robo de la información, ralentización de servicios y toma de control de la información.

- **Virus:** Diseñado para generar problemas al replicarse sin autorización.
- **Adware:** Muestra anuncios que no son permitidos por el usuario.
- **Spyware:** Escanea la información personal y la reenvía a un usuario remoto.
- **Troyanos:** Se infiltran en un equipo para realizar ataques de ingeniera social.
- **Backdoors:** Si se instalan en un equipo el delincuente tendrá el control total.
- **Stealers:** Analiza las credenciales del sistema y hace un seguimiento al usuario.
- **Ransomeware:** Cifra todo el dispositivo tomando el control del pc y solicitar accesos para ingresar.
- **Gusano:** Si se ejecuta en el sistema, la mayoría de veces altera el código del programa.
- **Rootkit:** Busca acceder al sistema de forma ilícita.
- **Botnets:** El uso de varios equipos infectados y controlados por ciberdelincuentes.
- **Rogueware:** Software que simula ser un antivirus o herramienta para

seguridad, mas su finalidad es el robo de la información.

- **Criptojacking:** Son softwares maliciosos que los delincuentes instalan en las computadoras para generar criptomonedas.
- **Apps maliciosas:** Softwares aparentemente de uso beneficioso pero su fin es destruir, robar o modificar la información.

2.2.7. IpTables y NetFilter.

2.2.7.1. Concepto.

El trabajo con firewalls se relaciona directamente con IpTables, siendo una herramienta que trabaja con servidores Linux y sirve para llevar el control del firewall, realizando modificaciones, tratamiento de filtros. Esta herramienta estrechamente trabaja de la mano del filtrado de la herramienta NetFiltrer (Lerena, 2001, p. 4).

IpTables trabaja como el backend que permite manejar las reglas de seguridad de un firewall, usando un lenguaje de tipo definido. La programación que es utilizada en IpTables es de tipo lineal y tiene una relación de orden con las líneas de código.

2.2.7.2. Comandos de uso básico en IpTables.

Al momento de realizar condicionamientos en el firewall, estas deben presentar la nomenclatura y las reglas de escritura exacta según lo requiere el firewall.

Figura 10

Principales comandos de IpTables.

Comando	**-A, --append**
Ejemplo	**iptables -A INPUT ...**
Explicación	Agrega una regla a una cadena especificada

Comando	**-D, --delete**
Ejemplo	**iptables -D INPUT --dport 80 -j DROP, iptables -D INPUT 1**
Explicación	Borra una regla de una cadena especificada. Se le puede pasar como argumento toda la regla la cual deberá coincidir exactamente con la existente o el número de línea que ocupa en la cadena.

Comando	**-R, --replace**
Ejemplo	**iptables -R INPUT 1 -s 192.168.0.1 -j DROP**
Explicación	Reemplaza una regla. Se le pasa como argumento el numero de linea dentro de la cadena y la nueva regla

Comando	**-I, --insert**
Ejemplo	**iptables -I INPUT 1 --dport 80 -j ACCEPT**
Explicación	Inserta una regla en el lugar de la cadena que le pasemos como argumento. Recordemos que in IPTables es de suma importancia el orden en que estan las regla dentro de las cadenas.

Comando	**-L, --list**
Ejemplo	**iptables -L INPUT**
Explicación	Muestra las reglas que contiene la cadena que le pasemos como argumento.

Comando	**-F, --flush**
Ejemplo	**iptables -F INPUT**
Explicación	Borra todas las reglas de una cadena.

Comando	**-Z, --zero**
Ejemplo	**iptables -Z INPUT**
Explicación	Pone en cero todos los contadores de una determinada cadena

Comando	**-N, --new-chain**
Ejemplo	**iptables -N allowed**
Explicación	Permite al usuario crear su propia cadena. En este ejemplo la cadena se llamará “allowed”

Tomado de *Manual de uso de IpTables* (p. 1), por Kleinerman, s.f.

2.2.7.3. Cadenas de Iptables

Son cada lugar donde se va a conocer toda regla de las políticas de seguridad de la organización. Muchos paquetes son filtrados en el firewall, pero cuando el paquete atraviesa el firewall, pasa a la interfaz de salida o, de entrada, por ello las cadenas de ipTables localizan la mejor opción para filtrado de paquetes. Existe la facilidad de crear cadenas de usuario, donde la filtración del paquete se da en relación a la organización quien envía el paquete y la comunicación con la propia organización (Lerena, 2001, p. 6).

2.2.8. Metodologías para la implementación de un firewall

El desarrollo o la implementación de un dispositivo tecnológico o diseño de red, debe contener la una metodología relacionada con el conocimiento del desarrollador.

Metodología Top Down

Empleada ampliamente en la implementación de circuitos, diseños de red, desarrollos de productos, etc. La metodología desmenuza toda la aplicación en módulos, donde se especifica lo que se ha realizado en relación a la acción tecnológica. Con la metodología Top Down se optimiza la implementación y se genera la pérdida de mucho dinero (Restrepo, 2009, p.27).

Saavedra (2017) indica sobre las fases de la metodología Top Down.

Tabla 5

Fases para la implementación de la metodología Top Down

Fase	Actividades
Requerimientos	Se analiza todas las metas del negocio y se verifica la red con la que cuenta la empresa del proyecto.
Diseño lógico	Diseña la topológica de la red, switching, routing, hostname y direccionamientos.

Diseño físico	Se selecciona los equipos participantes en la red
Pruebas	Se analiza si el diseño lógico se relaciona con el físico.
Implementar la red	Se implementa la red
Monitoreo	Se verifica que el funcionamiento de la red sea el correcto y si el diseño lógico se alinea al diseño físico.

Metodología Bottom Up

Reúne diferentes ideas para conceptualizar el diseño de la red, donde los sistemas se unen para lograr un todo. La metodología Bottom Up se asemeja a un modelo de semilla, debido a que se va formando con muchos componentes y termina con un sistema completo (Restrepo, 2009, p.24).

Economía (2011) indica sobre las fases de la metodología Bottom Up

Tabla 6

Fases para la implementación de la metodología Bottom Up

Fase	**Actividades**
Análisis	Se realiza un análisis general de la red y se conoce todos los puntos de conexión presentes, si se requiere modificar la red se solicita los requerimientos de modificación.
Implementación	Se implementa el diseño lógico y físico de la red en relación a los siguientes puntos: • Diseño lógico • Simulación • Diseño físico • verificación
Optimización	Se optimiza y se supervisa si la red trabaja en relación a los requerimientos solicitados. • Comprobar la integración de bloques • Verificaciones de la red

2.2.9. Definición de términos básicos.

Tráfico de red

Tráfico es un concepto que tiene su origen en un vocablo italiano que se refiere al tránsito o desplazamiento de medios de transporte por algún tipo de camino o vía. El concepto de tráfico puede hacer mención tanto a la acción del movimiento como a las consecuencias de dicha circulación. Por tanto, el tráfico de red se puede definir como la cantidad de información o datos enviados y recibidos por todos aquellos equipos de una red computadoras (Duarte y Paredes, 2016)**.**

Sistema de detección de intrusos

Detección de rupturas o intentos de rupturas bien sea manual o vía sistemas expertos de software que atentan contra las actividades que se producen en la red o contra la información disponible en la misma.

Ataque interior

Un ataque originado desde dentro de la red protegida.

Uso de Firewalls

Es un dispositivo de hardware o un software que nos permite gestionar y filtrar la totalidad de tráfico entrante y saliente que hay entre 2 redes u ordenadores de una misma red.

Autenticación

El proceso para determinar la identidad de un usuario que está intentando acceder a un sistema.

Autorización

Proceso destinado a determinar qué tipos de actividades se permiten. Normalmente, la autorización, está en el contexto de la autentificación: una vez autentificado el usuario en cuestión, se les puede autorizar realizar diferentes tipos de acceso o actividades.

2.3. Hipótesis de la investigación

H_i: La implementación de un firewall de seguridad influye positivamente en el control de accesos y protección de la red de datos en la empresa Ferretería Soto.

2.4. Operacionalización de variables

- **Variable independiente:** Implementación de un firewall.
- **Variable dependiente:** Control de accesos y protección de red de datos.

Tabla 7

Cuadro de operación de variables.

Variable	Definición	Definición Operacional	Dimensión	Indicador	Instrumento
Implementación de un firewall.	El cortafuegos o firewall en inglés, en el mundo de la informática es un sistema de seguridad para bloquear accesos no autorizados a un ordenador mientras sigue permitiendo la comunicación de tu ordenador con otros servicios autorizados (Fernández, 2019).	Se refiere a la configuración del firewall para controlar el acceso de los usuarios y malware a la red de datos.	Políticas	Número de virus	Cuestionarios. Hojas de Cotejo.
			Seguridad	Número de casos de usuarios que vulneran las políticas.	
Control de accesos y protección de red de datos.	La seguridad en una red de datos no se basa en un solo método concreto, sino que	Son políticas de seguridad que se usan para proteger los datos	Integridad	Casos de manipulación no autorizada	
			Seguridad	Casos de divulgación	

	utiliza un conjunto de barreras que defienden la infraestructura de diferentes formas; está permitirá: Proteger la infraestructura contra ataques informáticos, garantizar la privacidad, controlar el acceso a la información, trasformar la red en una zona confiable (Lisot, 2018).	sensibles de una red LAN y WAN.		de información no autorizada. Confidencialidad.
			Disponibilidad	Casos de problemas de servicios de TI

CAPÍTULO III: MÉTODO DE INVESTIGACIÓN

3.1. Tipo de investigación

La investigación es de tipo aplicada - tecnológica, a razón que se realizó la implementación de un firewall de hardware para realizar la medición de control de seguridad y proteger la red ante cualquier amenaza, por el lado de la investigación tecnológica, el uso de los dispositivos implementados y manipulados en la investigación presenta muchos aspectos en tecnología, generando una investigación de mucho aspecto tecnológico.

Hernández, Fernández y Baptista (2014). El presente estudio reúne las condiciones metodológicas de una investigación aplicada, ya que busca el porqué de los hechos, estableciendo relaciones de causa- efecto. Observa, analiza e interpreta el problema guardando relación básica, porque usa conocimientos para implementar políticas de seguridad lógica con el fin de mejorar la seguridad y acceso a la red interna (p. 42).

Espinoza (2010) una investigación tecnológica genera conocimiento experimental, a causa que la implementación del recurso involucra un proceso de tecnología, aprendizaje, producción y presentación de información. Toda investigación tecnológica presenta un gran número de recursos tecnológicos enfocados en el avance y desarrollo de la ciencia (pp. 29-30).

3.2. Diseño y método de la investigación

La investigación tiene un diseño no experimental, a razón que, si se consideró investigar el impacto que genera la implementación de un firewall sobre el control de accesos y protección de la red de datos, no existirá ninguna manipulación de las variables, a razón que el cuestionario es el único instrumento utilizado para contrastar la hipótesis, realizando un muestreo no probabilístico.

Hernández, Fernández y Baptista (2018) indican que, en un diseño no

experimental, la manipulación de las variables queda obsoleta, debido a que los fenómenos son analizados y medidos sin alterar ninguna variable. Además, los datos obtenidos son suficientes para demostrar o negar la hipótesis planteada. “El diseño no experimental no presenta la intención de realizar manipulaciones sobre ninguna de las variables, de otro modo, tiene el objetivo de observar, medir y presentar un fenómeno en su medio natural. (pp. 152-154).

Según Hernández, Fernández y Baptista (2014) indican que el diseño no experimental en la investigación, es como el plan o la estrategia concebida para responder las preguntas de investigación. El diseño señala al investigador lo que debe se debe hacer para alcanzar sus objetivos de estudio, contestar las interrogantes que se ha plantado y analizar a certeza la hipótesis formulada en un contexto particular (p. 128).

3.3. Enfoque de la investigación

La investigación tuvo un enfoque cuantitativo, debido a que se realizó un análisis secuencial de la implementación del firewall. En este caso la implementación de un firewall no puede saltar ninguna de sus fases, debido a que, si la configuración se realiza de otro modo, el dispositivo no protegerá la red de la manera que se debe.

Hernández, Fernández y Baptista (2014) indican que el enfoque cuantitativo se da en investigaciones que no se puede alterar el orden secuencial de los procesos, cuando la investigación tiene que cumplir rigurosamente cada parte investigativa (p. 4).

3.4. Área de investigación.

Todo el desarrollo de la investigación se ejecutó en la Ferretería Soto, cumpliendo con los requerimientos establecidos según la empresa requería, además que, para la implementación del firewall se tuvo un ambiente controlado y separado para realizar

mejor las configuraciones, mediciones y actualizaciones de la seguridad de la información.

3.5. Población

Debido a que la investigación busca medir la influencia que ha generado, la implementación del firewall sobre la seguridad de la red y el control de accesos que esta presenta, se tomó como población el número total de administrativos de la ferretería Soto, los mismos que a través del cuestionario verificaron si el firewall instalado proporciona una seguridad confiable en la red y si se realiza un control debido con los accesos a la red. Asimismo, se ha considerado solamente el análisis de protocolo ICMP (protocolo de control de acceso de mensajes de internet) y el protocolo TCP/UDP (protocolo de control de transporte), facilitando que la verificación por parte de los administrativos pueda ser sencilla ya que se está restringiendo solamente la consultas y peticiones con los servidores.

Hernández, Fernández y Baptista (2014) la población está conformada por el grupo de individuos o cosas que van a tener participación en una investigación, si el universo es muy amplio se especifica quién, quiénes o qué la conforman (p. 174).

Tabla 8

Personal perteneciente a la población

Personal Administrativo	Cargo
Elio Roger Soto Sánchez	Gerente General
Eduardo Soto Cotrina	Administrador
Carlos Chillón Cabrera	Jefe de logística
Milagros Bada Mejía	Asistente de Logística
Clarita Cerquin Torres	Jefe de contabilidad
Lourdes Martos Álvarez	Asistente de contabilidad
Cintia Pizarro Acuña	Créditos y Cobranzas

3.6. Muestra

A razón que, el grupo de administrativos de la empresa solamente se conforma por 7 administrativos, estos son los únicos que tendrán participación en la investigación, a la vez que los datos proporcionados por su persona, brindarán resultados para la medición de la influencia que genera la implementación del firewall sobre el control de accesos y protección a la red. En tal sentido se tiene una muestra no probabilística.

Con el propósito que la investigación brinde una constancia de la implementación del firewall, se ha considerado una muestra de un juicio de expertos, los cuales realizaron una validación a través de una hoja de cotejo que verificó la implementación del firewall y sus funciones en los accesos y seguridad de la red.

Cuando se realiza una investigación que la única manera de probar su veracidad depende exclusivamente de la verificación de conocedores en un área específica, surge la muestra del juicio de expertos, según Bolado, Ibáñez y Lantarón (1999) mencionan que la muestra del juicio de expertos en investigaciones es inevitable al momento de realizar investigaciones científico - técnicas, ya que es indudable que los análisis realizados no presenten aspectos con características profundas en la investigación (p. 11).

Hernández, Fernández y Baptista (2014) mencionan que la representatividad de la población es la muestra, por tal razón, se realiza una selección de los objetos, individuos, personas, etc. Que serán analizados para comprobar la afirmación de la hipótesis (p. 172).

Hernández, Fernández y Baptista (2014) refieren que las muestras dirigidas o muestras no probabilísticas, es el procedimiento que el investigador decide analizar para dar validez a su investigación, se utilizan cuando la población es específica y determinada, presentando la facultad de elegir casos específicos que le aporten valor científico a la investigación.

3.7. Unidad de análisis.

La investigación se desarrolló con el fin de medir el control de seguridad, para el control de accesos a la red y protección de datos en la sede principal de la ferretería Soto (CasaDekor), la unidad de análisis se conforma por cada administrativo de la ferretería soto, además de, cada representante del juicio de expertos.

La unidad de análisis se considera a cada ingeniero de sistemas quien bridará la información de verificación del firewall implementado a través de una hoja de cotejo. Por otra parte, se tiene la unidad de análisis de los administrativos, cada administrativo representa la unidad de análisis que se le implementará el cuestionario, el mismo que servirá para el tratamiento de datos y análisis estadístico.

Hernández, Fernández, y Baptista (2014) la unidad de análisis está conformada por la persona o el objeto que va a ser medido, se debe tener en cuenta que toda investigación presenta una unidad de análisis que tiene el propósito de proporcionar la información suficiente para la medición y contrastación de la investigación (p. 183).

3.8. Técnicas e instrumentos de recolección de datos

El desarrollo de la investigación presenta una parte de observación científica muy importante, a razón que los controles de accesos generados por firewall realizan esta acción, se utilizará el instrumento de observación. Por el lado de la recolección de datos, estos realizarán una medición de asociación de variables con el apoyo de un cuestionario desarrollado por los administrativos de la empresa.

3.8.1. Técnicas de recolección de datos

Observación científica.

Cárdenas, Huamán y Espíritu (2011) mencionaron que toda técnica de investigación se aplica mediante instrumentos; y todo instrumento aplicado corresponde a una técnica, ambos se corresponden.

Hernández, Fernández y Baptista (2014) la observación científica está presente en investigaciones de cualquier tipo, ya sea cuantitativa o cualitativa, en la observación se realiza un análisis profundo de los hechos, tomando en consideración cada dato recolectado, implementación del recurso y enfocada en un objeto de estudio específico (p.399).

3.8.2. Instrumentos de recolección de datos

Cuestionario.

Hernández, Fernández y Baptista (2014) el cuestionario es un instrumento de recolección de datos ampliamente utilizado en investigaciones de cualquier índole, se presenta en dos formas de realización, cuestionario de preguntas cerradas y de preguntas abiertas. El de preguntas cerradas se limita a las preguntas realizadas por el investigador, mientras que el de preguntas abiertas, el encuestado puede expresarse según fuere su consideración. Se debe tomar en consideración que, al realizar una investigación con el instrumento del cuestionario, existen pautas de realización, ya que el instrumento recolector de datos debe constar con preguntas relacionadas directamente con las variables de estudio (p. 217).

Según, Escofet Et. al. (2016) considera que una vez elaborado el cuestionario o instrumento, según el estudio de que se trate, antes de aplicarlo de manera definitiva en la muestra seleccionada, se deberá someter a prueba con el propósito de establecer su validez y confiabilidad en relación con el problema de la investigación (pp. 938-939).

Hojas de cotejo.

En la implementación de un software o equipo tecnológico se debe conocer los pasos estrictamente detallados. Por tal razón, la investigación utilizó hojas de cotejo para la verificación de la implementación del producto.

Espinoza (2010) las listas de cotejo o hojas de cotejo tienen la finalidad de indicar

la verificación de los pasos en la implementación o producción de un bien o servicio, verificando que cada paso que se ha realizado cumple con lo propuesto y si presenta un nivel aceptable de éxito (p. 130)

3.9. Técnicas e instrumentos para el procesamiento y análisis de datos.

El desarrollo de la investigación se realizó con un análisis de asociación entre variables, esto a razón que se busca conocer la influencia que genera la implementación del firewall sobre la seguridad en el control de accesos y la protección de la red de datos, comprobando mediante un análisis estadístico denominado Chi-Cuadrado, el grado de asociación entre las variables obtenidas y comprobar si la implementación del firewall genera una mejora en el control de acceso y seguridad en la Ferretería Soto.

Hurtado (2017) indica que, al realizar una investigación científica, se debe realizar un análisis estadístico que busque la corroboración del estudio. Un análisis estadístico produce la firmeza en una investigación y establece importancia teórica y práctica de la investigación (p.114).

Para el análisis estadístico se realizó la prueba de Chi-Cuadrado, esto a razón que las variables buscan medirse para conocer la mejora en relación a la asociación, asimismo estas variables son nominales. Por tal razón, la elección se realiza debido que la investigación busca demostrar la influencia que genera la implementación de un firewall, de igual modo que, la asociación de las variables muestra una distribución normal, lo que permite realizar una prueba no paramétrica, realizando una medición de asociación mediante una prueba estadística de influencia.

Tinoco (2008) indica que una prueba estadística Chi-Cuadrado, es utilizada en investigaciones de influencia, a razón que la distribución de sus datos es libre y no presenta un muestreo aleatorio, permitiendo que se encuentre entre una prueba no paramétrica. (pp. 75-76).

Para la recolección de datos se utilizaron las hojas de cotejo y los cuestionarios, estos últimos fueron contabilizados con la herramienta de Excel, mientras que, para el desarrollo del análisis estadístico se utilizó la herramienta SPSS, debido a la versatilidad con que las herramientas trabajan.

Pérez (2006) indica que el desarrollo del inventariado y contabilidad que utiliza Excel, calificando a dicha herramienta como la mejor para este propósito, aludiendo que su campo de utilización es muy amplio y de gran importancia para distribución, categorización y tabulación de información (p. 68).

Gonzáles (2009) refiere que SPSS es un software enfocado en el análisis, tratamiento y muestra de datos; siendo uno de los principales softwares dedicados a este fin. Si se busca demostrar la veracidad o negación de una hipótesis, un análisis estadístico es la mejor manera de mostrar los resultados acertados, puntuales y con pequeño margen de error en una investigación (p. 5).

3.10. Interpretación de datos.

Estadística Chi-Cuadrado.

Una vez analizadas las variables que se han utilizado en la investigación, además considerando que la muestra utilizada es no probabilística y a la vez no es aleatoria y teniendo una distribución libre. Ello indica que la prueba a utilizar es no paramétrica, considerando la prueba Chi-Cuadrado como la mejor opción para contrastar la investigación realizada, una prueba estadística que cumple con las características de la investigación y poder demostrar la influencia entre variables.

$$X^2 = \Sigma \frac{(f_o + f_t)^2}{f_t}$$

CAPÍTULO IV: IMPLEMENTACIÓN DEL PROYECTO

La investigación implementó la metodología Botton Up, dicha metodología es una metodología en semilla para implementación de equipos hardware, además que la versatilidad de trabajo con esta metodología es muy completa, la serie de pasos que implementa conforman la totalidad de pasos en una implementación de firewall.

Asana (2021) alude que la metodología Botton Up en relación a la Top Down es una metodología de menor complejidad, además que, los procesos que son realizados buscan dar a conocer las especificaciones propias del personal que solicita la implementación.

4.1. Fases de la metodología Botton Up

4.2.1. Fase de Análisis

Para analizar la red con la que cuenta la Ferretería Soto se realizó un análisis de la red de acuerdo a los equipos con los que cuenta dicha red, del mismo modo se realizó una conversación con el coordinador de la empresa. El coordinador de la empresa aludió que la red presente en la Ferretería Soto presenta características buenas y, que su único percance estaba relacionado a la sucursal principal de la ferretería, a causa que la seguridad de la empresa estaba siendo vulnerada. Dicho percance se debía a tres razones muy importantes, primero que la mayoría de máquinas reciben mantenimientos continuos por infestaciones de virus, segundo que la red presenta manipulaciones de la información no propicias para la red y; tercero que los equipos en la red presentan vulnerabilidad en relación a las nuevas tecnologías de información.

Con la información proporcionada por el coordinador se realizó la propuesta de implementación de un firewall Cisco, donde se realizó el análisis de la red para conocer el estado en que esta se encontraba y así determinar las falencias mencionadas por el coordinador de la Ferretería soto.

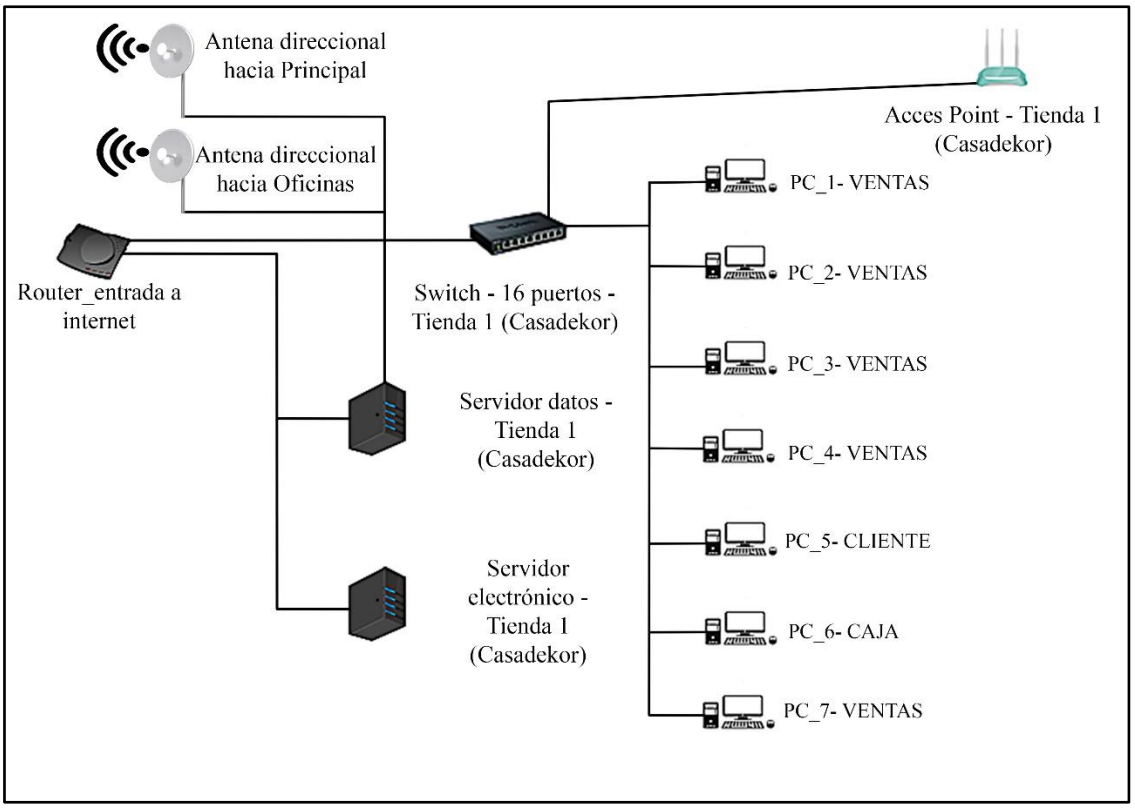
Análisis de red y configuraciones existentes.

El diseño de la red se obtuvo luego de conocer los equipos con los que contaba la red.

La red presenta 4 lugares de trabajo los cuales están conformados por la tienda n°1 (CasaDekor), tienda n°2 (Principal), tienda n°3 (FerreHome), tienda n°4 (Color Centro) y las Oficinas.

Figura 11

Diseño de red tienda n° 1 (CasaDekor)



Fuente: Diseño propio.

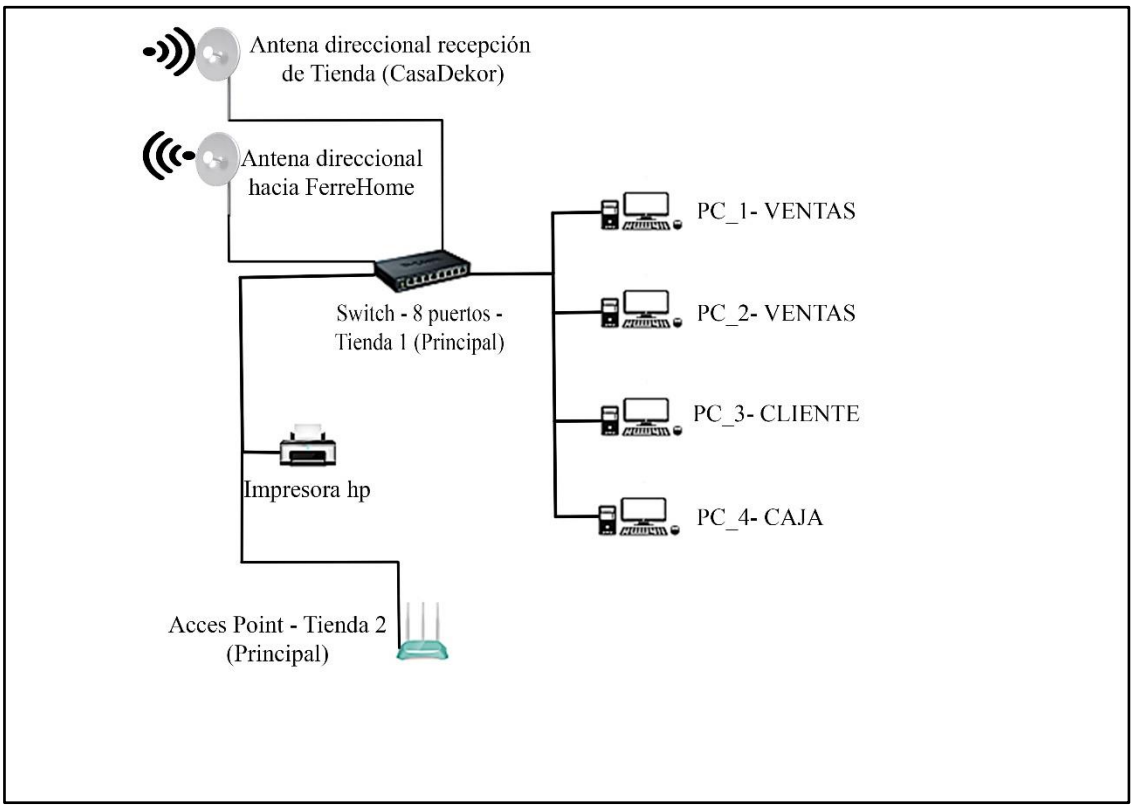
La tienda n°1 es la tienda base de todas las sucursales, debido a que la conexión de internet que se ha solicitado en la Ferretería Soto es una conexión centralizada, esta conexión presenta un router universal que brinda internet a un switch de 16 puertos, los cuales proporcionan internet a las 7 computadoras de escritorio de la ferretería; 5 computadoras encargadas de los puntos de ventas, 1 computadora encargada para pagos (caja) y 1 computadora para clientes, cuya norma se requiere para la visualización de precios.

Asimismo, se tiene dos servidores para protección de la red, el primer servidor es el encargado de los datos (almacenamiento), mientras que el segundo servidor presenta la funcionalidad de ser servidor electrónico (valida la comunicación con SUNAT).

Para que se realice una comunicación centralizada, el Router de la tienda n°1 proporciona internet al servidor de datos, siendo este el encargado de expandir la red a las demás tiendas a través de antenas direccionales. En la figura n° 11 se aprecia que la tienda CasaDekor presenta dos antenas direccionales, cada una de estas tiene la funcionalidad de proporcionar internet a dos sucursales, una para la tienda n°2 (Principal) y la otra para la tienda n°4 (Color Centro y Oficinas).

Figura 12

Diseño de red tienda n° 2 (Principal).



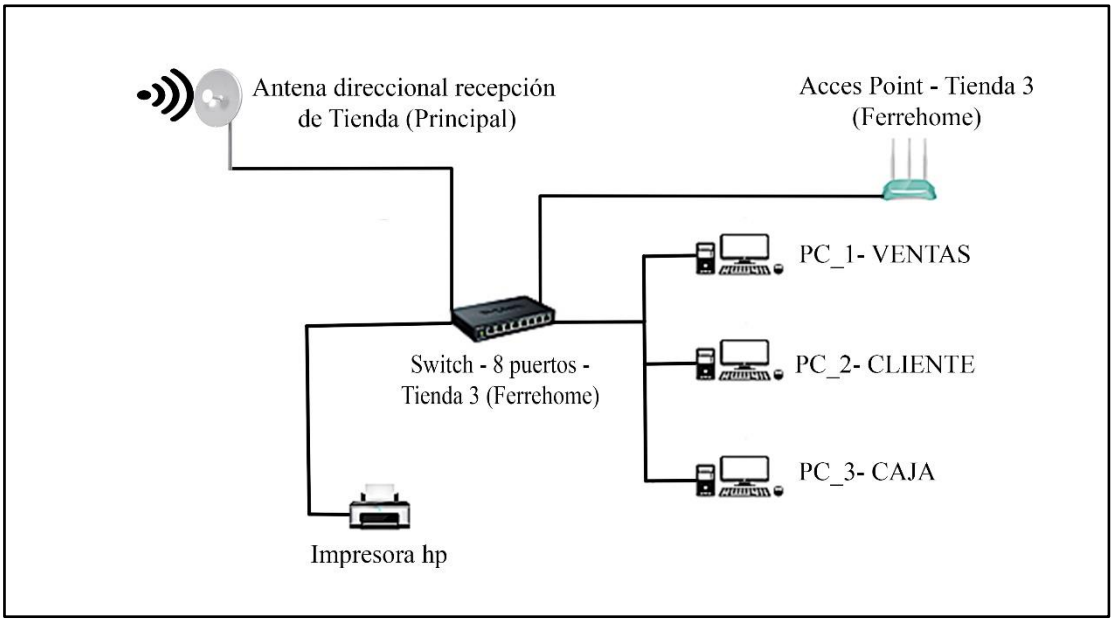
Fuente: Diseño propio.

La tienda n°2 es la primera sucursal de la Ferretería Soto, esta distribución de equipos se realiza con la llegada del internet a través de la antena direccional que recibe la llegada

del internet desde la tienda n°1 (CasaDekor), la distribución hacia los equipos en la empresa lo realiza un switch de 8 canales que realiza la transmisión a las 4 computadoras dentro de la empresa: 2 computadoras de ventas, 1 computadora de pagos (caja) y una computadora para consulta de precios (cliente). De igual modo el switch facilita de red, distribuyéndola sobre una impresora en red y un Access Point para proporcionar internet a equipos móviles y tabletas que hacen uso en la empresa, pero, que no presenta una conexión en red estable. Con el fin de seguir proporcionando la conexión de red a la tienda n° 3 (FerreHome), el switch brinda un canal para proporcionar internet a una segunda antena direccional, la que se encarga de enviar conexión de red hacia la tienda n°3 (FerreHome).

Figura 13

Diseño de red tienda n° 3 (FerreHome).



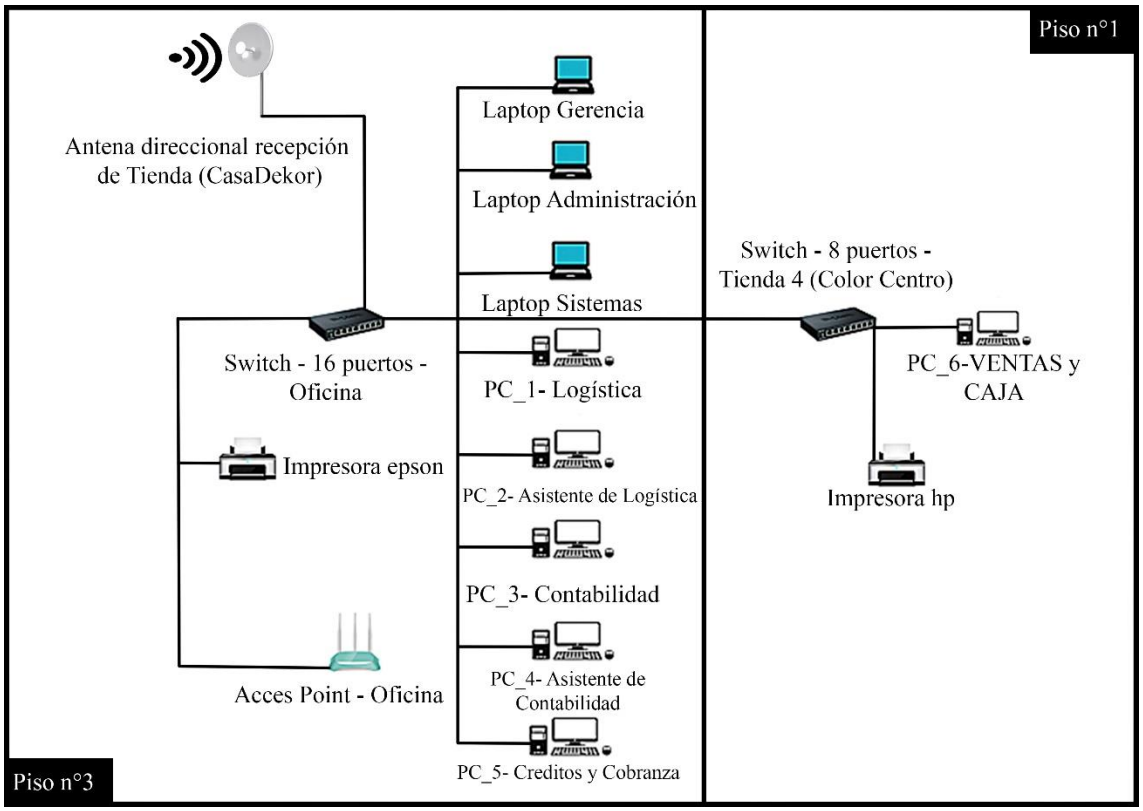
Fuente: Diseño propio.

La tienda n°3 es la segunda sucursal de la Ferretería Soto, esta distribución de equipos se realiza con la llegada del internet a través de la antena direccional que recepción la llegada del internet desde la tienda n°2 (Principal), la distribución hacia los equipos en

la empresa lo realiza un switch de 8 canales que realiza la transmisión a las 3 computadoras dentro de la empresa: 1 computadora de ventas, 1 computadora de pagos (caja) y 1 computadora para consulta de precios (cliente). De igual modo el switch facilita de red, distribuyéndola sobre una impresora en red y un Access Point para proporcionar internet a equipos móviles y tabletas que hacen uso en la empresa, pero, que no presentan una conexión en red estable.

Figura 14

Diseño de red tienda n° 4 (ColorCentro).



Fuente: Diseño propio.

La tienda n° 4 es la sucursal final de la Ferretería Soto, este local cuenta con tres pisos, el tercer piso funciona con las oficinas principales de las tiendas, en este piso la antena direccional recepción la entrada de internet de la tienda n°1 (CasaDekor), luego distribuye el internet sobre un switch de 16 canales, estos canales son ocupados por 3 computadoras portátiles: 1 laptop para Gerencia, 1 laptop para Administración y 1 laptop para Sistemas;

5 computadoras de mesa: 1 computadora para Logística, 1 computadora para el asistente de logística, 1 computadora para contabilidad, 1 computadora para el asistente de contabilidad y 1 computadora para créditos y cobranzas. Asimismo 2 canales de switch son ocupados por una impresora en línea y un Access Point.

En el piso n°2 no existen componentes tecnológicos, debido a que su uso es únicamente almacén; por otro lado, en el piso n°1 se encuentra la tienda ColorCentro, esta tienda al ser una sucursal que recién se encuentra implementando, solamente cuenta con un switch de 8 canales que recibe internet del switch de 16 canales del piso n°3, del mismo modo cuenta únicamente con una computadora de escritorio y una impresora, dicha computadora tiene la funcionalidad de ser caja, ventas y cliente al mismo tiempo.

4.2.2. Fase de Implementación.

Con los datos recabados en la fase de análisis, se realizó la implementación del firewall, dicho dispositivo fue financiado propiamente por la Ferretería Soto, pero, un firewall físico limita su protección al número de canales con los que cuente el dispositivo, además que la protección que brinda, solo se da para la zona donde se encuentra instalado. Por tal motivo, se realizó la implementación del firewall únicamente en la tienda n°1 (CasaDekor), esto se debió a que el firewall contratado por la empresa presenta únicamente 8 canales, lo que limitaba la protección de la red a solamente 8 dispositivos en redes. Considerando que los dispositivos de mayor importancia se fijaban principalmente en los servidores. Debido a que estos controlan la data en red y el tráfico de paquetes; se consideró por unanimidad la implementación del firewall en la tienda ya mencionada.

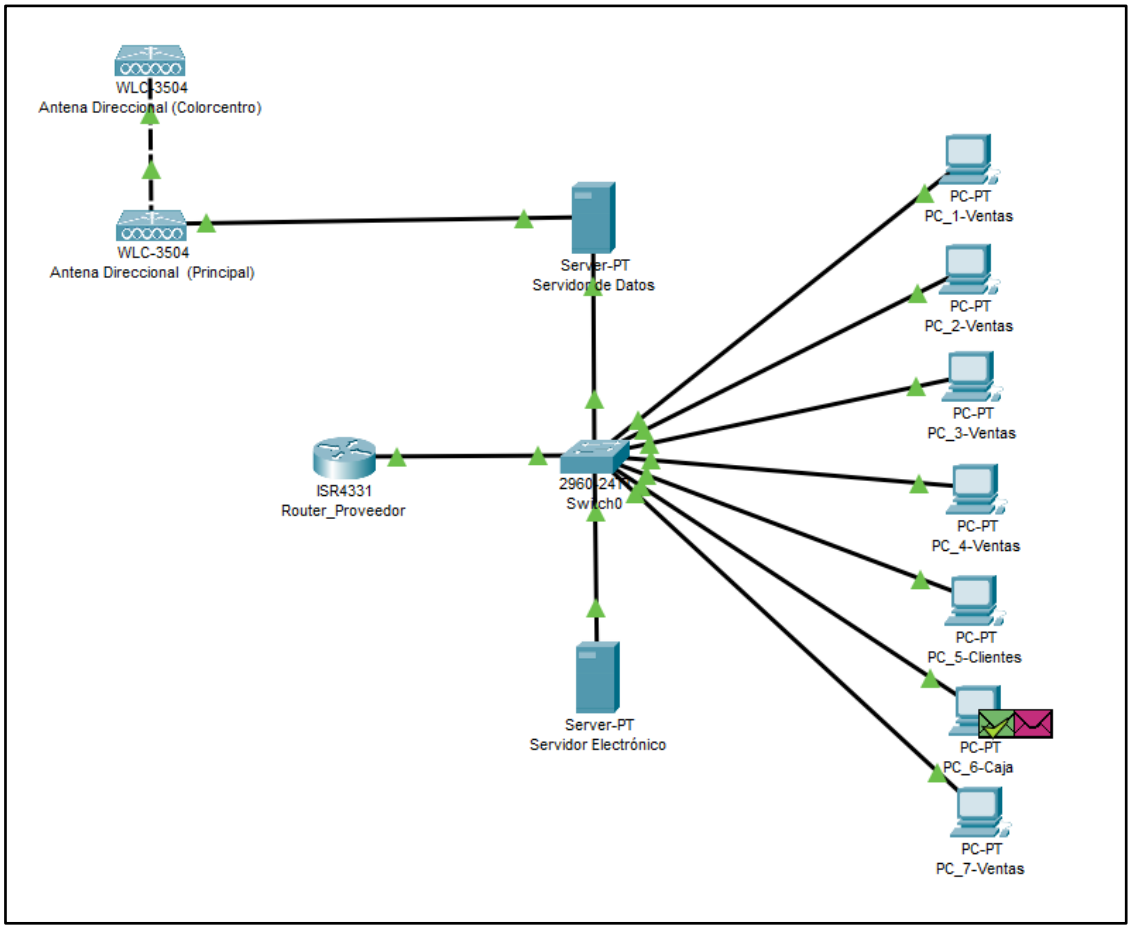
4.2.2.1. Diseño Lógico

Considerando que la implementación del firewall solamente se realizó en la tienda n°1 (CasaDekor), se realizó un diseño lógico de red únicamente en dicha tienda. El diseño

lógico se realizó con la herramienta de Cisco Packet Tracer, por el motivo que la adquisición del firewall de 16 canales es un equipo de la compañía Cisco.

Figura 15

Diseño de la red (CasaDekor) en Packet Tracer.



Fuente: Diseño propio.

La figura n° 15 muestra el diseño lógico de la red con que presentaba la Ferretería Soto (CasaDekor), apreciándose que los servidores se comunican con el router proveedor del servicio de internet a través de un switch, cuyo canal de comunicación es el mismo. Asimismo, la red solamente contaba con una única subred, lo que genera que cualquier persona que se cuelgue a la red pueda tener acceso al servidor.

Tabla 9

Direcciones IP, puerta de enlace y DNS de la tienda n°1 (CasaDekor).

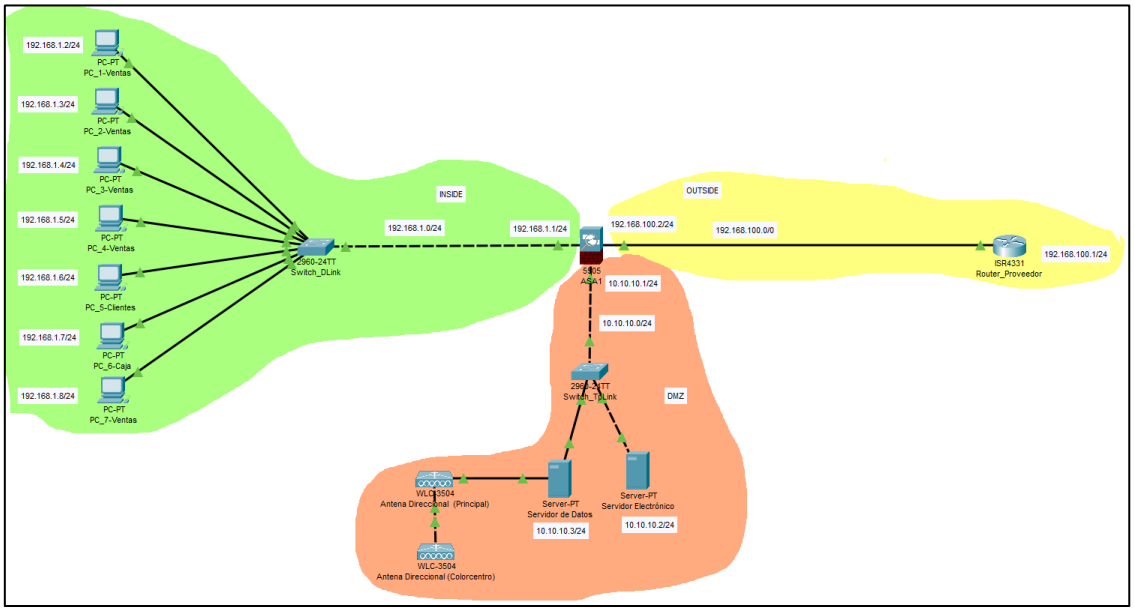
Dirección IP	Equipo	DNS	Puerta de Enlace
192.168.1.1	ROUTER proveedor de internet	190.113.220.51 190.113.220.54	192.168.1.1
192.168.1.2	Servidor Datos (Almacenamiento)	190.113.220.51 190.113.220.54	192.168.1.1
192.168.1.3	Servidor Electrónico (Comunicación con Sunat)	190.113.220.51 190.113.220.54	192.168.1.1
192.168.1.4	PC_ 1-Ventas	190.113.220.51 190.113.220.54	192.168.1.1
192.168.1.5	PC_ 2-Ventas	190.113.220.51 190.113.220.54	192.168.1.1
192.168.1.6	PC_ 3-Ventas	190.113.220.51 190.113.220.54	192.168.1.1
192.168.1.7	PC_ 4-Ventas	190.113.220.51 190.113.220.55	192.168.1.1
192.168.1.8	PC_ 5-Clientes	190.113.220.51 190.113.220.56	192.168.1.1
192.168.1.9	PC_ 6-Caja	190.113.220.51 190.113.220.57	192.168.1.1
192.168.1.10	PC_ 7-Ventas	190.113.220.51 190.113.220.58	192.168.1.1

Como se aprecia en la tabla n° 9 las distribuciones de IP con las que contaban dentro de la tienda CasaDekor presentaba un diseño de red muy inseguro, dicho diseño de red presentaba una única distribución de IP. Además, la red podría ser vulnerada desde cualquier punto de conexión con la red. En tal motivo, se realizó la comunicación con un acople del firewall, este dispositivo logró el filtrado de paquetes y la protección de la red

para la comunicación con al protocolo de mensajes ICMP, por ende, la comunicación de los paquetes presentó un filtrado de redes, una lista de accesos a la red, una VPN propia para la comunicación personal de los servidores y una serie de protocolos relacionados a la protección general del filtrado de softwares maliciosos.

Figura 16

Diseño de la red (CasaDekor) con firewall Cisco.

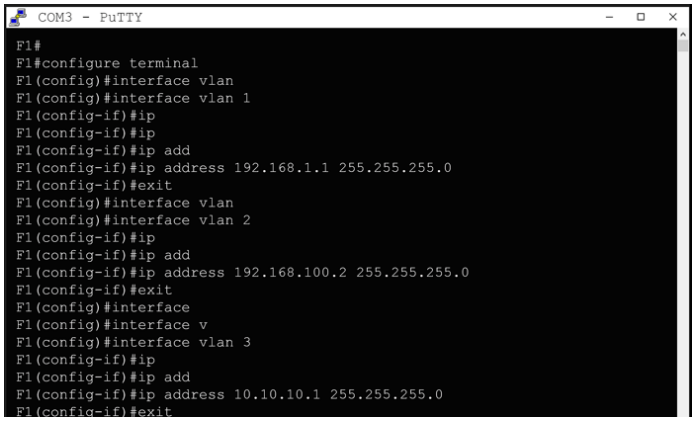


Fuente: Diseño propio.

Como se aprecia en la figura n° 16 se realizó la incorporación del firewall, este dispositivo consta específicamente de 3 entradas Ethernet, la funcionalidad de estas entradas permite que los dispositivos puedan crear una red diferente entre sus puertos, consiguiendo que los servidores presenten comunicaciones diferentes entre sus accesos. Con la división de subredes se logró administrar la red y conseguir un punto extra en seguridad.

Figura 17

Configuración del firewall para direccionamiento IP



Fuente: Pantallazo propio de la Pc de configuración

Como se aprecia en la figura n°17 para la realización de la configuración interna del Firewall Cisco se utilizó la herramienta Putty, dicha herramienta permite realizar configuraciones de dispositivos configurables de la marca Cisco, en la presente imagen se aprecia el desarrollo de la configuración interna de los 3 puertos de entrada a la interfaz del dispositivo, logrando la asignación de 3 subredes. Cada subred les permite a los dispositivos la comunicación con los servidores, pero dificulta la filtración de paquetes de intrusos externos. Con la asignación de los 3 puertos de configuración se tiene una seguridad en la capa de transporte de la red.

Configuración de las Vlans del Firewall Cisco ASA5505H-X, estas mismas Vlans formaron parte de las salidas ethernet 0/1,0/2 y 0/3, con direcciones Ip: 192.168.1.1, 192.168.100.2 y 10.10.10.1 respectivamente:

```
F1#
F1#configure terminal
F1(config)#interface vlan
F1(config)#interface vlan 1
F1(config-if)#ip
F1(config-if)#ip
F1(config-if)#ip add
F1(config-if)#ip address 192.168.1.1 255.255.255.0
```

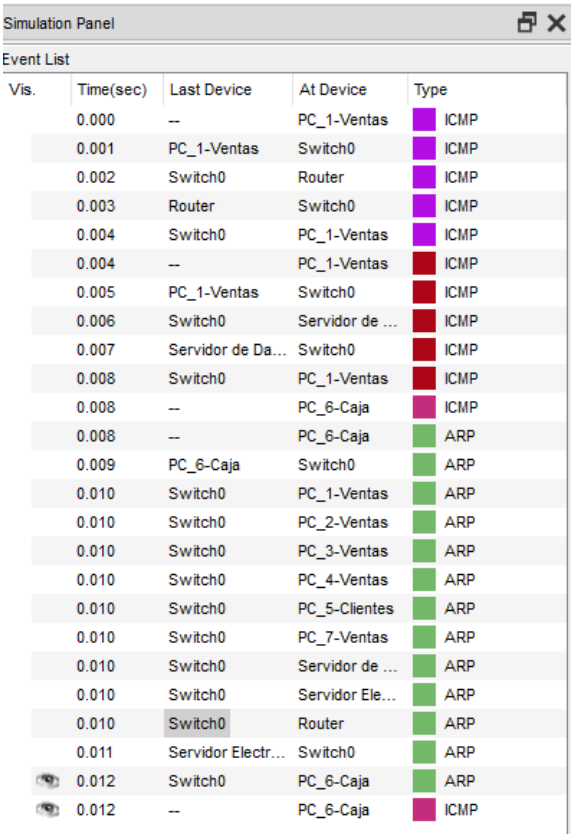
```
F1(config-if)#exit
F1(config)#interface vlan
F1(config)#interface vlan 2
F1(config-if)#ip
F1(config-if)#ip add
F1(config-if)#ip address 192.168.100.2 255.255.255.0
F1(config-if)#exit
F1(config)#interface
F1(config)#interface v
F1(config)#interface vlan 3
F1(config-if)#ip
F1(config-if)#ip add
F1(config-if)#ip address 10.10.10.1 255.255.255.0
F1(config-if)#exit
```

4.2.2.2. Simulación

De acuerdo a la verificación de los dispositivos, se realizó una simulación de paquetes en base a los protocolos de transporte, dicha simulación se realizó de dos maneras, la primera con la herramienta Cisco Packet Tracer, que tuvo el fin de monitorear el diseño realizado y si los paquetes se transferían de manera óptima. Por otro lado, la segunda simulación se realizó con la herramienta PING propia de Windows, la misma que proporcionó el resultado de compartir paquetes entre los servidores y dispositivos conectados a la red.

Figura 18

Simulación del diseño de red (CasaDekor) en Packet Tracer.



Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC_1-Ventas	ICMP
	0.001	PC_1-Ventas	Switch0	ICMP
	0.002	Switch0	Router	ICMP
	0.003	Router	Switch0	ICMP
	0.004	Switch0	PC_1-Ventas	ICMP
	0.004	--	PC_1-Ventas	ICMP
	0.005	PC_1-Ventas	Switch0	ICMP
	0.006	Switch0	Servidor de ...	ICMP
	0.007	Servidor de Da...	Switch0	ICMP
	0.008	Switch0	PC_1-Ventas	ICMP
	0.008	--	PC_6-Caja	ICMP
	0.008	--	PC_6-Caja	ARP
	0.009	PC_6-Caja	Switch0	ARP
	0.010	Switch0	PC_1-Ventas	ARP
	0.010	Switch0	PC_2-Ventas	ARP
	0.010	Switch0	PC_3-Ventas	ARP
	0.010	Switch0	PC_4-Ventas	ARP
	0.010	Switch0	PC_5-Clientes	ARP
	0.010	Switch0	PC_7-Ventas	ARP
	0.010	Switch0	Servidor de ...	ARP
	0.010	Switch0	Servidor Ele...	ARP
	0.010	Switch0	Router	ARP
	0.011	Servidor Electr...	Switch0	ARP
	0.012	Switch0	PC_6-Caja	ARP
	0.012	--	PC_6-Caja	ICMP

Fuente: Pantallazo propio de la simulación de Cisco Packet Tracer

La figura n°18 muestra la que las transferencias entre paquetes de red cumplen su objetivo, un ejemplo mostrado es el envio de paquetes desde la Pc_1_Ventas hacia el servidor de datos, el cual muestra una respuesta de mensaje afirmando la confirmación del envio de paquetes. Por otro lado, se realizó un envio de paquetes entre la Pc_6_Caja y el servidor electrónico, el cual muestra la comunicación entre paquetes de red y un flujo de datos transparente.

Para la configuración de los equipos físicos se realizó la incorporación de subredes necesarias para la primera protección de datos, configurando los dispositivos con las siguientes direcciones Ip.

Tabla 10

Direcciones IP, máscaras y DNS del diseño de red (CasaDekor).

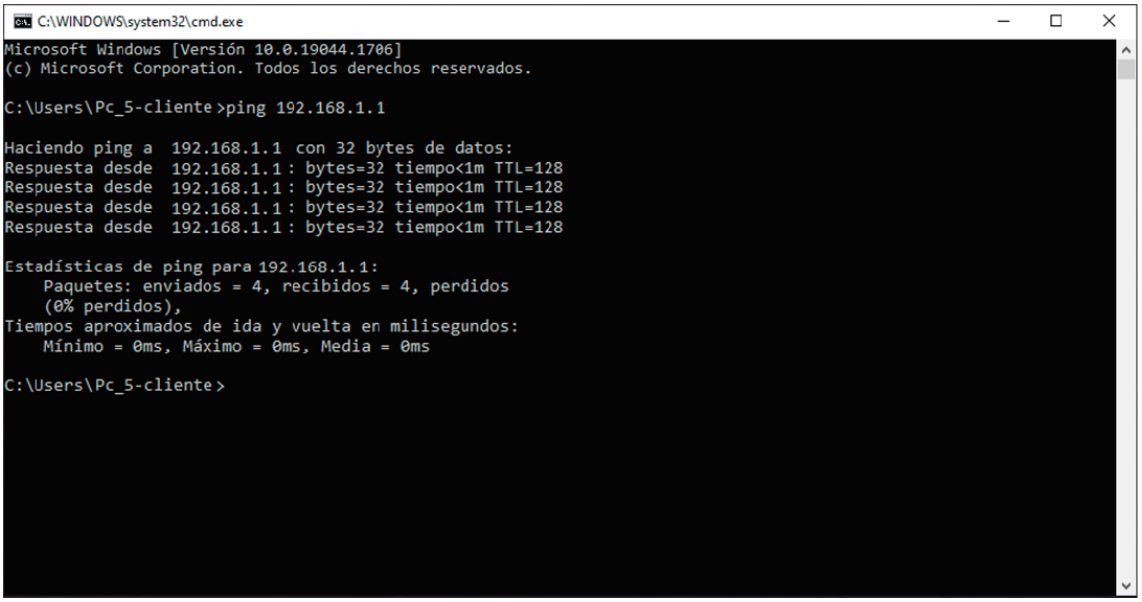
Dirección IP y Máscara	**Equipo**	**DNS**	**Puerta de Enlace**
Ethe. 0/1: 192.168.1.1 255.255.255.0 Ethe. 0/2: 192.168.100.2 255.255.255.0 Ethe. 0/3: 10.10.10.1 255.255.255.0	Firewall	-	Cada dirección Ip se convierte en una puerta de enlace.
192.168.100.1 255.255.255.0	ROUTER proveedor de internet	190.113.220.51 190.113.220.54	192.168.100.2
10.10.10.3 255.255.255.0	Servidor Datos (Almacenamiento)	190.113.220.51 190.113.220.54	10.10.10.1
10.10.10.2 255.255.255.0	Servidor Electrónico (Comunicación con Sunat)	190.113.220.51 190.113.220.54	10.10.10.1
192.168.1.2 255.255.255.0	PC_ 1-Ventas	190.113.220.51 190.113.220.54	192.168.1.100
192.168.1.3 255.255.255.0	PC_ 2-Ventas	190.113.220.51 190.113.220.54	192.168.1.100
192.168.1.4 255.255.255.0	PC_ 3-Ventas	190.113.220.51 190.113.220.54	192.168.1.100
192.168.1.5 255.255.255.0	PC_ 4-Ventas	190.113.220.51 190.113.220.55	192.168.1.100
192.168.1.6 255.255.255.0	PC_ 5-Clientes	190.113.220.51 190.113.220.56	192.168.1.100
192.168.1.7 255.255.255.0	PC_ 6-Caja	190.113.220.51 190.113.220.57	192.168.1.100

192.168.1.8 255.255.255.0	PC_ 7-Ventas	190.113.220.51 190.113.220.58	192.168.1.1 00

En la tabla n° 10 se aprecia el nuevo direccionamiento de red realizado en la Ferretería Soto (CasaDekor), esta comprende actualmente 3 subredes, una subred que comprende la dirección Ip 10.10.10.0/24, esta red contiene los servidores de la red; la segunda subred que comprende la dirección Ip 192.168.100.0/2, esta red presenta la salida con internet. Por último, la tercera subred comprende la dirección Ip 192.168.1.0/24, esta red presenta una seguridad interna y en la que se han realizado las modificaciones de los computadores que presentan direcciones Ip desde la 192.168.1.1/24 hasta 192.168.1.8 /24

Figura 19

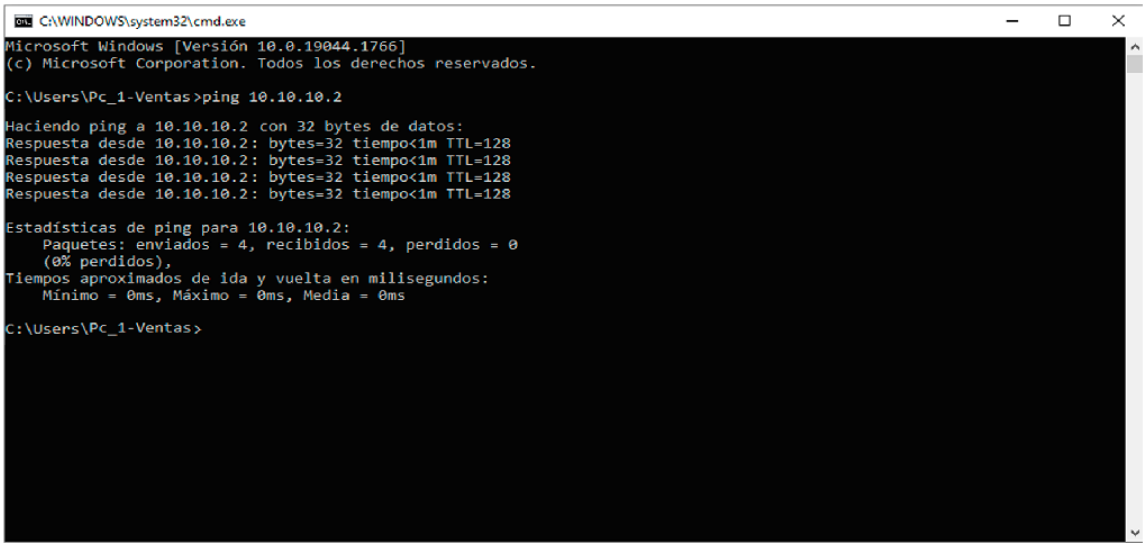
Simulación entre la Pc de Clientes y la salida a internet.



Fuente: Pantallazo propio de la Pc n°5 de cliente

Figura 20

Simulación entre la Pc de ventas y la comunicación con el servidor de datos.



Fuente: Pantallazo propio de la Pc n°1 de cliente

La figura n°19 y n°20 muestran la viabilidad de conexión entre los diferentes dispositivos de la red. Para la demostración se colocó los dos dispositivos de red con los que se realizaron un establecimiento de conexión y comprobar si las direcciones asignadas realizaban la funcionalidad debida. Para la salida de los dispositivos hacia la red (internet), se realizaron comunicaciones entre la Pc Cliente y el Router de salida hacia internet, comprobándose que la comunicación se realiza correctamente y que no existía la pérdida de paquetes. Por otro lado, se realizó la comprobación de la comunicación entre la Pc de Ventas y el servidor de datos, demostrando según la figura n°20 que la comunicación se realiza fluidamente y sin la presencia de paquetes perdidos.

Con lo realizado se logró la implementación del diseño lógico de la red, para posteriormente en el ítem de diseño físico lograrse la configuración general del firewall y así realizar el filtrado de paquetes, controles de acceso, direccionamientos y seguridad en los dispositivos.

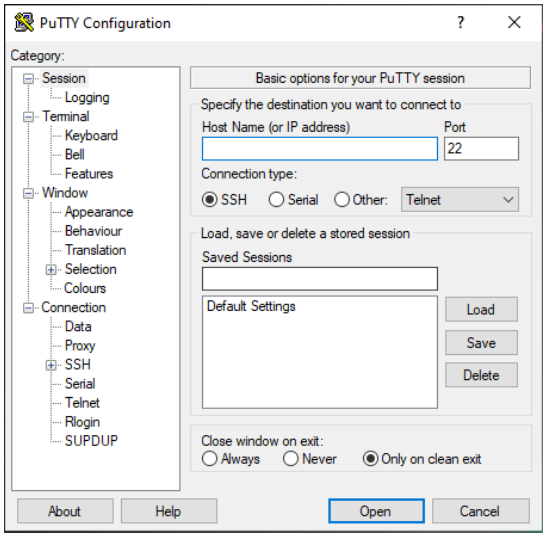
4.2.2.3. Diseño Físico.

Una vez realizada la división de subredes que se comunicarán con el firewall y que serán distribuidas en la red se realizó la configuración del dispositivo base, junto con las diferentes direcciones IP, para luego presentar un filtrado en los paquetes de comunicación y evitar la vulnerabilidad de la red en los servidores.

Para realizar la configuración de equipos externos, fue necesario utilizar los conectores de red BD-25 macho y hembra, además de la utilización del software Putty, así como se muestra en la figura n° 17 del documento presente, dicha herramienta según HostGator (2022) indica que la herramienta Putty es un terminal de simulación de código abierto, utilizado generalmente por programadores y administradores de red, dicha herramienta se utiliza para la configuración de conexiones seguras en el desarrollo de protocolos TCP, ICMP, Telnet, portal series, etc. Usado en equipos de terminales configurables, facilitando la conexión se acceso segura y remota a través del Shell.

Figura 21

Interfaz de entrada de herramienta Putty.



Fuente: Pantallazo propio de la herramienta de configuración Putty.

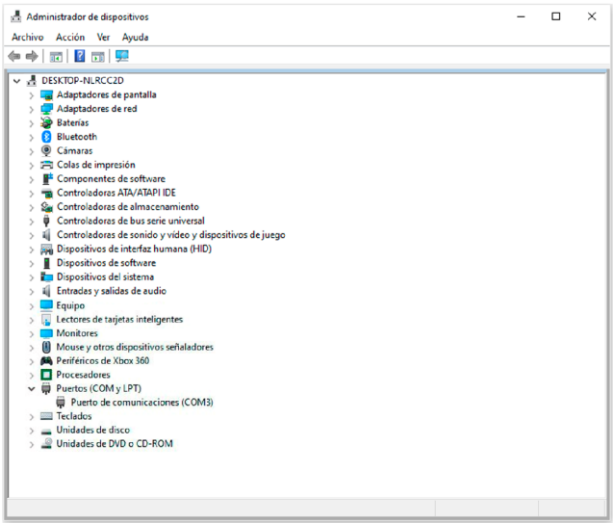
Como se aprecia en la figura n° 21, la interfaz de entrada de la herramienta Putty, para

realizar la configuración del terminal (firewall) Cisco, se procedió a realizar la conexión de los conectores DB-25 macho y hembra, para proceder con los lineamientos de configuración particulares.

Al momento de realizar la conexión con el terminar USB de la laptop, se aprecia en la siguiente imagen la entrada COM3 para la administración del terminal

Figura 22

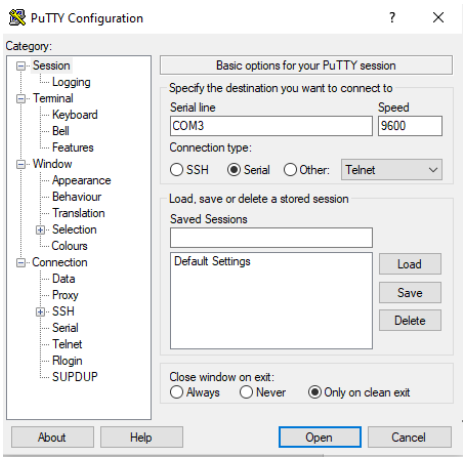
Administrador de dispositivos con la entrada COM3.



Fuente: Pantallazo propio de la administración de dispositivos para el puerto COM

Figura 23

Putty con la entrada serial COM3



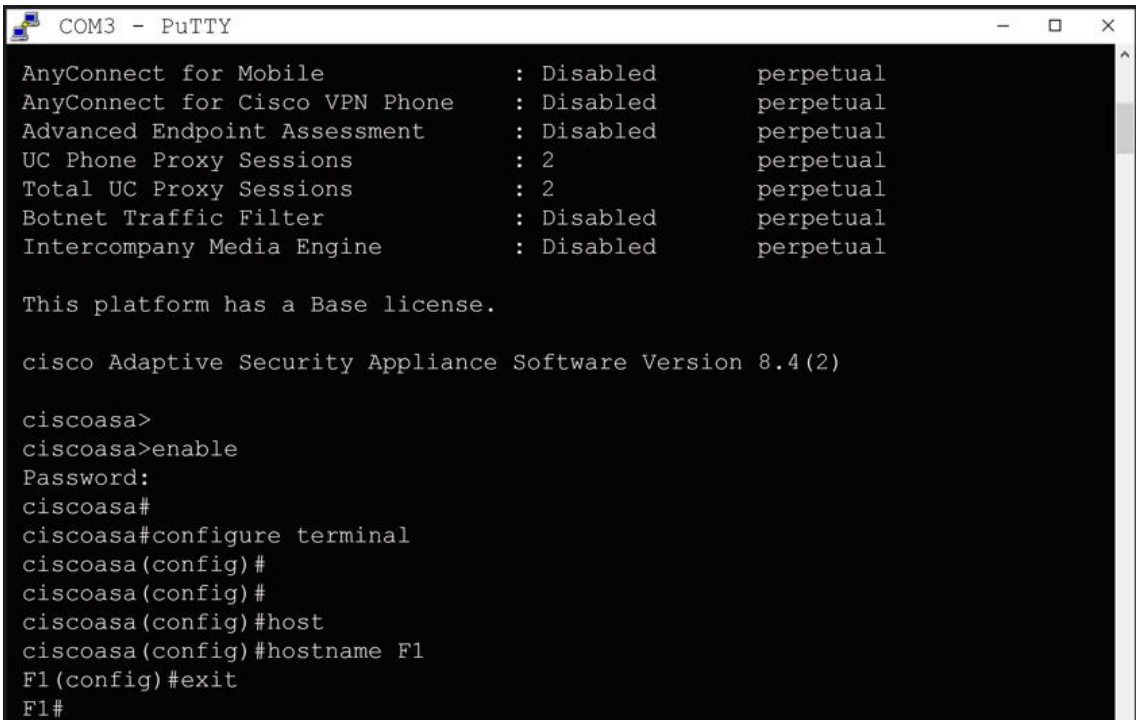
Fuente: Pantallazo propio de la herramienta de configuración Putty con el puerto activo.

Con los terminales instalados, se realiza las configuraciones del firewall Cisco:

Ingreso al firewall y cambio de nombre

Figura 24

Cambio de nombre en el firewall



Fuente: Pantallazo propio de la entrada a la configuración

La figura presenta los comandos relacionados al cambio de nombre; primero, se realiza la entrada al firewall Cisco ASA505, el comando de entrada es el “enable”, este comando permite el ingreso al firewall para realizar la configuración pertinente; seguidamente el firewall solicita una contraseña, pero al estar el firewall recientemente configurado no presenta contraseña actual. Seguidamente se debe realizar la entrada al terminal, cuyo comando es “configure terminal”, este comando permite la configuración interna del terminal. Finalmente se realiza el cambio de nombre con el comando “hostname” seguido del nombre que se desea cambiar, mostrando que el cambio realizado se aprecia en pantalla. El comando “exit” permite salir un nivel de la configuración actual.

Configuración de Valns para puertos y entradas del firewall

Figura 25

Configuración de las Vlan's

Fuente: Pantallazo propio de la configuración de Vlan´s

La imagen muestra el ingreso a la configuración de Vlan’s, este procedimiento se realiza con el fin de dividir la red en tres tipos de seguridad, debido a que el firewall físico realizar

una seguridad interna y externa, esta debe presentar un nivel de seguridad adecuado para las diferentes subredes, asimismo, el firewall debe contar con una licencia, en tal caso que se requiera la configuración de una tercera red, cuarta red, quinta, etc.

Para la configuración de la vlan 1 y vlan 2, se realiza la entrada al terminal mediante el comando “configure terminal”, luego se procede a las configuraciones de cada una de las interfaces de Vlan’s mediante el siguiente comando: “interface vlan (1 o 2)”, este comando permite el ingreso a la configuración directa del terminal elegido. Posteriormente al ingreso, se procede a configurar la dirección Ip con la que va a trabajar cada una de las Vlan’s, para la configuración de Ip, se realiza el siguiente comando: “ip address (dirección Ip) (máscara de subred)”.

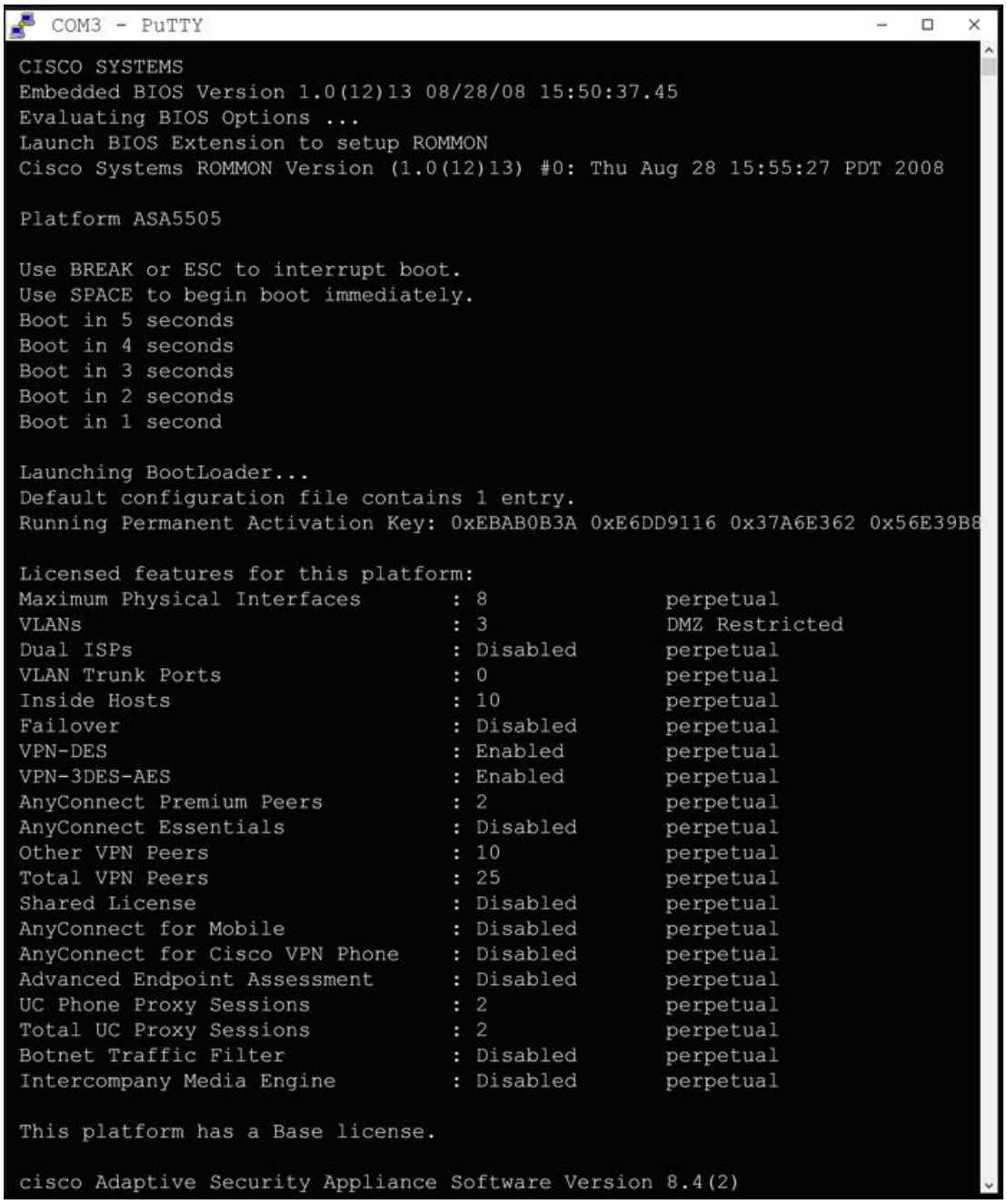
En el caso de la tercera vlan se consideró su utilización para los servidores, pero al ser un firewall físico, siempre se solicita una licencia de funcionamiento, la cual se adquirió con el proveedor, pero el mismo firewall permitía la configuración de una tercera vlan; esta vlan se configuró con la creación del siguiente comando: “interface vlan 3”, luego se procedió a darle un nombre de vlan, pero la licencia determinaba que el comando “nameif” no era permitido para subredes superiores. Por tal razón, se procedió en una segunda máquina a verificar la licencia adquirida, lo cual se refleja en la figura n°26. Luego se continuó con la configuración que ese estaba realizando, determinado que la licencia obtenida debería tomar el nombre DMZ y que debería tener un rango menor a la seguridad de la Vlan 1, para esto se realizó el siguiente comando “no forward interface vlan 1”. Finalmente se colocó el nombre de la Vlan y se le agregó una seguridad de nivel 50 mediante el comando “Security-Level 50”, esto permitió que la seguridad propia de los servidores tenga un nivel adicional de seguridad y que su manejo a nivel intermedio pueda realizar las peticiones con los computadores conectados al firewall.

El cambio de firewall se dio porque la empresa proveedora de los equipos solo contaba

con licencias para el firewall ASA5505.

Figura 26

Inicio del firewall y licencias



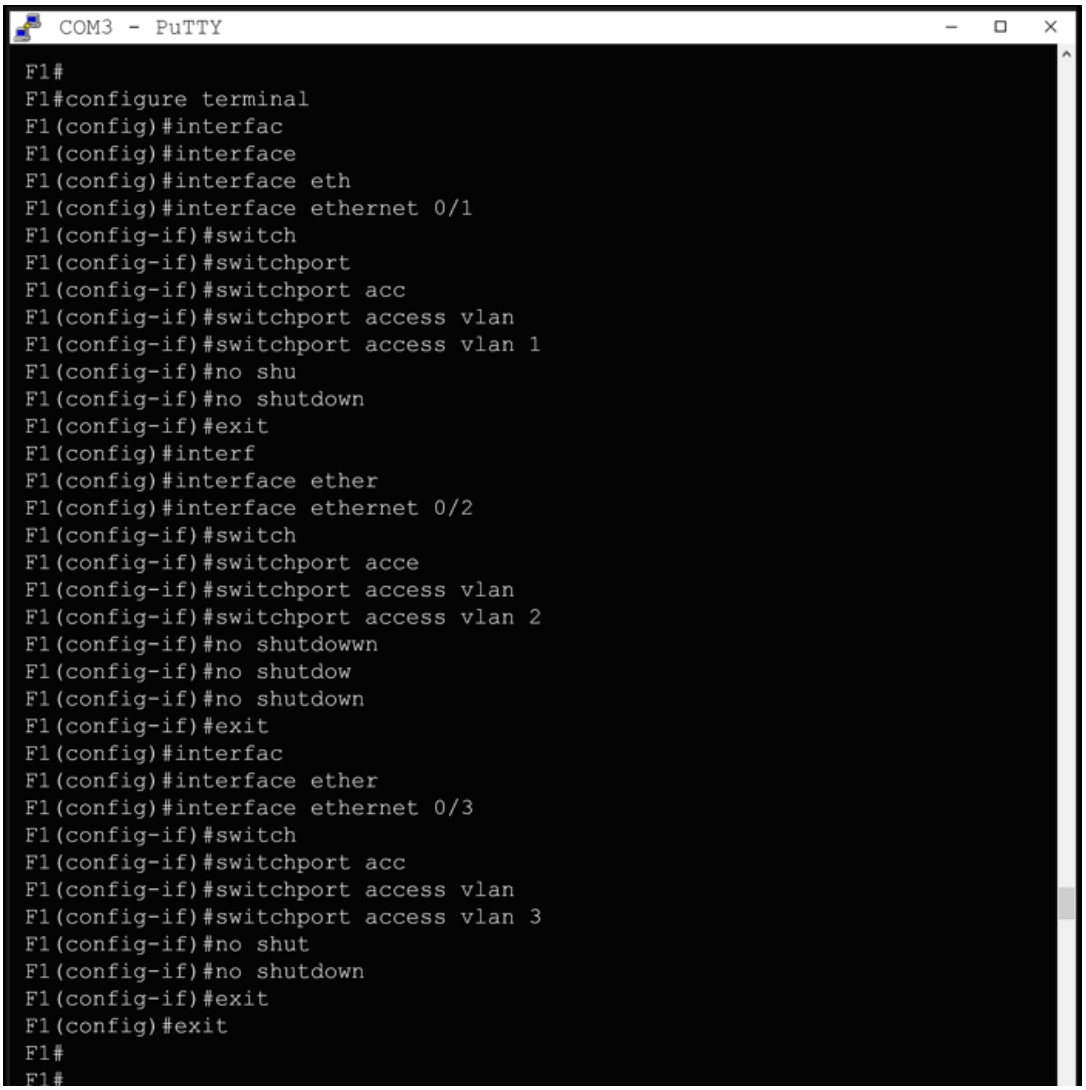
Fuente: Pantallazo propio de licencias del firewall Cisco ASA505

La imagen muestra el número de Vlans adquiridas, el cual facilita el uso de una tercera Vlan pero con la restricción DMZ, esta quiere decir que debe tener un nivel de seguridad inferior a la Vlan 1 y su uso debe ser únicamente para subredes internas.

Configuración de las entradas Ethernet para asignación de Vlan’s

Figura 27

Configuración de salidas Ethernet



Fuente: Pantallazo propio de la configuración de salidas ethernet

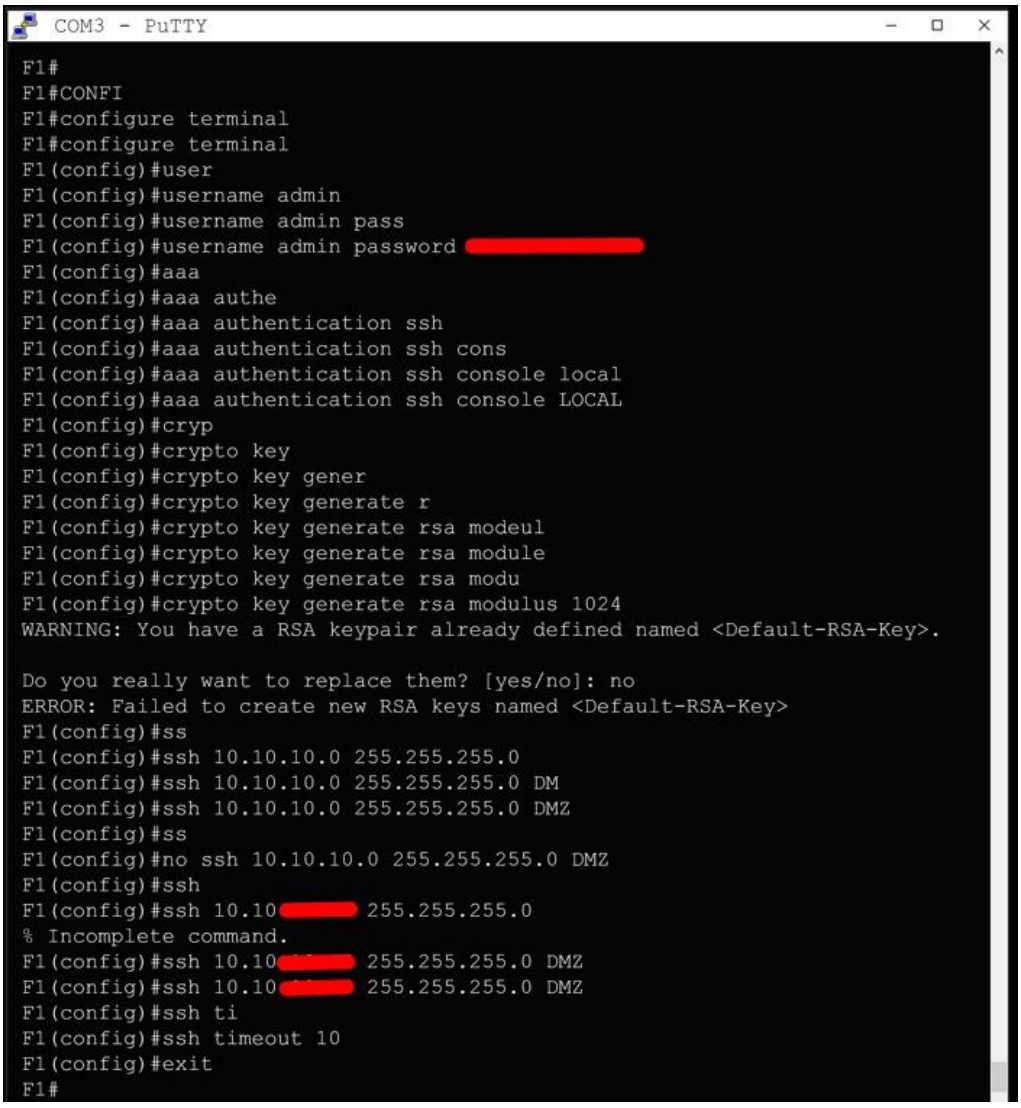
La figura muestra la configuración de los terminales ethernet, la facilidad de configurar el firewall Cisco 5055, es que permite asignar cada Vlan a cada salida ethernet, facilitando así la asignación de los terminales. Para esta configuración se ingresó al terminal mediante el comando “configure terminal”, luego se ingresó al ethernet con el comando “interface ethernet (número de ethernet)”; por defecto en el Cisco ASA5505 empieza con el ethernet 0/0, el cual se le asigna la vlan 2, para evitar conflictos no se escoge esta salida ethernet.

Por tal razón, se escogieron las salidas ethernet 0/1, 0/2 y 0/3. Para la asignación de Vlans a cada salida, se realiza la configuración mediante el comando “switchport Access vlan (número de Vlan)”, indicándole a la consola que la dirección Ip que contiene la Vlan elegida formará parte del ethernet de salida con quien se está comunicando la red; finalmente, se coloca el comando “no shutdown” con el fin que el terminal acepte guardar los cambios.

Configuración de SSH, administrador, clave y tiempo de respuesta.

Figura 28

Configuración de SSH.



Fuente: Pantallazo propio de la configuración de SSH

La figura 28 indica la configuración de SSH, mostrando una configuración de los accesos al terminal firewall para realizar modificaciones desde alguna Pc o alguna Subred, para la realización de esta configuración se tiene una serie de pasos y los cuales deben desarrollarse minuciosamente:

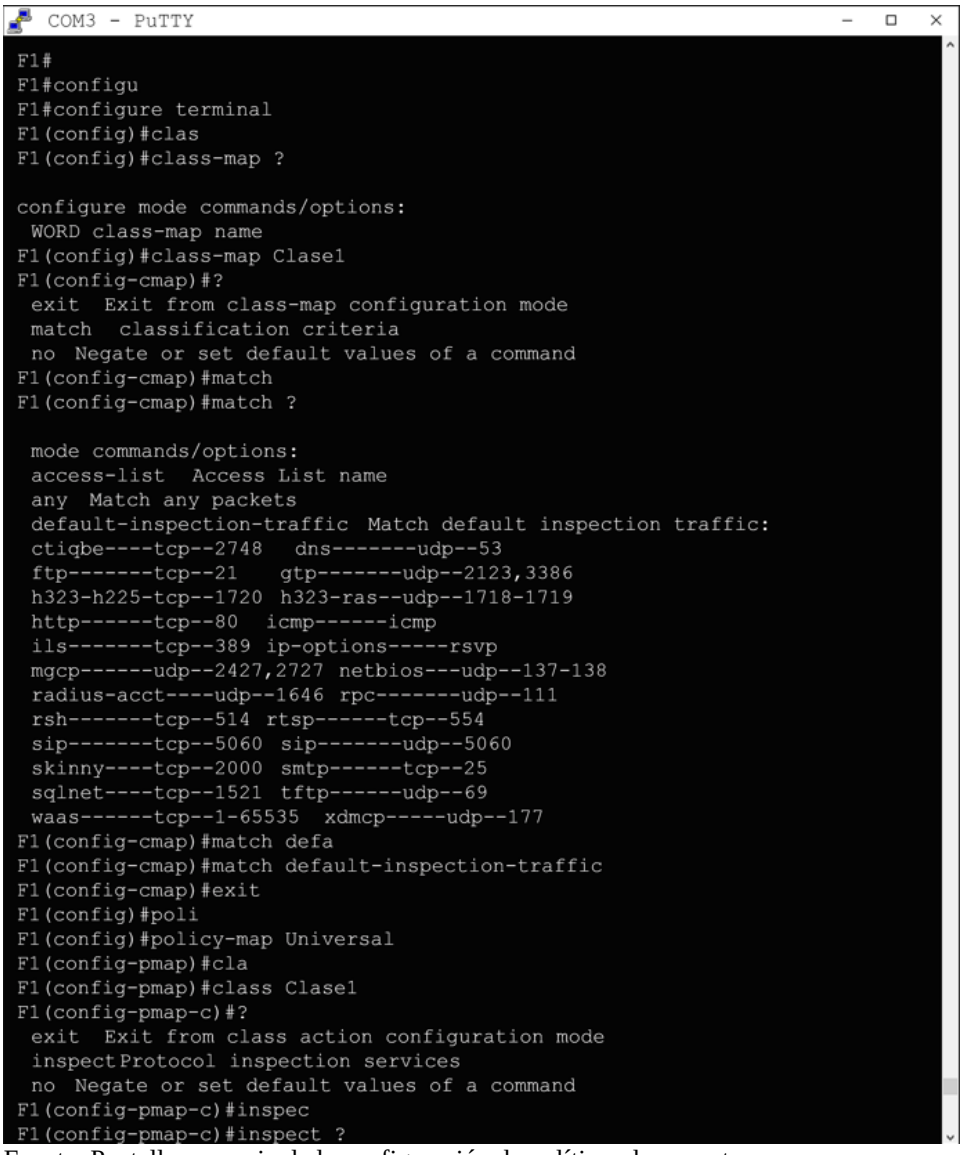
- **Paso 1:** El administrador ingresa al firewall a través de la consola y digita el comando “configure terminal”, este comando le permite ingresar a la configuración general del firewall, seguidamente coloca el comando “username (nombre del usuario)”, facilitando que el usuario creado tenga un nombre asignado para administrar todo el firewall (administrador), seguido del comando se digita el comando “password (contraseña)”, la contraseña es escogida por el encargado de administrar el firewall, en la imagen se restringe la contraseña debido a que su visualización representa vulnerabilidad para la empresa. Finalmente, se realiza la autenticación “aaa” permitiendo únicamente el acceso a la consola a los equipos que están conectados a la red.
- **Paso 2:** Cuando se realiza la protección mediante ssh (protocolo para acceso remoto) se debe considerar una encriptación de la contraseña, esta encriptación se realiza mediante el siguiente comando: “crypto key generate rsa module 1024”, este comando sirve para darle un tamaño al cifrado entre las llaves, para este caso se ha considerado el cifrado de 1024 bits.
- **Paso 3:** Finalmente se agrega la subred que va a tener conexión con el control remoto para el firewall, en este caso se realizó la conexión pertinente con la subred 10.10.10.0 con máscara 255.255.255.0. Pero, al encontrarse que cualquier computador con una dirección ip de la misma subred se podría conectar, se prefirió realizar la conexión con una única PC de dicha subred, en la imagen se colocan filtros rojos por seguridad de la empresa, el comando para realizar esta

acción es “ssh (dirección ip) (máscara de subred) (lugar de la subred)”. Por último y no menos importante es el tiempo para acceder al firewall, este es el tiempo de respuesta que debe tener el firewall en brindar la conexión remota, el comando debe ser “ssh timeout (n° en segundos)”, para esta configuración se tomó en consideración un tiempo de respuesta de 10 segundos.

Configuración de políticas de paquetes

Figura 29

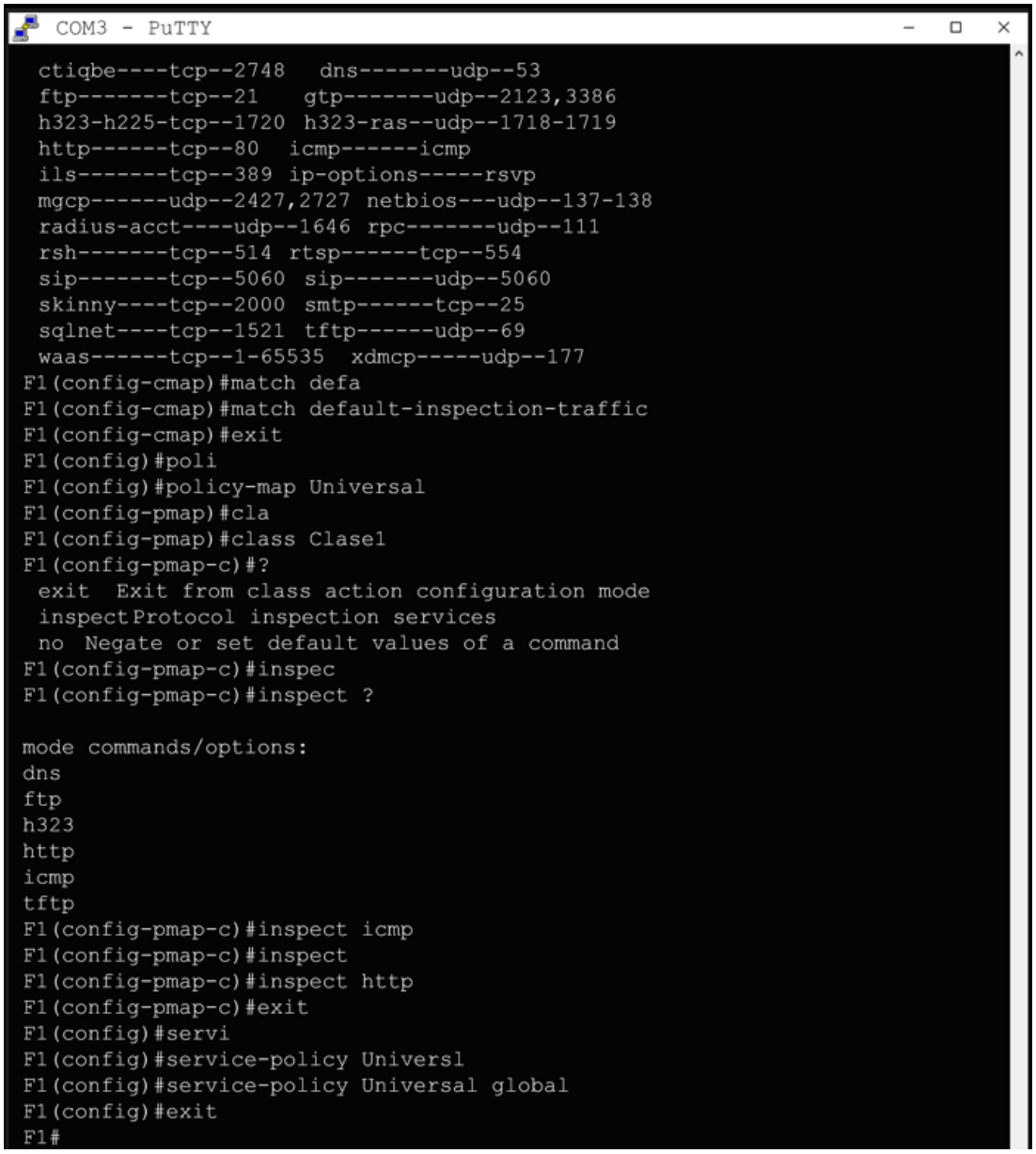
Políticas de paquetes



Fuente: Pantallazo propio de la configuración de políticas de paquetes

Figura 30

Políticas de paquetes



Fuente: Pantallazo propio de la configuración de políticas de paquetes

Cuando se realiza la configuración de políticas en el tráfico de paquetes para instrumentos firewall físicos, es de vital importancia crear dichas políticas, esto a razón que permitirá que, en los flujos de transmisión, existan políticas y reglamentos con los que va a trabajar la red, permitiendo en tal caso el filtrado de las políticas que aceptará el firewall, inspeccionándolas o denegándolas; para la configuración de estas políticas se ha utilizado

la configuración mediante pasos:

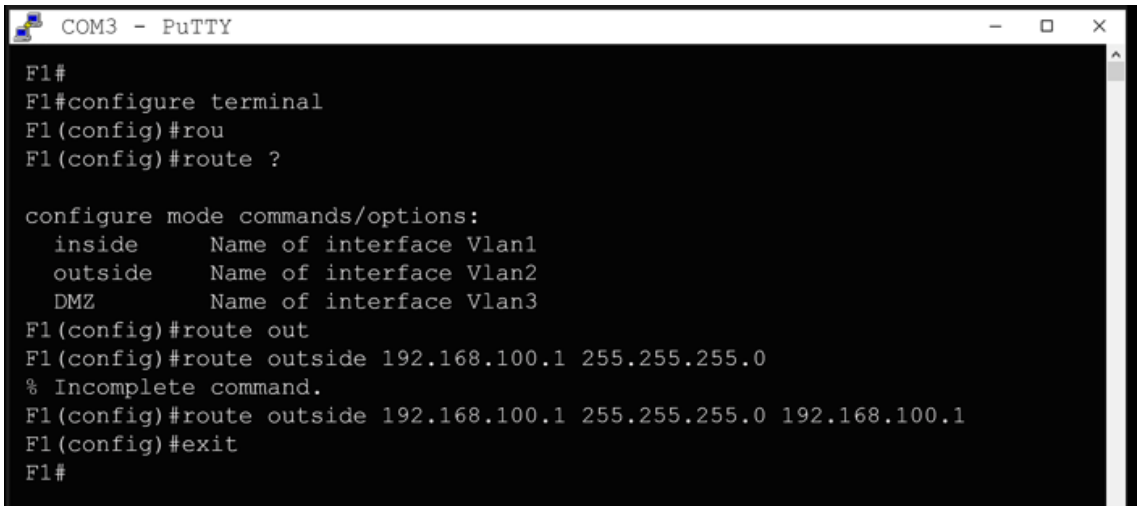
- **Paso 1:** Se realizó la creación de una clase con el fin de iniciar las estructuras de filtrados, para la creación de la clase se realizó el comando “class-map (nombre de la clase)”, para evitar confusiones se eligió el nombre Clase1. Seguidamente se utilizó el comando “match”, este comando facilita el inicio del filtrado, si el filtrado se realiza con una lista de acceso se escoge el comando “access list”, pero dicha configuración se realizó más adelante. Por tal razón, se escogió en primer lugar el filtrado general cuyo comando es “default inspection traffic”, este filtro es una inspección general de los principales protocolos, luego se colocó el comando “exit” para retroceder una línea en la configuración.
- **Paso 2:** Seguidamente se utiliza el comando “policy map”, este comando es utilizado para crear un mapa para las políticas que serán utilizadas en el cortafuego, el comando solicita un nombre al cual se le ha asignado “Universal”, ya que estas serán políticas universales con las que se realizarán los filtrados de paquetes y mantendrán a la información segura. Una vez creado el mapa de políticas se debe añadir la clase creada con el match por defecto, esta clase se añade con el comando “class Clase1”, para luego realizar una inspección de los protocolos con los que se desea trabajar, esta inspección se realiza mediante el comando “inspect (nombre protocolo)”, que para esta configuración solo se ha realizado la inspección de los protocolos ICMP y HTTP(TCP), ya que al ser una entidad de ventas requiere únicamente un control en el tráfico de paquetes con el internet y con la conexión entre cliente y servidor.
- **Paso 3:** Por último, para finalizar con la configuración de políticas estas deben estar en funcionamiento, este funcionamiento se realiza mediante el comando “service-policy Universal global”, este comando permite que la configuración

realizada se coloque en marcha y empiece la inspección de protocolos.

Enrutamientos de salida

Figura 31

Configuración de salida con el Router.



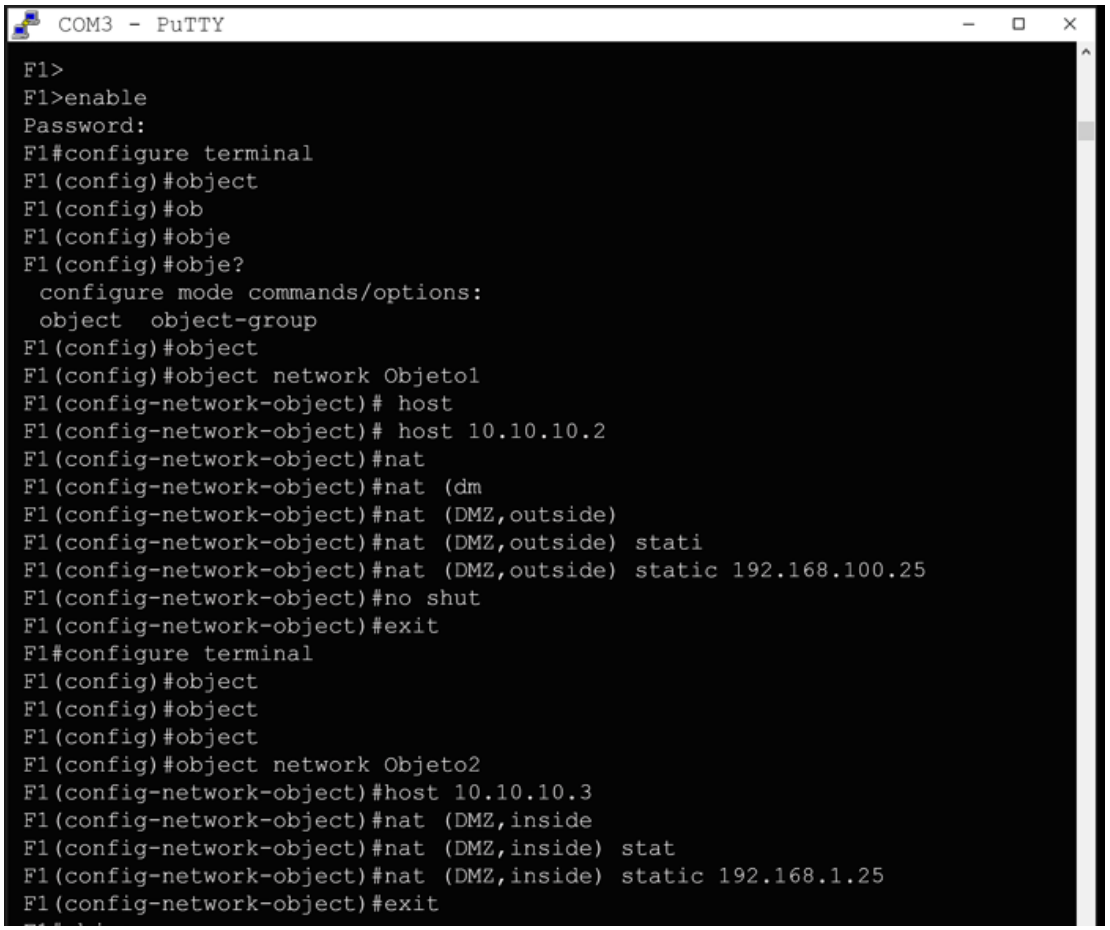
Fuente: Pantallazo propio de las salidas ethernet con las Vlan’s

Para que los ethernet configurados tengan una salida a internet se debe configurar la salida la red WAN mediante el comando “Route (vlan de salida) (dirección ip y máscara del router) (dirección ip puerta de enlace)”, la configuración favorece en hacer comprender a la red, cual es la dirección ip de salida por la que los computadores tendrán acceso al internet. Pero con todo esto, aún no existe conectividad en la red, esto a razón que se requiere de la configuración del NAT, esta configuración facilita que las direcciones IP de una entrada ethernet tengan comunicación con otras salidas, facilitando así la conexión en la red y que los paquetes se transmitan de forma normal, existe una comunicación de NAT universal y una delimitada. Para la red de la Ferretería Soto, se ha utilizado una conexión delimitada en la red de CasaDekor, ya que en esta red se encuentran ubicados los servidores. Por tal razón, la red universal de PAT (NAT con sobrecarga) se realizó con la encriptación de las direcciones ip públicas, evitando que al momento que se realicen peticiones con el servidor se muestre la dirección Ip universal y puedan filtrar la

red y vulnerarla.

Figura 32

Configuración de objetos y NAT.



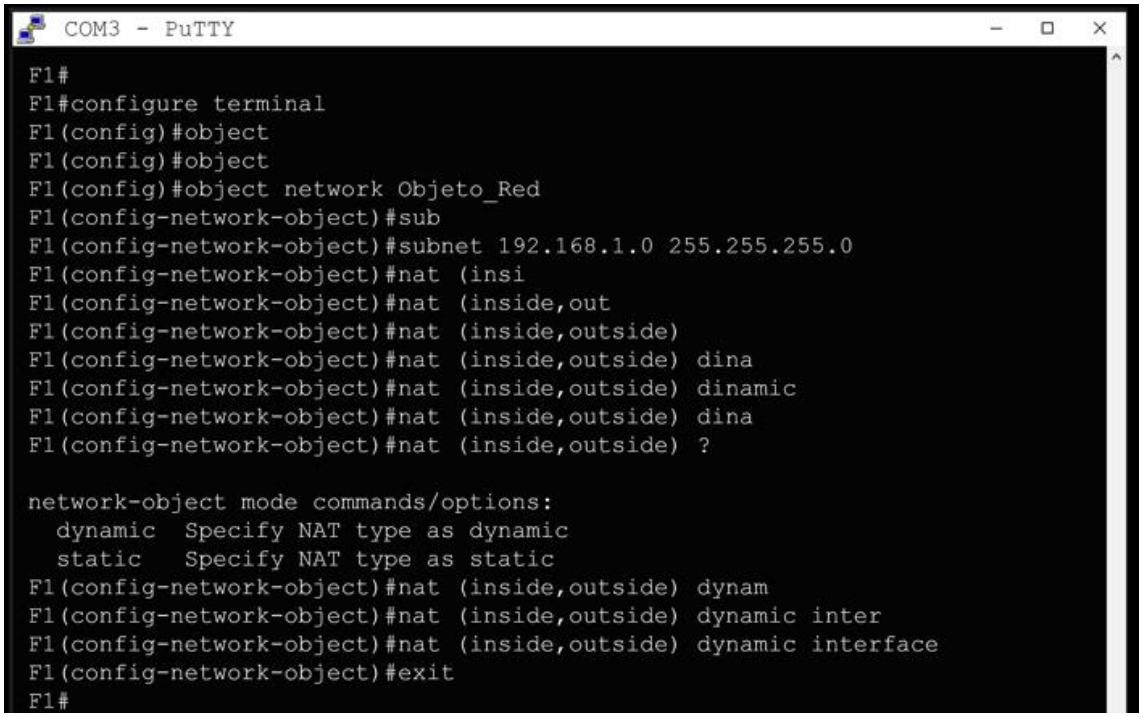
Fuente: Pantallazo propio de la configuración de objetos y NAT

Para tener una comunicación segura se realiza la creación de un objeto, este se realiza mediante el comando “object network”, a este objeto se le añade la dirección Ip con la que se va a comunicar entre las subredes internas, para este comando se utiliza la siguiente configuración “host (dirección ip)”, esto permitirá que el firewall reconozca que la red con quien busca la comunicación, permita un tráfico de paquetes y que, se oculte la dirección Ip. Seguidamente se coloca el comando “nat ((nombre de la Vlan que desea comunicar), (nombre de la Vlan a donde se realizará la comunicación)) static (dirección ip ficticia)”, este comando facilita que los paquetes salgan desde una V’lan a otra, pero

con distinta dirección Ip, lo que protegerá la dirección Ip del servidor ante cualquier ataque. Seguidamente se aprecia la creación de un segundo objeto, facilitando que los computadores de la red inside tengan comunicación con la red DMZ, en la cual están los servidores.

Figura 33

Configuración del PAT



Fuente: Pantallazo propio de la configuración del PAT

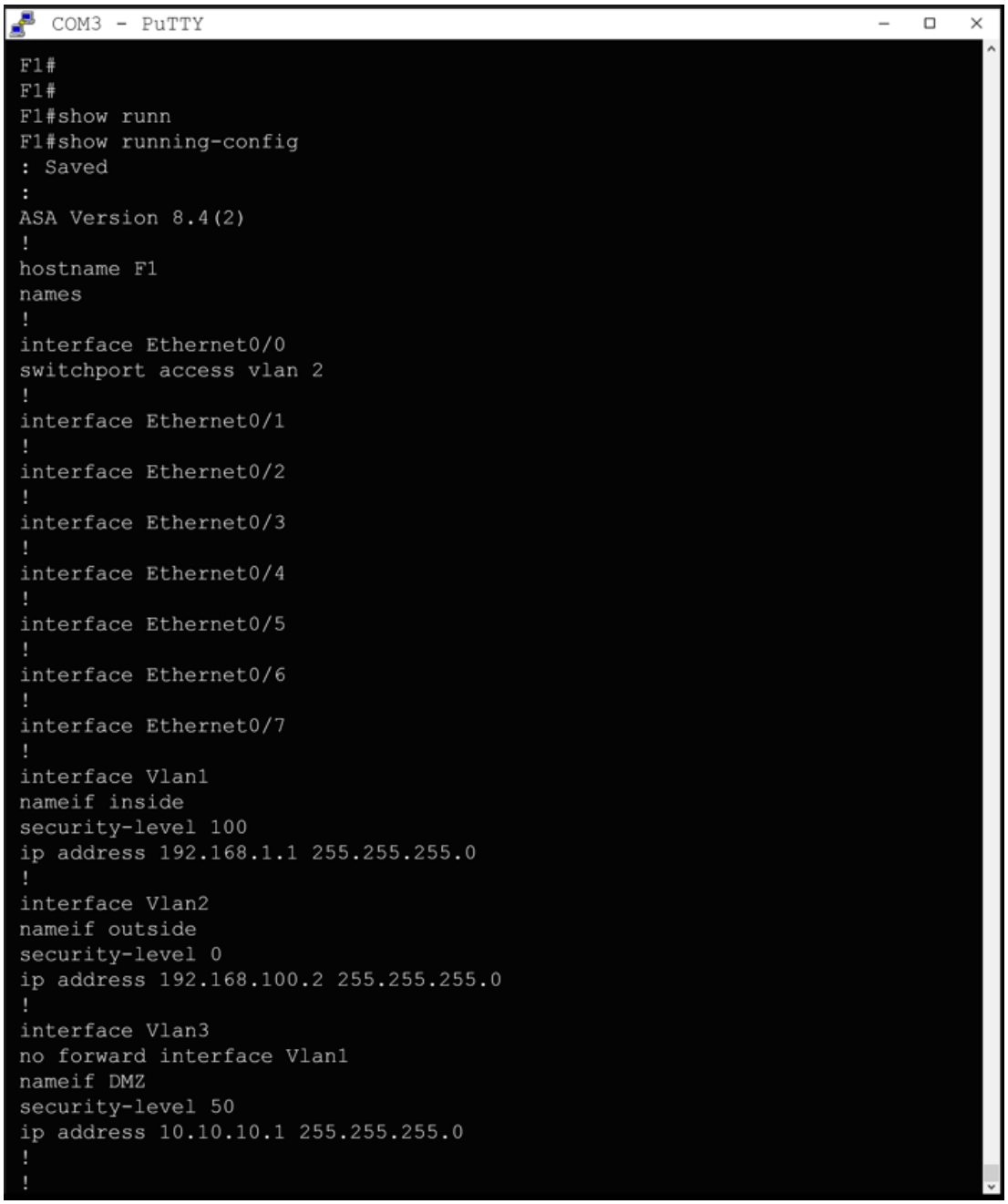
Para la configuración de un PAT se realiza el mismo procedimiento de configuración de un objeto, con la diferencia que se utilizan todas las direcciones Ip que están conectadas a la subred. Conociendo que la V’lan DMZ queda totalmente protegida con la única salida a la red mediante el servidor electrónico, pero que, el servidor de datos únicamente realiza la conexión con la subred inside, es necesario que los computadores internos de la red tengan la facultad de contar conexión con salidas a internet. Por tal razón, se realiza la configuración mediante la creación de un objeto y la selección de una subred completa, el comando para realizar la configuración es “nat ((nombre de la Vlan de inicio), (Nombre

de la Vlna que se solicita la salida) dynamic interface)”, el comando le indica al firewall que los computadores de la red interna se comunicarán con internet únicamente por la interface dinámica de salida.

4.2.2.4. Verificación.

Figura 34

Verificación de la configuración en Vlan's.

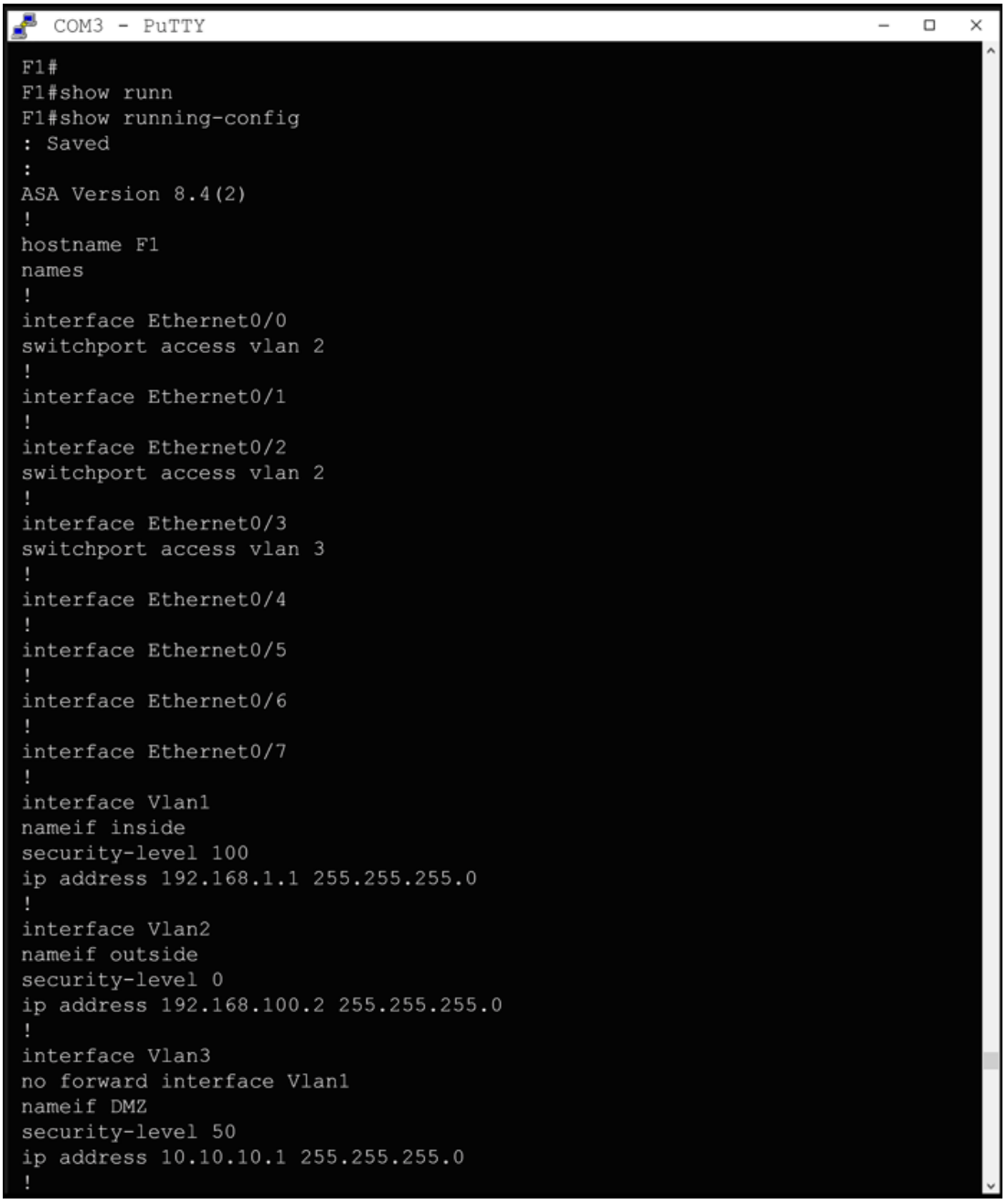


Fuente: Pantallazo propio de verificación de configuración en Vlan´s

La primera verificación del sistema se realizó para la configuración de Vlans, la verificación en las configuraciones se realizó mediate el comando “show running-config”, este comando permite visualizar la configuración general del firewall, apreciándose que la configuración de Vlans se realizó correctamente y cada una con su respectivo nombre, dirección Ip y nivel de seguridad.

Figura 35

Verificación de la configuración en puertos Ethernet

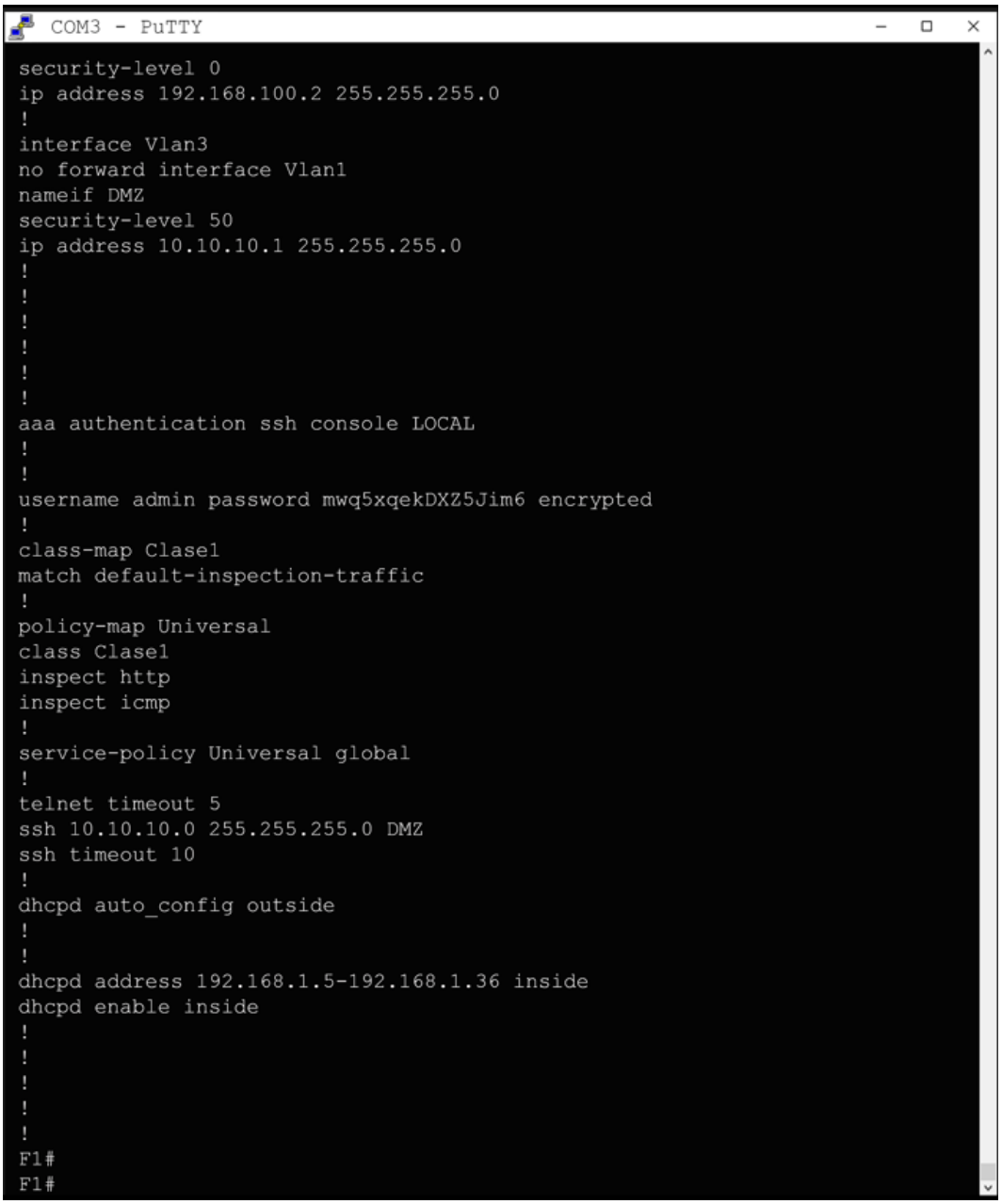


Fuente: Pantallazo propio de verificación de configuración en puertos Ethernet

La verificación de puertos ethernet se realizó para mostrar que cada una de las entradas Ethernet en donde se han realizado conexiones, se le ha asignado una Vlan específica y por ende la dirección Ip de cada Vlan ha migrado a la salida Ethernet.

Figura 36

Verificación de la configuración en protocolos.



Fuente: Pantallazo propio de verificación de configuración en Protocolos.

La configuración de protocolos se realizó para una inspección de protocolos ICMP y HTTP, como se aprecia en la figura se realizó la creación de una clase llamada Clase1,

luego un mapa de políticas el cual se denominó Universal. Finalmente se aprecia que la inspección que se asignó únicamente son los protocolos ICMP Y HTTP.

Figura 37

Verificación de la configuración SSH en la pc de administracion.

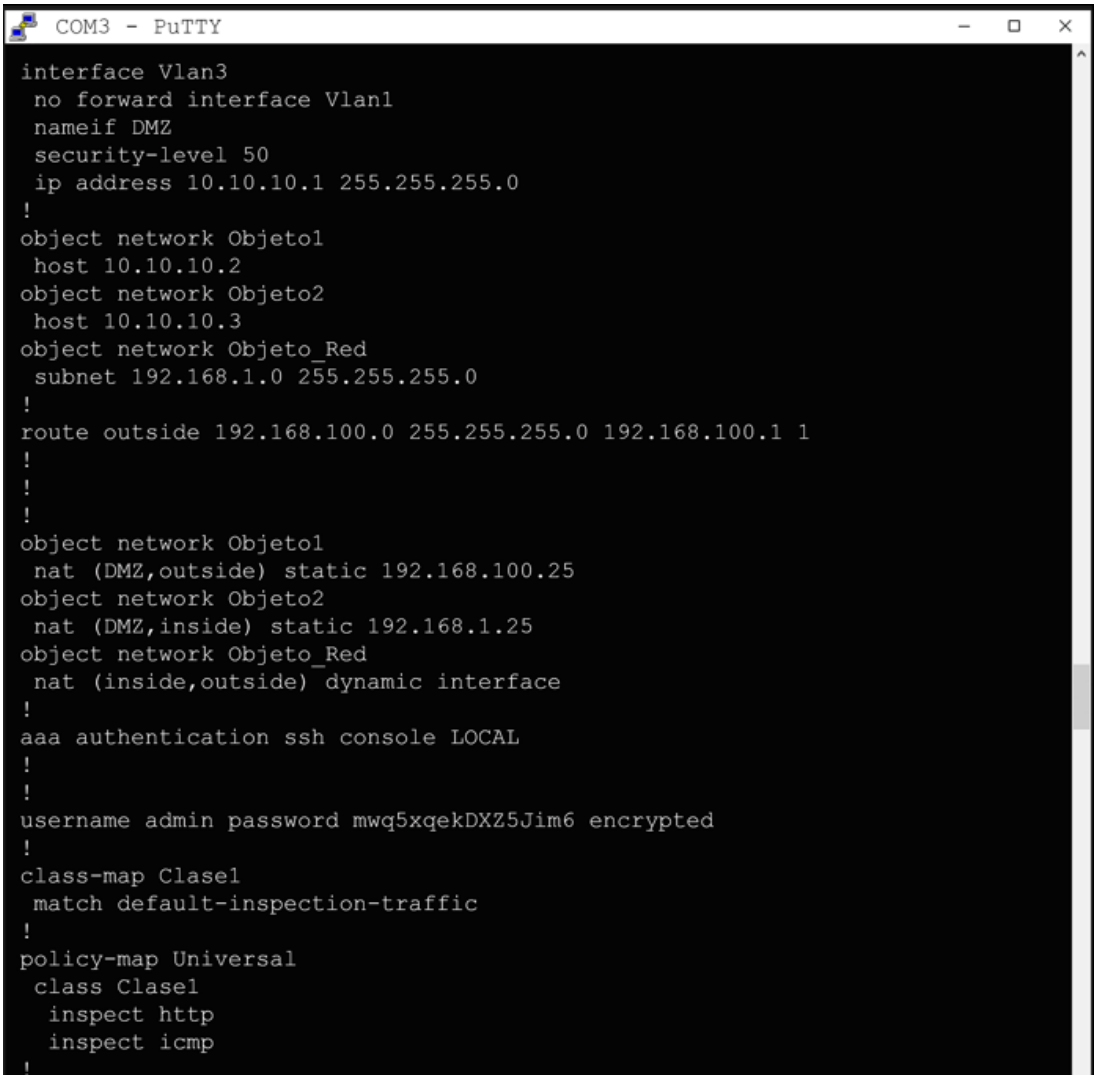
Fuente: Pantallazo propio de verificación de configuración SSH

Para la verificación del control de acceso remoto desde un pc se realizó la configuración en el pc del administrador, este pc llevo la dirección Ip con la máscara configurada.

Inicialmente se ingresa al CMD del pc, luego se coloca el comando “ssh –l admin 10.10.10.1”, esta última dirección es la puerta de enlace por donde se va a comunicar. Finalmente, el control remoto solicita la clave “xxxxxx”, se ingresa la clave y el sistema acepta correctamente el ingreso para tener un control remoto desde un pc a la configuración del terminal firewall.

Figura 38

Verificación de la configuración de objetos y NAT.



Fuente: Pantallazo propio de verificación de configuración en objetos y NAT

Con el objetivo de mejorar la seguridad se realizó la configuración de salidas con internet, para esto se protegió el servidor de red a través de un NAT con una dirección ip ficticia,

la cual se muestra al comunicarse con los equipos de la red y evita que los paquetes puedan ser vulnerados mediante la dirección Ip real. Seguidamente se aprecia la creación de un objeto adicional y que permite la comunicación de los computadores internos de la red con el servidor de datos, estos de igual forma presentan una configuración NAT con direccionamiento estático para comunicarse con el servidor mediante una dirección Ip ficticia, esto protegerá los datos a través de la configuración de NATEO. Finalmente, se realizó la configuración de un tercer objeto, el cual facilita configurar el firewall para que los equipos en la V’lan 1 presenten salida a la internet mediante una configuración dinámica. Esta configuración tiene la facilidad de registrar los paquetes que son necesarios de la red de internet, pero faculta de otro puerto a las restricciones con la comunicación del servidor.

4.2.1. Fase de Optimización.

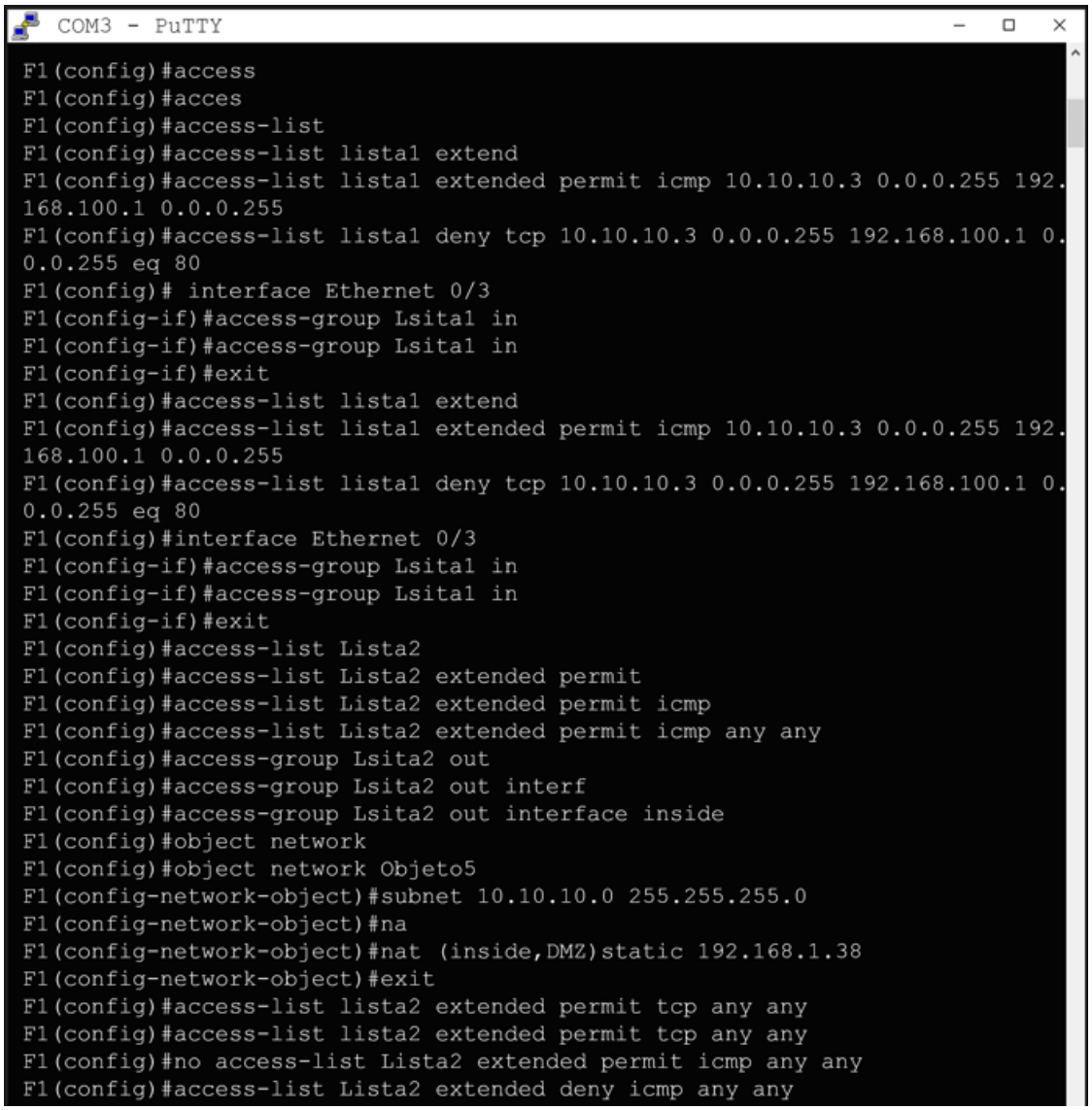
Con la configuración del firewall terminada se realiza la optimización de la configuración, para esto, el firewall de cisco presenta la posibilidad de realizar listas de acceso con la creación de objetos y grupos. Debido a ello se realizó la optimización de la configuración centrándose únicamente en el tráfico de datos de las direcciones Ip con que trabaja la ferretería, esto le brinda una seguridad adicional a la Ferretería Soto, ya que la protección se limita únicamente a cada dirección Ip que trabaja en la red, en la mayoría de configuraciones no se realiza las listas de control de acceso, debido a que la configuración representa mucho cuidado, si un dirección Ip o lista de acceso creada, no tiene la dirección correcta o no está asignada en el grupo correcto, las direcciones ip no tendrán salida ni acceso a los servidores o las puertas de enlace que se han configurado.

En las siguientes configuraciones se aprecia la creación de listas de acceso para delimitar la subred y asignar permisos de tráfico de paquetes TCP e ICMP, a su vez se mostrará las

pruebas realizadas en el firewall Cisco 5505H.

Figura 39

Configuración de listas de acceso, NAT y objetos.



Fuente: Pantallazo propio de la configuración en listas de acceso, objetos y NAT.

La optimización para las direcciones Ip y las subredes se realizó mediante la configuración de dos listas de acceso, la primera lista se colocó el comando “access-list (nombre de la lista) extended permit (protocolo de acceso) (dirección ip salida y su wilcard) (dirección ip de salida y su wilcard)”, este comando se realiza para fijar una dirección ip específica y, permitirle o denegarle la salida a internet; para este caso se le

permitió a la dirección Ip del servidor electrónico (10.10.10.3) tener salida a la internet y poder realizar la facturación electrónica como se debe. Pero, por el contrario, se le realiza la denegación del servicio TCP, debido a que esto les denegará a los usuarios externos no poder tener conexión con sus DNS y evitar el filtrado de paquetes, esta lista de acceso presenta la funcionalidad de estar instalada directamente en la salida Ethernet 0/3 que es la salida desde la subred 10.10.10.0/24. Por otro lado, se realiza otra configuración directamente en firewall, esta configuración se realiza mediante la creación una nueva lista de acceso, la cual es asignada al grupo universal del firewall, esta configuración se realizó a los computadores de la red inside, con el fin de realizar una comunicación entre los protocolos TCP y evitar la comunicación de protocolos ICMP. En una empresa como la Ferretería Soto, donde se tiene la única funcionalidad de realizar ventas y comunicar sus computadores principales con los servidores, estos no requieren del protocolo ICMP, la única funcionalidad es que presente comunicación con el DNS de los servidores, por tal motivo se realizó una configuración para controlar a la subred inside, permitiendo la comunicación con protocolos TCP, pero negando toda comunicación ICMP.

CAPÍTULO V: RESULTADOS Y DISCUSIÓN

Con la implementación del firewall se realizó una charla a todo el personal administrativo de la ferretería Soto, dicha charla se realizó con el fin que todo el personal administrativo de la empresa tenga el conocimiento necesario sobre lo realizado y los cambios que ha generado la implementación del dispositivo firewall.

De igual modo, la charla se realizó para proporcionar conocimiento y afianzar ideas en el personal administrativo, ya que ellos, tendría que responder el instrumento recolector de datos (cuestionario), el mismo que ha pasado por un análisis estadístico para medir la influencia que ha generado una variable sobre la otra en la investigación.

5.1. Presentación, análisis e interpretación de los resultados.

La investigación consideró realizar la implementación de un firewall físico en la Ferretería Soto, que permita tener un control de accesos y protección en la red de datos, a esto se le añade que la hipótesis de la investigación buscó conocer la influencia que generaba dicha implementación en los controles de acceso y protección de la red, motivo por el que se consideró la estadística Chi-Cuadrado como instrumento estadístico para obtener el resultado necesario para demostrar la hipótesis planteada. Por tal razón, para la verificación de los instrumentos de recolección de datos, se realizó una validación por tres magísteres de la carrera profesional de ingeniería de sistemas (anexos. 1, 2 y 3).

Para afianzar un conocimiento y brindar resultados eficientes es necesario la validación de un grupo de expertos que, acrediten que los criterios de validación en relación a la investigación son los correctos (Escobar y Cuervo, 2007, p. 29).

5.1.1. Presentación de los datos.

A razón que la investigación desarrollada consideró la utilización de dos instrumentos de recolección de datos (Hoja de cotejo y Cuestionario), la presentación de cada instrumento se dio en relación a la verificación de la implementación de firewall y, por otro lado, la

verificación de la hipótesis de la investigación.

Las hojas de cotejo se realizaron para la comprobación de la instalación del firewall, debido a que, al ser una implementación de un dispositivo físico, las verificaciones de los comandos presentaban muchos términos en telecomunicaciones, siendo términos poco entendibles para especialistas en otras áreas. Para facilitar la comprobación del dispositivo firewall se consideró únicamente dos términos: “logrado” y “no logrado”, a razón que esto facilitó realizar el análisis de asociación en la hoja de cotejo dirigida a los expertos.

Por otra parte, el cuestionario que fue enfocado en el personal administrativo de la Ferretería Soto presentó una escala de Likert de 5 ítems con una valoración del 1 al 5, la consideración se tomó en cuenta para que el personal tenga mayor opción a escoger un ítem que se acomode a la perspectiva de su respuesta.

- **Presentación de datos de expertos obtenidos con las hojas de cotejo.**

La hoja de cotejo se realizó por un juicio de expertos de 3 ingenieros en sistemas, los cuales al realizar la hoja de cotejo acreditaron que se había logrado la implementación del firewall en su totalidad, según se aprecia en los anexos 4, 5 y 6; donde se indican que los resultados son unánimes en relación a los 16 ítems de la hoja de cotejo.

La hoja de cotejo realizó una validación en relación a las descripciones (“logrado” y “no logrado”), las descripciones elegidas en la hoja de cotejo fueron necesarias para validar y confirmar que la implementación del firewall se ha realizado correctamente.

Asimismo, fue necesario aplicar una hoja de cotejo que fuere realizada por expertos para acreditar que la configuración e implementación del firewall cumple su propósito. Tobón (2013) mencionan sobre el instrumento de hoja o lista de cotejo, indicando que son instrumentos que brindan características de aprendizaje para evaluar las actividades experimentale y prácticas, indicando que se ha realizado, logrando o presentado una

actividad, implementación o experimentación (p. 4).

Debido a lo mencionado, es que se consideró la utilización de dos respuestas en la hoja de cotejo, para que de este modo se pueda apreciar si se ha logrado correctamente la implementación del firewall y verificar la realización del instrumento según cada experto.

Tabla 11

Respuestas por los expertos en relación a la hoja de cotejo.

Experto 1, 2 y 3		
Ítem	**Dimensión variable independiente**	**Respuesta**
1, 2, 3 y 4	Políticas	Logrado en todos los ítems
5, 6, 7 y 8	Seguridad	Logrado en todos los ítems
Ítem	**Dimensión variable dependiente**	**Respuesta**
1, 2 y 3	Integridad	Logrado en todos los ítems
4, 5 y 6	Seguridad	Logrado en todos los ítems
7 y 8	Disponibilidad	Logrado en todos los ítems

Nota: La respuesta de los tres expertos fue unánime en relación a la implementación del firewall, permitiendo dar acreditación de la implementación. Cada respuesta se aprecia en los anexos 4, 5 y 6 en el apartado de ANEXOS del presente documento.

Como se aprecia en la tabla n°11, cada uno de los expertos consideró una respuesta de logrado en todos los ítems, con ello se ha demostrado que la implementación del firewall para control de accesos y protección de la red, presenta una implementación totalmente correcta y con las políticas necesarias para mantener un control de la red.

- **Presentación de datos de administrativos obtenidos con el cuestionario**

El cuestionario implementado al grupo de administrativos de la Ferretería Soto se ha realizado con el fin de apreciar el impacto, importancia, mejora, etc.; que ha generado la implementación del firewall sobre los accesos y la protección de la red.

La implementación del cuestionario fue realizado al grupo de 7 administrativos de la Ferretería soto, dicho cuestionario estuvo conformado por 10 ítems, estos divididos equitativamente con 5 ítems por cada variable. De igual modo, el cuestionario presentó

una escala de Likert en relación a 5 categorías: *“siempre”* con un valor de “1”, *“generalmente”* con un valor de “2”, *“ocasionalmente”* con un valor de “3”, *“casi nunca”* con un valor de “4” y *“nunca”* con un valor de “5”. Los valores mencionados se denotan textualmente para mostrar en la siguiente tabla que valor acreditó cada personal administrativo en relación a cada ítem del cuestionario.

Tabla 12

Respuestas por los administrativos en relación al Cuestionario.

Ítem	**Dimensión**	**Administrativos**						
Variable independiente		**1**	**2**	**3**	**4**	**5**	**6**	**7**
1	Políticas	1	2	1	1	1	2	1
2	Políticas	1	1	1	1	1	1	1
3	Seguridad	1	1	1	1	1	1	1
4	Seguridad	1	1	1	2	1	2	2
5	Seguridad	1	1	1	1	1	1	1
Variable Dependiente		**1**	**2**	**3**	**4**	**5**	**6**	**7**
6	Integridad	1	1	1	1	1	1	1
7	Seguridad	1	1	1	1	1	2	1
8	Seguridad	1	1	1	1	1	1	1
9	Disponibilidad	1	1	1	1	1	2	1
10	Disponibilidad	1	1	1	2	1	2	2

Nota: En la tabla se aprecia la respuesta de cada uno de los 7 administrativos de la ferretería Soto, dichas respuestas son confirmadas y corroboradas en el anexo n°7 en el apartado de ANEXOS del presente documento.

Con los datos obtenidos del cuestionario realizado al grupo de administrativos se logró obtener los datos necesarios para realizar una influencia y determinar el impacto y la mejora que ha presentado la implementación del firewall sobre el control de accesos y la seguridad en la red de datos.

5.1.2. Análisis de los datos.

Los análisis de los datos se realizaron con la herramienta Excel, asimismo para verificar

que la influencia es correspondiente y tener la acreditación de la significancia, se realizó el análisis en la herramienta SPSS, esto ayudó a que se conozca el proceso de desarrollo de la estadística de Chi-Cuadrado.

- **Análisis de datos de los expertos obtenidos con las hojas de cotejo.**

Figura 40

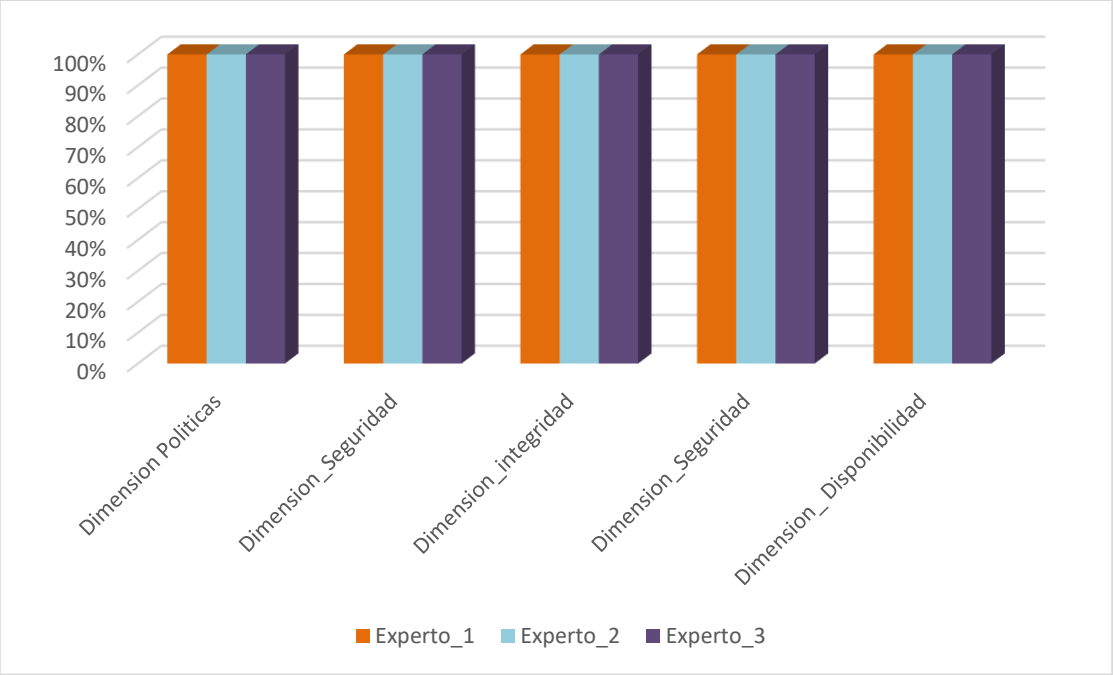
Resultados en Excel de la hoja de cotejo realizada a expertos.

/		Items	Experto_1	Experto_2	Experto_3
Variable Independiente	Dimensión_Políticas	1	Logrado	Logrado	Logrado
		2	Logrado	Logrado	Logrado
		3	Logrado	Logrado	Logrado
		4	Logrado	Logrado	Logrado
	Dimensión_Seguridad	5	Logrado	Logrado	Logrado
		6	Logrado	Logrado	Logrado
		7	Logrado	Logrado	Logrado
		8	Logrado	Logrado	Logrado
Variable dependiente	Dimensión_Integridad	9	Logrado	Logrado	Logrado
		10	Logrado	Logrado	Logrado
		11	Logrado	Logrado	Logrado
	Dimensión_Seguridad	12	Logrado	Logrado	Logrado
		13	Logrado	Logrado	Logrado
		14	Logrado	Logrado	Logrado
	Dimensión_ Disponibilidad	15	Logrado	Logrado	Logrado
		16	Logrado	Logrado	Logrado

Según la hoja de cotejo realizada a los expertos solo hay dos respuestas disponibles: “Logrado” y “no logrado”. Como se aprecia en la figura 40 los tres expertos han realizado una marcación del 100% de la descripción de: *logrado*, lo que afirma que el firewall implementado cumple cada una de las dimensiones en relación al firewall y la seguridad en el control de accesos.

Figura 41

Porcentajes de los expertos en relación a las dimensiones en la hoja de cotejo.



Con la figura 40 y 41 se tiene una apreciación global e informativa que la implementación del firewall ha sido un éxito, debido a que ha cumplido con cada uno de los ítems que se debe considerar en una implementación de este tipo de dispositivos.

- **Análisis de datos obtenidos con el cuestionario.**

Los análisis de los datos se realizaron con la herramienta Excel y SPSS debido a que la precisión de los datos debe estar alineada con la realización del estadístico. En primer lugar, se ha realizado el conteo de los valores que cada administrativo ha marcado en relación a las preguntas propuestas, luego se ha realizado una sumatoria por cada dimensión y la obtención de un promedio por cada una de estas. Finalmente se ha logrado obtener un promedio universal por cada variable para tener un valor estadístico promedio en relación a la variable nominal, permitiendo así tener la significancia entre las variables de los valores obtenidos de los administrativos.

Figura 42

Toma de datos y obtención de promedios por variable.

Administrativos	Variable Independiente					Variable dependiente				
	Dimension_Politicas		Dimension_Seguridad			Dimension_Integrida	Dimension_Seguridad		Dimension_Disponibilidad	
1	1	1	1	1	1	1	1	1	1	1
2	2	1	1	1	1	1	1	1	1	1
3	1	1	1	1	1	1	1	1	1	1
4	1	1	1	2	1	1	1	1	1	2
5	1	1	1	1	1	1	1	1	1	1
6	2	1	1	2	1	1	2	1	2	2
7	1	1	1	2	1	1	1	1	1	2

Administrativos	Variable Independiente		Variable dependiente		
	Dimension_Politicas	Dimension_Seguridad	Dimension_Integrida	Dimension_Seguridad	Dimension_Disponibilidad
1	1	1	1	1	1
2	1.5	1	2	1	1
3	1	1	1	1	1
4	1	1.333333333	1	1	1.5
5	1	1	1	1	1
6	1.5	1.333333333	1	1.5	2
7	1	1.333333333	1	1	1.5

Administrativos	Variable Independiente	Variable dependiente
	Promedio_Variable	Promedio_Variable
1	1	1
2	1.25	1.333333333
3	1	1
4	1.166666667	1.166666667
5	1	1
6	1.416666667	1.5
7	1.166666667	1.166666667

Como se aprecia en la figura 42, los datos obtenidos han sido plasmados en Excel con el fin de tener una contabilidad de cada dato, luego se ha obtenido un promedio por cada dimensión, con el fin de obtener el mismo número de datos.

Para la realización de una prueba de Chi-Cuadrado se debe analizar el número de los datos obtenidos en relación a la escala categórica de las variables, ya que esto permitirá observar y evidenciar un resultado favorable que se tiene en relación a cada una de las variables, logrando así determinar un valor correcto y no uno al alzar. Para dicho análisis se ha utilizado la herramienta estadística IBM SPSS, la misma que arrojado los siguientes valores cruzados de la dependencia y de la significancia entre ambas variables.

Figura 43

Tabla cruzada entre variables

Tabla cruzada Var_Inde*Var_Depe

			Var_Depe				
			Siempre	1,17	1,33	1,50	Total
Var_Inde	Siempre	Recuento	3	0	0	0	3
		Recuento esperado	1,3	,9	,4	,4	3,0
		% dentro de Var_Inde	100,0%	0,0%	0,0%	0,0%	100,0%
		% dentro de Var_Depe	100,0%	0,0%	0,0%	0,0%	42,9%
		Residuo corregido	2,6	-1,4	-,9	-,9	
	1,17	Recuento	0	2	0	0	2
		Recuento esperado	,9	,6	,3	,3	2,0
		% dentro de Var_Inde	0,0%	100,0%	0,0%	0,0%	100,0%
		% dentro de Var_Depe	0,0%	100,0%	0,0%	0,0%	28,6%
		Residuo corregido	-1,4	2,6	-,7	-,7	
	1,25	Recuento	0	0	1	0	1
		Recuento esperado	,4	,3	,1	,1	1,0
		% dentro de Var_Inde	0,0%	0,0%	100,0%	0,0%	100,0%
		% dentro de Var_Depe	0,0%	0,0%	100,0%	0,0%	14,3%
		Residuo corregido	-,9	-,7	2,6	-,4	
	1,42	Recuento	0	0	0	1	1
		Recuento esperado	,4	,3	,1	,1	1,0
		% dentro de Var_Inde	0,0%	0,0%	0,0%	100,0%	100,0%
		% dentro de Var_Depe	0,0%	0,0%	0,0%	100,0%	14,3%
		Residuo corregido	-,9	-,7	-,4	2,6	
Total		Recuento	3	2	1	1	7
		Recuento esperado	3,0	2,0	1,0	1,0	7,0
		% dentro de Var_Inde	42,9%	28,6%	14,3%	14,3%	100,0%
		% dentro de Var_Depe	100,0%	100,0%	100,0%	100,0%	100,0%

Figura 44

Significancia: Chi-Cuadrado

Pruebas de chi-cuadrado

	Valor	df	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	21,000[a]	9	,013
Razón de verosimilitud	17,878	9	,037
Asociación lineal por lineal	5,919	1	,015
N de casos válidos	7		

a. 16 casillas (100,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,14.

5.1.3. Interpretación de los datos.

Con el objetivo de evidenciar el proceso realizado mediante la prueba estadística Chi-Cuadrado y poder interpretar los valores obtenidos, se citó ciertos autores que indican la interpretación de los datos obtenidos.

IBM (2022) indica que el cruce de tablas entre los valores muestra la inlfuencia que tiene una variable con la otra en relación a las categorías, Chi-cuadrado, brinda un resultado más acertado en relación a las asociaciones a diferencia de las estadísticas correlativas de Spearman o Pearson, pero limita su estadística únicamente a pruebas no paramétricas.

Estemática (2021) brinda mediante un ejemplo la interpretación de los valores en relación a dos variables categóricas según un ejemplo, el cual permite evidenciar los porcentajes e interpretación de los valores.

Figura 45

Ejemplo para interpretación de tablas cruzadas.

Tabla cruzada Localización (1=Urbano; 2=Rural)*Practica deporte (1=No; 2=Ocasional; 3=Frecuente)

			Practica deporte (1=No; 2=Ocasional; 3=Frecuente)			
			No	Ocasionalmente	Frecuentemente	Total
Localización (1=Urbano; 2=Rural)	Urbano	Recuento	95	199	271	565
		Recuento esperado	76,8	239,5	248,6	565,0
		% dentro de Localización (1=Urbano; 2=Rural)	16,8%	35,2%	48,0%	100,0%
		Residuo corregido	2,7	-4,2	2,3	
	Rural	Recuento	150	565	522	1237
		Recuento esperado	168,2	524,5	544,4	1237,0
		% dentro de Localización (1=Urbano; 2=Rural)	12,1%	45,7%	42,2%	100,0%
		Residuo corregido	-2,7	4,2	-2,3	
Total		Recuento	245	764	793	1802
		Recuento esperado	245,0	764,0	793,0	1802,0
		% dentro de Localización (1=Urbano; 2=Rural)	13,6%	42,4%	44,0%	100,0%

En los Resultados de las tablas de contingencia, se aprecian los **residuos corregidos significativos (>1,96)**, que expresan diferencias en el contraste de % de las respectivas categorías

Tomado de *Estemática.* 2021.

IBM (2022) hace mención a la interpretación en relación a la significación bilateral de los valores obtenidos en la estadística Chi-Cuadrado. Cuya interpretación está relacionada con los valores obtenidos en relaciona la significancia de Chi-cuadrado-Pearson, razón de verisimilitud y la asociación lineal por lineal.

Figura 46

Ejemplo para interpretación de significación en Chi- cuadrado.

Chi-Square Tests

Statistics	Value	df	Values Asymptotic Significance (2-sided)
Pearson Chi-Square	37.677[a]	3	.000
Likelihood Ratio	37.313	3	.000
Linear-by-Linear Association	36.537	1	.000
N of Valid Cases	6400		

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 228.73.

Chi-cuadrado de Pearson contrasta la hipótesis que afirma que las variables de fila y columna son independientes. El valor real del estadístico no es muy informativo. El valor de significación (*Sig. Asintótica Sig.*) contiene la información que estamos buscando. Cuanto menor sea el valor de la significación, menor posibilidad habrá de que las dos variables sean independientes (no estén relacionadas). En este caso, el valor de significación es tan bajo que aparece como ,000, lo que quiere decir que parece que las dos variables están, de hecho, relacionadas.

Tomado de *IBM.* 2021.

Fallas (2012) menciona que, la significancia de influencia se relaciona con el porcentaje de error y confianza, dicho porcentaje está relacionado con el resultado proporcionado por la herramienta estadística, si la significancia a desarrollarse es con el 5%, la interpretación presenta la correspondencia que: Si el P valor es menor a 0.05 se acepta la hipótesis planteada y se rechaza toda hipótesis nula. Por otro lado, si el P valor es mayor a 0.05 se acepta la hipótesis nula y se rechaza la hipótesis alternativa (p. 13).

Fallas (2012) también considera que el grado de significancia con mayor estatus, es aquel que presenta un porcentaje de error menor al 5% lo que significa que, si existe una significancia del 0.01, la probabilidad de certeza en aceptar o negar la hipótesis haciende, ya que la estadística se desarrolla en base a un nivel de confianza del 99%; teniendo que, si el P valor es menor a 0.01 se acepta la hipótesis con un 99% de confianza

y se rechaza toda hipótesis nula, mientras que , si el P valor es mayor a 0.01 se niega la hipótesis con un 99% de confianza y se acepta la hipótesis nula (p. 14).

Con los autores tomados, se puede realizar la interpretación de los valores obtenidos mediante la estadística de Chi-Cuadrado, por tal motivo se puede determinar que en las figuras n° 43, se muestra que los valores de la tabla cruzada entre las variables son los siguientes:

Tabla 13

Valores obtenidos en la tabla cruzada de Chi-Cuadrado.

Var. / Var.	Siempre	1,17	1,33	1,42	Resultados	Residuo Corregido
Siempre	3				42,9%	2,6
1,17		2			28,6%	2,6
1,25			1		14,3%	2,6
1,50				1	14,3%	2,6

Mostrando los valores obtenidos en las tablas cruzadas, podemos determinar mediante la interpretación de Estemática, que los valores obtenidos en el residuo corregido son superiores a 1,96 lo que permite determinar que los valores son significativos. Asimismo, se aprecia en la tabla que, en valor de relación entre variables no supera el 1,5, lo que admitite que la relación entre valores es aceptada con la descripción de siempre. Finalmente, se tiene un porcentaje en el resultado del cruce, afirmando que existe un 49% de individuos indican que la implementación del firewall siempre tendrá una mejora en relación al control de accesos y la protección de datos. De igual modo sucede con los otros valores, pero como ninguno supera el 1.5 de valor, se puede afirmar que el 100% de

los administrativos, mencionan que existe una mejora en todas las políticas. Es así que: “El grupo de administrativos afirma que el sistema web siempre cumple con las políticas, seguridad, integridad y disponibilidad”. Afirmando que el 100% de administrativos aprueba la mejora que ha realizado implementación del firewall.

Seguido a ello se ha realizado la recolección de los valores en relación a la significancia, permitiendo en tal sentido poder interpretación la relación entre las variables e interpretar la hipótesis.

Tabla 14

Cuadro de valores con los datos obtenidos de la prueba estadistica Chi-Cuadrado.

Descripción	Valor
Chi-Cuadrado (significancia)	0,013
Razón de verosimilitud (significancia)	0,037
Asociación Lineal por Lineal (significancia)	0,015

Como se muestra en la tabla 14, se encuentra una similitud muy significante entre ambas variables, cuya interpretación según lo mencionado por IBM, se tiene que, tanto en la significancia de Chi-Cuadrado, la razón de verosimilitud y la asociación lineal por lineal; los cuales presentan, los valores de: 0,013, 0,037 y 0,015 respectivamente, determinando que el **P** valor al tomar un número más cercano o igual **0,000,** determina que existe una relación más estrecha entre las variables. Por ello se puede determinar que, la influencia existente entre ambas variables es de 0,013, la verosimilitud de 0,37 y la lineal por lineal de 0,015. Esta última afirma la creciente que existe entre una variable y la otra, mostrando la mejora que existe entre las variables en relación a la implementación del firewall; dicho en otro modo: con un 98.5% se afirma que la implementación del firewall mejora el

control de accesos y la protección de la red de datos. De igual modo la significancia de Chi cuadrado y verosimilitud son suficientes para demostrar la hipótesis planteada en la investigación, donde se acepta con total seguridad. Asimismo, tomando la descripción de fallas al realizarse la interpretación de la significación en base al 0,000 se trata de una investigación desarrollada al 100% considerando que los valores obtenidos tienen menos del 2% de error, por ello con un 98% de seguridad se afirma la hipótesis desarrollada en la presente investigación: “*La implementación de un firewall de seguridad influye positivamente en el control de accesos y protección de la red de datos en la empresa Ferretería Soto.”*

5.2. Discusión de resultados.

El desarrollo investigativo de la presente tesis, mostró una aceptación del 100% del grupo de expertos en relación a la seguridad del firewall, mostrando equidad con los resultados brindados por Chicaiza en la tesis: “Implementación de un firewall construido a partir de software y una placa de circuitos compacta o SBC (single Board Computer)”, a razón que, en el desarrollo de la investigación se encontró que el 100% de los usuarios consideró la protección de los servicios utilizados. Determinando que en ambas investigaciones el 100% de los encuestados afirmaron que una seguridad en las empresas se logra con la implementación de un firewall.

La utilización del cuestionario para la recolección de datos mostró que el 100% de los administrativos de la Ferretería Soto consideraron que la implementación del firewall desarrollado siempre está seguro, disponible, es íntegro y controla las amenazas. A diferencia de la investigación realizada por Roba, Vento y García, denominada: “Metodología para la detección de vulnerabilidades en las redes de datos utilizando Kali-Linux”, la cual no realizó la implementación de un firewall como tal, sin embargo, la aceptación de los encuestados en relación a la seguridad solo obtuvo un 47% de aceptación mientras que el 53% consideró que la metodología desarrollada no protegía las redes. De otra parte, sucedió con la investigación desarrollada por Esparza en la tesis: “Implementación de un firewall sobre la plataforma LINUX en la empresa de contabilidad y finanzas Armas & Asociados”, la cual obtuvo un valor superior, debido a que el 80% de usuarios de la empresa aceptaron la seguridad del firewall, pero un 20% consideró que no realiza la seguridad en relación a la tradicional. Esto muestra que, la implementación de un firewall debe realizarse de forma precisa, ya que esto permitirá tener una seguridad posterior contundente.

Para conocer el impacto que genera la implementación del firewall sobre la protección de datos de la Ferretería Soto se realizó un procedimiento estadístico denominado Chi-Cuadrado, dicha influencia se realizó con un 98% de confianza, brindado un resultado de significancia de 0,013. Dicho resultado mostró la aceptación de la hipótesis al 99% ya que la significancia estuvo por debajo del grado de error. Con igual similitud se realizó la investigación de Joaquín en la tesis: “Implementación de firewall para el control de servicio de internet en la filial Chanchamayo de la universidad Peruana los Andes”, la investigación desarrollada por otra parte, realizó una estadística denominada wilcoxon, la que proporcionó un resultado de significancia de 0,000, con una probabilidad del 95% y 5% de error, dicha significancia en relación a la probabilidad permitió demostrar la hipótesis planteada en un 95% de confianza. Mostrando que en ambas investigaciones el valor de la significancia determina la aceptación o negación de la hipótesis, además que este valor debe estar por debajo del margen de error que se determina en la prueba.

En suma, de las dos investigaciones con análisis estadísticos se le añade la investigación de Villanueva y Riveros denominada: “Diseño de un esquema lógico para la seguridad perimetral de una red de comunicaciones”, la misma que para la constrastacion de su hipótesis consideró la utilización de una prueba estadística Z-Teórica, debido a que dicha prueba se utiliza para la demostración de un supuesto, debido a que no existe implementación como tal, con el desarrollo de la prueba estadística se ha mostrado una mejora del 66%, asimismo con la prueba estadística ha mostrado una significancia del 0,05, dicha significancia se ha realizado con un 95% de confianza y un 5% de error, como la significancia es igual al 0.05 permitido, está dentro del rango aceptable, pero con cierta desestabilidad, debido a que la significancia toma exactamente el punto de separación entre la confianza y el error. Pero, sin dejar de lado que aún está en el rango aceptable.

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

La implementación de un firewall resultó un total éxito, debido a que el personal experto participante en la investigación demostró a través de una hoja de cotejo que el 100% de las políticas, controles seguridad, controles de datos y protección de la red ha sido implementada correctamente en el firewall. De igual modo, el personal administrativo de la empresa mediante un cuestionario brindó los datos para el análisis de influencia pertinente. El cual proporcionó una significancia de 0,013 y una significancia de verosimilitud de 0,037 siendo un resultado suficiente para demostrar la influencia positiva que ha tenido la implementación del firewall frente al control de accesos y protección de la red de datos. Asimismo, apreciar la mejora en el control de accesos y protección a la red de datos en relación a que el 100% de entrevistados afirmó dicha mejora.

El desarrollo de un firewall debe evidenciar los problemas pre-implementación, los mismos que servirán de guía para eliminar la problemática que presenta la empresa. Para ello, se evaluó la zona de trabajo antes de la implementación, se realizó una conversación con los responsables de la empresa y se concluyó que la implementación del firewall presentaría una zona de trabajo segura y protegida para evitar robos o manipulaciones indebidas, además que, serían los administrativos los únicos involucrados en la investigación para evitar amenazas en la empresa ferretera.

El análisis de la red se realizó con la técnica de observación investigativa, debido a que la presencia del cableado e información es abundante, ya que los servidores proporcionan gran cantidad de información entre sucursales de la empresa. Por ello, se fijó implementar el firewall solamente en la sucursal principal (CasaDekor) de la ferretería Soto, ya que el

firewall físico adquirido solo tenía licencia para tres zonas de seguridad (inside, outside y DMZ).

La implementación de un dispositivo firewall presentó lineamientos que permitieron tener una seguridad confiable, además de las políticas de seguridad con la conexión de las salidas a la red. Por tal razón, las políticas utilizadas en la inspección de los servicios se limitaron a los protocolos TCP/HTTP e ICMP, los mismos que restringen las salidas/entradas al internet y a las páginas en red, dichas políticas y limitaciones permiten que, las solicitudes que realizan los trabajadores en la empresa se realicen con total normalidad, pero, con la filtración de protocolos. Esto ha permitido que los protocolos que no pertenecen o no han sido agregados a la lista de inspecciones no pueden atravesar hacia la empresa o los servidores.

Con el firewall implementado se encontró una aceptación general del 100% de expertos, los mismos que consideraron que el firewall ha sido desarrollado correctamente y que brinda la seguridad correcta; filtrando, restringiendo y negando protocolos. De igual modo se realizó una influencia de Chi-Cuadrado de los datos del personal administrativo que brindó una significancia de 0,013, permitiendo demostrar que, el impacto entre la implementación del firewall con el control de accesos y seguridad a la red de datos es muy estrecha, además que mientras el firewall se siga puliendo, mayor será la protección en la red de datos y el control de accesos.

6.2. Recomendaciones

Se recomienda a la empresa realizar el mantenimiento necesario del equipo, debido a que como cualquier equipo físico necesita un mantenimiento este no es excluyente, inclusive al ser un equipo de características particulares necesita un mantenimiento continuo y por el personal capacitado para no afectar o vulnerar la red de datos.

Conociendo que la red ha adquirido una licencia para contar con tres directivas de seguridad una inside, otra outside y la tercera una DMZ, dicha licencia debe ser contratada anualmente entre los administrativos de la empresa y con quien contrataron el servicio, ya que si la licencia caduca, el equipo cuenta con un chip de verificación, el mismo que realiza una validación de acuerdo al contrato realizado con el servicio brindado. Por tal razón, se recomiendo tener en cuenta los tiempos para renovar la licencia y evitar el corte de una directiva.

Al ser un firewall un instrumento que protege la red de datos este requiere una manipulación adecuada y con los permisos que se han configurado en el dispositivo, Por tal razón, se recomienda que si existe algún personal nuevo que va a realizar la manipulación del equipo, este tenga una capacitación con el jefe encarado de la manipulación de los equipos de la empresa, esto permitirá tener un control de qué personal maneja el dispositivo y, si existen filtraciones; se podrá conocer quiénes fueron los responsables.

El dispositivo firewall se ha instalado cercanamente a los servidores, esto permite que todos los equipos estén en un lugar único para mantener el control de los mismos. Por ello, se recomienda que en cualquier accidente que presente un dispositivo ajeno al firewall, no se realice manipulación alguna sobre el mismo, ya que las configuraciones en el firewall cisco ASA 5505 no son volátiles, estas se mantienen tal como se ha configurado el dispositivo. De ser el caso que se realice configuración distinta por los puertos ethernet por parte de los servidores, la configuración debe realizarse en los servidores mas no en el firewall.

REFERENCIAS BIBLIOGRÁFICAS

Agramunt (s.f.). Direccionamiento IP, cálculo de redes TCP/IP. *Ciclos formativos de grados superior*, pp. 3-18. [Archivo digital PDF]. http://virtualbook.weebly.com/uploads/2/9/6/2/2962741/tcp_ip.pdf

Aguilar Barojas, S. (2005). Fórmulas para el cálculo de la muestra en investigaciones de salud en Tabasco. *Salud en Tabasco, volumen* (11), pp. 333-338 https://www.redalyc.org/pdf/487/48711206.pdf

AMBIT (10 de Noviembre de 2020). *Tipos de Vulnerabilidades y Amenazas informáticas*.AMBIT BST. https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

Asana, T. (24 de agosto de 2021). Top-down vs. bottom-up: cuál es la diferencia y el mejor enfoque para tu equipo. asana. https://asana.com/es/resources/top-down-approach

Barceló Ordinas, J.M., Íñigo Griera, J., Martí Escale, R., Peig Olive, E. y Perramon, Tornil, X. (2004). *Redes de computadoras.* Eureca Media. https://libros.metabiblioteca.org/bitstream/001/341/9/84-9788-117-6.pdf

Bejarano Ramírez, A., Miranda Castillo, D. y Henríquez Celedon, J. (2008). Redes LAN y MAN (IPv4 y IPv6) [Maestría en telemática] Repositorio Universidad Rafael Belloso Chacín. https://www.urbe.edu/info-consultas/web-profesor/12697883/articulos/Redes%20Informaticas/IPv4%20Vs%20IPv6.pdf

Bolado, R.; Ibañez, J. y Lantarón, A. (1999). *El juicio de Expertos.*Neografis S.L. Madrid.

Caballa Torres, E. y Torres Flores, W. L. (2010). *Implementación de una solución de*

seguridad. [Tesina], Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Lima.

Cárdenas Ayala, A., Huamán Huayta, L. y Espíritu Yarin, L. (2011). El informe final de investigación. Huancayo – Perú: Grapex Perú.

Carles, J. (6 de Julio de 2013). *Que es y para que sirve un firewall*.GEEKLAND. https://geekland.eu/que-es-y-para-que-sirve-un-firewall/

Castillo Palomino, R.G., Dominguez Chavez, M.A. y Sulca Galarza, C.I. (2017). *Implementación de un Firewall TMG Forefront para la Seguridad Perimetral de la Red de Datos de la Clínica Aliada.* [Tesis de Pregrado], Universidad Peruana de las Américas , Escuela Profesional de Ingeniería Computación y Sistemas, Lima.

Chicaiza Pareja, J.S. (2018). *Implementación de un Firewall Construido a Partir de Software y una Placa de Circuitos Compacta o SBC (Single Board Computer) en la Empresa Taio Systems de la Ciudad de Popayán.* [Tesis de Posgrado] Universidad Nacional Abierta y a Distancia UNAD, Escuela de Ciencias Básicas Tecnología e Ingeniería , Popayán.

CISCO. (s.f.). *¿Qué es un firewall?*. CISCO. https://www.cisco.com/c/es_es/products/security/firewalls/what-is-a-firewall.html

Crespo Martínez, LM. y Candelas Herías, F.A. (1998). *Introducción a TCP/IP*. *Sistemas de transporte de datos*. Espagrafic. https://rua.ua.es/dspace/bitstream/10045/4328/1/Crespo_Candelas_TCP_IP.pdf

CUTI. (06 de Noviembre de 2019). *Importancia de la Seguridad de la Información en la Organización* .Industria TICs. https://www.cuti.org.uy/novedades/1324-importancia-de-la-seguridad-de-la-

informacion-en-la-organizacion

Díaz, R.G. y Silva Ledesma, J.R. (2016). *Efecto de la Implementación del Sistema PFSENSE en la Seguridad Perimetral Logica en los servicios de la Red Troncal de la Universidad Nacional de la Amazonia Peruana, Iquitos-2016.* [Tesis de Pregrado], Universidad Privada de la Selva Peruana , Facultad de Ingeniería , Iquitos.

Duarte Martínez, R. F., y Paredes Rios, S. J. (2016). *Análisis del uso que hacen los usuarios conectados a un punto de acceso inalámbrico, sin autenticación, con conexión a Internet, ubicado en el edificio CIDS de la Universidad Nacional Autónoma de Nicaragua (Unan-León).* [Tesis de Pregrado], Universidad Nacional Autónoma de Nicaragua, Facultad de Ciencias y Tecnología, Léon, Nicaragua.

Economía (6 de julio de 2011). ¿Qué es y cómo se realiza un análisis bottom-up?. Encomia simple net. https://www.economiasimple.net/analisis-macroeconomia-bottom-up.html

Escobar Pérez, J. y Cuervo Martínez, A. (2008). Validación de contenido y Juicio de Expertos una aproximación a su utilización. *Revista Avances en Medición, vol. 6,* pp. 27-36. https://www.researchgate.net/publication/302438451_Validez_de_contenido_y_juicio_de_expertos_Una_aproximacion_a_su_utilizacion

Escofet, A., Folgueiras, P., Luna, E. y Palou B. (2016). Elaboración y Validación de un Cuestionario para la valoración de proyectos de Aprendizaje-Servicio. *Revista Mexicana de Investigación Educativa, volumen (21),* pp. 929-949. http://www.scielo.org.mx/pdf/rmie/v21n70/1405-6666-rmie-21-70-00929.pdf

Esparza Morocho, J.P. (2013). Implementación de un firewall sobre la plataforma

LINUX en la empresa de contabilidad y finanzas Armas & Asociados. [Tesis de titulación]. Repositorio Escuela Politécnica Nacional. https://bibdigital.epn.edu.ec/bitstream/15000/6056/1/CD-4785.pdf

Espinoza Montes, C. (2010), *Metodología de investigación tecnológica Pensando en sistemas.* Perú-Huancayo: ISB (978-612-00-0222-3).

Estemática (13 de enero 2021). *Chi-Cuadrado y SPSS: Tablas de contingencia de la Chi-cuadrado en SPSS*. Estemática. https://estamática.net/chi-cuadrado-en-spss/

Estrada, E., unás, G. y Flórez, R. (2021). Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá. *Revista Logos ciencia & tecnología, volumen* (3), pp. 98-103.

Fallas, J. (2012). Correlación Lineal: Midiendo la relación entre dos variables. CC BY-NC-SA de Creative Commons. [Libro digital]. https://www.ucipfg.com/Repositorio/MGAP/MGAP-05/BLOQUE-ACADEMICO/Unidad-2/complementarias/correlacion_lineal_2012.pdf

Federación de enseñanza de CC.OO. de Andalucía (2010). Direccionamiento IP. *Revista digital para profesionales de la enseñanza, volumen* (8), pp. 1-13. https://www.feandalucia.ccoo.es/docu/p5sd7257.pdf

Fernández, L. (19 de abril de 2022). *Los mejores firewalls OpenSource para proteger tu red.* Redes Zona. https://www.redeszone.net/tutoriales/seguridad/mejores-firewall-open-source-proteger-red/

García Bellido, R., Gonzáles Such, J. y Jornet Meliá, J.M. (2010). SPSS: Prueba T. *InnovaMide.* [Archivo digital PDF]. https://www.uv.es/innomide/spss/SPSS/SPSS_0701b.pdf

Grajales Bartolo, M. (2011). *Análisis De Tráfico Para La Red De Datos De Las Instituciones.* [Tesis de Pregrado], Universidad Tecnológica De Pereira, Facultad de Ingenierías Eléctrica, Electrónica, Física y Ciencias de la Computación , Pereira.

Gonzáles Gonzáles, J.A. (2009). Manual Básico SPSS. *Universidad de Talca*, pp. 1-63. [Archivo digital PDF]. https://www.fibao.es/media/uploads/manual_basico_spss_universidad_de_talca.pdf

Hernández Sampieri, R., Fernández Collado, C. y Baptista Lucio, P. (2014). *Metodología de la Investigación.* Mexico D.F: McGRAW-HILL.

Hernández Lalinde, J.D.; Espinoza Castro, F.; Rodríguez, J.E.; … Bermúdez Pírela, Valmore José (2018). Sobre el uso adecuado del coeficiente de correlación de Pearson: definición, propiedades y suposiciones. *Redalyc, vol. (37),* pp. 587-601. https://www.redalyc.org/journal/559/55963207025/55963207025.pdf

Hurtado Sánchez, M. (2017). La Estadística en la Investigación Científica. *UsanPedro, volumen (8),* pp. 113-120. https://revista.usanpedro.edu.pe/index.php/CPD/article/view/256/246

Instituto Nacional de Ciberseguridad - INCIBE (2020). *Guia de Ciberataques*. Oficina de Seguridad del Internauta. [Archivo digital PDF]. https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf

IBM (7 de diciembre 2022). *Pruebas de significación de tablas cruzadas.* IBM. https://www.ibm.com/docs/es/spss-statistics/beta?topic=tables-significance-testing-crosstabulation

IBM (13 de septiembre 2022). *Pruebas de Chi-Cuadrado.* IBM.

https://www.ibm.com/dos/es/spss-statistics/saas?topic=tests-chi-square-test

ISO 27001 (2016). *ISO 27001 gestión de la seguridad de la información.* Normas ISO https://www.normas-iso.com/iso-27001/

Joaquin Cajahuaringa, J. C. (2020). *Implementación De Firewall Para El Control De Servicio De Internet En La Filial Chanchamayo De La Universidad Peruana Los Andes.* [Tesis de Pregrado], Universidad Peruana Los Andes, Facultad de Ingenieria, Huancayo.

Kleinerman, J.E. (s.f.). *Manual de uso de IPTables.* [Archivo digital PDF]. https://pabloyela.files.wordpress.com/2013/08/manual-de-uso-de-iptables-jorge-kleinerman.pdf

Lerena, S. (2001). Guia de aprendizaje de IPTables/NetFilter. *NetFilter Guide, volumen* (1), pp. 1-21. https://artica.es/docs/Guia_Netfilter.pdf

Lisot. (06 de Junio de 2018). *Seguridad en una red de datos*. Lisot. https://www.lisot.com/seguridad-en-una-red-de-datos/

Luke, J. (2019). Guia sobre direccionamiento IP, subredes y enrutamiento, Versión 0.3 pp. 1-31. [Archivo digital PDF]. https://riull.ull.es/xmlui/bitstream/handle/915/14702/Guia_sobre_direccionamiento_IP__subredes_y_enrutamiento.pdf?sequence=1

Márquez, D. (2019). Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas. *Revista de Bioética y Derecho, volumen* (46), pp. 85-100. https://scielo.isciii.es/pdf/bioetica/n46/1886-5887-bioetica-46-00085.pdf

Martínez Molina, K.J., Pacheco Meneses, J. y Zúñiga Silgado, I. (2009). Firewall – Linux: Una Solución De Seguridad Informática Para Pymes (Pequeñas Y

Medianas Empresas). *Revista UIS Ingenierías, volumen* (8), pp. 155-165 https://www.redalyc.org/pdf/5537/553756879003.pdf

Mieres, J. (2009). Ataques informáticos Debilidades de seguridad comúnmente explotadas. EvilTingers, pp. 1-17. [Archivo digital PDF]. https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf

Morales, P. (2011). El coeficiente de correlación. Universidad Rafael Landívar. [Archivo digital PDF]. https://ice.unizar.es/sites/ice.unizar.es/files/users/leteo/materiales/01._documento_1_correlaciones.pdf

Ozten, T. y Manterola, C. (2017). Técnicas de Muestreo sobre una Población a Estudio. *Revista del instituto Morphol, vol (35),* pp. 227-232. [Archivo digital PDF]. https://www.scielo.cl/pdf/ijmorphol/v35n1/art37.pdf

Pacheco Meneses, J. y Martínez Molina, K. (2009). *Diseño e implementación de un servidor firewall en linux.* [Tesis de pregrado]. Universidad tencologica de bolivar. https://repositorio.utb.edu.co/

Pacotaype Huamán, R.J. (2018). *Metodología integral para evaluar el rendimiento de firewalls.* [Tesis de Pregrado], Universidad Cesar Vallejo, Facultad de Ingenieria, Lima.

Peñafiel, L. (2021). Factores que determinan la Vulneración Informática y el Desarrollo de una aplicación móvil para concientizar sobre los Impactos en los Activos. *Fides Et Ratio, volumen* (21), pp. 143-172. http://www.scielo.org.bo/pdf/rfer/v21n21/v21n21_a09.pdf

Pérez Gonzales, L.O. (2006). Microsoft Excel: una herramienta para la investigación.,

Revista electrónica MediSur volumen (4), pp. 68-71. https://www.redalyc.org/articulo.oa?id=180019873015

PRAKMATIC. (13 de Diciembre de 2016). *La importancia de la protección de datos informáticos*. PRAKMATIC. http://www.prakmatic.com/seguridad-ti/la-importancia-de-la-proteccion-de-datos-informaticos/

RedFibra (28 de Septiembre de 2020). *¿Que es un Firewall y como funciona?. Tipos de firewall*. RedFibra. https://redfibra.mx/que-es-un-firewall-y-como-funciona-tipos-de-firewall/

Restrepo Múñoz, V.P. (2009). Aplicación Y Comparación De La Metodología De Diseño Top Down Y Bottom. [Tesis de titulación]. Repositorio Universidad Eafit. https://repository.eafit.edu.c

Roba Iviricu, L.R., Vento Alvarez, J.R. y García Concepción, L.E. (2016). Metodología para la Detección de Vulnerabilidades en las Redes de Datos utilizando Kali-Linux. *Avances, volumen* (4), pp. 334-344. https://dialnet.unirioja.es/servlet/articulo?codigo=6210110

Roca Fernández, A.P. y Pereira Suarez, J.A. (s.f.). Firewalls. [Archivo digital PDF]. http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/06%20-%20Firewalls%20%5Bupdated%5D.pdf

Rojas Álvarez, C.J. (2013). La instrucción geométrica y la representación plana de módulos multicubos en un grupo de alumnos: un diseño experimental. *Revista del Instituto de Estudios en Educación Universidad del Norte. ISS N 2145-9444.* http://www.scielo.org.co/pdf/zop/n19/n19a05.pdf

Romero Castro, M.I., Figueroa Maorán, G.L., Vera Navarrete, D.S., Álava Cruzatty, J.E., Parrales Anzúlez, G.R., Álava Mero, C.J., Murillo Quimiz, A.L. y Castillo

Merino, M.A. (2018). *INTRODUCCIÓN A LA SEGURIDAD.* CIENCIAS. https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Romero Goyzueta, C.A., Pineda Ancco, F.E. y López Flores, J.V. (2016). Márquez, D. (2019). Diseño de un cortafuego para bloquear sistemas de evasión de censura de internet basados en proxy. *Investigación Altoandin, volumen* (18), pp. 475-482. http://dx.doi.org/10.18271/ria.2016.240.

Saavedra, J.C. (18 de junio de 2017). Metodología Top-Down para el Diseño de Redes. JuanCarlosSaavedra.net. https://juancarlossaavedra.me/2017/06/infografia-metodologia-top-down-para-el-diseno-de-redes/

Silva Coelho, F.E., Segadas Araujo, L.G. y Kowask Bezerra, E. (2010). *Gestión de la seguridad de la información.* RedCedia.

Stallings (2004). *Comunicaciones y Redes de computadoras.* Prentice Hall.

Tanenbaum (2003). *Redes de computadoras.* Pearson Educación

TechClub (20 de Febrero de 2017). *Vulnerabilidades en redes*. TechClub. https://techclub.tajamar.es/vulnerabilidades-en-redes/#:~:text=DEFINICION%3A,un%20punto%20d%C3%A9bil%20del%20sistema.

Tinoco Gómez, O. (2008). Una aplicación de la prueba chi cuadrado con SPSS. *Industrial Data,* vol. (11), pp. 73-77. https://www.redalyc.org/pdf/816/8161121101.pdf

Tobón, S. (2013). Issuu. Obtenido de Lista de cotejo por competencias. https://issuu.com/cife/docs/ebook__listas_de_cotejo_por_compet_cf32e06e110

043

TotalPlay (14 de noviembre de 2019). *Los 10 mejores firewalls de hardware para redes domésticas y de pequeñas empresas (2019)*. TotalPlay Empresarial. https://tpempresas.com/los-10-mejores-firewalls-de-hardware-para-redes-domesticas-y-de-pequenas-empresas-2019

Unión Internacional de Telecomunicaciones (2005). *Manual sobre redes basadas en el protocolo Internet (IP) y asuntos conexos.* UIT-D. [Archivo digital PDF]. https://www.itu.int/dms_pub/itu-d/opb/hdb/D-HDB-IP-2005-PDF-S.pdf

Vega Briceño, E. (2021). *Seguridad de la información.* Área de innovación y desarrollo, S.L. https://www.3ciencias.com/wp-content/uploads/2021/03/LIBRO-SEGURIDAD-INFORMACIO%CC%81N.pdf

Vila Fuentes, J. (2019). *Implementación de un Firewall que permita optimizar la seguridad y los servicios de red en Cineplanet.* [Tesis de Pregrado], Universidad Tecnológica del Perú , Facultad de Ingeniería, Lima.

Villanueva Alvarado, R.R. y Riveros Díaz, R.H. (2014). *Diseño de un esquema lógico para la seguridad perimetral de una red de comunicaciones.* [Tesis de Pregrado], Universidad Nacional de Trujillo , Facultad de Ciencias Fisicas y Matematicas, Trujillo.

Fernádez, Y. (17 de Octubre de 2019). *Firewall: qué es un cortafuegos, para qué sirve y cómo funciona*. Xataka. https://www.xataka.com/basics/firewall-que-cortafuegos-sirve-como-funciona

ANEXOS

Anexo 1

Validación de los instrumentos por el Mg. Ing. Juan Carlos Cabanillas Chávez.

VALIDACIÓN DE INSTRUMENTOS

Validación de expertos para los instrumentos de hoja de cotejo y cuestionario en la investigación: Análisis e implementación de un Firewall de seguridad para el control de accesos y protección de la red de datos de la empresa Ferretería Soto, 2021.

Mediante el presente documento se acredita la confiabilidad y validación de los instrumentos de recolección de datos.

I. Datos del validador

Validador(a):	Juan Carlos Cabanillas Chávez
Profesión:	Ingeniero de Sistemas
Grado profesional:	Magister
Fecha de validación:	02/09/2022
Firma y Sello:	Juan Carlos Cabanillas Chávez Ingeniero de Sistemas Reg.CIP. N° 199906

II. Hoja de cotejo dirigida a expertos.

Criterios	Excelente	Bueno	Regular	Deficiente
Transparencia en los indicadores.	X			
Idóneo para medir las variables.		X		
Adecuado con la investigación.	X			
Lenguaje oportuno.	X			

III. Cuestionario dirigido al personal administrativo de la Ferretería Soto.

Criterios	Excelente	Bueno	Regular	Deficiente
Transparencia en los indicadores.		X		
Idóneo para medir las variables.		X		
Adecuado con la investigación.	X			
Lenguaje oportuno.	X			

Anexo 2

Validación de los instrumentos por el Mg. Ing. Freddy Wilmer Cervera Estela.

VALIDACIÓN DE INSTRUMENTOS

Validación de expertos para los instrumentos de hoja de cotejo y cuestionario en la investigación: Análisis e implementación de un Firewall de seguridad para el control de accesos y protección de la red de datos de la empresa Ferretería Soto, 2021.

Mediante el presente documento se acredita la confiabilidad y validación de los instrumentos de recolección de datos.

I. Datos del validador

Validador(a):	Freddy Wilmer Cervera Estela
Profesión:	Ingeniero Informática y de Sistemas
Grado profesional:	Magister
Fecha de validación:	05/09/2022
Firma y Sello:	Freddy Wilmer Cervera Estela INGENIERO INFORMÁTICA Y DE SISTEMAS Reg. CIP N° 136166

II. Hoja de cotejo dirigida a expertos.

Criterios	Excelente	Bueno	Regular	Deficiente
Transparencia en los indicadores.	X			
Idóneo para medir las variables.	X			
Adecuado con la investigación.		X		
Lenguaje oportuno.	X			

III. Cuestionario dirigido al personal administrativo de la Ferretería Soto.

Criterios	Excelente	Bueno	Regular	Deficiente
Transparencia en los indicadores.		X		
Idóneo para medir las variables.		X		
Adecuado con la investigación.	X			
Lenguaje oportuno.	X			

Anexo 3

Validación de los instrumentos por la Mg. Ing. Evelyn Janeth Gutiérrez Fernández.

VALIDACIÓN DE INSTRUMENTOS

Validación de expertos para los instrumentos de hoja de cotejo y cuestionario en la investigación: Análisis e implementación de un Firewall de seguridad para el control de accesos y protección de la red de datos de la empresa Ferretería Soto, 2021.

Mediante el presente documento se acredita la confiabilidad y validación de los instrumentos de recolección de datos.

I. Datos del validador

Validador(a):	Evelyn Janeth Gutierrez Fernandez
Profesión:	Ing. de sistemas
Grado profesional:	Magister
Fecha de validación:	05 - 09 - 2022
Firma y Sello:	Ing. EVELYN J. GUTIERREZ FERNANDEZ INGENIERO DE SISTEMAS Registro de Colegio de Ingenieros del Perú N° 100051

II. Hoja de cotejo dirigida a expertos.

Criterios	Excelente	Bueno	Regular	Deficiente
Transparencia en los indicadores.		X		
Idóneo para medir las variables.	X			
Adecuado con la investigación.	X			
Lenguaje oportuno.		X		

III. Cuestionario dirigido al personal administrativo de la Ferretería Soto.

Criterios	Excelente	Bueno	Regular	Deficiente
Transparencia en los indicadores.	X			
Idóneo para medir las variables.	X			
Adecuado con la investigación.		X		
Lenguaje oportuno.	X			

Anexo 4

Hoja de Cotejo realizada por el experto en Telecomunicaciones, Ing. Juan Carlos Cabanillas Chávez.

TESIS: “ANÁLISIS E IMPLEMENTACIÓN DE UN FIREWALL DE SEGURIDAD PARA EL CONTROL DE ACCESOS Y PROTECCIÓN DE LA RED DE DATOS DE LA EMPRESA FERRETERÍA SOTO, 2021”

Hoja de Cotejo

Ingeniero(a): Juan Carlos Cabanillas Chávez

Profesión: Ingeniero de Sistemas - Especialista en telecomunicaciones

I. Medición.

Valores de medición	
Logrado	*1*
No logrado	*0*

II. Instrucciones: Lea cuidadosamente cada pregunta y maque con una (X) cada respuesta en relación a las configuraciones del firewall mostradas luego de la hoja de cotejo.

Configuración Firewall	¿Realizada?	
	Logrado	No logrado
Dimensión Políticas		
Cambio de nombre e ingreso correcto al terminal para control de accesos no deseados.	X	
Distribución correcta de salidas Ethernet con Vlan’s para distribución de la red.	X	
Configuración correcta de salida/entrada de tráfico a internet.	X	
Asignación correcta de políticas universales para tráfico de paquetes en mantener seguridad a la red interna.	X	
Dimensión Seguridad		
Configuración y definición de zonas de seguridad para controlar accesos a las redes.	X	
Correcta determinación de objetos para la seguridad en vulnerabilidades.	X	
Registro de URL’S para evitar amenazas.	X	
Configuración de bloqueo de protocolos, servicios y puertos inseguros.	X	
Control de accesos y protección de la red de datos	**Logrado**	**No logrado**
Dimensión Integridad		
Se restringió el acceso a usuarios ajenos.	X	
Restricciones en los Ethernet mediante listas de control acceso.	X	
Control de acceso de solicitudes de aplicaciones web.	X	
Dimensión Seguridad		
Correcto PAT para negación de protocolos y evitar salida de información.	X	
Protección de la red mediante filtración de paquetes.	X	
Escaneo de tráfico de aplicaciones.	X	
Dimensión Disponibilidad		
Disponibilidad de servicios ante cualquier amenaza o vulnerabilidad.	X	
Disponibilidad de la red ante cualquier amenaza o vulnerabilidad.	X	

Juan Carlos Cabanillas Chávez
Ingeniero de Sistemas
Reg.CIP. N° 199906

Firma y Sello

Anexo 5

Hoja de Cotejo realizada por el experto en Telecomunicaciones, Ing. Christian Hernán Abanto Segura.

TESIS: “ANÁLISIS E IMPLEMENTACIÓN DE UN FIREWALL DE SEGURIDAD PARA EL CONTROL DE ACCESOS Y PROTECCIÓN DE LA RED DE DATOS DE LA EMPRESA FERRETERÍA SOTO, 2021”

Hoja de Cotejo

Ingeniero(a): Christian Hernán Abanto Segura

Profesión: Ingeniero de Sistemas

I. Medición.

Valores de medición	
Logrado	*1*
No logrado	*0*

II. Instrucciones: Lea cuidadosamente cada pregunta y maque con una (X) cada respuesta en relación a las configuraciones del firewall mostradas luego de la hoja de cotejo.

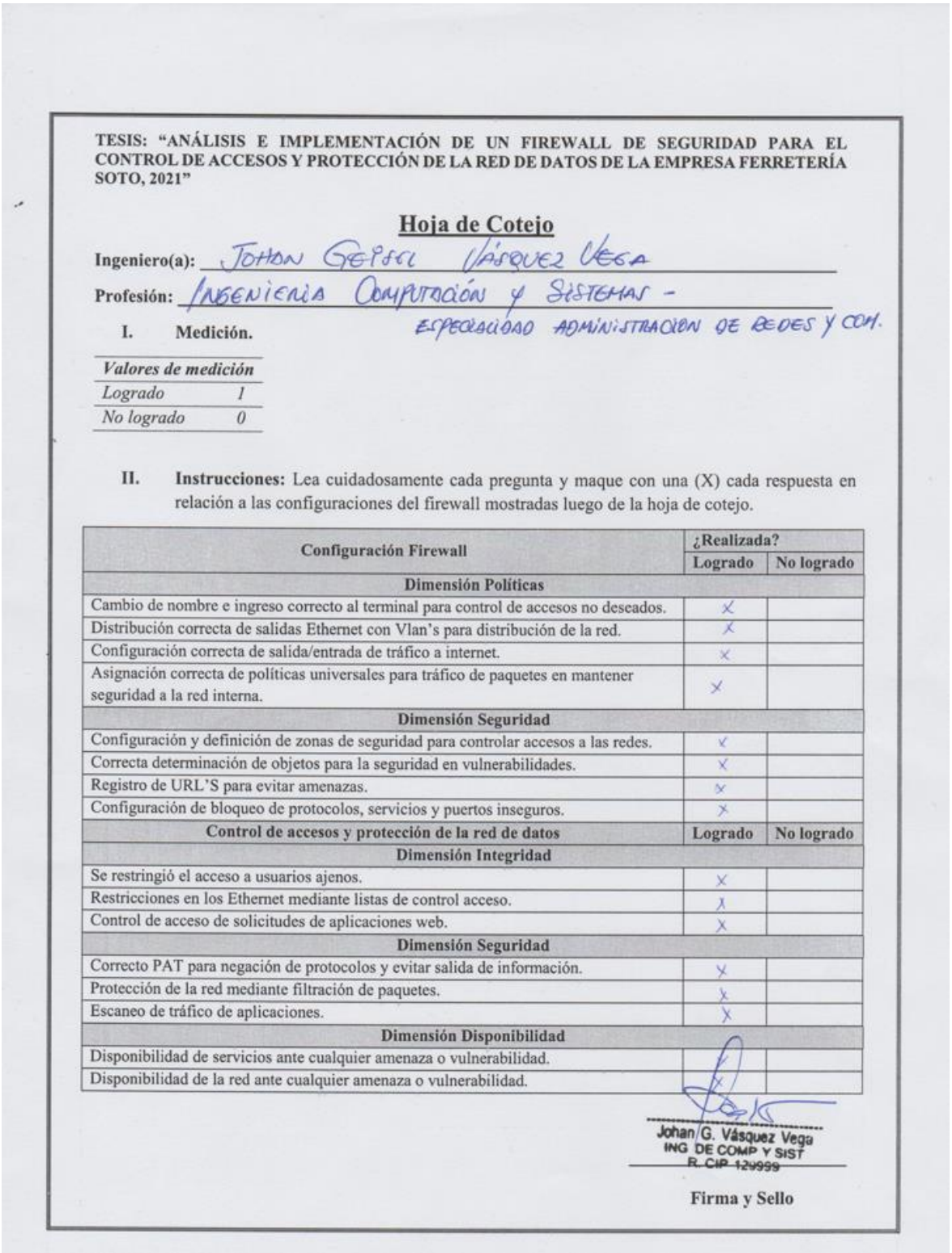
Configuración Firewall	¿Realizada?	
	Logrado	No logrado
Dimensión Políticas		
Cambio de nombre e ingreso correcto al terminal para control de accesos no deseados.	X	
Distribución correcta de salidas Ethernet con Vlan’s para distribución de la red.	X	
Configuración correcta de salida/entrada de tráfico a internet.	X	
Asignación correcta de políticas universales para tráfico de paquetes en mantener seguridad a la red interna.	X	
Dimensión Seguridad		
Configuración y definición de zonas de seguridad para controlar accesos a las redes.	X	
Correcta determinación de objetos para la seguridad en vulnerabilidades.	X	
Registro de URL’S para evitar amenazas.	X	
Configuración de bloqueo de protocolos, servicios y puertos inseguros.	X	
Control de accesos y protección de la red de datos	**Logrado**	**No logrado**
Dimensión Integridad		
Se restringió el acceso a usuarios ajenos.	X	
Restricciones en los Ethernet mediante listas de control acceso.	X	
Control de acceso de solicitudes de aplicaciones web.	X	
Dimensión Seguridad		
Correcto PAT para negación de protocolos y evitar salida de información.	X	
Protección de la red mediante filtración de paquetes.	X	
Escaneo de tráfico de aplicaciones.	X	
Dimensión Disponibilidad		
Disponibilidad de servicios ante cualquier amenaza o vulnerabilidad.	X	
Disponibilidad de la red ante cualquier amenaza o vulnerabilidad.		

Christian Hernán Abanto Segura
INGENIERO DE SISTEMAS
Registro del colegio de Ingenieros del Perú N° 122352

Firma y Sello

Anexo 6

Hoja de Cotejo realizada por el experto en Administración de Redes y Computación, Ing. Johan Geisel Vásquez Vega.



TESIS: “ANÁLISIS E IMPLEMENTACIÓN DE UN FIREWALL DE SEGURIDAD PARA EL CONTROL DE ACCESOS Y PROTECCIÓN DE LA RED DE DATOS DE LA EMPRESA FERRETERÍA SOTO, 2021”

Hoja de Cotejo

Ingeniero(a): JOHAN GEISEL VÁSQUEZ VEGA

Profesión: INGENIERIA COMPUTACIÓN Y SISTEMAS - ESPECIALIZADO ADMINISTRACION DE REDES Y COM.

I. Medición.

Valores de medición	
Logrado	*1*
No logrado	*0*

II. Instrucciones: Lea cuidadosamente cada pregunta y maque con una (X) cada respuesta en relación a las configuraciones del firewall mostradas luego de la hoja de cotejo.

Configuración Firewall	¿Realizada?	
	Logrado	No logrado
Dimensión Políticas		
Cambio de nombre e ingreso correcto al terminal para control de accesos no deseados.	X	
Distribución correcta de salidas Ethernet con Vlan’s para distribución de la red.	X	
Configuración correcta de salida/entrada de tráfico a internet.	X	
Asignación correcta de políticas universales para tráfico de paquetes en mantener seguridad a la red interna.	X	
Dimensión Seguridad		
Configuración y definición de zonas de seguridad para controlar accesos a las redes.	X	
Correcta determinación de objetos para la seguridad en vulnerabilidades.	X	
Registro de URL’S para evitar amenazas.	X	
Configuración de bloqueo de protocolos, servicios y puertos inseguros.	X	
Control de accesos y protección de la red de datos	**Logrado**	**No logrado**
Dimensión Integridad		
Se restringió el acceso a usuarios ajenos.	X	
Restricciones en los Ethernet mediante listas de control acceso.	X	
Control de acceso de solicitudes de aplicaciones web.	X	
Dimensión Seguridad		
Correcto PAT para negación de protocolos y evitar salida de información.	X	
Protección de la red mediante filtración de paquetes.	X	
Escaneo de tráfico de aplicaciones.	X	
Dimensión Disponibilidad		
Disponibilidad de servicios ante cualquier amenaza o vulnerabilidad.	X	
Disponibilidad de la red ante cualquier amenaza o vulnerabilidad.	X	

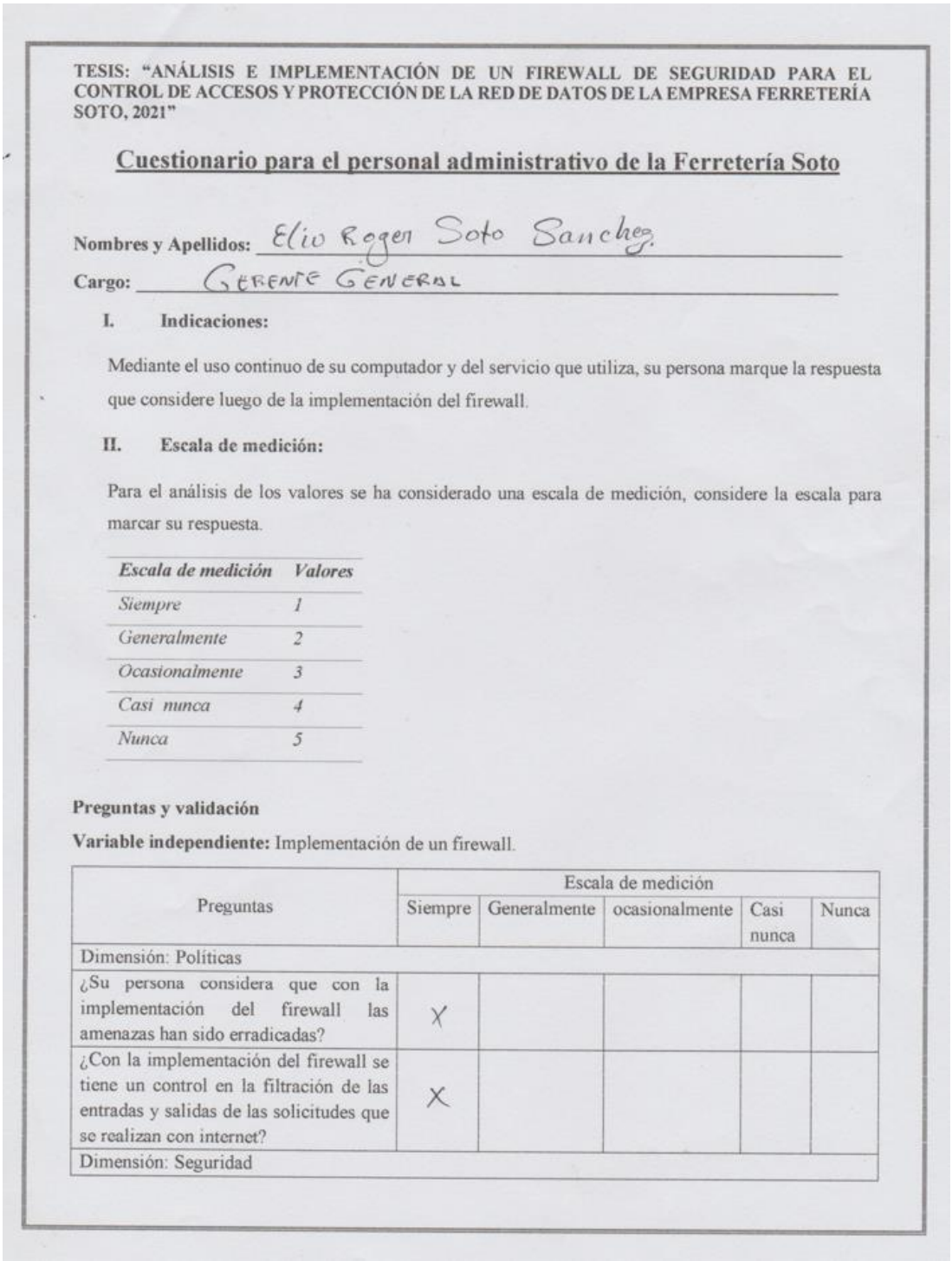
Johan G. Vásquez Vega
ING DE COMP Y SIST
R. CIP 129999

Firma y Sello

Anexo 7

Algunos cuestionarios realizados por los administrativos de la Ferretería Soto.

Cuestionario del Gerente General: Elio Roger Soto Sánchez.



TESIS: “ANÁLISIS E IMPLEMENTACIÓN DE UN FIREWALL DE SEGURIDAD PARA EL CONTROL DE ACCESOS Y PROTECCIÓN DE LA RED DE DATOS DE LA EMPRESA FERRETERÍA SOTO, 2021”

Cuestionario para el personal administrativo de la Ferretería Soto

Nombres y Apellidos: Elio Roger Soto Sanchez.

Cargo: GERENTE GENERAL

I. Indicaciones:

Mediante el uso continuo de su computador y del servicio que utiliza, su persona marque la respuesta que considere luego de la implementación del firewall.

II. Escala de medición:

Para el análisis de los valores se ha considerado una escala de medición, considere la escala para marcar su respuesta.

Escala de medición	*Valores*
Siempre	*1*
Generalmente	*2*
Ocasionalmente	*3*
Casi nunca	*4*
Nunca	*5*

Preguntas y validación

Variable independiente: Implementación de un firewall.

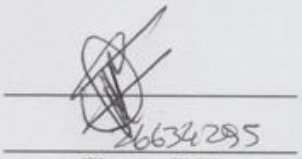
Preguntas	Escala de medición				
	Siempre	Generalmente	ocasionalmente	Casi nunca	Nunca
Dimensión: Políticas					
¿Su persona considera que con la implementación del firewall las amenazas han sido erradicadas?	X				
¿Con la implementación del firewall se tiene un control en la filtración de las entradas y salidas de las solicitudes que se realizan con internet?	X				
Dimensión: Seguridad					

TESIS: "ANÁLISIS E IMPLEMENTACIÓN DE UN FIREWALL DE SEGURIDAD PARA EL CONTROL DE ACCESOS Y PROTECCIÓN DE LA RED DE DATOS DE LA EMPRESA FERRETERÍA SOTO, 2021"

¿Con la implementación del firewall, el dispositivo solo puede ser manipulado por el personal especifico?	X				
¿La implementación del firewall presenta una zona segura para el manejo de las redes?	X				
¿Considera que el firewall implementado, brinda una seguridad correcta para evitar vulnerabilidades?	X				

Variable dependiente: Control de accesos y protección de red de datos.

Preguntas	Escala de medición				
	Siempre	Generalmente	ocasionalmente	Casi nunca	Nunca
Dimensión: Integridad					
¿El firewall permite tener un control de la manipulación en los equipos?	X				
Dimensión: Seguridad					
¿El firewall restringe el tráfico de paquetes no acordes a sus labores?	X				
¿El Firewall realiza restricciones dependiendo a la aplicación utilizada?	X				
Dimensión: Disponibilidad					
Con la implementación del firewall. ¿Existe disponibilidad de los servicios en todo momento?	X				
¿El firewall permite que la red utilizada en la empresa este en todo momento segura y disponible?	X				



Firma y DNI

Cuestionario del Administrador: Eduardo Soto Cotrina

TESIS: "ANÁLISIS E IMPLEMENTACIÓN DE UN FIREWALL DE SEGURIDAD PARA EL CONTROL DE ACCESOS Y PROTECCIÓN DE LA RED DE DATOS DE LA EMPRESA FERRETERÍA SOTO, 2021"

Cuestionario para el personal administrativo de la Ferretería Soto

Nombres y Apellidos: Eduardo Soto Cotrina

Cargo: Administrador

I. Indicaciones:

Mediante el uso continuo de su computador y del servicio que utiliza, su persona marque la respuesta que considere luego de la implementación del firewall.

II. Escala de medición:

Para el análisis de los valores se ha considerado una escala de medición, considere la escala para marcar su respuesta.

Escala de medición	*Valores*
Siempre	*1*
Generalmente	*2*
Ocasionalmente	*3*
Casi nunca	*4*
Nunca	*5*

Preguntas y validación

Variable independiente: Implementación de un firewall.

Preguntas	Escala de medición				
	Siempre	Generalmente	ocasionalmente	Casi nunca	Nunca
Dimensión: Políticas					
¿Su persona considera que con la implementación del firewall las amenazas han sido erradicadas?	X				
¿Con la implementación del firewall se tiene un control en la filtración de las entradas y salidas de las solicitudes que se realizan con internet?	X				
Dimensión: Seguridad					

TESIS: “ANÁLISIS E IMPLEMENTACIÓN DE UN FIREWALL DE SEGURIDAD PARA EL CONTROL DE ACCESOS Y PROTECCIÓN DE LA RED DE DATOS DE LA EMPRESA FERRETERÍA SOTO, 2021”

¿Con la implementación del firewall, el dispositivo solo puede ser manipulado por el personal específico?	X				
¿La implementación del firewall presenta una zona segura para el manejo de las redes?	X				
¿Considera que el firewall implementado, brinda una seguridad correcta para evitar vulnerabilidades?	X				

Variable dependiente: Control de accesos y protección de red de datos.

Preguntas	Escala de medición				
	Siempre	Generalmente	ocasionalmente	Casi nunca	Nunca
Dimensión: Integridad					
¿El firewall permite tener un control de la manipulación en los equipos?	X				
Dimensión: Seguridad					
¿El firewall restringe el tráfico de paquetes no acordes a sus labores?	X				
¿El Firewall realiza restricciones dependiendo a la aplicación utilizada?	X				
Dimensión: Disponibilidad					
Con la implementación del firewall. ¿Existe disponibilidad de los servicios en todo momento?	X				
¿El firewall permite que la red utilizada en la empresa este en todo momento segura y disponible?	X				

40714776

Firma y DNI

Cuestionario del Jefe de Logística: Carlos Chilón Cabrera

TESIS: “ANÁLISIS E IMPLEMENTACIÓN DE UN FIREWALL DE SEGURIDAD PARA EL CONTROL DE ACCESOS Y PROTECCIÓN DE LA RED DE DATOS DE LA EMPRESA FERRETERÍA SOTO, 2021”

Cuestionario para el personal administrativo de la Ferretería Soto

Nombres y Apellidos: Carlos Chilón Cabrera

Cargo: Jefe de Logística

I. Indicaciones:

Mediante el uso continuo de su computador y del servicio que utiliza, su persona marque la respuesta que considere luego de la implementación del firewall.

II. Escala de medición:

Para el análisis de los valores se ha considerado una escala de medición, considere la escala para marcar su respuesta.

Escala de medición	*Valores*
Siempre	*1*
Generalmente	*2*
Ocasionalmente	*3*
Casi nunca	*4*
Nunca	*5*

Preguntas y validación

Variable independiente: Implementación de un firewall.

Preguntas	Escala de medición				
	Siempre	Generalmente	ocasionalmente	Casi nunca	Nunca
Dimensión: Políticas					
¿Su persona considera que con la implementación del firewall las amenazas han sido erradicadas?	X				
¿Con la implementación del firewall se tiene un control en la filtración de las entradas y salidas de las solicitudes que se realizan con internet?	X				
Dimensión: Seguridad					

TESIS: "ANÁLISIS E IMPLEMENTACIÓN DE UN FIREWALL DE SEGURIDAD PARA EL CONTROL DE ACCESOS Y PROTECCIÓN DE LA RED DE DATOS DE LA EMPRESA FERRETERÍA SOTO, 2021"

¿Con la implementación del firewall, el dispositivo solo puede ser manipulado por el personal específico?	X				
¿La implementación del firewall presenta una zona segura para el manejo de las redes?		X			
¿Considera que el firewall implementado, brinda una seguridad correcta para evitar vulnerabilidades?	X				

Variable dependiente: Control de accesos y protección de red de datos.

Preguntas	Escala de medición				
	Siempre	Generalmente	ocasionalmente	Casi nunca	Nunca
Dimensión: Integridad					
¿El firewall permite tener un control de la manipulación en los equipos?	X				
Dimensión: Seguridad					
¿El firewall restringe el tráfico de paquetes no acordes a sus labores?	X				
¿El Firewall realiza restricciones dependiendo a la aplicación utilizada?	X				
Dimensión: Disponibilidad					
Con la implementación del firewall. ¿Existe disponibilidad de los servicios en todo momento?	X				
¿El firewall permite que la red utilizada en la empresa este en todo momento segura y disponible?	X				

47031714

Firma y DNI

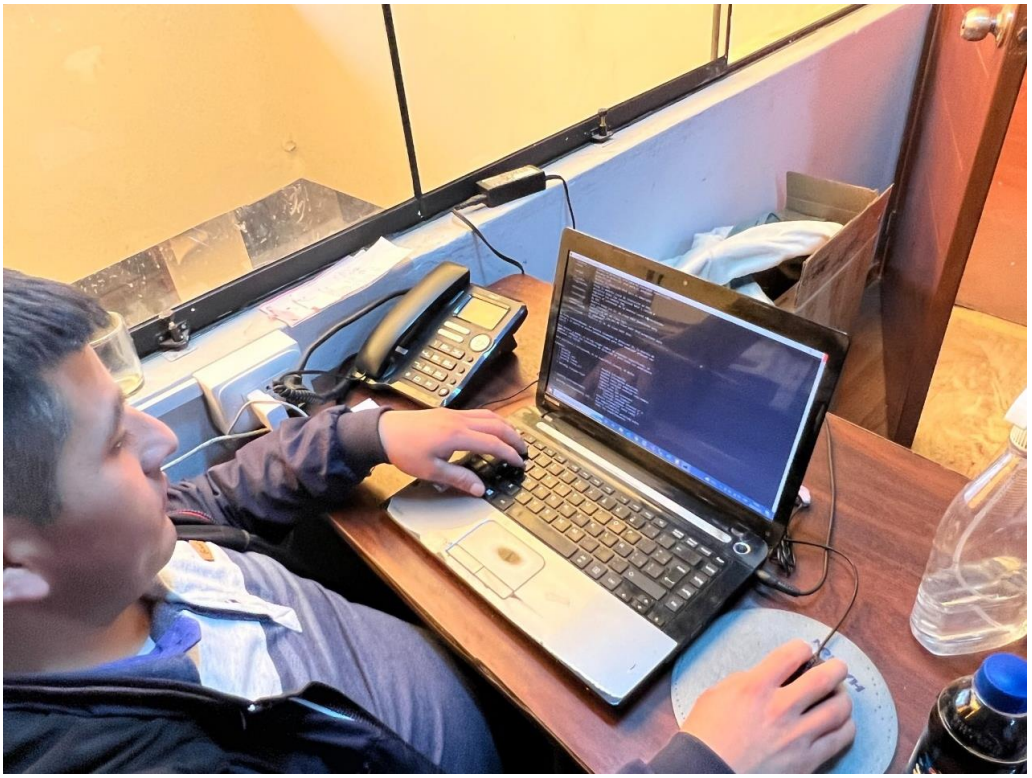
Anexo 8

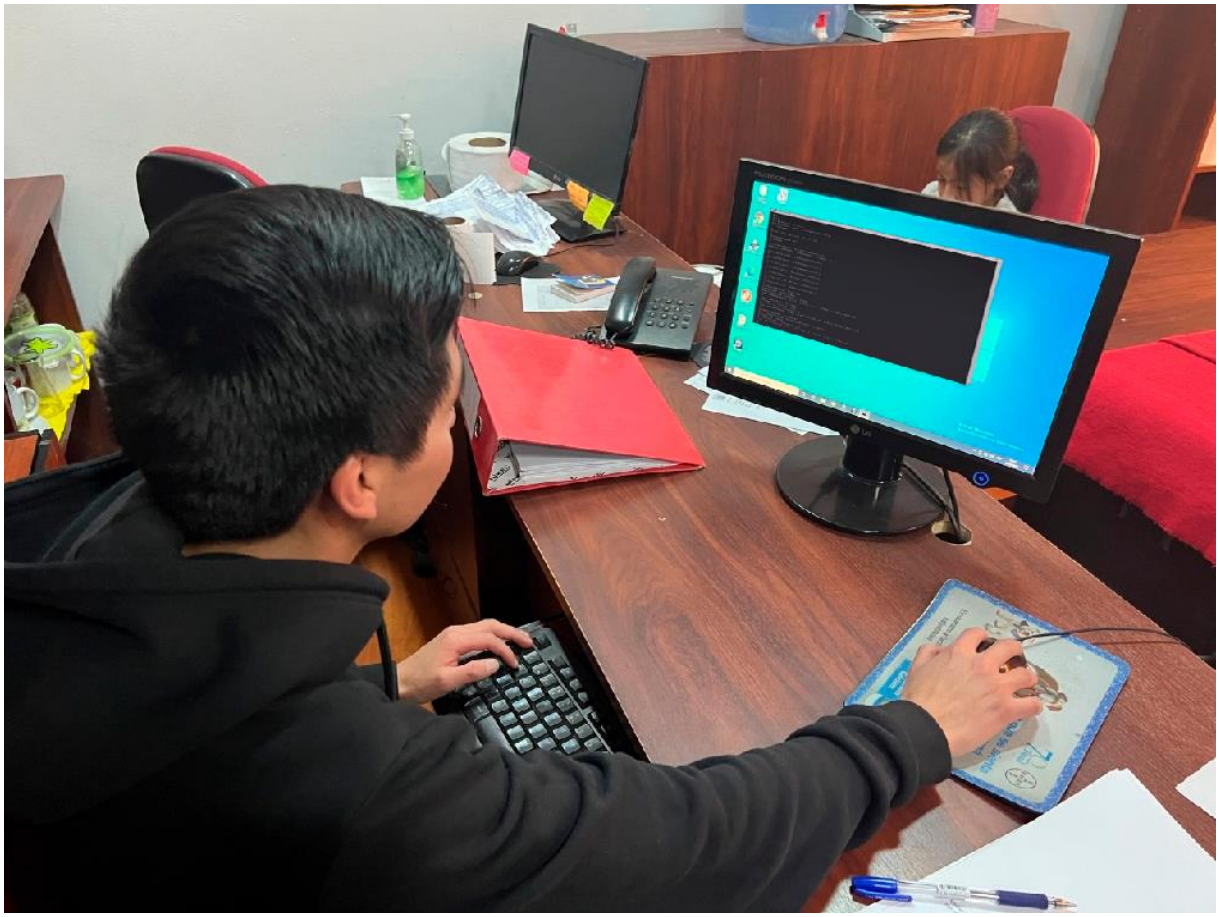
Fotografías durante la implementación de Firewall


976804038

Anexo 9

Fotografías durante las pruebas del firewall





Anexo 10

Fotografías luego de la charla con los administrativos