UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

"Implementación de un servidor Linux y su influencia en la seguridad perimetral de la red local de la empresa Junefield Group S.A., Lima 2017"

TESIS PARA OBTENER EL TITULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTOR:

Omar Ivo Bautista Pillaca

ASESOR:

Dra. Yesenia del Rosario Vásquez Valencia

LINEA DE INVESTIGACION:

Infraestructura y servicios de redes y comunicaciones

LIMA – PERÚ

2017

UCV UNIVERSIDAD CÉSAR VALLEJO	ACTA DE APROBACIÓN DE LA TESIS	Código : F07-PP-PR-02.02 Versión : 09 Fecha : 23-03-2018 Página : 1 de 1

El Jurado encargado de evaluar la tesis presentada por don(a) **BAUTISTA PILLACA OMAR IVO** cuyo título es: **"IMPLEMENTACIÓN DE UN SERVIDOR LINUX Y SU INFLUENCIA EN LA SEGURIDAD PERIMETRAL DE LA RED LOCAL DE LA EMPRESA JUNEFIELD GROUP S.A., LIMA 2017"** Reunido en la fecha, escuchó la sustentación y la resolución de preguntas por el estudiante, otorgándole el calificativo de: **(**11**) (ONCE).**

Lima, San Juan de Lurigancho, 19 de diciembre del 2017

.....	.....
VASQUEZ VALENCIA YESENIA RENEE	**RIVERA CRISOSTOMO**
PRESIDENTE	SECRETARIO

.....

CRISPIN SANCHEZ IVAN

VOCAL

Elaboró	Dirección de Investigación	Revisó	Responsable del SGC	Aprobó	Vicerrectorado de Investigación

DEDICATORIA

El presente trabajo está dedicado a mi madre, esposa e hijos, quienes estuvieron en todo momento apoyándome incondicionalmente, para culminar satisfactoriamente mi carrera profesional.

AGRADECIMIENTO

Agradezco de manera especial al señor Wei Ching Chang, Sub Director del área de Administración y RRHH de la empresa Junefield Group S.A., quien inicialmente aceptó que desarrolle mi tema de tesis en el área que tiene a su cargo y me brindó todas las facilidades del caso en la elaboración de la presente investigación.

DECLARATORIA DE AUTENTICIDAD

Yo, OMAR IVO BAUTISTA PILLACA estudiante de la Escuela Académico Profesional de Ingeniería de Sistemas de la Facultad de Ingeniería de la Universidad Cesar Vallejo, identificado con DNI N°41868746.

Declaro bajo juramento que:

1. Soy autor de la tesis titulada:
   "Implementación de un servidor Linux y su influencia en la seguridad perimetral de la red local de la empresa Junefield Group S.A., Lima 2017", la misma que presento para optar el título profesional de Ingeniero de Sistemas.
2. La tesis no ha sido plagiada ni total ni parcialmente, por el contrario, se ha respetado las normas Internacionales de citas y referencias para las fuentes consultadas.
3. La tesis presentada no atenta contra derechos de terceros.
4. La tesis no ha sido publicada ni presentada anteriormente para obtener algún grado académico previo o título profesional.
5. Los datos presentados en los resultados son reales, no han sido falsificados, ni duplicados.

De identificarse fraude, piratería, plagio, falsificación o que el trabajo de investigación haya sido publicado anteriormente; asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a la normatividad vigente de la Universidad Cesar Vallejo.

Lima, 12 de diciembre de 2017.

Omar Ivo Bautista Pillaca

DNI N°41868746

PRESENTACIÓN

Señores Miembros del Jurado, presento ante ustedes la tesis titulada ***"Implementación de un servidor Linux y su influencia en la seguridad perimetral de la red local de la empresa Junefield Group S.A., Lima 2017"***, en complimiento del Reglamento de Grados y Títulos de la Universidad César Vallejo para obtener el Título Profesional de ***Ingeniero de Sistemas.***

El primer capítulo, comprende la introducción, así como la realidad problemática en los diferentes aspectos, los antecedentes y justificaciones que se han tomado en cuenta; se analiza la formulación del problema para finalmente realizar el planteamiento de las hipótesis y objetivos.

En el segundo capítulo, se detallan aspectos relacionados al tipo y diseño de la investigación, así como la definición conceptual y operacional de las variables y sus indicadores, se definen las variables, población y muestra, de igual manera las técnicas que se utilizará para la recolección de datos y el método de procesamiento de estos.

En el tercer capítulo, se presentan los resultados obtenidos en la investigación y su análisis en el SPSS v.25.0.0. Asimismo, se procede con el desarrollo de la investigación propuesto, para luego realizar las pruebas correspondientes.

En el cuarto capítulo, se presenta la discusión de los resultados. En el quinto capítulo, se describen las conclusiones a las que se llegó en la investigación. En el sexto capítulo, se pueden apreciar las recomendaciones. En el séptimo capítulo, se muestran las referencias utilizadas en la investigación. Finalmente, en el octavo capítulo, se presentan los anexos de la investigación.

Esperando cumplir con los requisitos de aprobación.

Omar Ivo Bautista Pillaca

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

RESUMEN

El objetivo principal de la investigación se basa en implementar un servidor Linux para determinar su influencia en la seguridad perimetral de la red local de la empresa Junefield Group S.A., para lograr dicho objetivo se debe tener en cuenta que el tipo de investigación es aplicada de enfoque cuantitativo, asimismo el diseño utilizado es experimental de tipo pre experimental, se utilizó como población a 27 trabajadores de la empresa Junefield Group S.A., sede Lima. El tipo de muestra que se tomó fue con el método no probabilístico de tipo intencional, el cual indica que la selección es directa, en este caso la muestra ha sido de 11 personas que laboran en el área administrativa y están ubicados en un solo piso. Los resultados de los datos se han obtenido mediante fichas de observación, finalmente para el análisis de los datos se ha utilizado el programa estadístico SPSS versión 25.0.0.

La implementación se desarrolló utilizando la metodología Top Down las cuales comprende cuatro fases: Identificación de necesidades del negocio, diseño lógico, diseño físico, pruebas y optimización del servidor Endian, los resultados observados se han basado en 11 muestras mediante fichas de observación, permitiendo llegar a la conclusión que la seguridad de la red local utilizando un firewall como equipo perimetral es apropiada para la organización.

Palabras Clave: Confidencialidad, Integridad, Disponibilidad

ABSTRACT

The purpose of this research work is to enforce a LINUX server to determine its influence Junefield Group SA's local network perimeter security. To achieve this goal, it should be considered this work is applied in quantitative approach, furthermore the design used is experimental (type pre-experimental). It was used as a population to twenty seven (27) employees from the company Junefield Group SA, Lima headquarters. The sample type to be taken will be with the non-prababilistic method (intentional type), which indicates that the selection will be direct, in this case the sample will be of eleven (11) people who work in the administrative area and are located in a single floor. The result of the data will be obtained by means of observation cards then for the analysis of the data will be used the stadistical program SPSS version 25.0.0.

The implement will be developed using TOP-DOWN methodology which comprises four phases, identification of business needs, logical design, physical design, testing and optimization of the Endian server, the results taken have been based on eleven (11) samples by observations cards, allowing the conclusion that the safety of the local network using a firewall as perimeter equipment is appropriate for the organization.

Password: Confidenciality, Integrity, Availability.

I. INTRODUCCIÓN

1.1. Realidad problemática

En la actualidad, la seguridad de las redes empresariales respecto al correcto dimensionamiento de los equipos perimetrales ha sido y será el principal problema para disponer de una red local segura y estable, ya que muchas organizaciones no cuentan con infraestructura adecuada para controlar los ataques provenientes en muchos casos desde internet y tienen como objetivo alterar los datos o en el peor de los casos al robo de la información.

Para Chacón (2017), en el último año el 28% de empresas ha sido víctima de violaciones a su sistema de de seguridad perimetral, una investigación desarrollada por Gemalto reveló que a nivel global las empresas están confiadas y creen que logran mantener al margen de sus actividades a los hackers, pero en realidad persiste la inseguridad de los datos y son vulnerables de ataques.

Según el estudio, realizado en 1.050 empresas, existe la creencia de que tomar medidas para mantener la seguridad perimetral ("cerrar las puertas informáticas") los tiene a salvo. El 94% está de acuerdo que es muy eficaz para mantener a los usuarios no autorizados fuera de sus redes. Sin embargo, el 65% no cree que sus datos estén protegidos si se viola el perímetro.

Según detalló Gemalto, existe una carencia de comprensión sobre la vulnerabilidad en la que se encuentran los datos y se sienten confiados solo con medidas intermedias. Un 68% acepta que los usuarios no autorizados para revisar algún determinado dato de la organización pueden acceder a ellos y un 53% no cumple con los reglamentos de protección de datos que existen.

A pesar de que ha aumentado la cantidad de filtraciones de información y la pérdida o el robo de la misma en el último año - se han vulnerado alrededor de 1,4 mil millones de registros de datos en 2016 según el Índice de infracción,

la gran mayoría cree que su red no podrá ser accedida por usuarios extraños a ella y un 76% basa esa confianza en que han aumentado la inversión para lograrlo.

Según Zambrano (2015), en un estudio realizado, manifiesta que Perú es el quinto país en Latinoamérica que es víctima de ataques cibernéticos, teniendo la cifra de 11.22% de referencia. Siendo el 19% de los ataques informáticos corresponden a los efectuados en el continente a nivel global. Este dato se obtuvo de dicho estudio en el cual se recopilaron la información de más de 13,000 dispositivos monitoreados.

Debido a que el número de internautas es cada vez mayor que las políticas y estrategias de defensa digital que son implementadas por usuarios y por empresas, el Perú se encuentra presente en este ranking a nivel latinoamericano. En cuanto a incidentes cibernéticos, a nivel regional, el sector financiero cobró relevancia y pasó del segundo al primer lugar, con el 75.29% de las ocurrencias. Se han contabilizado 6.6 millones de ataques diarios.

Digiware, que es en Latinoamérica el primer integrador de seguridad informática, ha hecho la advertencia que los ciberdelincuentes utilizan las redes sociales para obtener datos privados de los internautas y realizar ataques cibernéticos.

Zambrano, también afirmó que la red social de profesionales, LinkedIn, es utilizada por los ciberdelincuentes para robar valiosa información que es expuesta por los usuarios en esta red. Por ejemplo, al manifestar sus cargos en sus respectivas empresas se vuelven objetos de interés para este tipo de robo de información, es por ello que los ataques son cada vez más “personalizados y dirigidos a los empleados de una compañía”, con el fin de acceder a los datos de la empresa.

Según Tenorio (2017), el grupo “Peruvian Hackers” lanzó una amenaza de ataque, entró en la web de un ministerio y aseguró tener datos de la Policía Nacional. El colectivo “Peruvian Hackers” desde el miércoles 24 de mayo del 2017 advirtió en su cuenta de Twitter que llevaría a cabo un ataque informático en el país local. Según lo descrito por el propio grupo, se trató de la “brigada de ataque informático” de Anonymous en el Perú.

En dicha fecha, se reconoció una intervención en la página web del Ministerio del Ambiente pasada las 6.00pm. Este ataque fue asumido por el grupo “Peruvian Hackers", ellos colgaron un aviso y videos en dicha página web que evidenciaban los hechos. Luego, este grupo anuncio en su cuenta de Twitter, información sensible a través de imágenes que fueron compartidas y pertenecían a algunos miembros de la Policía Nacional del Perú, que al parecer, estaban involucrados en problemas medio ambientales, esta información fue conseguida mediante técnicas de hackeo cibernético.

En más de un centenar de países se vieron afectadas compañías e instituciones públicas debido a un ciberataque mundial, esto ha marcado un antecedente reciente que ha puesto en alarma a las autoridades locales. Aunque aún no ha habido confirmación de la empresa Telefónica del Perú, esta empresa ha enviado un comunicado a todos sus socios corporativos exhortándolos a que refuercen sus medidas de seguridad, asimismo que revisen el estado de sus firewalls y también que tengan siempre copias de seguridad de su información actualizadas.

Añadió Tenorio, profesional de la UNI, que le fue facilitado alguno de los documentos oficiales de la cual obtuvo valiosa información y refirió que, de realizarse el ataque, este se estaría valiendo de una brecha de seguridad informática encontrado con bastante antelación por los hackers. “Creo que en este caso pueden haber encontrado una brecha de seguridad que el proveedor de telefonía probablemente no ha reportado de una manera abierta”, señaló el ingeniero informático. “Siempre que ha habido un ataque

de hackers, se produce porque conocen cuál es la falla de seguridad y ya saben por dónde acceder".

La empresa Junefield Group S.A., es una empresa dedicada al rubro de la minería, fue fundada en Perú en mayo del 2008, la oficina principal está ubicada en Av. República de Panamá N°3545 Int. 1301 – San Isidro, en el departamento de Lima; después de varios años de actividad y desarrollo ya posee más de 700,000 hectáreas de petitorios mineros y proyectos adquiridos a nivel nacional, abarcando provincias como Arequipa, Apurímac, Moquegua, Tacna, La Libertad, Puno, entre otras. Actualmente se han establecidos bases en ciudades como Arequipa y Tacna para la ejecución de trabajos de producción y exploración de recursos.

Con los antecedentes antes descritos se tiene una idea más clara de la realidad problemática (vulnerabilidades) que existe dentro y fuera de las redes corporativas a nivel mundial, se afirma que implementar mecanismos de seguridad perimetral (firewall) en la empresa Junefield Group S.A., es importante porque permitirá minimizar el riesgo por intentos de ataques que provengan desde internet hacia la red local, de esa manera resguardar los datos de la empresa.

Actualmente la infraestructura de red de la empresa Junefield Group S.A. cuenta con escasas medidas de seguridad que no garantizan la confidencialidad, integridad y disponibilidad de los datos, comprometiendo así la productividad de la organización. Asimismo, la seguridad de la red local respecto al correcto dimensionamiento de los equipos perimetrales es el problema principal para disponer de una red local segura y estable.

Por otro lado, la falta de control de accesos a los servicios de internet hace que los usuarios puedan acceder a las distintas páginas web sin restricción alguna, exponiendo de esa manera a ser víctima de alteraciones o robos de la información que se distribuye a través de la red local. Por esta razón no existe un momento en el que se deje de pensar los distintos métodos que

existen para resguardar y garantizar la seguridad de los datos, es por ello que se establece tomar medidas preventivas que ayuden a detectar múltiples ataques externos a la red local.

La falta de seguridad perimetral en las redes de datos, son las causas principales para desarrollar el presente estudio, se realizará un diseño de la red local lógico y físico para controlar las debilidades existentes que provienen de los accesos sin restricción a los distintos servicios, se implementará políticas y protocolos de seguridad para mitigar los riesgos de vulnerabilidad que intervienen en el proceso de intercambio de información que ayuden a lograr una infraestructura que cubra las necesidades operativas de la empresa.

En este sentido se afirma que las redes se basan en la eficiencia y respuesta operativa que se puede brindar al usuario, sin dejar a un lado el tema de seguridad, es por eso que la organización debe planear un esquema de seguridad perimetral, basado en las necesidades de negocio y sus objetivos.

1.2. Trabajos previos

De acuerdo a la investigación realizada para mejorar la seguridad perimetral de la red local en la organización, se encontraron los siguientes antecedentes:

1.2.1. Internacional

León Bustamante, L. (2012) en su investigación *"Diseño e implementación de una infraestructura de servicios y red de resguardo de servidores Linux a través de Open Source en la empresa Proteco Coasin SA"*, para optar el título de Ingeniero de Sistemas y Telecomunicaciones, en la Universidad Internacional SEK – Ecuador.

La investigación tiene como objetivo diseñar e implementar una infraestructura de red que afiance la seguridad de la información de la empresa Proteco Coasin S.A.

El autor resaltó que la implementación basada en Open Source es una infraestructura segura y confiable, mencionó que la seguridad de la información es primordial para el entorno empresarial, por ese motivo implementó servicios perimetrales para mitigar el riesgo de vulnerabilidad a su información, la cual permitió acceder de manera confiable a la red. Esto, contribuyó considerablemente en el estado económico de la empresa, permitiendo el aprovechamiento de recursos y disminución de gastos al no tener que adquirir nuevos equipos, además de no ser necesario un pago por licencia del software. Por estas razones tomamos un modelo para poder diseñar la infraestructura con servidores Linux que servirá como barrera perimetral y de esa manera poder resguardar la información y el tráfico que por ese medio se transmite.

En base a lo mostrado el autor aportó con su investigación, la implementación en la red local de servicios basados en Linux, tales como: proxy Squid, servidor de correo electrónico, servicio DHCP, asignación específica de rangos IP para usuarios visitantes; con lo cual logra el mejoramiento, el rendimiento y una adecuada administración de la red actual.

Bueno Rosales, J. (2013), en su tesis *"Sistema de control y seguridad Endian firewall para la empresa Frada Sport",* para optar el título de Ingeniero Informático, en la Universidad Tecnológica Israel – Ecuador.

La investigación tiene como objetivo, establecer un firewall o sistema de control y seguridad informático que posibilite disminuir vulnerabilidades y riesgos, instaurando grados de performance y rendimiento óptimos en el campus informático de la empresa Frada Sport.

El autor utilizó un tipo de investigación aplicada en base a documental, ya que se determina y se establece la investigación de información correspondiente a revistas, libros, manuales y artículos que son vitales para poder plantear y ser parte de la estabilidad lógica y física de la productividad de los equipos. En cuanto a la metodología, aplicó el método de síntesis, ya que el investigador reunió y analizó una serie de elementos que provocan un problema para buscar una solución y ejecutarla.

El autor concluyó con su investigación que, el sistema de seguridad firewall Endian representa una manera planificada y bien direccionada de seguridad, rendimiento, control, rendimiento, administración y disponibilidad de la red general de datos. Asimismo, se puso de manifiesto que en la empresa Frada Sport, es posible adaptar el sistema de seguridad open source, esto debido a los bajos costos que representan para la empresa y que la ayuda a tener principalmente seguridad centralizada de alta disponibilidad, es por ello se recomienda.

En base a lo mostrado el autor aportó con su investigación, establecer un esquema de gestión de información seguro, que se base en la organización y verificación de datos en la red, también mejoró la productividad de la red y de los equipos, mediante protocolos de seguridad diseñados para cada usuario que pertenezca a la empresa, mediante los cuales se pueda permitir y denegar los accesos correspondientes.

Jaramillo Remache, D. (2014), en su tesis *"Auditoría de seguridad informática para el Gobierno Autónomo Descentralizado de Santa Ana de Cotacachi, basada en la norma NTP-ISO/IEC 17799:2007 y la Metodología OSSTMM V2",* para optar el título de Ingeniero en Electrónica y Redes de Comunicación, en la Universidad Técnica del Norte – Ecuador.

La investigación tiene como objetivo, brindar sugerencias adecuadas mediante las cuales se puedan establecer acciones a realizarse que puedan contribuir a optimizar el nivel de seguridad de la información, las

cuales incluyan protocolos de seguridad, para de esta forma disminuir los riesgos que eventualmente puedan generarse más adelante.

El autor concluyó con su investigación que, no está definido el esquema de seguridad de la información, el cual pueda cubrir completamente los peligros probables, no obstante, es posible estar capacitado y predispuesto a responder a las amenazas y vulnerabilidades que suelen presentarse en el rubro de la informática.

En base a lo mostrado el autor aportó con su investigación, el análisis y estudio de ciertos eventos que demuestran la seguridad de la información en el sistema de red es escasa y vulnerable a fallas, y al optimizar ello, se busca ser constante en el servicio que diariamente brinda a los habitantes de la zona, permitiendo optimizar la calidad en el servicio que brinda en el GAD Municipal de San Ana de Cotacachi.

Fabuel Díaz, C. (2013), en su tesis *"Implantación de un sistema de seguridad perimetral"*, para optar el título de Ingeniero de Telecomunicaciones, en la Universidad Politécnica de Madrid – España.

La investigación tiene como objetivo, informar a la población los conceptos más relevantes en los que está basada la seguridad perimetral, ejecutando una prueba de cómo sería la instauración de un proyecto estándar en una supuesta organización creada para tal fin.

El autor concluyó con su investigación que, este tipo de implementación asegura un nivel de óptimo de seguridad para los peligros de la mayoría de las instituciones, pero no es recomendable encomendar toda la confiabilidad de nuestra información a los cortafuegos como único salvaguarda de nuestra seguridad. Estos firewalls deben combinarse con otros elementos que son también necesarios y efectivos, como sondas de detección de intrusos, antivirus, gestores de ancho de banda, proxis, etc.

En base a lo mostrado el autor aportó con su investigación, un análisis que determina que el progreso en las ciencias de la información conlleva el surgimiento de nuevas amenazas y, por lo tanto, será primordial establecer nuevos protocolos de protección que reduzcan a su mínima expresión los peligros que se vayan presentando, el mejoramiento de nuevos protocolos de seguridad es necesario, y será de vital importancia e imprescindibles como los son ahora los antivirus o cortafuegos, será preciso ajustar la infraestructura ya en desuso a las nuevas tecnologías, ya sea, bien ampliando los medios existentes o sustituyéndolos por otros recursos más avanzados.

1.2.2. Nacional

Bravo Valero, L. (2015), en su tesis *"Modelo diagnóstico y análisis de la red LAN para la mejora del rendimiento y seguridad en la Red de Salud Valle del Mantaro mediante la metodología CISCO"*, para optar el título de Ingeniera de Sistemas, en la Universidad Nacional del Centro del Perú – Perú.

La investigación tiene como objetivo, optimizar el nivel de seguridad y rendimiento de la red LAN en la Red de Salud Valle del Mantaro mediante el juicio, análisis y la conclusión de los defectos de la red y su estructura, con la finalidad de presentar un ofrecimiento de diseño de una red basada en la metodología CISCO.

La autora concluyó con su investigación que, es de vital importancia dirigir la red de forma eficiente hoy en día, debido a que gran parte de procedimientos que realizan en una institución se dan en línea, y un error que altere la red originaría perjuicios, por ello el valor agregado del diagnóstico y análisis actual de la red LAN, del cual se plantea un diseño de red basado en la metodología CISCO, el mismo que incluye la creación de VLANs y políticas de seguridad.

En base a lo mostrado la autora aportó con su investigación, que la metodología Cisco (Top-Down Network Design), posibilitó realizar un análisis total de las necesidades de la institución y los objetivos que espera lograr como tal.

Guevara Pérez, O. y Miranda Zelada, A. (2014), en su tesis *"Diseño de una red de datos para el Policlínico Señor de los Milagros S.R.L. usando metodología Top Down Network Design y aplicando estándares ISO/IEC 27002"*, para optar el título de Ingeniero de Computación y Sistemas, en la Universidad Privada Antenor Orrego – Perú.

La investigación tiene como objetivo, el diseño de una red de datos para el Policlínico Señor de los Milagros SRL usando metodología Topdown Network Desing y aplicando estándares ISO/IEC 27002. Resaltando el diseño de una red lógica y un modelo de conectividad, además de establecer las políticas de seguridad adecuadas.

Los autores concluyeron con su investigación que, mediante el análisis y diseño se logró implementar el modelo lógico de la red con ayuda de la metodología Top Down Network Design.

En base a lo mostrado los autores aportaron con su investigación que, gracias al análisis de las 20 encuestas obtenidas se ha podido diseñar políticas de seguridad de Información, políticas de respaldo de red, política de internet, políticas de password, políticas de firewall y un plan de contingencias en caso de alguna falla o siniestro, lo que permitirá tener un mayor control sobre todos los activos que maneja el policlínico a un 100%.

Barrantes Porras, C. y Hugo Herrera, J. (2012), en su tesis *"Diseño e implementación de un sistema de gestión de seguridad de información en procesos tecnológicos"*, para optar el título de Ingeniero de Computación y Sistemas, en la Universidad de San Martín de Porres – Perú.

La investigación tiene como objetivo, reducir y mitigar los riesgos de los activos de información de los procesos que se encuentran bajo la gerencia de tecnología de Card Perú S.A. que ponen en peligro los recursos, servicios y continuidad de los procesos tecnológicos.

El autor concluyó con su investigación que, la acreditación de los procedimientos es un instrumento poderoso para la conservación y optimización de cualquier proceso de gestión organizacional.

En base a lo mostrado el autor aportó con su investigación que, diseñando e implementando una buena metodología para gestionar los riesgos y ejecutando los planes de tratamiento de riesgos planteados, se logra reducir a niveles aceptables gran porcentaje de riesgos que afecten a los activos de información.

1.3. Teorías relacionadas al tema

En este aspecto se menciona algunas definiciones que ayudarán a comprender términos y procesos para la exposición de la presente investigación.

1.3.1. Variable independiente:

1.3.1.1. Servidor Linux

Según Gonzales-Valle (2014), el crecimiento en el uso de sistemas Linux, tanto por usuarios de PC´s tradicionales como por usuarios de servidores, se debe a diversos factores, entre los cuales se pueden contar la búsqueda de la reducción de costos del sistema, la mejora de la seguridad y el apoyo a los principios del código abierto. A lo largo de los últimos años varios gobiernos de diferentes naciones han aprobado

políticas para migrar de los sistemas propietarios de que disponían a sistemas basados en Linux.

Barrios (2014, p. 36), al respecto dice que:

> El uso de Linux en los servidores es cada vez mayor, ya que cuenta con las siguientes ventajas: *Estabilidad*, ya que una instalación típica puede correr durante años sin presentar fallas. *Seguridad*, Linux responde mucho más rápido ante un fallo debido a las características propias del software, además que es atacado con menos frecuencia por virus y malware. *Manejo de Aplicaciones*, las distribuciones de Linux usan repositorios oficiales para sus aplicaciones aplicando controles de calidad y políticas de seguridad que garantizan la integridad y sanidad de los paquetes instalados. *Flexibilidad*, Linux puede reconfigurarse para incluir sólo los servicios esenciales para el tipo de negocio y así optimizar el uso de los recursos. *Costos*, la mayoría del software que se usa en Linux es gratuito lo que hace de éste que sea el rey indiscutible en costos de implementación y difícilmente podrá ser derrocado. *Comunidad*, Linux es y siempre ha sido algo comunitario, este esfuerzo mancomunado permite que se publiquen actualizaciones cada 6 meses en la mayoría de sus distribuciones. *Libertad*, con Linux es libre de usar, modificar y combinar lo que desees para satisfacer las necesidades y las de la empresa.

Asimismo, señala que existen miles de programas libres para Linux adaptados a diversos propósitos y disponibles en Internet para poder utilizarlos. Además, recordemos que para Linux existe gran cantidad de documentación libre, como se puede observar en muchas webs, existe infinidad de información técnica que servirá de ayuda, desde la página oficial de Linux, hasta foros de desarrolladores y programadores.

Finalmente, indica que Linux es la opción más recomendable del presente siglo para los usuarios que no solo buscan libertad, sino que también se adaptan a las necesidades, ya que existen numerosas distribuciones y se eligen la que mejor se ajuste a los requerimientos. Todas ellas comparten el núcleo del sistema y la mayoría de funcionalidades, pero cada una en una línea diferente.

1.3.1.2. Linux como servidor perimetral

Villalón (2002) dice que, por el aumento de las redes en las distintas áreas empresariales, muchas organizaciones se vieron en la necesidad de buscar mecanismo de protección que ayuden a minimizar los ataques provenientes desde internet, es por ello que al hablar de seguridad para una organización se recomienda utilizar plataformas seguras, estables y sobre todo robustas ya que en ella se implementará diversas configuraciones, políticas de acceso y restricciones.

Se puede considerar a Linux, un sistema operativo que ha entendido a la perfección las necesidades del usuario actual en cuanto a usabilidad y simplicidad; y algunas distribuciones son aún más fáciles de usar que el clásico entorno de Windows, dando esto una alta probabilidad de que sea manejado sin problema alguno. Asimismo, se dispone en Linux de gran cantidad de herramientas que gestionan todos los parámetros del sistema, tales como, monitorizar el rendimiento, ver los procesos en ejecución, limpiar el sistema, controlar los servicios habilitados, entre otros; demostrando así que este sistema operativo brinda a los usuarios el soporte que necesitan para lograr sus objetivos.

De igual manera Villalón indicó que Linux no deja abierta la posibilidad del ingreso de virus al sistema operativo, por lo tanto tampoco es necesario el uso de antivirus. Este software libre es mucho más seguro que cualquier otro con sistema de protección, lo que hace de este sistema operativo sea estable y de muy alta confiabilidad y seguridad.

Las plataformas en Linux son multitarea y multiusuario, lo que lo hace muy eficiente, robusto, estable y rápido, siendo ideal para servidores y aplicaciones distribuidas. Así mismo deja libertad al usuario elegir la distribución que mejor se adecue a sus necesidades.

1.3.2. Variable dependiente:

La empresa Junefield Group S.A., ha entendido que la implementación de mecanismos de seguridad perimetral es fundamental para minimizar el riesgo de vulnerabilidad hacia la red local.

Stallings (2004, p. 724), afirma que:

> Con la llegada de los equipos de cómputo, se puso de manifiesto la necesidad de instrumentos automáticos para salvaguardar la información guardada en dichos equipos. Éste es el caso de los sistemas que son compartidos por dos o más usuarios, a los cuales se les denomina multiusuarios. Esta necesidad se pone de manifiesto con mayor énfasis en los sistemas a los que se puede ingresar desde las redes de datos o de telefonía públicas. La denominación general del conjunto de instrumentos diseñados para salvarguardar la información y hacerle frente a los ataques de los hackers se denomina seguridad de la información.

Así mismo, Stallings (2004, p. 725) al respecto manifiesta que:

> Para comprender las variables de riesgos a la seguridad de la información que se presentan hoy en día, es preciso conocer el significado de las diferentes condiciones que se deben cumplir en seguridad. La seguridad de la información conlleva cumplir cuatro requisitos fundamentales:
>
> - Privacidad: Es preciso que solo las instituciones con autorización tengan los permisos correspondientes para acceder a la información. Este tipo de premisos incluye la impresión, la visualización y otras formas de manipulación, incluyendo además el hecho de conocer la existencia de cierta información o datos.
> - Integridad: Es preciso que la información sean alterados solo por personal con autorización. En dichas alteraciones se consideran la escritura, la modificación del estado, la supresión y la creación.
> - Disponibilidad: Es preciso que la información este apta o disponible para el personal autorizado.
> - Autenticidad: Es preciso que un equipo de cómputo o servicio pueda validar la identidad de todos los usuario de la red.

Para Fabuel (2013, p. 225), la “seguridad perimetral ha evolucionado a un ritmo imparable en la última década. El número de amenazas ha crecido de manera exponencial y un entorno de seguridad perimetral se convierte en algo imprescindible actualmente”.

Así mismo, Fabuel (2013, p. 226) sostiene al respecto:

> El número de amenazas en los últimos años se ha disparado y el concepto de seguridad perimetral se ha convertido en una necesidad básica para cualquier organismo con acceso a Internet. Sin embargo, esta evolución no ha hecho más que empezar y lo que ahora puede parecer un entorno seguro, dentro de unos años sin duda se habrá quedado obsoleto. El avance en las tecnologías trae consigo la aparición de nuevas amenazas y sin duda serán necesarios también nuevos sistemas de protección que minimicen los riesgos que vayan surgiendo.

Como bien expresa Fabuel (2013), debemos prescindir de un servidor perimetral a la hora de diseñar una red de cualquier organización, para ello debemos tener en cuenta ciertos aspectos de la infraestructura actual que cuenta cada empresa.

De igual manera, Baltazar y Campuzano (2011, p. 41), manifiesta que:

> En un ambiente en el que día a día se añaden más dispositivos se suman a la misma red para el intercambio de datos, es necesario estar alertas a los peligros que esto acarrea. La seguridad significa que el valor para corromperla excede al costo del bien del equipo de cómputo asegurado, esto es, el tiempo necesario para quebrar la seguridad, sobrepasa el tiempo de vida útil del activo de cómputo, este último pudiendo ser hardware, software o información.

Cuando se hace alusión a la palabra *Seguridad* tiene conceptos como certeza, firmeza, confianza, solidez, estabilidad, veraz, firmes y libres de peligro o riesgo, se dice de los objetos que están bajo protección, confianza, tranquilidad, a salvaguarda de una persona, esto deriva de la premisa de que no hay ningún riesgo que temer. Cuando se hace referencia a

seguridad de la información se dice de todas aquellas medidas para prevenir perjuicios de cualquier clase, quiere decir que se consideran tres puntos de vista primordiales de los sistemas vinculado con la información: confidencialidad, integridad y disponibilidad.

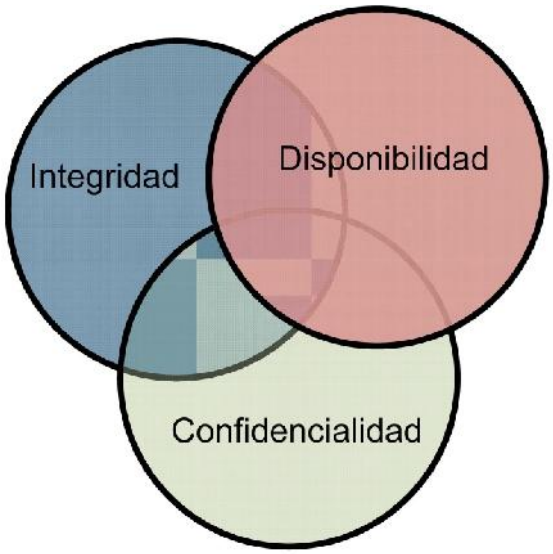


Figura 1. Principios de seguridad
Baltazar y Campuzano, Diseño e Implementación de un esquema de seguridad perimetral para redes de datos, 2011, p.30

De igual manera, se aprecia en la figura 1, los tres principios básicos que contempla la norma ISO/IEC 27002 respecto a la seguridad de la información (Confidencialidad, Integridad, Disponibilidad) el cual engloba distintos procesos que deben ser considerados para implementar exitosamente mecanismos de seguridad que ayuden a minimizar el riesgo por pérdida de información dentro de la organización. Para el presente caso se tomará en cuenta el dominio 11 (control de acceso) y los controles que contempla los objetivos de control 22, 23, 24, 25,26, 27, de la norma ISO en mención. De esa manera se pretende mejorar la seguridad perimetral de la red local de la empresa Junefield Group S.A.

Aguirre (2014, p.30) en su investigación menciona que:

ISO/IEC 27000

> Es una norma internacional que busca dar información general sobre los sistemas de gestión de seguridad de información, así como definir algunos términos que son usados por todos los estándares de la familia 27000.
>
> *ISO/IEC 27001:* El estándar principal de la familia, brinda los requerimientos para el desarrollo y operación de SGSI incluyendo una lista de controles para el manejo y mitigación de los riesgos asociados a los activos de información. Se puede confirmar la eficacia de la implementación del SGSI mediante una auditoria o certificación.
>
> *ISO/IEC 27002:* Este estándar brinda la guía de implementación de la lista de las mejores prácticas y los más aceptados objetivos de control presentados como anexo en la ISO/IEC 27001, con el objetivo de facilitar la elección de controles para asegurar la seguridad de los activos de información.

No obstante, desde el 1 de julio de 2007 la norma ISO/IEC 17799:2005 modificó su nombre a ISO/IEC 27002:2005, pero mantuvo su año de edición y no alteró su contenido.

1.3.2.1. Confidencialidad de los datos

Jaramillo (2014, p. 3) al respecto sostiene que:

> En el entorno de seguridad de la información, la confidencialidad quiere decir que la información que debe mantenerse a buen recaudo y sólo las personas que cuenten con autorización a dicha información, podrán acceder a ella.

El acceso sin autorización a la información reservada es posible que traiga consecuencias demoledoras para la organización, no sólo en lo concerniente de seguridad nacional, sino también en la industria y el comercio. Los instrumentos principales de resguardo de la confidencialidad en los sistemas de información son los controles de acceso y criptografía, como por ejemplo en las amenazas a la confidencialidad se tiene los malware, los intrusos, la ingeniería social, las redes inseguras, y los sistemas mal administrados.

1.3.2.2. Integridad de los datos

Según Gelbstein (2011, p. 3), manifiesta que:

> Los ataques a la integridad de los datos consisten en la modificación intencional de los datos, sin autorización alguna, en algún momento de su ciclo de vida. La modificación no autorizada de sistemas operativos (servidores y redes) y/o de software de aplicaciones (como los "backdoors" o códigos no documentados), tablas de bases de datos, datos de producción y configuración de infraestructura también se consideran ataques a la integridad de los datos. Cabe destacar que muchos de estos sistemas de control no están conectados a Internet y que, en el caso de la inyección del software Stuxnet, debió realizarse una intervención manual, hecho que confirma la teoría de que el "hombre" sigue siendo el eslabón más débil de la cadena de aseguramiento/seguridad de la información.

Para Baltazar y Campuzano (2011, p. 52), la integridad de los datos: "…es un punto de vista fundamental que no sólo se toma en cuenta en el aspecto computacional, hoy en día las empresas y sus sistemas de seguridad de la información hacen frente a riesgos y vulnerabilidades que provienen de una gran diversidad de orígenes, medios tecnológicos, humanos y físicos".

Asimismo, Baltazar y Campuzano (2011, p. 53), sostienen que:

> La puesta en marcha del sistema de seguridad en los centros de informática necesita además de los medios tecnológicos, capacitación y personal especializado, este objetivo es complicado de alcanzar ya que presentan constantes cambios. Con el transcurrir de los años se han suscitado ataques más novedosos con los que se ha aprovechado las vulnerabilidades tanto en el diseño de las redes TCP/IP, en la configuración, operación de los equipos y sistemas que conforman las redes enlazadas a internet. Estas formas de ataque se han mecanizado y esperan entrar a la red interna para dañar la integridad de los datos, es por ello que se requiere en la mayoría de casos un conocimiento técnico elemental para llevarlo a cabo. Cualquier cibernauta

> actualmente puede ingresar a variadas aplicaciones para llevar a cabo estos ataques.

Las instituciones deben considerar el planeamiento de la seguridad, revisar sus protocolos, estudiar su marco referencial y diagramar planes para optimizarlos, el manejo de sus sistemas es el pilar de todo el conjunto, en la cual se debe considerar un encargado del manejo y sistemas de seguridad, es fundamental considerar que para poner en marcha un proyecto, se debe tener primero una administración bien definida, lo siguiente es el diseño del proyecto de seguridad, el que se determina basándose en el análisis del sistema actual: los recursos económicos, las necesidades de la organización y la aprobación de la gerencia. Es preciso hacer un análisis de riesgos y vulnerabilidades, teniendo en cuenta la arquitectura de la red, políticas de seguridad actuales, mecanismos de detección de intrusos, robos, desastres naturales, instrucciones que siguen los usuarios, seguridad interna, seguridad en redes inalámbricas y mantenimiento primordialmente, aquí se consideran tanto la seguridad física como la lógica para asegurar la red y cada terminal, ocasionando lo que hoy en día se le conoce como seguridad convergente.

1.3.2.3. Disponibilidad de los datos

Jaramillo (2014, p. 4) sostiene al respecto:

> La disponibilidad hace referencia a la aptitud de emplear el recurso deseado, en este caso la información, en cualquier momento determinado. La disponibilidad es un aspecto fundamental de fiabilidad, ya que un sistema no disponible es como si no hubiera sistema. El punto de vista de la disponibilidad puede quedar expuesto cuando alguien haga arreglos intencionalmente para prohibir el acceso a los datos o a un servicio, es decir ya no estarán disponible. Hay quienes pueden manejar los recursos, o el tráfico de red, esto quiere decir que los instrumentos para conservar el recurso o la información disponible no trabajan en un ambiente para el que no fueron diseñados. Como resultado, por lo general se obtendrá un error.

Luego de conocer la base para desarrollar la presente investigación con éxito, se determinan algunos aspectos importantes para elaborar el diseño de una red segura y confiable, utilizando estrategias para su implementación.

1.3.2.4. Estrategias de seguridad

Al respecto, Baltazar y Campuzano (2011, p. 54) dicen que:

> Para poner en marcha un esquema de seguridad, es preciso de un planteamiento, las tecnologías por sí solas no aseguran la red, de la misma forma invertir en equipos no necesariamente es garantía de seguridad de la red, el problema es comprender que todas las tecnologías son nulas si no se toman en cuenta las aplicaciones, el método de almacenamiento, los terminales, el tránsito de la información, el perímetro, las configuraciones y lo primordial, el capital humano, ya que no es posible confiar sólo en la tecnología para salvaguardar la red, ya que las personas que han diseñado las tecnologías pueden cometer errores también, no es preciso confiar solo en la tecnología para que proteja a las empresas u organizaciones contra el crimen cibernético.

Una solución integral es precisar proyectos de seguridad, estos proyectos abarcan la seguridad física, lógica y de procedimientos, es fundamental recalcar que el proyecto que sea diseñado para la protección de información en cada empresa es independiente y responsabilidad solo de esta, es claro que las organizaciones presentan con un proyecto de seguridad que quizás no sea el más recomendable, pero trata de ajustarse a las necesidades de la seguridad y posibilidades de la misma. Las aplicaciones, el almacenamiento de la información, las computadoras, los dispositivos de red, y los dispositivos de seguridad perimetral forman parte de un modelo integral de seguridad. Tal como se aprecia en la figura 2, se observa el esquema de la seguridad perimetral para resguardar la información.

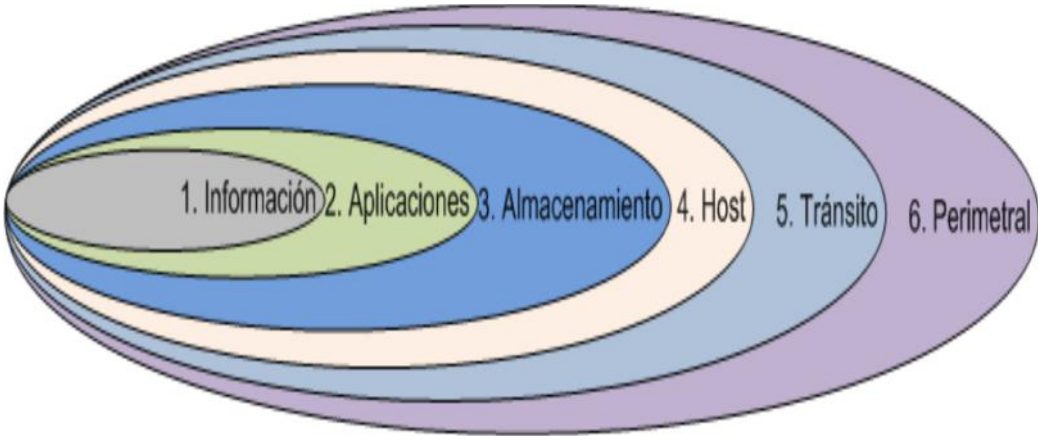


Figura 2. Esquema de la seguridad perimetral

Baltazar y Campuzano, Diseño e Implementación de un esquema de seguridad perimetral para redes de datos, 2011, p. 54

1.3.2.5. Seguridad en profundidad

Para Baltazar y Campuzano (2011, p. 55), refiere que:

> El origen general de la definición en profundidad, la que se encuentra relacionada a tres ámbitos: militar, industrial y seguridad de sistemas de información, define varias barreras independientes, esta táctica es el mejor esquema de defensa, es el más robusto, ya que su interés primordial es fortalecer y supervisar cada sistema.

Está basada en la puesta en marcha de distintos sectores que son resguardados por instrumentos variados, donde cada uno es pieza clave y fortalece a los otros, de esta forma se logra que si uno de ellos colapsa no se deje indefenso toda la red ya que están presentes otros instrumentos que aniquilar. Es decir, se trata de que el proceso sea más costoso y difícil para un agresor al intentar vulnerar la seguridad de una red, esto se va a llevar a cabo con la multiplicidad y redundancia de la protección, constituida en múltiples niveles de seguridad, cada instrumento respalda a otro que se

encuentre en una capa inferior, cubriendo en ocasiones aspectos traslapados.

Un aspecto fundamental de esta táctica busca controlar y evitar fallas de modo común, es decir, que los instrumentos utilizados deben ser configurados con extremo cuidado para así evitar que las fallas de uno no se extiendan al resto, la defensa en profundidad recomienda que los instrumentos sean de diferentes marcas, debido a que si se logra violar por algún medio uno de ellos, el siguiente no pueda ser vulnerado en la misma magnitud.

1.3.2.6. Plataforma de seguridad de la red

En la actualidad existen diversas plataformas que ayudan a mejorar la seguridad perimetral de la red local en una organización como son los firewalls, proxy, VPN, antivirus, etc. las cuales permite organizar y gestionar adecuadamente los distintos servicios que se brinda a los usuarios. Asimismo, protege y resguarda la información que se distribuye a través de la red, implementando mecanismos para formar una barrera de los ataques provenientes desde internet, fortaleciendo de esa manera la seguridad de los datos. En este sentido cabe resaltar la importancia de elegir una buena arquitectura y plataforma que ayuda a cumplir con el propósito esperado.

1.3.2.7. Seguridad perimetral

Tanenbaum (2003, p. 776), afirma lo siguiente:

> El diseño de defensa perimetral es una similitud a un castillo rodeado por una fosa, cuando se utiliza este diseño para asegurar una red, las instituciones refuerzan o robustecen los estándares de sus sistemas y las fronteras de sus redes, es por ello que la defensa perimetral es un grupo de tácticas, maniobras y normas, las cuales defienden y establecen un seguimiento de la parte externa de la red, las técnicas más empleadas para límites de acción

son las que se aplican por medio de los firewalls, proxy, VPN, y NAT. Estos mecanismos, toleran una gestión centralizada de la red, ya que se concentran los esfuerzos en algunos puntos de acceso que definen al perímetro. Cabe resaltar que este diseño no hace nada para salvaguardar los sistemas de ataques internos, puede presentar fallas casuales como se pueden dar en otro diseño.

Para una adecuada decisión acerca de los instrumentos a emplear se deben considerar los siguientes puntos de vista:

- **Recursos físicos:** Establecer ambientes (Data center) que garanticen seguridad de los servidores y demás equipos utilizados para el manejo de la información.

- **Infraestructura de red:** Debe contar con diseño bien estructurado para garantizar el flujo de información y la estabilidad de la red local.

- **Flujo de información:** Se refiere a la cantidad de información que es transmitida a través de la red local.

- **Políticas establecidas:** Establecer mecanismos y controles de seguridad que garanticen la integridad de la información.

- **Cantidad de información:** Activo de la empresa que se almacena en los servidores principales, razón de ser para implementar políticas de seguridad.

Es preciso tener claro cuáles son las amenazas que se quieren evitar provenientes del exterior antes de poner en funcionamiento el sistema, esto para establecer cuáles son las medidas más adecuadas para proteger este bien, así como las políticas actuales de la institución.

1.4. Formulación del problema

1.4.1. Problema principal

¿De qué manera la implementación de un servidor Linux influye en la seguridad perimetral de la red local de Junefield Group S.A.?

1.4.2. Problemas específicos

¿De qué manera la implementación de un servidor Linux influye en la confidencialidad de la red local de la empresa Junefield Group S.A.?

¿De qué manera la implementación de un servidor Linux influye en la integridad de la red local de la empresa Junefield Group S.A.?

¿De qué manera la implementación de un servidor Linux influye en la disponibilidad de la red local de la empresa Junefield Group S.A.?

1.5. Justificación del estudio

Todo estudio está dirigido a dar solución algún problema o inquietud. Asimismo, es posible que se vaya a investigar una manifestación o un hecho que sea necesaria su investigación; es por ello que, es preciso demostrar o acreditar, las razones por las que se está realizando el estudio. Igualmente, se debe señalar su magnitud, extensión o dimensión para comprender su viabilidad. Según Méndez (2011, p. 195) “la justificación en la investigación puede ser de carácter teórico, práctico o metodológico”.

1.5.1. Justificación teórica

La presente investigación se realiza con la finalidad de contribuir conocimiento al ya existente en la actualidad, respecto a la implementación de un servidor Linux y su influencia en la seguridad perimetral de la red local, cuyos resultados de esta investigación permitirá adoptar estrategias como propuesta para incorporarse como conocimiento, debido a que se estaría demostrando que el uso de estrategias de seguridad minimiza el riesgo de vulnerabilidades de la red local.

Según, Bermúdez y Bailón: (2015, p. 8)

> La información es parte fundamental y crítica de toda la empresa, y a su vez es uno de los recursos más propensos a vulnerabilidades, siendo necesario protegerlos de amenazas internas y externas. En la actualidad las empresas necesitan que la información que manejan esté siempre disponible, sin alteraciones en sus datos y sea confiable.

1.5.2. Justificación práctica

La investigación se realiza porque existe la necesidad de mejorar la seguridad perimetral de la red local de la empresa Junefield Group S. A., con el uso de estrategias de seguridad que se pretende implementar para minimizar el riesgo de vulnerabilidades de la red local.

Bueno (2013, p. 146), en su investigación manifiesta que la implementación del sistema de seguridad Endian firewall:

> […] significa una forma planificada de comprobación, aseguramiento, productividad, disponibilidad y manejo de la red general de datos, es decir, es un análisis de la organización tácticas de la investigación, basada en la observación directa, encuestas descriptivas y referencia cruzada, para así poder precisar la línea más importante de la problemática de la organización y comprender procedimientos fundamentales para su desarrollo.

1.5.3. Justificación metodológica

El diseño e implementación de estrategias de seguridad para cada dimensión que se estudia en la presente investigación se realizó siguiendo los pasos de la metodología científica, las cuales son en la mayoría de casos investigados por la ciencia, una vez que se demuestre su validez y confiabilidad podrán ser utilizados en otros proyectos de estudios afines.

Bueno (2013, p. 75) también dice, "…todo el procedimiento y manejo justifica el resguardo cuyos lineamientos están basados en mecanismos de seguridad, a través de medios centralizados, tácticas y metodologías de seguridad mostradas para disminuir riesgos y aumentar expuestas para reducir vulnerabilidades y aumentar el rendimiento o desempeño del software y hardware en los equipos informáticos de la red".

1.5.4. Justificación institucional

Implementar un servidor Linux para la empresa Junefield Group S.A., tiene como objetivo proteger la integridad de los datos de ataques enfocados a la sustracción de información, falsificación, modificación, denegación de servicios, suplantaciones, vulnerabilidades, entre otras, que se distribuyen a través de los distintos sistemas de información de la red local, provenientes de usuarios internos o externos ocasionando alteración de los datos o en el peor de los casos pérdida de la información, por tal sentido la implementación pretende mejorar la seguridad perimetral para proteger los servicios e información de la empresa partiendo desde el análisis de la situación actual de la red local para determinar los problemas existentes, identificar amenazas, vulnerabilidades, buscando posteriormente el diseño que permita minimizar los riesgos.

Con estas medidas lo que se pretende lograr es brindar un nivel óptimo de confianza y seguridad para la organización; sobre todo obtener como resultado la confidencialidad, integridad y disponibilidad de los datos, para cumplir con dicho propósito se busca seguir una metodología que

brinde un nivel de aseguramiento ideal para los objetivos planteados por la organización. Es importante resaltar, que a mayor número de controles o pruebas se lleven a cabo, el nivel de confianza que logrará la empresa es sin duda, de mejores proporciones.

1.5.5. Justificación económica

La razón principal para implementar un servidor Linux, dado que la información es un activo muy importante y crítico de una organización se deben buscar mecanismos de seguridad que minimicen los riesgos de cualquier eventualidad que pueda existir en el medio donde se encuentran, de no ser así el impacto que generen puede ocasionar pérdidas considerables que afectaran económicamente a la empresa, ya que en los servidores de datos se encuentran información clasificada de todos los proyectos a nivel nacional que a su vez son utilizados para la toma de decisiones, se puede afirmar lo antes mencionado porque se tiene como valor referencial las inversiones que se realiza en cada proyecto y que se ve reflejado en los archivos e información almacenados en los servidores principales. Por otro lado, la alteración de los datos puede ser considerable, porque en muchos casos es casi imposible recuperar información vulnerada, afectando la estabilidad y el prestigio de la organización.

1.5.6. Justificación técnica

Se afirma entonces que la importancia de implementar un servidor basado en Linux; cumple absolutamente todas las necesidades tal cual el primer instrumento de resguardo de las redes y equipos que una empresa desea para resguardarse de los atentados de otras redes, pero, esta sólo es la primera línea de defensa, hoy en día se ha aumentado sobremanera la utilización de estos instrumentos para reguardarse de ciertos atentados y así de esta forma, disminuir la posibilidad de que la red sea vulnerada al estar conectada a internet. Un firewall es un sistema o conjunto de sistemas

que permiten implementar políticas o normas (filtros web, control de aplicaciones, filtro de direcciones IP, protocolos de enrutamiento, etc.) para el adecuado manejo de los permisos entre dos o más redes. Dentro de él, se establecen políticas que permiten el acceso o salida de paquetes de datos a la red, estas políticas están conectadas principalmente con el tipo de información o datos que se dejarán pasar a una red interna o salir de esta, su objetivo es entonces, aprobar o denegar el tráfico de datos de una red a otra, así mismo, es importante mencionar que la implementación un servidor firewall basado en Linux reducirá los costos en el diseño de la arquitectura de la red local.

1.5.7. Justificación personal

Realizar la implementación del servidor Linux tiene como propósito acercar al alumno a una realidad clara, es así que se analizó una serie de metodologías que ayudarán a mejorar los procesos actuales y a garantizar el buen funcionamiento de los sistemas de información que conlleva a su vez al éxito de la empresa, repotenciando de esa manera, las habilidades de este autor en la solución de problemas que se muestran en la organización utilizando estrategias para su realización. Asimismo, desarrollar los conocimientos adquiridos a lo largo de la carrera profesional, motivo por el cual esto impulsó a este investigador a contribuir con el diseño e implementación de tecnologías, específicamente en redes y comunicaciones, donde se tiene un mayor desempeño y el aporte de nuevas ideas para mejorar la seguridad de la red local de la empresa Junefield Group S.A., a su vez adquirir y fortalecer los conocimientos que resulta de mucho apoyo para obtener un óptimo desarrollo como futuro profesional en la carrera de Ingeniería de Sistemas.

1.6. Hipótesis

1.6.1. Hipótesis general

- La implementación de un servidor Linux influye significativamente en la seguridad perimetral de la red local de la empresa Junefield Group S.A.

1.6.2. Hipótesis específica

- La implementación de un servidor Linux influye significativamente en la confidencialidad de la red local de la empresa Junefield Group S.A.

- La implementación de un servidor Linux influye significativamente en la integridad de la red local de la empresa Junefield Group S.A.

- La implementación de un servidor Linux influye significativamente en la disponibilidad de la red local de la empresa Junefield Group S.A.

1.7. Objetivos

1.7.1. Objetivo general

- Determinar la influencia del servidor Linux en la seguridad perimetral de la red local de la empresa Junefield Group S.A.

1.7.2. Objetivos específicos

- Determinar la influencia del servidor Linux en la confidencialidad de la red local de la empresa Junefield Group S.A.

- Determinar la influencia del servidor Linux en la integridad de la red local de la empresa Junefield Group S.A.

- Determinar la influencia del servidor Linux en la disponibilidad de la red local de la empresa Junefield Group S.A.

II. MÉTODO

2.1. Diseño de investigación

El diseño de investigación de la presente tesis es *experimental*, de tipo pre – experimental porque su grado de control es mínimo. Se realizará un análisis inicial (pre – test) que determinará la situación del problema antes del estímulo (servidor Linux) y final (post – test) que permitirá determinar y evaluar su influencia en la variable dependiente (Mejora de la Seguridad Perimetral de la Red Local).

Según Hernández S., Roberto, Fernández C., Carlos y Baptista L., Pilar (2014), se denota de la siguiente manera:

G: O1 → X → O2

Donde:

G : Grupo de sujetos

X : Tratamiento, estimulo o condición experimental.

O1, O2 : Medición de los sujetos de un grupo (pre y post prueba)

Tipos de estudio

De acuerdo a su finalidad, el tipo de investigación es *aplicada,* porque busca solucionar problemas específicos relacionados a la gestión de la seguridad perimetral de la red local de la empresa Junefield Group S.A., aplicando los conocimientos obtenidos en los servidores Linux y su implementación en dicha red.

Uno de los propósitos fundamentales de la *investigación científica* es el de resolver problemas, a lo que conocemos como Investigación Aplicada. (Hernández S. et al., 2014)

De acuerdo a su profundidad, el alcance de esta investigación es *explicativa*, ya que pretende establecer las causas de los eventos, sucesos o fenómenos que se estudian, es decir se centra en explicar por qué ocurre un fenómeno y en qué condiciones se manifiesta en la mejora de la seguridad perimetral de la red local de la implementación de un servidor Linux para la empresa Junefield Group S.A.

De acuerdo a su alcance, el tipo de investigación es *longitudinal,* porque puede extender el análisis a una sucesión de momentos temporales, es decir, cuando a un mismo grupo se le aplican 2 medidas, *pre-test* y *post-test*.

Para Hernández S. et al. (2014, p. 159), los estudios longitudinales son los que "… obtienen datos en diferentes puntos del tiempo, para realizar inferencias sobre la evolución del problema de investigación o fenómeno, sus causas y sus efectos".

Metodología

El enfoque de la presente investigación es *cuantitativo*, porque se va a verificar la hipótesis a través de la medición y comparación de resultados ejecutados sobre las variables además de establecer una relación entre ellas, fundamentando sus resultados con la estadística.

El enfoque cuantitativo usa la recolección de datos para probar hipótesis, en base en la medición numérica y el análisis estadístico, para establecer patrones de comportamiento y probar teorías. (Hernández S. et al., 2014, p. 5). Asimismo, tal como se aprecia en la figura 3, se observa las fases que comprende el proceso cuantitativo de la metodología de la investigación.

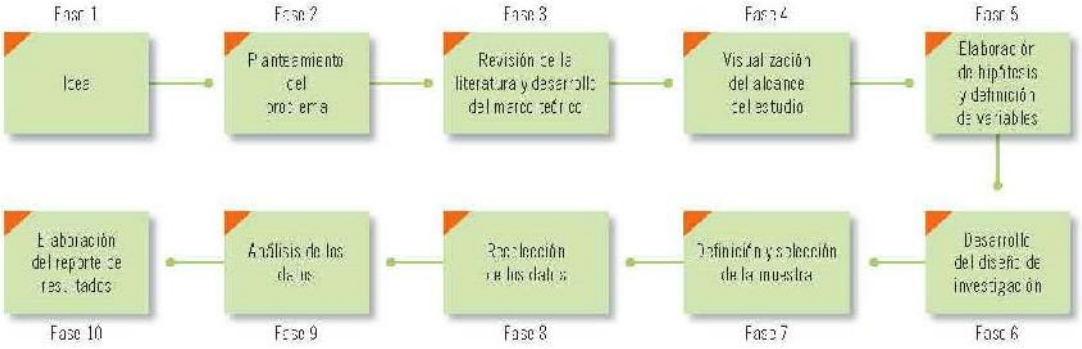


Figura 3. Proceso cuantitativo de la metodología de la investigación

Hernández, Fernández y Baptista, Metodología de la Investigación, 2014, p. 5

2.2. Variables, operacionalización

Se han determinado las siguientes variables:

2.2.1. Variable independiente (VI)

Servidor Linux.

2.2.2. Variable dependiente (VD)

Seguridad perimetral de la red local

2.2.3. Operacionalización de variables

Teniendo en cuenta las variables anteriormente descritas, tanto independientes como dependientes, se ha elaborado las tablas correspondientes a la operacionalización de variables para cada caso.

Tabla 1. Operacionalización de variable independiente

Variable	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Escala de Medición
Variable independiente: Servidor Linux	El núcleo Linux fue combinado con el sistema GNU. El Sistema Operativo formado por esta combinación se conoce como GNU/Linux. GNU/Linux® es un robusto, estable y sumamente versátil sistema operativo con licencia libre y que implementa el estándar POSIX (acrónimo de Portable Operating System Interface), que se traduce como Interfaz de Sistema Operativo Portable. (Barrios, 2014, pág. 897)	Se obtendrán datos de la muestra para analizar el comportamiento del servidor realizando pruebas y verificar el desempeño de los servicios a implementar.	Funcionalidad	Nivel de estabilidad del servidor	Nominal <Sí, No>
				Cumplimiento de servicios que brinda a la red	
			Confiabilidad	Tolerancia a fallos	

Tabla 2. Operacionalización de variable dependiente

Variable	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Escala de Medición
Variable dependiente: Seguridad Perimetral de la Red Local de la empresa Junefield Group S.A.	El objetivo de la seguridad en la red es otorgar alternativas para evitar las fallas que se pueden presentar en los sistemas que se relacionan con el empleo de hardware, software, manejo de información digital. (Baltazar	Para poder comprender las clases de amenazas a la seguridad que existen, es preciso empezar desde una definición de requisitos en seguridad. La seguridad en computadores y en redes conlleva los siguientes requisitos;	Confidencialidad	Nivel de políticas de seguridad	Ordinal <1-4> 4. Muy Alto <76%-100%> 3. Alto <51%-75%> 2. Regular <26%-50%> 1. Bajo <1%-25%>
				Nivel de confidencialidad de los datos	Ordinal <1-4> 4. Muy Alto <76%-100%> 3. Alto <51%-75%> 2. Regular <26%-50%> 1. Bajo <1%-25%>
			Integridad	Nivel de riesgo de los datos	Ordinal <1-4> 4. Muy Alto <76%-100%> 3. Alto <51%-75%> 2. Regular <26%-50%> 1. Bajo <1%-25%>
				Manipulación de datos	Ordinal <1-4> 4. Muy Alto <76%-100%> 3. Alto <51%-75%> 2. Regular <26%-50%> 1. Bajo <1%-25%>

	y Campusano, 2011, pág. 53)	confidencialidad, integridad y disponibilidad (Stallings, 2004, pág. 725)	Disponibilidad	Nivel de disponibilidad de los datos	Ordinal <1-4> 4. Muy Alto <76%-100%> 3. Alto <51%-75%> 2. Regular <26%-50%> 1. Bajo <1%-25%>

2.3. Población y muestra

2.3.1. Población

Para Hernández S. et al (2014, p. 174), "La población es el conjunto de todos los casos que concuerdan con una serie de especificaciones".

Asimismo, Hernández S. et al (2014, p. 174) hacen énfasis en que:

> Un estudio no será mejor por tener una población más grande; la calidad de un trabajo de investigación estriba en delimitar claramente la población con base en el planteamiento del problema. Las poblaciones deben situarse claramente en torno a sus características de contenido, lugar y tiempo.

Teniendo en cuenta lo expuesto en el párrafo anterior se ha determinado que para este proyecto de investigación, la población para estudiar el problema y cumplir con los objetivos propuestos está conformada por un total de 27 personas distribuido en dos pisos, primer piso conformado por 11 usuarios que conforman las áreas de administración, contabilidad, legal, TI, y el segundo piso conformado por 16 usuarios que forman el área de geología, medio ambiente y relaciones comunitarias.

2.3.2. Muestra

Para Hernández S. et al (2014, p. 173), "…es un subgrupo de la población del cual se recolectan los datos y debe ser representativo de ésta", las cuales se pueden categorizar en dos grandes ramas: Las muestras probabilísticas y las muestras no probabilísticas. En las muestras probabilísticas todos los elementos de la población tienen la misma posibilidad de ser elegidos para la investigación y se consiguen definiendo las propiedades de la población y el tamaño de la muestra, a través de una selección al azar o mecánica de las unidades de análisis. En las muestras no probabilísticas, como su nombre lo indica, la elección de los elementos no depende de la probabilidad, sino de causas concernientes con las características del estudio o de quien realiza la muestra. En este caso, el método selección no es mecánico ni a base de fórmulas de probabilidad, sino por el contrario, va a depender del proceso de toma de decisiones del investigador según las características particulares del estudio.

Para esta investigación se ha tomado como muestra a 11 trabajadores de la población total, es decir, a las personas involucradas directamente con la implementación de seguridad perimetral de la red local. El tipo de muestra a tomar será *no probabilístico* de tipo *intencional* porque se realizará la muestra en un área específica, en este caso, correspondiente a todos los usuarios que están distribuidos en el primer piso, quienes serán sometidos a distintas pruebas para comprobar la efectividad de la implementación, para luego ser comparados con la población que no se verá afectado directamente.

2.3.3. Muestreo

Para Hernández S. et al (2014), “el muestreo es el proceso de selección de un número de individuos para un estudio, tal que los individuos representen al grupo más grande del cual fueron seleccionados, para lo cual existen diversos métodos”.

Para la presente investigación se ha utilizado el método *no probabilístico o dirigida de tipo causal o accidental*. La selección será directa, de manera intencional de selección.

2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad

Según Carrasco (2005), estas “son un conjunto de reglas y pautas que guían las actividades que realizan los investigadores en cada una de las etapas de la investigación”.

La recolección de datos ocurre en los ambientes naturales y cotidianos de los participantes o unidades de análisis. (Hernández S. et al, 2014)

El origen de la información es exclusiva propiedad de la empresa Junefield Group SA. Para la investigación se ha utilizado como técnica e instrumentos la observación de parte del investigador en todo momento del proceso, debido a que se tiene la necesidad de obtener como resultados mejorar la seguridad perimetral de la red local.

2.4.1. Técnicas: Observación

Para Hernández S. et al (2014, p. 252), “La técnica empleada en la investigación es la *observación*, este método de recolección de datos

consiste en el registro sistemático, válido y confiable de comportamientos y situaciones observables, a través de un conjunto de categorías y subcategorías".

Esta técnica ayudará a recolectar la información respecto a la seguridad perimetral de la red local de la empresa Junefield Group S.A., a través del diseño *pre-test* y *post-test* se probará evaluar el comportamiento significativo de los usuarios, y si contará con la aprobación y/o preferencia por parte de ellos.

2.4.2. Instrumentos: Ficha de observación

Según Hurtado de Barrera (2010), las fichas de observación, "se usan cuando el investigador debe registrar datos que aportan otras fuentes como son personas, grupos sociales o lugares donde se presenta la problemática. Son el complemento del diario de campo, de la entrevista y son el primer acercamiento del investigador a su universo de trabajo".

Para la presente investigación, la ficha de observación está orientada a indagar información con respecto a determinar cuáles son los eventos y las situaciones particulares que se podrían presentar, tanto antes como a lo largo de la implementación para mejorar la seguridad perimetral de la red local de la empresa Junefield Group S.A. Para ello se ha entrevistado al personal seleccionado, ya que ellos son los involucrados directamente en la investigación.

Tabla 3. Técnicas e instrumentos

Técnicas	Instrumentos
Observación de los Procesos	Ficha de Observación

2.4.3. Validación y confiabilidad del instrumento

La técnica utilizada es la observación, para conocer el grado de mejoras que la implementación de un servidor Linux ha realizado con respecto a la seguridad perimetral de la red local de la empresa Junefield Group S.A. La validez de un instrumento *"se explica como el grado en que un instrumento verdaderamente mide la variable que pretende medir".*

2.4.3.1. Validez

Explica si el instrumento de medición que se está empleando mide lo que verdaderamente se desea medir. Abarca a su vez, tres tipos de validez: relacionada con el contenido, con el criterio y de constructo. El presente estudio emplea la validez de contenido, en la cual se ha tomado como fundamento el marco teórico como respaldo de la ejecución de esta investigación.

2.4.3.2. Confiabilidad

Según Hernández S. et al, (2014, p. 208), "la confiabilidad de un instrumento de medición es el grado con que la aplicación que se repite al mismo sujeto u objeto produce los mismos resultados".

2.5. Métodos de análisis de datos

Respecto al análisis de datos se utilizará la estadística descriptiva, luego de haber aplicado como instrumento la ficha de observación en la muestra en las diferentes áreas de la empresa Junefield Group S.A.

Luego se ha procedido a analizar las hipótesis a la luz de las pruebas estadísticas obtenidas bajo los parámetros de la estadística descriptiva y de la estadística inferencial, con la finalidad de probar las hipótesis y difundir los resultados obtenidos en la muestra a la población (estimación de parámetros). Es decir, probaremos la hipótesis general descrita en el presente estudio: La implementación de un servidor Linux mejora la seguridad perimetral de la red local de la empresa Junefield Group S.A., además de las hipótesis específicas, cuyo procedimiento es explicado en la figura 4, donde se observa el procedimiento de la estadística inferencial que ha de desarrollar el investigador.

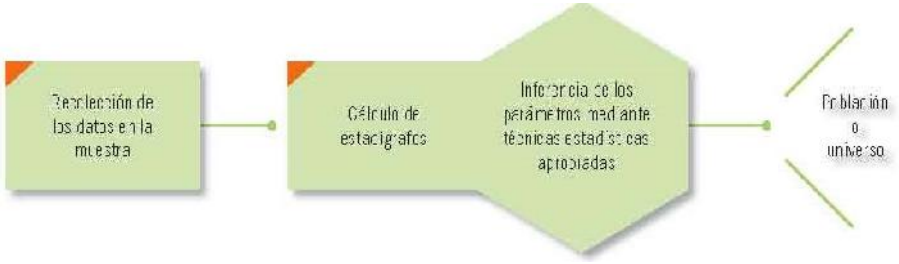


Figura 4. Procedimiento de la estadística inferencial

Hernández, Fernández y Baptista, Metodología de la Investigación, 2014, p. 299

Para analizar los datos colocados en una matriz de tabulación se ha utilizado el análisis cuantitativo, que consiste en comparar diferencias entre el mismo grupo de la muestra, a través del programa estadístico SPSS v.25.0.0 se desarrolla el análisis de datos y se presentan los resultados, dado que la muestra es de 11 elementos entonces se ha utilizado la distribución T-Student, debido a que los especialistas en estadística suelen asociar la distribución “t” con estadísticas de muestras pequeñas.

La prueba t, se utiliza para comparar los resultados de un pre-test y de un post-test, donde se comparan las medias y varianzas del grupo en dos momentos diferentes. La media se calcula aplicando una fórmula estadísticas, más conocida como la fórmula del promedio, dado que pre-

test y post-test fueron en momentos diferentes, ambos promedios después son comparados para determinar las conclusiones de la investigación.

Para las pruebas de pre-test y post- test se utilizaron métodos como la prueba de normalidad para conocer el tipo de datos que se empleó en el estudio, además de las pruebas de la hipótesis, las cuales se detallan en los siguientes puntos:

2.5.1. Prueba de normalidad

Para verificar la probabilidad de las variables se tienen las pruebas de Kolgomorov-Smirov (K-S) y de Shapiro-Wilk, la utilización de cualquiera de ellas va a depender de la cantidad de la muestra que se tenga:

Donde:

N > 30 Prueba de Kolgomorov-Smirov (K-S)

N ≤ 30 Prueba de Shapiro Wilk

Para ello se ha utilizado el programa SPSS v. 25.0.0 para conseguir el valor de significancia, con esto se definirá si es posible adoptar una distribución normal o no normal.

Sig. > α (0.05) se adopta una distribución normal

Sig. ≤ α (0.05) se adopta una distribución no normal.

Se ha utilizado el método de Shapiro-Wilk en los indicadores de la presente investigación, ya que la población es menor a 30, se han aplicado además pruebas no paramétricas porque el resultado de normalidad de los indicadores dio como resultado un nivel de significancia menor a 0.05, lo cual acredita una distribución normal por parte de los indicadores.

2.5.2. Desviación estándar

La desviación estándar es el promedio de desviación de las puntuaciones con respecto a la media. Se simboliza como “σ”. Esto es, la desviación en cada puntuación respecto a la media es elevada al cuadrado, se suman todas las desviaciones cuadradas, se divide entre el número total de puntuaciones y a esta división se le saca la raíz cuadrada (Hernández, Fernández y Baptista, 2014, p. 288).

$$\sigma = \sqrt{\frac{\sum_{i=1}^{N}(X - \bar{x})^2}{N}}$$

2.5.3. Varianza

Hernández, Fernández y Baptista (2014, p. 288), definieron a la varianza como el valor elevado al cuadro de la desviación estándar y se simboliza como σ^2.

$$\sigma^2 = \frac{\sum_{i=1}^{N}(X - \bar{x})^2}{N}$$

2.5.4. Prueba para muestras relacionadas

Este tipo de muestra permite corroborar si existen diferencias entre las distribuciones de dos poblaciones, partiendo de dos muestras dependientes o relacionadas, es decir, que un elemento de la primera muestra está relacionado con un elemento de la segunda muestra, además estos deben ser lo más parecidos posible para que las características a medir sean las más relevantes (Guillén, Alea, Muñoz et al. 2001, p. 117).

2.6. Aspectos éticos

Se mantendrá el respeto a la información recibida y con la cual se va a trabajar por un tema de confidencialidad, asimismo, la información encontrada es mostrada en la bibliografía de esta tesis. Se muestran los resultados de la investigación de forma trasparente sin atentar contra la reserva de los datos que forma parte de esta investigación.

Este estudio se adapta a los aspectos éticos profesionales. Se ha respetado la exactitud de los resultados obtenidos así como los datos brindados por los usuarios de la empresa Junefield Group SA, también se ha respetado a los autores y se les menciona en la referencias bibliográficas como respaldo de la presente investigación. Además se ha mantenido en reserva la información confidencial a la que se ha podido tener acceso en la empresa.

III. RESULTADOS

Se realizó una ficha de observación para definir si lo planteado corresponde con las hipótesis, por ello se muestra cada indicador mencionado en la *operacionalización de variables*.

3.1. Análisis de resultados

Antes de pasar con la validación de hipótesis se muestra los resultados de las fichas de observación que muestran un cambio significativo en la seguridad perimetral de la red local de la empresa Junefield Group S.A.

Tabla 4. Ficha de observación – Variable dep.: Seguridad perimetral (Pre - test)

Escala de medición Pre-test:											
1. Bajo <1%-25%> **2. Tolerable <26%-50%>** **3. Alto <51%-75%>** **4. Muy alto <76%-100%>**											
Dimensiones	**Indicadores**	**MUESTRA**									
		M1	**M2**	**M3**	**M4**	**M5**	**M6**	**M7**	**M8**	**M9**	**M10**	**M11**
Confidencialidad	Nivel de políticas de seguridad	27	28.33	37	40	30	40	37	40	30	30	22
	Nivel de confidencialidad de los datos	17	37	37	58.3	10	47	27	37	27	47	43.3
Integridad	Nivel de riesgo de los datos	75	72.5	70	55	70	65	70	65	70	70	77.5
	Manipulación de datos	80	60	70	50	90	50	75	70	75	50	60
Disponibilidad	Nivel de disponibilidad de los datos	90	92	88.3	92	92	88.3	87	87	90	90	93

Tabla 5. Ficha de observación – Variable dep.: Seguridad perimetral (Post - test)

Escala de medición Post-Test:												
1. Bajo <1%-25%> **2. Tolerable <26%-50%>** **3. Alto <51%-75%>** **4. Muy alto <76%-100%>**												
Dimensiones	**Indicadores**	**MUESTRA**										
		M1	**M2**	**M3**	**M4**	**M5**	**M6**	**M7**	**M8**	**M9**	**M10**	**M11**
Confidencialidad	Nivel de políticas de seguridad	89.3	89	93.3	95	82	91	97	92	91	88.3	93.3
	Nivel de confidencialidad de los datos	94	95	96	97	96	96.3	97	94	96	96.3	95
Integridad	Nivel de riesgo de los datos	15	14	9	10	15	12.5	3.5	10	12.5	15	7.5
	Manipulación de datos	4	5	6	4	3	3	2.5	6	4	3	5
Disponibilidad	Nivel de disponibilidad de los datos	96	92	96	95	94	96	95	95	93.3	92.3	96.3

Se analizaron los resultados de la ficha de observación (Pre – test y post – test), para cada uno de los indicadores en las diferentes dimensiones, mostrando los siguientes resultados:

3.1.1. Dimensión: Confidencialidad

3.1.1.1. Indicadores: Nivel de políticas de seguridad

Para el indicador nivel de políticas de seguridad se puede observar en la tabla 6 los resultados obtenidos de las muestras, las cuales mejoraron en un promedio de 63.96% en post – test vs pre – test.

Tabla 6: Resultados del nivel de políticas de seguridad

	MUESTRA											
	M1	**M2**	**M3**	**M4**	**M5**	**M6**	**M7**	**M8**	**M9**	**M10**	**M11**	**Promedio**
Pre-test	27	28.3	37	40	30	40	37	40	30	30	22	**32.8**
Post-test	89.3	89	93.3	95	82	91	97	92	91	88.33	93.33	**91.0**
Variación %	69.2	68.2	60.4	57.9	63.4	56	61.9	56.5	67	66	76.4	**63.96**

Asimismo, se aprecia en la figura 5 que el nivel de políticas de seguridad incrementó de una manera significativa en relación del pre-test vs post-test.

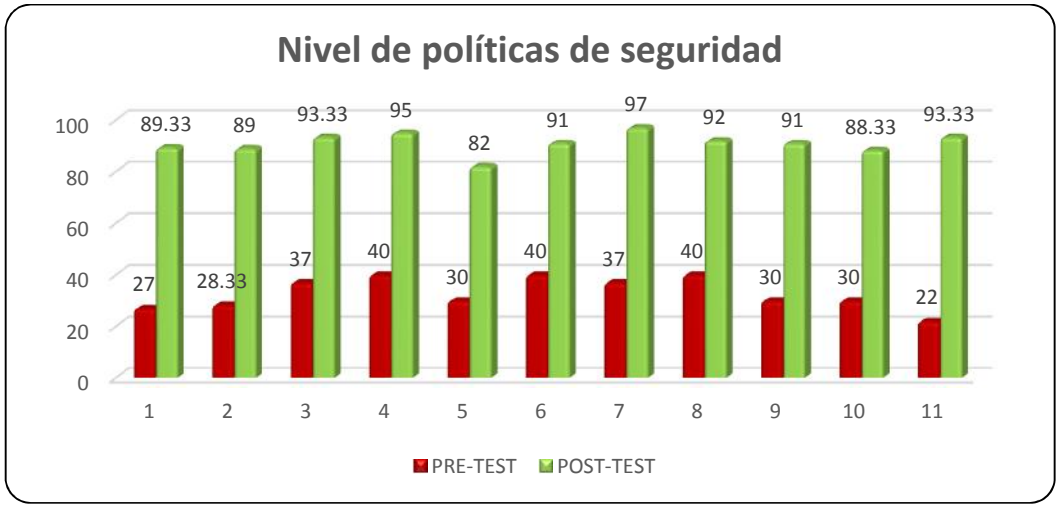


Figura 5. Resultados del nivel de políticas de seguridad

3.1.1.2. Indicadores: Nivel de confidencialidad de los datos

Para el indicador nivel de confidencialidad de los datos se puede observar en la tabla 7 los resultados obtenidos de las muestras, las cuales mejoraron en un promedio de 63.2% en post – test vs pre – test.

Tabla 7. Resultados del nivel de confidencialidad de los datos

	MUESTRA											
	M1	**M2**	**M3**	**M4**	**M5**	**M6**	**M7**	**M8**	**M9**	**M10**	**M11**	**Promedio**
Pre-test	17	37	37	58.33	10	47	27	37	27	47	43.33	**35.2**
Post-test	94	95	96	97	96	96.33	97	94	96	96.33	95	**95.7**
Variación %	81.9	61.1	61.5	39.9	89.6	51.2	72.2	60.6	71.9	51.2	54.4	**63.2**

Asimismo, se aprecia en la figura 6 que el nivel de confidencialidad de los datos incrementó de una manera significativa.

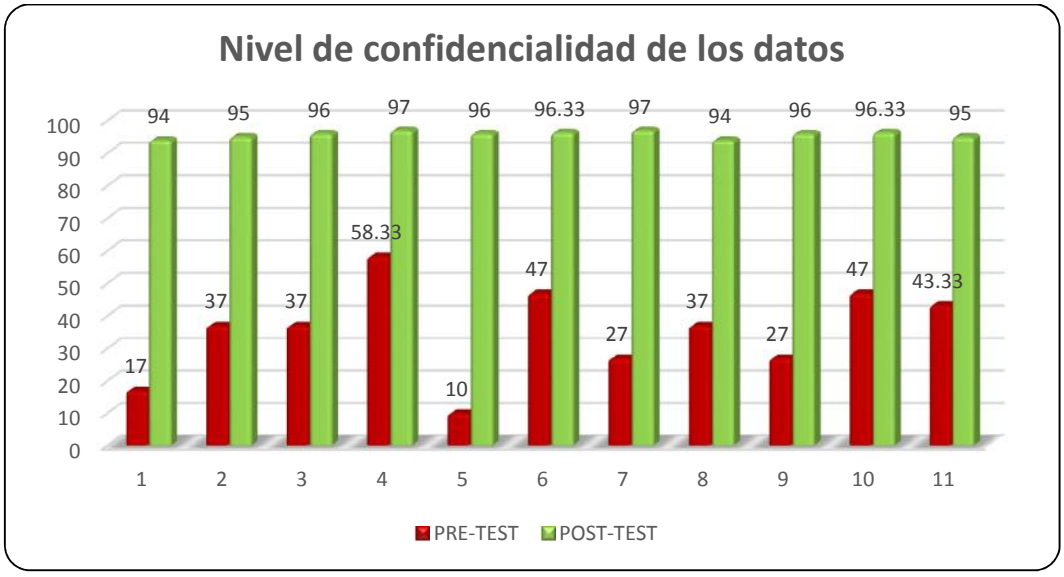


Figura 6. Resultados del nivel de confidencialidad de los datos

3.1.2. Dimensión: Integridad

3.1.2.1. Indicadores: Nivel de riesgo de los datos

Para el indicador nivel de riesgo de los datos se puede observar en la tabla 8 los resultados obtenidos de las muestras, las cuales mejoraron en un promedio de -69.10% en post – test vs pre – test.

Tabla 8. Resultados del nivel de riesgo de los datos

	MUESTRA											
	M1	**M2**	**M3**	**M4**	**M5**	**M6**	**M7**	**M8**	**M9**	**M10**	**M11**	**Promedio**
Pre-test	75	72.5	70	55	70	65	70	65	70	70	77.5	**69.09**
Post-test	15	14	9	10	15	13	3.5	10	13	15	7.5	**11.36**
Variación %	-60	-79.3	-64.3	-72.7	-71.4	-76.9	-57.1	-69.2	-64.3	-71.4	-73.5	**-69.10**

Asimismo, se aprecia en la figura 7 que el nivel de riesgo de los datos disminuyó de una manera significativa.

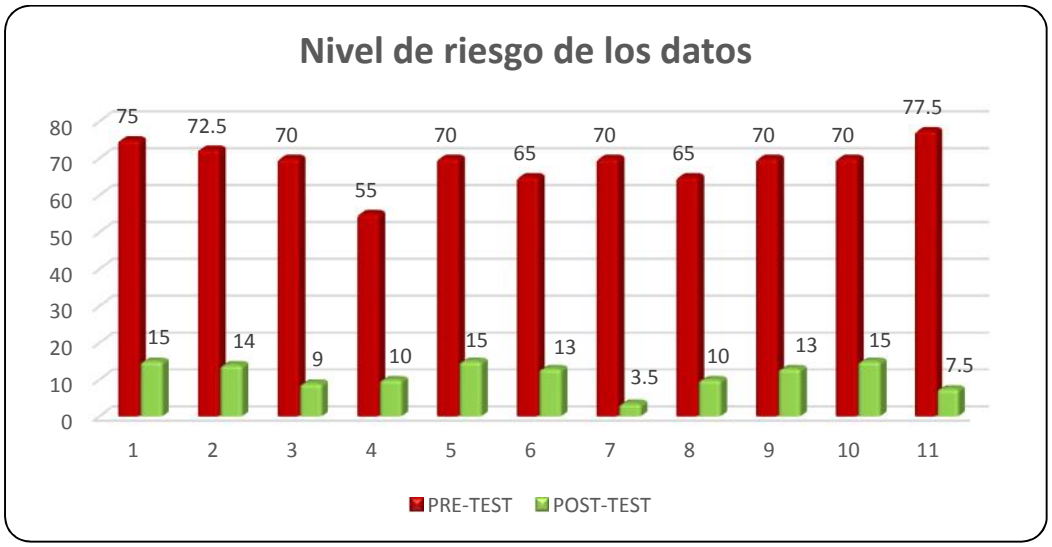


Figura 7. Resultados del nivel de riesgo de los datos

3.1.2.2. Indicadores: Manipulación de datos

Para el indicador manipulación de los datos se puede observar en la tabla 9 los resultados obtenidos de las muestras, las cuales mejoraron en un promedio de -93.56% en post – test vs pre – test.

Tabla 9. Resultados de manipulación de los datos

	MUESTRA											
	M1	**M2**	**M3**	**M4**	**M5**	**M6**	**M7**	**M8**	**M9**	**M10**	**M11**	**Promedio**
Pre-Test	80	60	70	50	90	50	75	70	75	50	60	**66.4**
Post-Test	4	5	6	4	3	3	2.5	6	4	3	5	**4.1**
Variación %	-95	-91.7	-91.4	-92	-96.7	-94	-97	-91.4	-94.7	-94	-91.7	**-93.56**

Asimismo, se aprecia en la figura 8 que la manipulación de los datos disminuyó de una manera significativa.

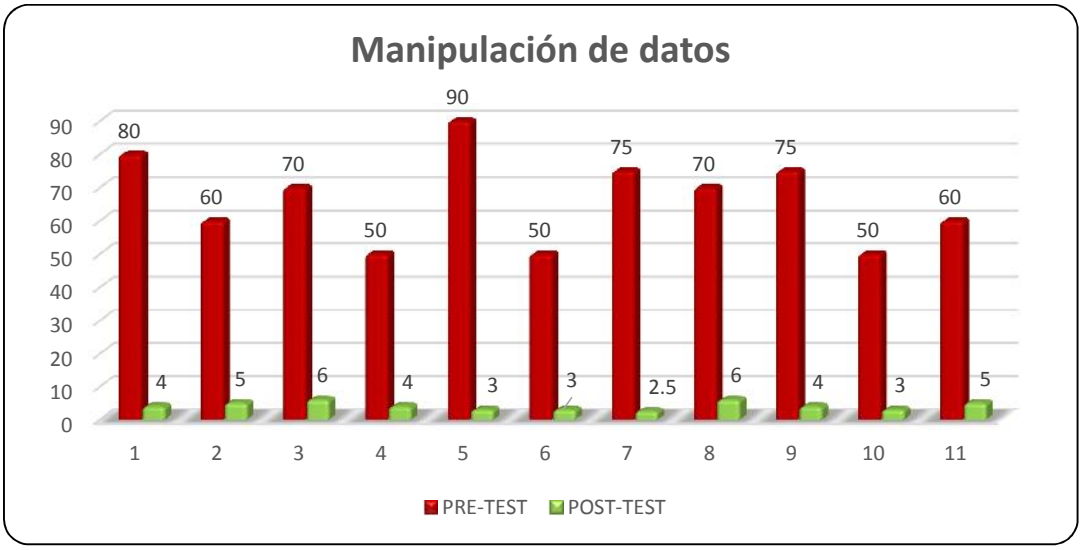


Figura 8. Resultados de manipulación de los datos

3.1.3. Dimensión: Disponibilidad

3.1.3.1. Indicadores: Nivel de disponibilidad de los datos

Para el indicador nivel de disponibilidad de los datos se puede observar en la tabla 10 los resultados obtenidos de las muestras, las cuales mejoraron en un promedio de 5.25% en post – test vs pre – test.

Tabla 10. Resultados del nivel de disponibilidad de los datos

	MUESTRA											
	M1	**M2**	**M3**	**M4**	**M5**	**M6**	**M7**	**M8**	**M9**	**M10**	**M11**	**Promedio**
Pre-Test	90	92	88.3	92	92	88	87	87	90	90	93	**90.0**
Post-Test	96	92	96	95	94	96	95	95	93.3	92.3	96.3	**94.6**
Variación %	6.7	0	8.7	3.3	2.2	8.7	9.2	9.2	3.7	2.6	3.6	**5.25**

Asimismo, se aprecia en la figura 9 que el nivel de disponibilidad de los datos aumentó de una manera significativa.

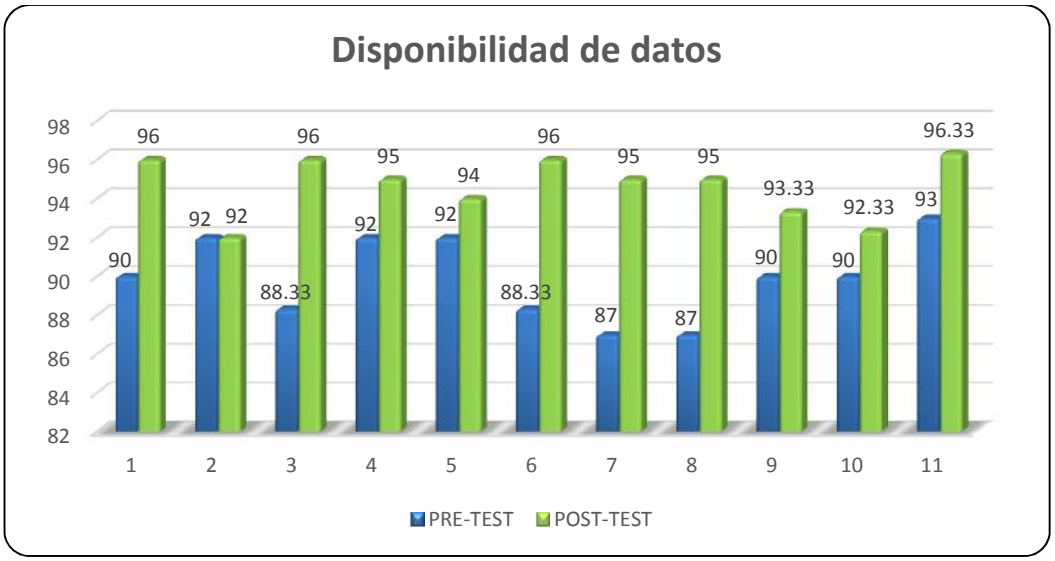


Figura 9. Resultados del nivel de disponibilidad de los datos

3.2. Análisis y validación de hipótesis

3.2.1. Análisis descriptivo

En el estudio se realizó la implementación de un servidor Linux para evaluar los diferentes indicadores que muestren la mejora de la seguridad perimetral de la red local de la empresa Junefield Group S.A.; para ello, en primera instancia se aplicó un pre-test que permitió conocer las condiciones iniciales de cada indicador, posteriormente se realizó la implementación del servidor Linux y nuevamente se realizaron las fichas de observación para

evaluar los indicadores. Los resultados descriptivos de estas medidas se observan a continuación:

3.2.1.1. Indicador: Nivel de políticas de seguridad

Para el indicador, nivel de políticas de seguridad, los resultados descriptivos se muestran a continuación:

Tabla 11. Estadísticas descriptivas del nivel de políticas de seguridad

	N	Mínimo	Máximo	Media	Desviación estándar
Nivel de políticas de seguridad - Pre_test	11	22,00	40,00	32,8482	6,20125
Nivel de políticas de seguridad - Post_test	11	82,00	97,00	91,0291	3,98455
N válido (por lista)	11				

Se observa en la tabla 11 las estadísticas descriptivas para el indicador nivel de políticas de seguridad, teniendo un valor mínimo de 22% y máximo de 40% para pre-test, y, un valor mínimo de 82% y máximo de 97% para post-test.

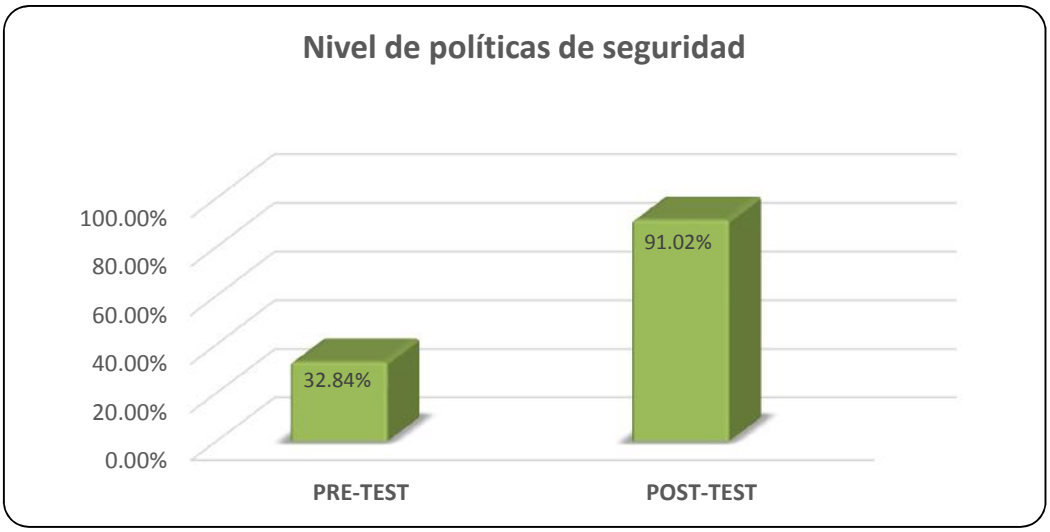


Figura 10. Nivel de políticas de seguridad en pre-test y post-test

Asimismo, se puede apreciar en la figura 10, que en el pre-test de las muestras se obtuvo una media de 32.84%, mientras que en el post-test fue de 91.02%, esto indica una diferencia significativa entre el antes y el después de la implementación del servidor Linux, evidenciando así una mejora del indicador nivel de políticas de seguridad al haber un aumento de sus valores.

3.2.1.2. Indicador: Nivel de confidencialidad de los datos

Para el indicador, nivel de confidencialidad de los datos, los resultados descriptivos se muestran a continuación:

Tabla 12. Estadísticas descriptivas del nivel de confidencialidad de los datos

	N	Mínimo	Máximo	Media	Desviación estándar
Nivel de confidencialidad de los datos - Pre_test	11	10,00	58,33	35,2418	14,10686
Nivel de confidencialidad de los datos - Post_test	11	94,00	97,00	95,6964	1,05847
N válido (por lista)	11				

Se observa en la tabla 12 las estadísticas descriptivas para el indicador nivel de confidencialidad de los datos, teniendo un valor mínimo de 10% y máximo de 58.33% para pre-test, y, un valor mínimo de 94% y máximo de 97% para post-test.

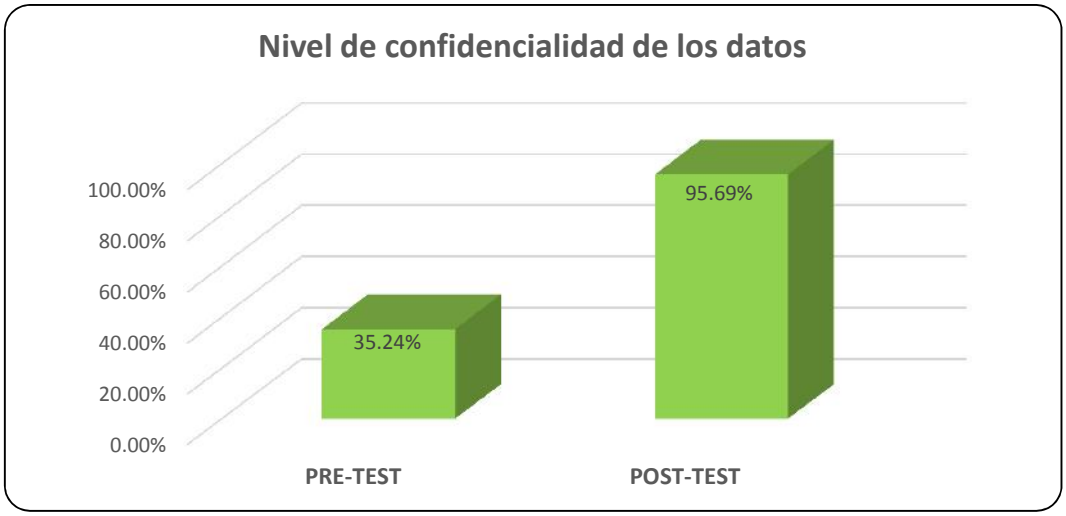


Figura 11. Nivel de confidencialidad de los datos en pre-test y post-test

Asimismo, se puede apreciar en la figura 11, que en el pre-test de las muestras se obtuvo una media de 35.24%, mientras que en el post-test fue de 95.69%, esto indica una diferencia significativa entre el antes y el después de la implementación del servidor Linux, evidenciando así una mejora del indicador nivel de confidencialidad de los datos al haber un aumento de sus valores.

3.2.1.3. Indicador: Nivel de riesgo de los datos

Para el indicador, nivel de riesgo de los datos, los resultados descriptivos se muestran a continuación:

Tabla 13. Estadísticas descriptivas del nivel de riesgo de los datos

	N	Mínimo	Máximo	Media	Desviación estándar
Nivel de riesgo de los datos - Pre_test	11	55,00	77,50	69,0909	5,94482
Nivel de riesgo de los datos - Post_test	11	3,50	15,00	11,3636	3,71545
N válido (por lista)	11				

Se observa en la tabla 13 las estadísticas descriptivas para el indicador nivel de riesgo de los datos, teniendo un valor mínimo de 55% y máximo de 77.50% para pre-test, y, un valor mínimo de 3.5% y máximo de 15% para post-test.

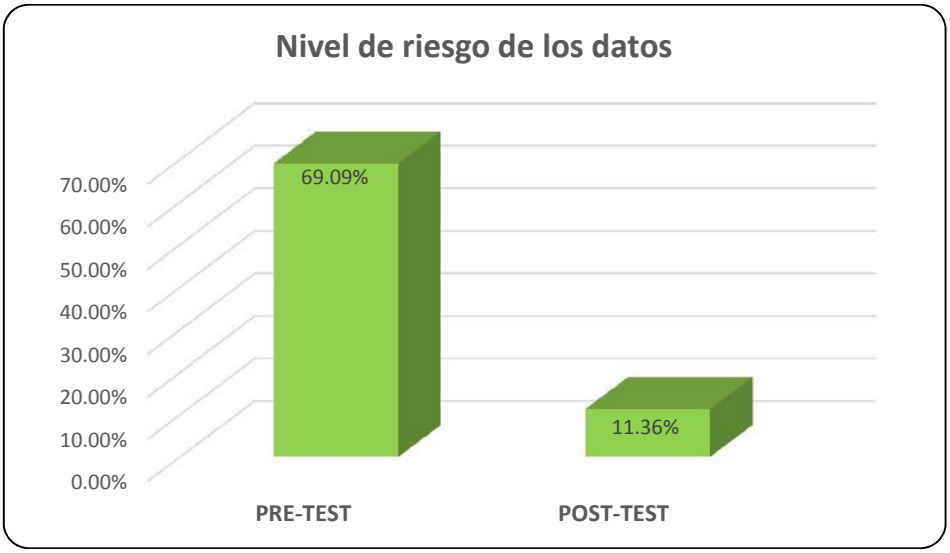


Figura 12. Nivel de riesgo de los datos en pre-test y post-test

Asimismo, se puede apreciar en la figura 12, que en el pre-test de las muestras se obtuvo una media de 69.09%, mientras que en el post-test fue de 11.36%, esto indica una diferencia significativa entre el antes y el después de la implementación del servidor Linux, evidenciando así una mejora del indicador nivel de riesgo de los datos al haber una disminución de sus valores.

3.2.1.4. Indicador: Manipulación de datos

Para el indicador, manipulación de datos, los resultados descriptivos se muestran a continuación.

Tabla 14. Estadísticas descriptivas de manipulación de datos

	N	Mínimo	Máximo	Media	Desviación estándar
Manipulación de datos - Pre_test	11	50,00	90,00	66,3636	13,43334
Manipulación de datos - Post_test	11	2,50	6,00	4,1364	1,22660
N válido (por lista)	11				

Se observa en la tabla 14 las estadísticas descriptivas para el indicador manipulación de datos, teniendo un valor mínimo de 50% y máximo de 90% para pre-test, y, un valor mínimo de 2.50% y máximo de 6% para post-test.

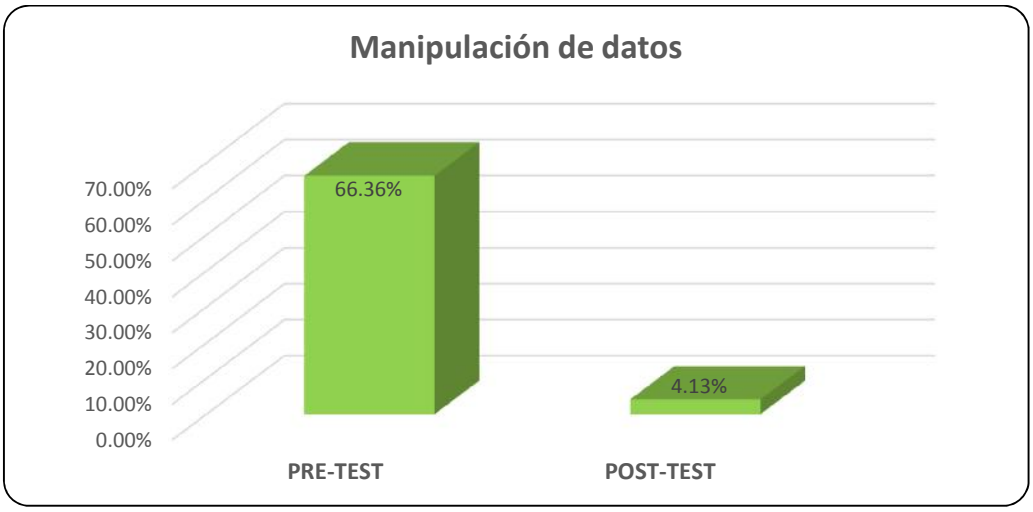


Figura 13. Manipulación de datos en pre-test y post-test

Asimismo, se puede apreciar en la figura 13, que en el pre-test de las muestras se obtuvo una media de 66.36%, mientras que en el post-test fue de 4.37%, esto indica una diferencia significativa entre el antes y el después de la implementación del servidor Linux, evidenciando así una mejora del indicador manipulación de datos al haber una disminución de sus valores.

3.2.1.5. Indicador: Nivel de disponibilidad de los datos

Para el indicador, nivel de disponibilidad de los datos, los resultados descriptivos se muestran a continuación:

Tabla 15. Estadísticas descriptivas del nivel de disponibilidad de los datos

	N	Mínimo	Máximo	Media	Desviación estándar
Nivel de disponibilidad de los datos - Pre_test	11	87,00	93,00	89,9691	2,11110
Nivel de disponibilidad de los datos - Post_test	11	92,00	96,33	94,6355	1,52397
N válido (por lista)	11				

Se observa en la tabla 15 las estadísticas descriptivas para el indicador nivel de disponibilidad de los datos, teniendo un valor mínimo de 87% y máximo de 93% para pre-test, y, un valor mínimo de 92% y máximo de 96.33% para post-test.

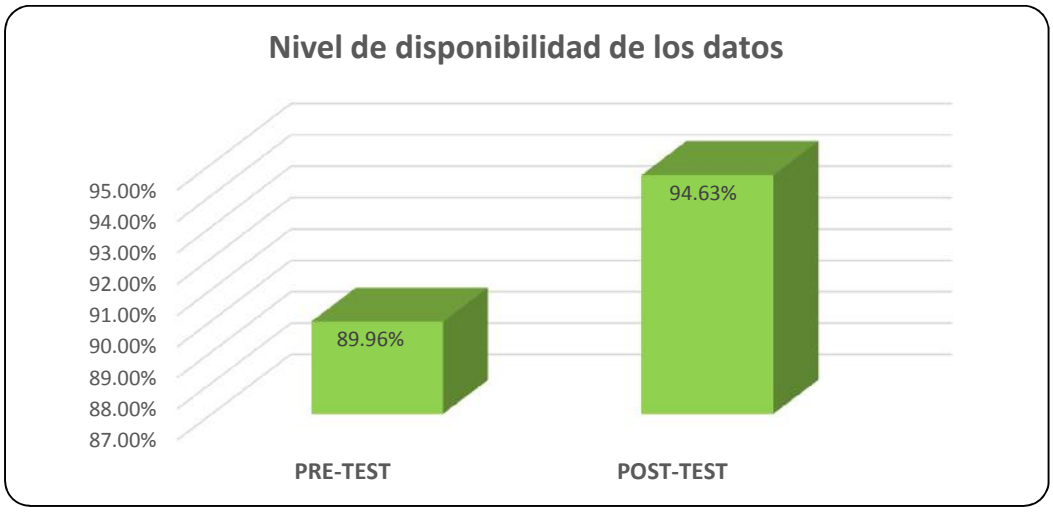


Figura 14. Nivel de disponibilidad de los datos en pre-test y post-test

Asimismo, se puede apreciar en la figura 14, que en el pre-test de las muestras se obtuvo una media de 89.96%, mientras que en el post-test fue de 94.63%, esto indica una diferencia significativa entre el antes y el después de la implementación del servidor Linux, evidenciando así una

mejora del indicador nivel de disponibilidad de los datos al haber un aumento de sus valores.

3.2.2. Análisis inferencial

3.2.2.1. Determinación de la prueba T-Student

Debido a que el presente estudio es de tipo *longitudinal*, es decir, que en un mismo grupo se aplican 2 medidas en momentos diferentes de tiempo, en este caso se tiene la variable aleatoria o dependiente *"Mejora de la seguridad perimetral de la red local de Junefield Group S.A."*, que será la variable de comparación, el cual ha sido objeto de estudio a través de las fichas de observación que se les entregó a las 11 personas que forman parte de la muestra; de las cuales se obtuvieron datos numéricos, por lo que se puede determinar que para el análisis de los datos con el programa estadístico SPSS v.25.0.0 se ha realizado la prueba *T – Student* para muestras relacionadas.

3.2.2.2. Normalidad

Debido a que la muestra es de 11 personas, la prueba de normalidad para comprobar si los resultados son normales será la de Shapiro-Wilk (n<30). Dicha prueba se realizó introduciendo los datos de cada indicador en el software estadístico SPSS 25.0.0, bajo las siguientes condiciones:

Si:

p-valor > 0.05 adopta una distribución normal

p-valor ≤ 0.05 adopta una distribución no normal.

3.2.2.3. Validación de hipótesis: Confidencialidad

Hi: La implementación de un servidor Linux influye significativamente en la confidencialidad de la red local de la empresa Junefield Group S. A.

Ho: La implementación de un servidor Linux no influye significativamente en la confidencialidad de la red local de la empresa Junefield Group S. A.

Para analizar la confidencialidad de la red local se ha evaluado los indicadores “Nivel de políticas de seguridad” y “Nivel de confidencialidad de los datos”.

Primero, se analizó el indicador “Nivel de políticas de los datos”, donde se obtuvo lo siguiente:

Tabla 16. Pruebas de normalidad – Nivel de políticas de seguridad

	Shapiro-Wilk		
	Estadístico	**gl**	**Sig.**
Nivel de políticas de seguridad – Pre_test	,892	11	,146
Nivel de políticas de seguridad - Post_test	,943	11	,551

Donde: Sig. = p-valor

Se muestra en la tabla 16 “Pruebas de normalidad – Nivel de políticas de seguridad” los valores, tanto en pre-test como en post-test, presentan un nivel de significancia mayor a 0.05, por lo tanto, se afirma que los datos provienen de una distribución normal. Por lo que se corrobora que se cumple con el supuesto de que la dimensión *confidencialidad* en su indicador *nivel de políticas de seguridad* se comporta normalmente y es posible continuar con el procedimiento.

Luego se realiza la prueba de muestras relacionadas, prueba t-student, cuyos resultados se muestran a continuación:

Tabla 17. Prueba de muestras relacionadas – Nivel de políticas de seguridad

	Media	Prueba t Student		
		t	gl	Sig. (bilateral)
Nivel de políticas de seguridad – Pre_test / Nivel de políticas de seguridad – Post_test	-58,18091	-32,659	10	,000

Al ejecutar la prueba de t-Student para muestras relacionadas se observa la tabla 17, “Prueba de muestras relacionadas – Nivel de políticas de seguridad”, en la cual se obtuvo una significancia de 0.000, ya que el valor de significancia es mucho menor que el valor alfa 0.05, se puede rechazar entonces la hipótesis nula y se acepta la hipótesis alterna, afirmando que:

“Hay una diferencia significativa en las medias del indicador nivel de políticas de seguridad de la dimensión *confidencialidad* antes y después de la implementación, por el cual se puede afirmar que la implementación del firewall Endian, influye considerablemente en el nivel de políticas de seguridad de la red local de la empresa Junefield Group S.A.”

Luego, analizaremos el indicador “Nivel de confidencialidad de los datos”, donde se obtuvo lo siguiente:

Tabla 18. Pruebas de normalidad – Nivel de confidencialidad de los datos

	Shapiro-Wilk		
	Estadístico	Gl	Sig.
Nivel de confidencialidad de los datos - Pre_test	,967	11	,856
Nivel de confidencialidad de los datos - Post_test	,895	11	,158

DónDonde: Sig. = p-valor

Se muestra en la tabla 18 “Pruebas de normalidad – Nivel de confidencialidad de los datos” los valores, tanto en pre-test como en post-test, presentan un nivel de significancia mayor a 0.05, por lo tanto, se afirma que los datos provienen de una distribución normal. Por lo que se corrobora que se cumple con el supuesto de que la dimensión *confidencialidad* en su indicador *nivel de confidencialidad de los datos* se comporta normalmente y es posible continuar con el procedimiento.

Luego se realiza la prueba de muestras relacionadas, prueba t-student, cuyos resultados mostramos a continuación:

Tabla 19. Prueba de muestras relacionadas – Nivel de confidencialidad de los datos

	Media	**Prueba t Student**		
		t	**Gl**	**Sig. (bilateral)**
Nivel de confidencialidad de los datos – Pre_test / Nivel de confidencialidad de los datos – Post_test	-60,45455	-14,509	10	,000

Al ejecutar la prueba de t-Student para muestras relacionadas se observa la tabla 19, “Prueba de muestras relacionadas – Nivel de confidencialidad de los datos”, en la cual se obtuvo una significancia de 0.000, ya que el valor de significancia es mucho menor que el valor alfa 0.05, se puede rechazar entonces la hipótesis nula y se acepta la hipótesis alterna, afirmando que:

“Hay una diferencia significativa en las medias del indicador *nivel de confidencialidad de los datos* de la dimensión *confidencialidad* antes y después de la implementación, por el cual se puede afirmar que dicha implementación, si mejoró considerablemente el nivel de confidencialidad de los datos de la red local de la empresa Junefield Group S.A”.

Entonces, se concluye tanto descriptiva como estadísticamente que para la dimensión *confidencialidad* existe una mejora significativa.

Por lo tanto, se demuestra:

La Hipótesis Hi: La implementación de un servidor Linux influye significativamente en la confidencialidad de la red local de la empresa Junefield Group S. A.

3.2.2.4. Validación de hipótesis: Integridad

Hi: La implementación de un servidor Linux influye significativamente en la Integridad de la red local de la empresa Junefield Group S. A.

Ho: La implementación de un servidor Linux no influye significativamente en la Integridad de la red local de la empresa Junefield Group S. A.

Para analizar la integridad de la red local se ha evaluado los indicadores “Nivel de riesgo de los datos” y “Manipulación de datos”.

Primero, analizó el indicador “Nivel de riesgo de los datos”, donde se obtuvo lo siguiente:

Tabla 20. Pruebas de normalidad – Nivel de riesgo de los datos

	Shapiro-Wilk		
	Estadístico	**gl**	**Sig.**
Nivel de riesgo de los datos - Pre_test	,878	11	,097

Nivel de riesgo de los datos - Post_test	,887	11	,127

Donde: Sig. = p-valor

Se muestra en la tabla 20 “Pruebas de normalidad – Nivel de riesgo de los datos” los valores, tanto en pre-test como en post-test, presentan un nivel de significancia mayor a 0.05, por lo tanto, se afirma que los datos provienen de una distribución normal. Por lo que se corrobora que se cumple con el supuesto de que la dimensión *integridad* en su indicador *nivel de riesgo de los datos* se comporta normalmente y es posible continuar con el procedimiento.

Luego se realiza la prueba de muestras relacionadas, prueba t-student, cuyos resultados mostramos a continuación:

Tabla 21. Prueba de muestras relacionadas – Nivel de riesgo de los datos

	Media	**Prueba t Student**		
		t	**gl**	**Sig. (bilateral)**
Nivel de riesgo de los datos – Pre_test / Nivel de riesgo de los datos – Post_test	57,72727	28,178	10	,000

Al ejecutar la prueba de t-Student para muestras relacionadas se observa la tabla 21, “Prueba de muestras relacionadas – Nivel de riesgo de los datos”, en la cual se obtuvo una significancia de 0.000, ya que el valor de significancia es mucho menor al valor alfa 0.05, se puede rechazar entonces la hipótesis nula y se acepta la hipótesis alterna, afirmando que:

“Hay una diferencia significativa en las medias del indicador *nivel de riesgo de los datos* de la dimensión *integridad* antes y después de la implementación, por el cual se puede afirmar que la implementación del

firewall Endian, influye considerablemente el nivel de riesgo de los datos de la red local de la empresa Junefield Group S.A".

Luego, analizaremos el indicador "Manipulación de datos", donde se obtuvo lo siguiente:

Tabla 22. Pruebas de normalidad – Manipulación de datos

	Shapiro-Wilk		
	Estadístico	**gl**	**Sig.**
Manipulación de datos - Pre_test	,924	11	,357
Manipulación de datos - Post_test	,907	11	,222

Donde: Sig. = p-valor

Se muestra en la tabla 22 "Pruebas de normalidad – Manipulación de datos" los valores, tanto en pre-test como en post-test, presentan un nivel de significancia mayor a 0.05, por lo tanto, se afirma que los datos provienen de una distribución normal. Por lo que se corrobora que se cumple con el supuesto de que la dimensión *integridad* en su indicador *manipulación de datos* se comporta normalmente y es posible continuar con el procedimiento.

Luego se realiza la prueba de muestras relacionadas, prueba t-student, cuyos resultados mostramos a continuación:

Tabla 23. Prueba de muestras relacionadas – Manipulación de datos

	Media	**Prueba t Student**		
		t	**gl**	**Sig. (bilateral)**
Manipulación de datos - Pre_test / Manipulación de datos - Post_test	62,22727	15,283	10	,000

Al ejecutar la prueba de t-Student para muestras relacionadas se observa la tabla 23, "Prueba de muestras relacionadas – Manipulación de datos", en la cual se obtuvo una significancia de 0.000, ya que el valor de

significancia es mucho menor que el valor alfa 0.05, se puede rechazar entonces la hipótesis nula y se acepta la hipótesis alterna, afirmando que:

"Hay una diferencia significativa en las medias del indicador *manipulación de datos* de la dimensión *integridad* antes y después de la implementación, por el cual se puede afirmar que dicha implementación, si disminuyo considerablemente la manipulación de datos de la red local de la empresa Junefield Group S.A".

Entonces, se concluye tanto descriptiva como estadísticamente que para la dimensión integridad existe una mejora significativa.

Por lo tanto, se demuestra:

La Hipótesis Hi: La implementación de un servidor Linux influye significativamente en la integridad de la red local de la empresa Junefield Group S.A.

3.2.2.5. Validación de hipótesis: Disponibilidad

Hi: La implementación de un servidor Linux influye significativamente en la disponibilidad de la red local de la empresa Junefield Group S. A.

Ho: La implementación de un servidor Linux no influye significativamente en la disponibilidad de la red local de la empresa Junefield Group S. A.

Para analizar la disponibilidad de la red local se evalúa el indicador "Nivel de disponibilidad de los datos", donde se obtuvo lo siguiente:

Tabla 24. Pruebas de normalidad – Nivel de disponibilidad de los datos

	Shapiro-Wilk		
	Estadístico	**gl**	**Sig.**
Nivel de disponibilidad de los datos - Pre_test	,911	11	,253
Nivel de disponibilidad de los datos - Post_test	,884	11	,118

Donde: Sig. = p-valor

Se muestra en la tabla 24 “Pruebas de normalidad – Nivel de disponibilidad de los datos” los valores, tanto en pre-test como en post-test, presentan un nivel de significancia mayor a 0.05, por lo tanto, se afirma que los datos provienen de una distribución normal. Por lo que se corrobora que se cumple con el supuesto de que la dimensión *disponibilidad* en su indicador *nivel de disponibilidad de los datos* se comporta normalmente y es posible continuar con el procedimiento.

Luego se realiza la prueba de muestras relacionadas, prueba t-student, cuyos resultados mostramos a continuación:

Tabla 25. Prueba de muestras relacionadas – Nivel de disponibilidad de los datos

		Prueba T Student		
	Media	**t**	**Gl**	**Sig. (bilateral)**
Nivel de disponibilidad de los datos - Pre_test / Nivel de disponibilidad de los datos - Post_test	-4,66636	-5,380	10	,000

Al ejecutar la prueba de t-Student para muestras relacionadas se observa en la tabla 25 “Prueba de muestras relacionadas – Nivel de disponibilidad de los datos”, en la cual se obtuvo una significancia de 0.000, ya que el valor de significancia es mucho menor que el valor alfa 0.05, se puede rechazar entonces la hipótesis nula y se acepta la hipótesis alterna, afirmando que:

“Hay una diferencia significativa en las medias del indicador *nivel de disponibilidad de los datos* de la dimensión *disponibilidad* antes y después de la implementación, por el cual se puede afirmar que la implementación del firewall Endian, influye considerablemente el nivel de disponibilidad de los datos de la red local de la empresa Junefield Group S.A”.

Entonces, se concluye tanto descriptiva como estadísticamente que para la dimensión Disponibilidad existe una mejora significativa.

Por lo tanto, se demuestra:

La Hipótesis Hi: La implementación de un servidor Linux influye significativamente en la disponibilidad de la red local de la empresa Junefield Group S. A.

3.2.2.6. Conclusión de hipótesis

Se concluye, que al realizar la implementación de un servidor Linux, influye en la seguridad perimetral de la red local de la empresa Junefield Group S.A., pues satisface los requerimientos de confidencialidad, integridad y disponibilidad de los datos en la red local.

3.3. Desarrollo

Para el proceso de implementación del servidor Linux y determinar su influencia en la seguridad perimetral de la red local de la empresa Junefield Group S.A., se empleó la metodología Top Down, en la figura 15 se aprecia el ciclo de vida de redes PDIOO.

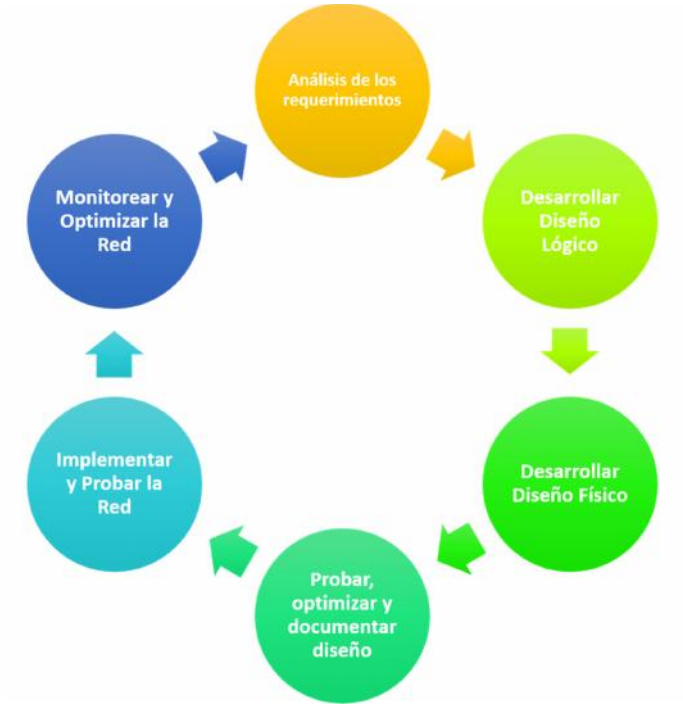


Figura 15. Diseño de redes Top – Down

Oppenheimer, Top-Down Network Design, 2010

Bravo al respecto sostiene que:

> Los diseños actuales de redes son muy complejos, tanto que el proceso para una actualización o modificación se vuelve más difícil. La solución a este problema es utilizar una metodología dinámica, sistemática, que permita a la red ser diseñada de manera descendente. Un buen diseño de red debe reconocer los requerimientos del cliente tales como las metas comerciales y metas técnicas (disponibilidad, escalabilidad, accesibilidad y seguridad). La metodología CISCO (TOP DOW) permite encontrar los requerimientos del cliente antes de diseñar la red. (2015, p. 19).

Teniendo como referencia lo sostenido por Bravo, se procedió a desarrollar la metodología que básicamente comprende cuatro fases principales.

3.3.1. Fase I: Análisis de negocio y objetivos

3.3.1.1. Análisis de negocio

La empresa Junefield Group S.A, es una empresa dedicada al rubro de la minería, fue fundada en Perú en mayo del 2008, después de varios años de actividad y desarrollo ya posee más de 700,000 hectáreas de petitorios mineros y proyectos adquiridos a nivel nacional, abarcando provincias como Arequipa, Apurímac, Moquegua, Tacna, La Libertad, Puno, entre otras. Actualmente se han establecidos bases en ciudades como Arequipa y Tacna para la ejecución de trabajos de perforación y extracción de minerales.

1) Datos Generales

- Razón social : Junefield Group S.A.
- RUC : 20330511401
- Rubro : Minería
- Dirección : Av. República de Panamá N° 3545, oficina 1301
- Distrito : San Isidro
- Provincia : Lima

2) Misión

Contribuir con el progreso local, nacional y global, así como con el éxito de los accionistas, a través de la transformación cuidadosa de recursos naturales.

3) Visión

Al 2025 ser reconocidos como una empresa minera de primer nivel, debido a la alta eficiencia y la calidad de su gestión.

4) Organigrama institucional

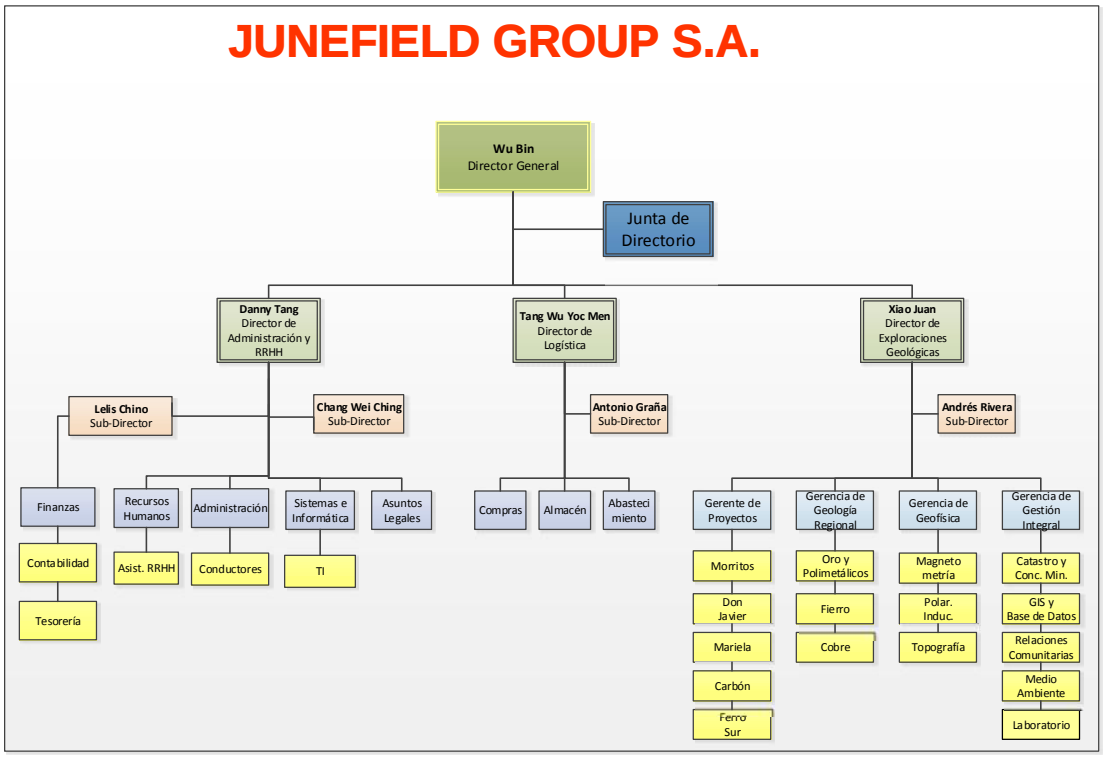


Figura 16. Organigrama institucional de la empresa Junefield Group SA

5) Identificación de problemas

En esta etapa se identificó las escasas medidas de seguridad y dificultades en la infraestructura de red de la empresa en mención, las cuales se detalla a continuación:

a) El departamento administrativo cuenta con dos infraestructuras de redes, cuyo cableado es UTP Cat.6, tanto para telefonía IP y datos. Así mismo ambos servicios van conectados a un solo switch de 48 puertos.
b) Las políticas de filtrado y contenido web no son las adecuadas, los usuarios pueden acceder a distintas páginas web, vulnerando las escasas medidas de seguridad.

c) En la red se ha detectado riesgo de la información, ya que existen carpetas visibles para cualquier usuario, el cual puede ocasionar alteración o pérdida de los datos.
d) Se ha observado que mucho de los equipos que almacena la información, no cuenta con claves complejas, siendo muy sencillo vulnerarlas.
e) No existe clasificación de la información según el nivel de criticidad para mantener la confidencialidad de los datos.
f) Toda la red de la empresa maneja un único segmento de clase C 192.168.0.0 /24, tanto para los usuarios de la empresa como para los invitados.

6) Planificación y requerimiento de negocio

De acuerdo a los alcances del proyecto para mejorar los procesos de negocio, se comenzaron a definir los principales requerimientos que son realmente lo que la Sub-Dirección de la empresa lo considera:

- Mejorar la infraestructura de la red actual.
- Implementar medidas de seguridad para resguardar la información (control de acceso, autentificación, filtrado web, etc.)
- Tener buena cobertura inalámbrica en la empresa.
- Garantizar la estabilidad del servicio de internet.
- Establecer segmentos distintos para la red de usuarios e invitados.
- Proporcionar tiempos de respuesta razonables entre clientes y servidor.
- Mantener la disponibilidad de la información cuando se requiera.

7) Metas técnicas

Se realizó una *"Ficha de observación"* de acuerdo a los procesos de negocio, permitiendo mayor entendimiento del proyecto y lograr el objetivo deseado, en la tabla 26 se aprecia las metas técnicas según prioridad a implementar.

Tabla 26. Metas técnicas del negocio

N°	Aspectos	Metas	Prioridad (1-100%)
01	Seguridad	Implementar niveles de políticas de filtrado y aplicaciones web para mejorar la seguridad.	20
		Complejidad de las contraseñas de los equipos que almacena información	15
02	Integridad	El acceso a la información, deber ser solo para el personal que lo requiere	15
		Disminuir el nivel de riesgo de los datos.	20
03	Disponibilidad	Dentro de la red local, la información debe ser disponible cuando se requiere	15
		Fuera de la red local, la información debe ser disponible entre sedes	15

3.3.1.2. Objetivos de negocio

Básicamente la solución se centraliza en la implementación de un servidor Linux y determinar la influencia de la seguridad perimetral de la red local de la empresa Junefield Group S.A., las cuales según la metodología top down debemos cumplir los siguientes aspectos:

- **Escalabilidad**

  Este aspecto es muy importante a la hora de diseñar una red, ya que de ello depende el crecimiento futuro e integración de nuevos equipos dentro de la red.

- **Disponibilidad**

  La red debe estar disponible según requerimiento de negocio, en este caso la red debe estar disponible las 8 horas del día, los 5 días de la semana. Las cuales se calculan según la fórmula que se muestra a continuación:

$$D = \frac{H \quad T \quad - H \quad p \quad p \quad m}{H \quad T \quad t}$$

En este caso para realizar el cálculo de disponibilidad, tomaremos los siguientes datos:

Horas laborables: 8 horas
Días laborables al mes: 22
Total de horas: 176
Horas de mantenimiento por mantenimiento: 4

Aplicando la fórmula:

$$Di = \frac{176 - 3}{176} x100$$

$$Di = 0.982\, x\, 100$$

$$D = 98.29\ \%$$

Con el resultado antes mostrado, se indica que el nivel de disponibilidad de la red será 98.29%, el cual es aceptable.

Por otro lado, es preciso mencionar que la disponibilidad se puede ver afectado por causas ajenas a lo planificado, como por ejemplo fallas en el equipo, mantenimientos no programados, etc.

- **Funcionalidad**

  La red proporcionará conectividad continua a todos los recursos que se encuentren dentro del diseño de red.

- **Adaptabilidad**

  La red debe se diseñará de tal forma que pueda ser adaptado ante cambios de nuevas tecnologías en el futuro.

3.3.1.3. Características de la red existente

Actualmente la empresa Junefield Group S.A., cuenta con un solo segmento de red, tanto para los usuarios de la empresa, servidores de datos y visitantes.

Este hecho fue preocupante para la gerencia de la empresa el cual solicitó realizar levantamiento de información sobre el estado actual de la red local para luego diseñar mejoras en la infraestructura de red, el cual garanticen la seguridad de los datos y la fluidez de las comunicaciones.

1) Estructura actual de la red LAN

Es por ello que el diseño de la red se basa en la estructura organizacional de la empresa, las cuales conforman las siguientes áreas:

- Área de administración
- Área de contabilidad
- Área legal
- Área de TI

En la tabla 27 se puede visualizar la distribución de los equipos de cómputo en las distintas áreas, así como las características de los mismos.

Tabla 27. Equipos de cómputo existentes por área

Área	Desktop	Marca	Laptop	Marca	Descripción

Administración	3	Compatible	1	Lenovo	Desktop: Core i5 2.4 Ghz, memoria de 4Gb, HDD 500 GB Laptop: Core i7 2.9 Ghz, memoria 8 Gb, HDD de 1TR
Contabilidad	4	Compatible			Desktop: Core i5 2.4 Ghz, memoria de 4Gb, HDD 500 GB
Legal	2	Compatible			Desktop: Core i5 2.4 Ghz, memoria de 4Gb, HDD 500 GB
Sistemas	2	Compatible			Desktop: Core i5 2.4 Ghz, memoria de 4Gb, HDD 500 GB

Por otro lado, en la tabla 28, se puede observar la distribución de los equipos de red existentes actualmente en la empresa.

Tabla 28. Equipos existentes en la red de la empresa

Descripción	Cantidad	Marca	Modelo	Áreas	Detalles
Servidor	2	IBM	X3550	Todas	Servidores de BD
Servidor	2	IBM	X3200	Todas	Servidores de aplicación
Switch	1	D-Link	DGS-1210	Todas	Switch de 48 puertos
Acces Point	1	TP-Link	TL-WA901	Todas	Wifi para usuarios e invitados
impresora	1	Konica Minolta	bizhub 363	Todas	Multifuncional de red
impresora	1	Epson	LX300	Contabilidad	Impresión de facturas

2) Software y aplicaciones

La empresa cuenta con dos aplicaciones que fueron desarrollados a medida, una para el área de administración y la otra para el área de contabilidad, las cuales trabajan bajo las plataformas Windows, mayor detalle se muestra en la tabla 29.

Tabla 29. Software y servicios utilizados en la red

Área	Software	Aplicaciones y servicios de red
Administración	Windows 10, Windows 7, Office 2016, antivirus Smart Security 10	Sistema de administración, sistema biométrico, carpetas compartidas, impresora de red
Contabilidad	Windows 10, Office 2016, antivirus Smart Security 10	Sistema contable consaf 2016, carpetas compartidas, impresora de red
Legal	Windows 10, Office 2016, antivirus Smart Security 10	Carpetas compartidas, impresora de red
Sistemas	Windows 10, Office 2016, antivirus Smart Security 10	Carpetas compartidas, impresora de red

3) Servicios contratados

Se levantó información respecto a los servicios contratados, tanto para el servicio de internet como para el de telefonía.

- Internet dedicado de 5 MB con overbooking 1:1
- Servicio de telefonía (RDSI) con 16 canales simultáneos.

4) Análisis de la red actual

Luego de conocer la estructura actual y la distribución de los equipos utilizados para el intercambio de la información, se pudo determinar lo siguiente:

- La red cuenta con una topología de estrella y es plana en su diseño.
- Cuenta con un solo segmento de red 192.168.0.0/24, tanto para los equipos de cómputo, servidores y wifi.
- Las características técnicas del Access point TP-Link modelo TL-WA901 son básicos.
- Los usuarios invitados pueden utilizar el wifi de la empresa, las cuales se encuentra en el mismo segmento que la red de servidores.
- La contraseña del wifi y de los equipos de cómputo, son fáciles de vulnerar.
- No existe políticas de seguridad para resguardar la información que esté acorde a los procesos de la organización.

En la figura 17, se muestra el diagrama de red actual, el segmento de red utilizado y la conexión entre sedes.

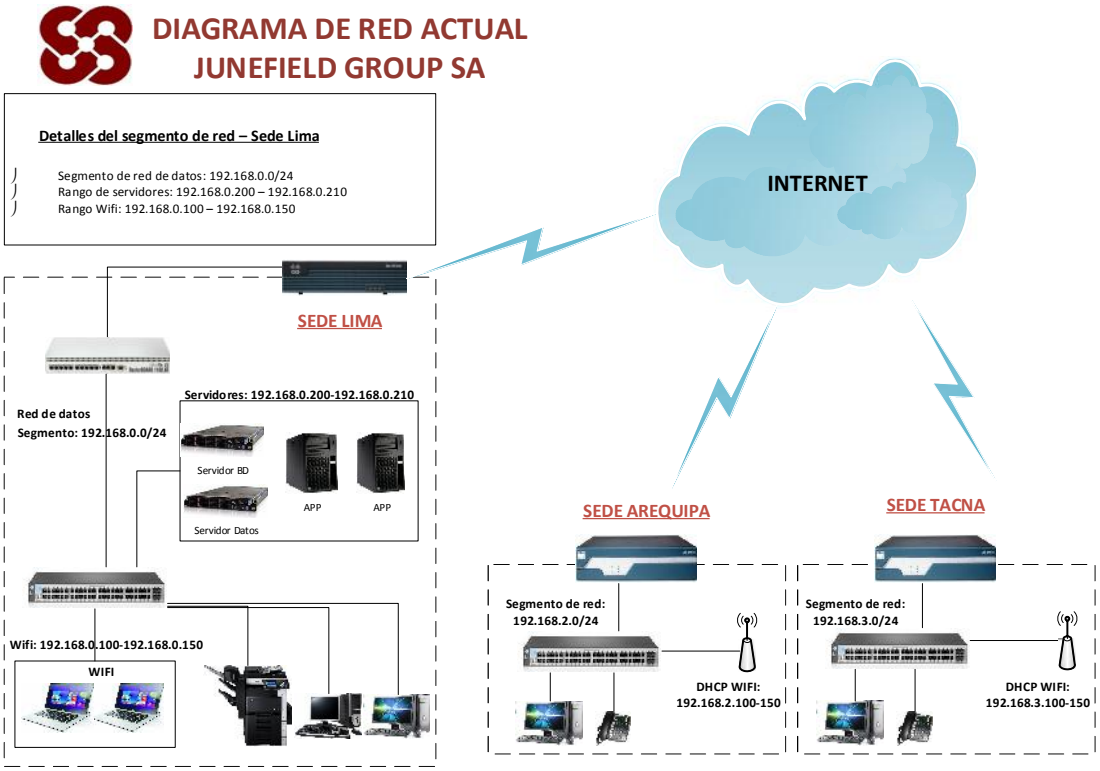


Figura 17. Diseño de red de la empresa Junefield Group S.A.

5) Identificación de responsabilidades

El propósito de este proyecto es mejorar la seguridad perimetral de la red local de la empresa Junefield Group S.A., para ese sentido es importante identificar las responsabilidades que debe cumplir las áreas involucradas, ver tabla 30.

Tabla 30. Identificación de responsabilidades

Responsable	Funciones	Roles
Personal de Sistemas e Informática	- Proponer plataformas tecnológicas para mitigar los riesgos de vulnerabilidad de la red local. - Velar por el buen funcionamiento de la red y los sistemas de información.	- Identificar la problemática actual respecto a la vulnerabilidad de la red. - Analizar requerimientos para la implementación de equipos de seguridad. - Diseñar plataformas tecnológicas para mejorar la seguridad perimetral de la red local. - Diseño lógico de la red, utilizando la metodología Top Down para su implementación. - Elaborar requerimientos para la implementación de los equipos a utilizar. - Realizar pruebas post implementación. - Generar reportes del consumo de ancho de banda por cada host. - Monitorear el funcionamiento de la red local. - Realizar correcciones de ser necesarios.
(Director de Administración)	- Autoriza estudios de factibilidad del área de TI.	- Evalúa proyecto a implementar. - Autoriza la implementación del proyecto.
(Sub director de Finanzas)	- Autorizar pagos para la implementación.	- Recepción requerimientos del proyecto. - Analiza montos a desembolsar. - Realiza pagos para la implementación.

6) Controles para reducir el riesgo

Teniendo en cuenta lo antes mencionado, se determina los objetivos trazados por la gerencia de la empresa, en la tabla 31 se detallan los cambios que el proyecto generará según el nivel de prioridad que tendrá que cumplir el diseño de red para garantizar la seguridad de la información.

Tabla 31. Controles de seguridad

Objetivos del proyecto		
N°	**Descripción**	**Prioridad (1– 100%)**
01	Mejorar las políticas de seguridad para el filtrado de aplicaciones y páginas web, autentificación	30
02	Segmentar la red de datos, servidores y Wifi	20
03	Garantizar la confidencialidad de los datos	30
04	Garantizar la continuidad del servicio	20

3.3.2. Fase II: Diseño lógico de la red

En esta segunda fase, se ha empleado técnicas para desarrollar el diseño de una topología lógica para luego plasmar el diseño en la construcción de la red física.

En la figura 18, se muestra la estructura del diseño lógico propuesto, las cuales tiene una serie de cambios a comparación del diagrama inicial, con dicha implementación se ha logrado mejorar la seguridad perimetral de la red local.

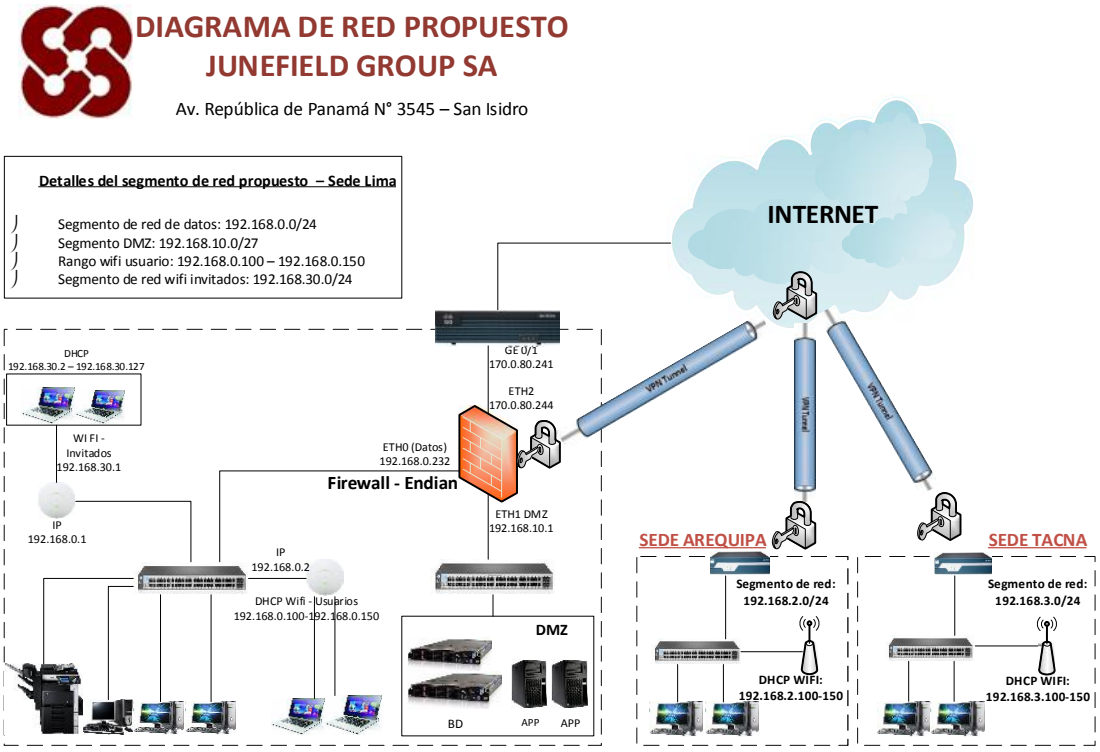


Figura 18. Diseño lógico de la red

3.3.2.1. Direccionamiento de la red y nombres

En esta etapa se definió el segmento que se asignó a los servidores (DMZ), datos, y la red de invitados, se recomendó segmentar la red para mejorar el desempeño y seguridad de la infraestructura y los servicios de red.

Como se aprecia en la figura 19, a la interfaz de la red LAN se le denominó red verde, asimismo la interfaz asignada para la DMZ se le denominó red naranja y por último a la interfaz WAN se le denominó red roja.

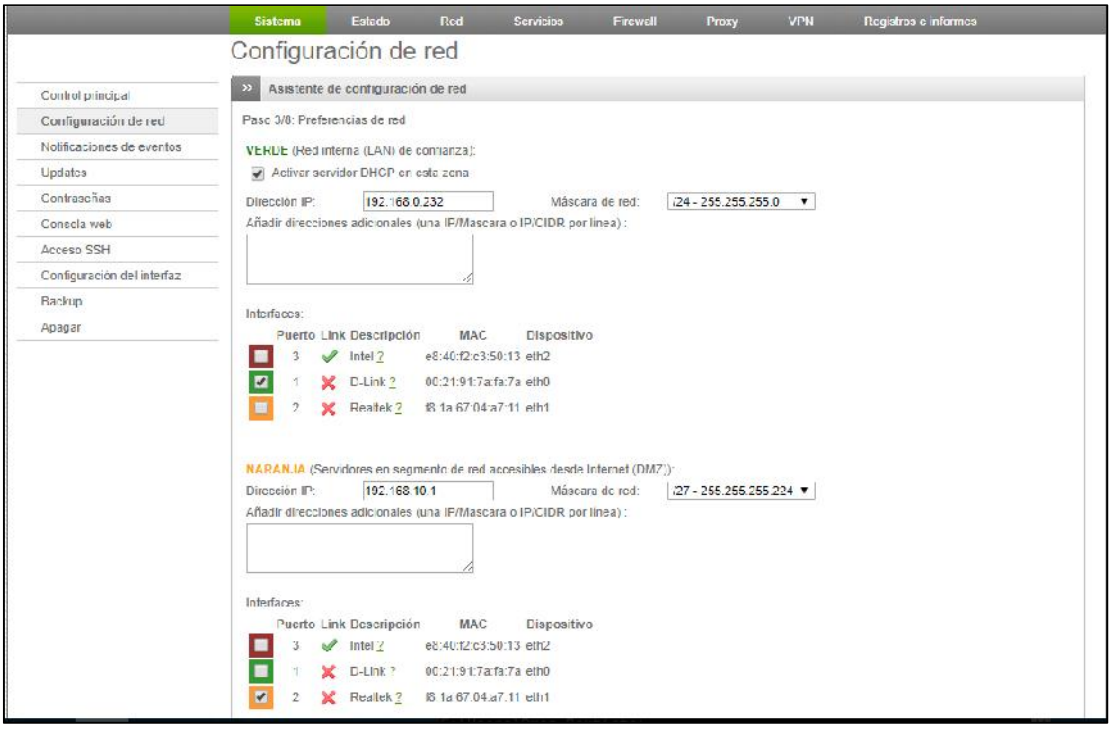


Figura 19. Asignación de IP´s por interfaz

El segmento Wifi de invitados no está considerado en la configuración del firewall, se utilizó un AP marca Ubiquiti modelo UNIFI UAP-LR, para crear otra sub red que sea independiente a las redes que propaga el firewall, en la tabla 32 se aprecia el segmento de red que se utilizó para brindar dicho servicio.

Tabla 32. Segmento WIFI para invitados

Segmento WI Fi Invitados 192.168.1.0/25					
Equipo	**Interfaz**	**Gateway**	**M. de Sub red**	**DNS**	**DHCP**
UNIFI	GE	192.168.30.1	255.255.255.0	190.107.183.2 190.107.182.2	192.168.30.2 192.168.30.127

3.3.2.2. Direccionamiento de red

El direccionamiento de red ayuda a identificar las rutas por donde cada segmento dirige el tráfico de cada host de acuerdo al servicio que desea alcanzar, ver tabla 33, para realizar dicha acción se especificó la

interfaz y el segmento que utilizó cada dispositivo que se encuentre conectado a la red mediante una dirección IP, ésta se utilizó para identificar tanto a un ordenador en particular como a la red a la que pertenece de manera que sea posible distinguir a los dispositivos que se encuentran en los distintos segmentos con la finalidad de intercambiar los servicios que se propaga a través de la red LAN.

Tabla 33. Direccionamiento de la red

Interfaz	Equipo	Dirección IP	M. de Sub red	Conectado al dispositivo	Conectado a la interfaz
ETH02 WAN	Firewall	170.0.80.244	255.255.255.248	Router Cisco	GE 0/1
ETH1 DMZ	Firewall	192.168.10.1	255.255.255.224	Switch D-Link DMZ	GE 0/1
ETH0 LAN	Firewall	192.168.0.232	255.255.255.0	Switch D-Link datos	GE 0/1

3.3.2.3. Protocolos de comunicación

Actualmente no se utiliza protocolos de conmutación debido a que en la infraestructura de la red actual no lo requiere. Sin embargo, de acuerdo al crecimiento de la empresa, se propone implementar a futuro el protocolo STP (Spanning Tree Protocol), que servirá para mejorar la disponibilidad de la red mediante rutas alternas. Esto quiere decir que cuando se pierda conexión con un switch, otro enlace deberá reemplazarlo rápidamente, de esa manera la interrupción de una sola ruta no genera impacto en la conectividad de los dispositivos de la red.

En la tabla 34 detallaremos el enrutamiento que utilizará cada segmento de red de acuerdo a los servicios que desea alcanzar.

Tabla 34. Enrutamiento

Interfaz Entrada	IP Origen	Interfaz Salida	IP Destino	Servicios	Acción
DMZ (ETH1)	RED DMZ	WAN (ETH2)	ALL	ALL	Denegar
WAN (ETH2)	190.234.250. 161	DMZ (ETH1)	RED DMZ	TCP - UDP	Aceptar
LAN (ETH0)	Red Datos	WAN (ETH2)	ALL	ALL	Aceptar
LAN (ETH0)	Red Datos	DMZ (ETH1)	192.168.10.0/24	ALL	Aceptar
DMZ (ETH1)	DMZ	LAN (ETH0)	ALL	ALL	Denegar

Según tabla 35, para poder publicar un servicio específico ubicado en un host de la red LAN a través de internet, se debe realizar un direccionamiento de puertos (port forwarding) el cual reenvía los datos de un extremo a otro, pasando por un puerto y protocolo específico por medidas de seguridad, dicha acción se denomina DNAT.

Tabla 35. Destination Network Address Translation (DNAT)

Nombres	Interface	IP Pública	IP Privada	Protocolo	Puerto
Servidor SQL	ETH0	170.0.80.244	192.168.10.2	TCP	1433
Escritorio Remoto (Servidor BD)	ETH0	170.0.80.244	192.168.10.2	TCP	9558
Intranet (Servidor Aplicaciones)	ETH0	170.0.80.244	192.168.10.3	TCP	80
Escritorio Remoto (Servidor Aplicaciones)	ETH0	170.0.80.244	192.168.10.3	TCP	9559
Polycom Conferencia	ETH0	170.0.80.244	192.168.0.25 0	TCP-UDP	5070

3.3.2.4. Estrategia de seguridad

La seguridad es un aspecto fundamental cuando se diseña una infraestructura de red por más sencilla que sea, es preciso un planeamiento, no sólo requiere recursos tecnológicos, se deben tomar en cuenta también procesos de entrenamiento y recursos humanos especializados, este objetivo es complicado de alcanzar por los constantes cambios. Las instituciones o empresas deben considerar la planeación de la seguridad, revisar sus prácticas, aprender del entorno y desarrollar planes para mejorarlas de esa manera garantizar la confiabilidad, seguridad e integridad de los datos.

Según la realidad problemática de la empresa, la implementación de un equipo Firewall será la solución para mejorar la seguridad perimetral de la red local, el cual, según requerimiento por la alta gerencia, debe cumplir con las siguientes exigencias:

1) Implementación de control de acceso (ACL)

Se ha implementado listas de acceso para permitir el ingreso de ciertas direcciones IP's públicas a equipos que se encuentren dentro de la red local, ver figura 20, de esa manera se pretende minimizar los ataques hacia la red local.

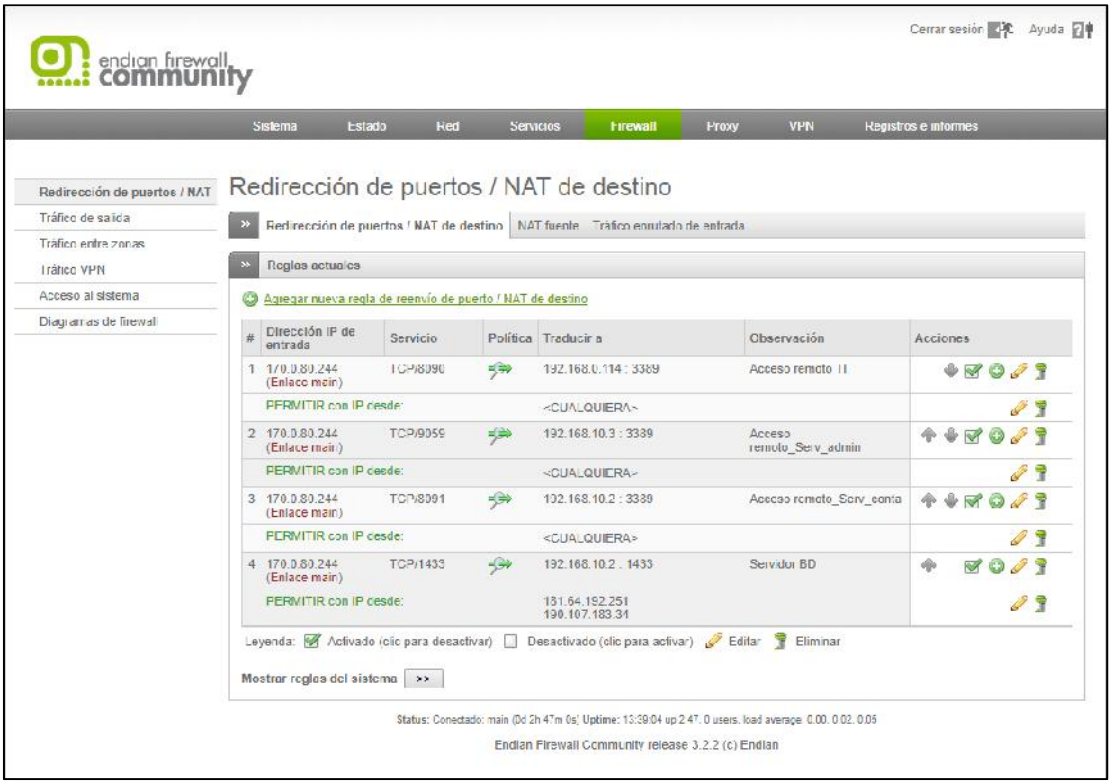


Figura 20. Redirección de puertos / tráfico de entrada

Asimismo, se observa en la figura 21, la configuración que tendrá los hosts de la red interna que deseen navegar por internet, las cuales se ha priorizado de acuerdo al grado jerárquico de cada usuario de la empresa.

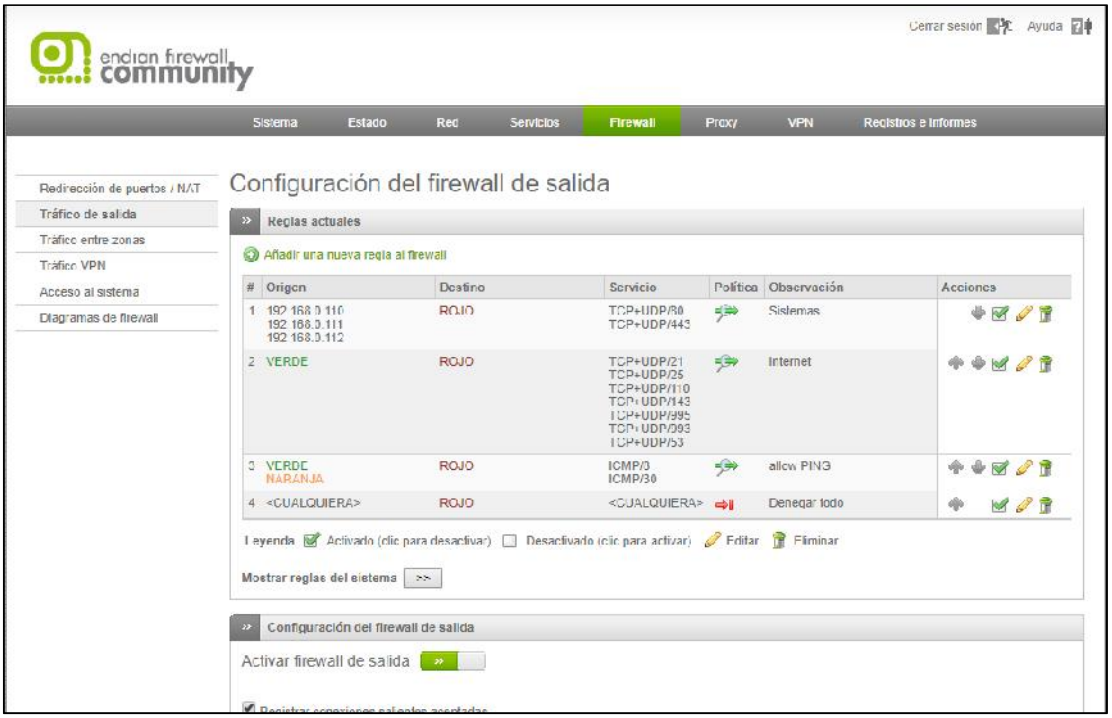


Figura 21. Configuración firewall de salida

De igual manera se observa en la figura 22, que se ha restringido el tráfico entre zonas, eso quiere decir que todos los usuarios de la red interna (red verde) tienen accesos totales entre sí, luego se observa que la red interna (red verde) también tiene acceso a la red DMZ (red naranja), sin embargo la red DMZ no tiene acceso a la red interna (red verde), dicha configuración se ha realizado para mantener la integridad de los datos que se almacena en los servidores.

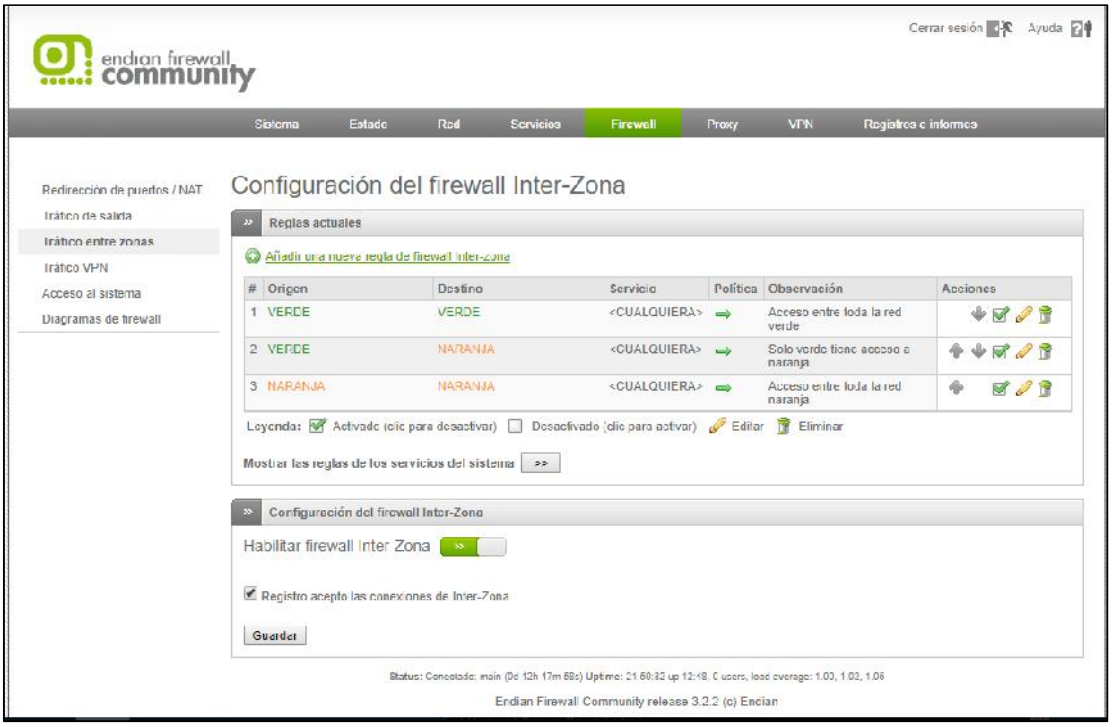


Figura 22. Configuración firewall entre zonas

2) Proxy HTTP

En la configuración del proxy HTTP, se ha considerado ciertos parámetros que ha permitido al firewall ser aún más restrictivo, en la figura 23 se aprecia que el servidor proxy ha trabajado en modo no transparente, eso quiere decir que cada host de la red interna está apuntando a la dirección IP del firewall para poder navegar por internet, también se limitó el ancho de banda de carga y descarga de archivos a 50MB, eso quiere decir, que ningún usuario podrá enviar o descargar archivos superiores a lo mencionado.

Figura 23. Configuración proxy HTTP

3) Filtrado Web (URL)

El filtrado web que se ha implementado está de acuerdo a las funciones laborales de cada área, las cuales se detallan a continuación:

- La gerencia tendrá acceso a la gran mayoría de páginas web, solo estarán bloqueadas las categorías de pornografía, web proxys, malware, robo de identidad.
- El área de sistemas tendrá acceso a la gran mayoría, solo estarán bloqueadas las categorías de pornografía, drogas.
- El área contable solo tendrá acceso a páginas de los bancos, gubernamentales, cuentas de correo y a otras páginas afines a sus funciones.
- El área de administración solo tendrá acceso a páginas de bancos, gubernamentales, correo, compras y a otras páginas afines a sus funciones.

- El área legal solo tendrá acceso a páginas gubernamentales, cuentas de correo, y a otras páginas afines a sus funciones.

En la figura 24, se observa un ejemplo del filtrado web realizada al área de administración bloqueando la mayor parte de categorías.

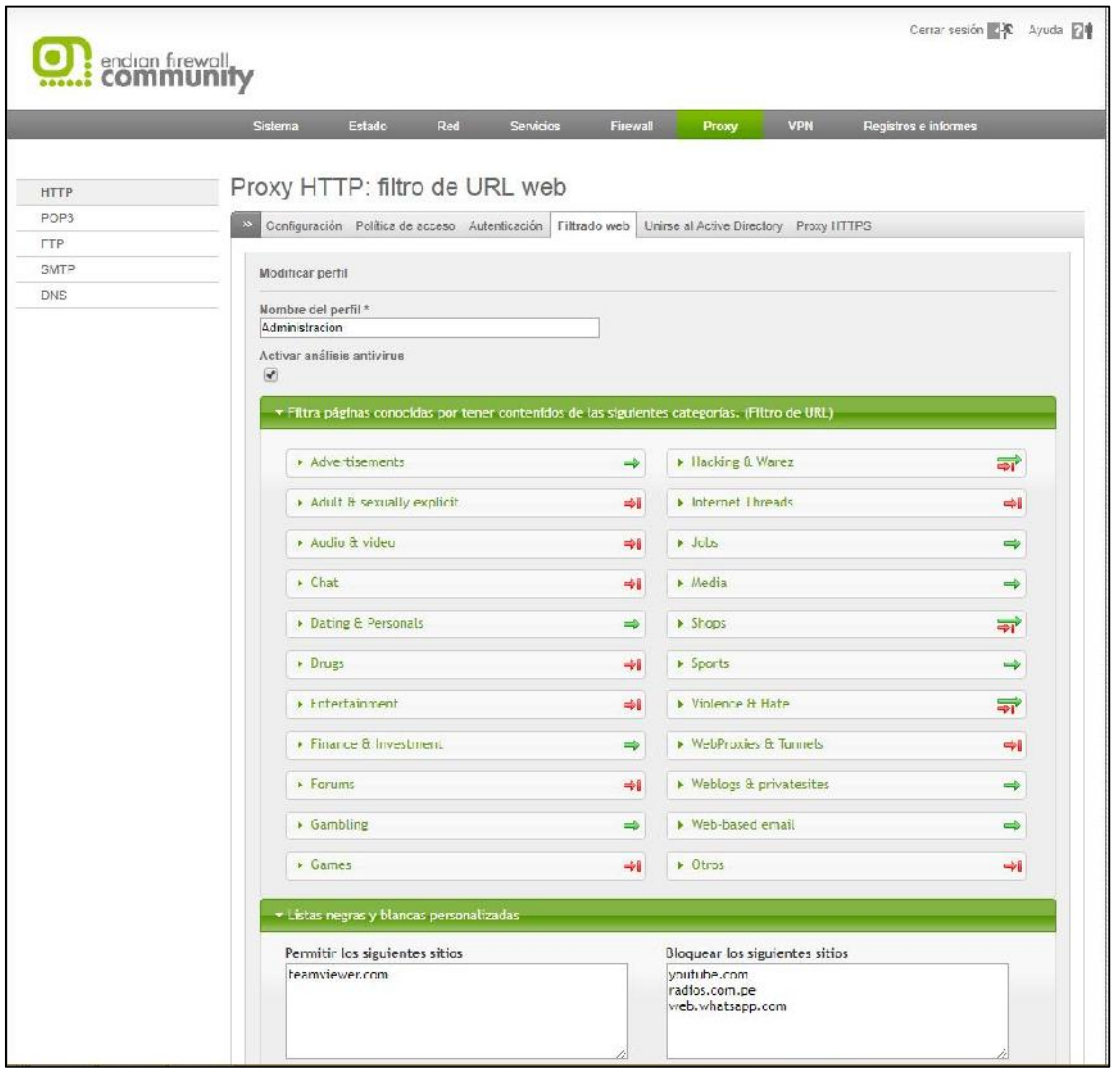


Figura 24. Filtrado web (URL)

4) Autentificación de usuarios

Se han creado políticas de autenticación por cada usuario y se han agrupado por área, el tipo de autentificación a utilizar será del firewall

(NCSA), la autentificación está relacionada al filtrado web, eso quiere decir que cada usuario según su autentificación está autorizado para navegar por internet. Cada autentificación está asociada solo a una dirección IP, si por alguna razón el usuario olvida sus credenciales no podrá acceder a los servicios de internet.

En la figura 25, se aprecia la relación de usuarios y al grupo al que pertenecen.

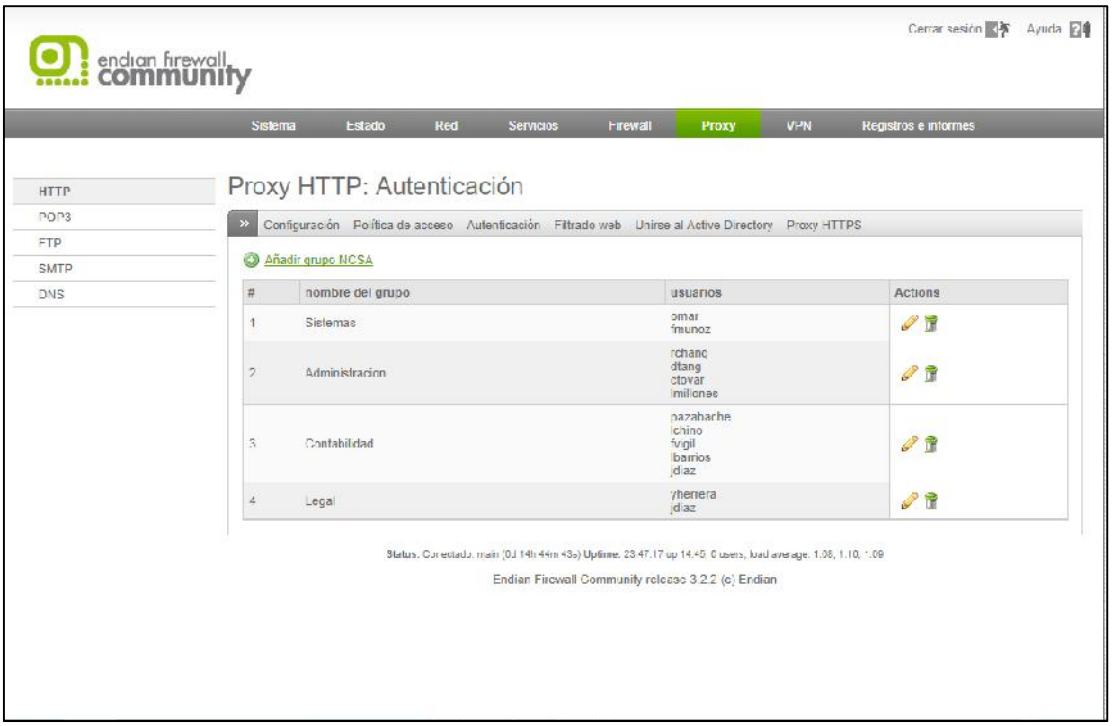


Figura 25. Autentificación de usuarios

5) Políticas de acceso

En las políticas de acceso, se han creado perfiles de navegación por cada área funcional, los accesos y limitaciones para acceder a distintas páginas web son de acuerdo a las funciones de cada usuario, por otro lado se han creado un perfil de navegación libre considerando para ello las horas no laborables, es quiere decir que todos los usuarios podrán acceder fuera del horario de oficina (horario de almuerzo, horario después de las 18

horas, sábados y domingos todo el día) a páginas como Youtube, Facebook, etc., considerando siempre el bloqueo a páginas pornográficas, paginas P2P entre otras, ver figura 26.

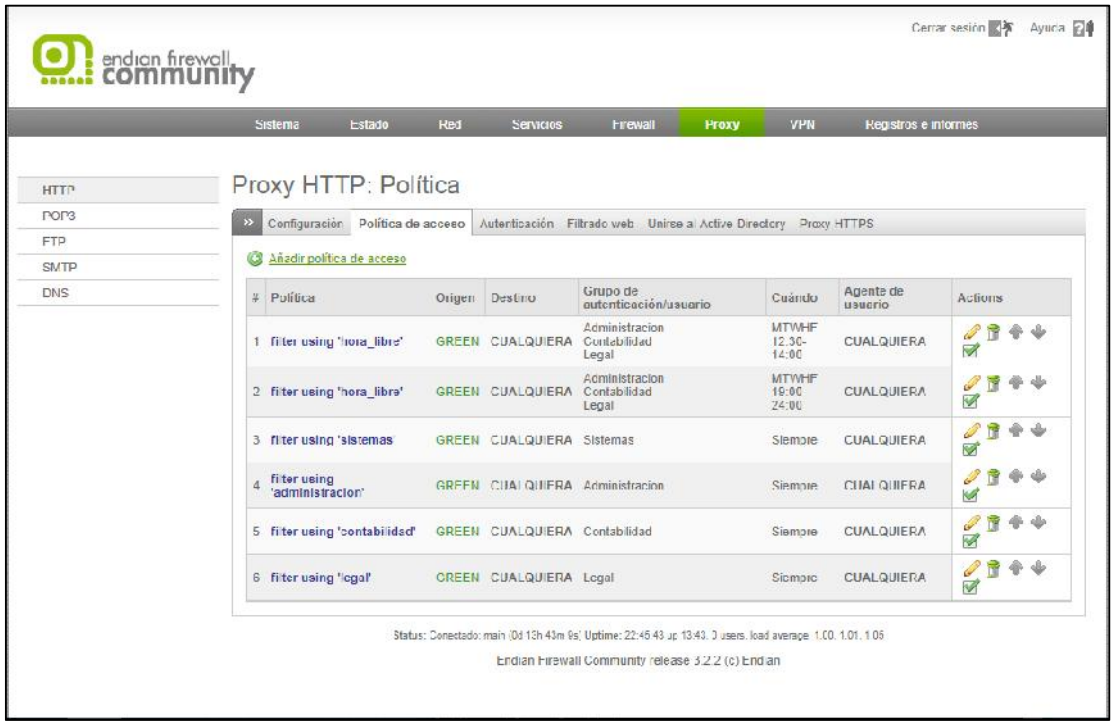


Figura 26. Políticas de acceso

3.3.3. Fase III: Diseño físico de la red

Luego de conocer las debilidades de la red local y el consumo actual de ancho de banda del servicio de Internet, se propuso un diseño de red que cubra las necesidades de la empresa garantizando siempre la estabilidad y seguridad. Para tal efecto se considera utilizar la topología estrella, como primera instancia se procedió a segmentar la red actual, se creó el segmento 192.168.0.0/24 para la red de datos, el segmento 192.168.10.0/27 para la red de servidores, y el segmento 192.168.30.0/24 para la red wifi de invitados.

Otro de los motivos para el nuevo diseño de la red será minimizar el riesgo de vulnerabilidad, implementando un servidor firewall cuyas políticas de filtrado web y direccionamiento de rutas sea la más eficiente para un buen desempeño de la red y sobre todo que garantice la confiabilidad de los datos que se transmiten a través de ella.

3.3.3.1. Tecnología a utilizar

Las tecnologías utilizadas para la implementación del servidor LINUX en el diseño de red cableado será Ethernet IEEE 802.3 y para el diseño de red inalámbrica será la IEEE 802.11, ambas tecnologías han ayudado a proponer una red robusta y estable. La tecnología Ethernet es pasiva esto significa que no requiere una fuente de alimentación propia, por lo tanto no falla a menos que el cable se corte físicamente o su terminación sea incorrecta. El método de acceso que utiliza Ethernet es el CSMA/CD, que agrupa un conjunto de reglas que determina el modo de respuesta cuando dos dispositivos conectados a una misma red intentan enviar datos simultáneamente.

3.3.3.2. Acceso remeto

Se estableció acceso remoto a ciertos host y servidores que se encuentran dentro de la red interna, todo tráfico entrante ha sido supervisado por el servidor Endian, solo se dejó pasar tráfico a través de los puertos establecidos (ver figura 27).

Figura 27. Puertos de acceso remoto

3.3.3.3. Red privada virtual (VPN)

Se ha implementado el servido VPN para los usuarios que deseen alcanzar ciertos servicios que se encuentran dentro de la red local de la empresa Junefield Group S.A., el objetivo de dicha implementación es mejorar los accesos hacia los sistemas de información, así como a los datos mediante el método de autentificación de dos factores que cuenta el servidor Endian, ver figura 28.

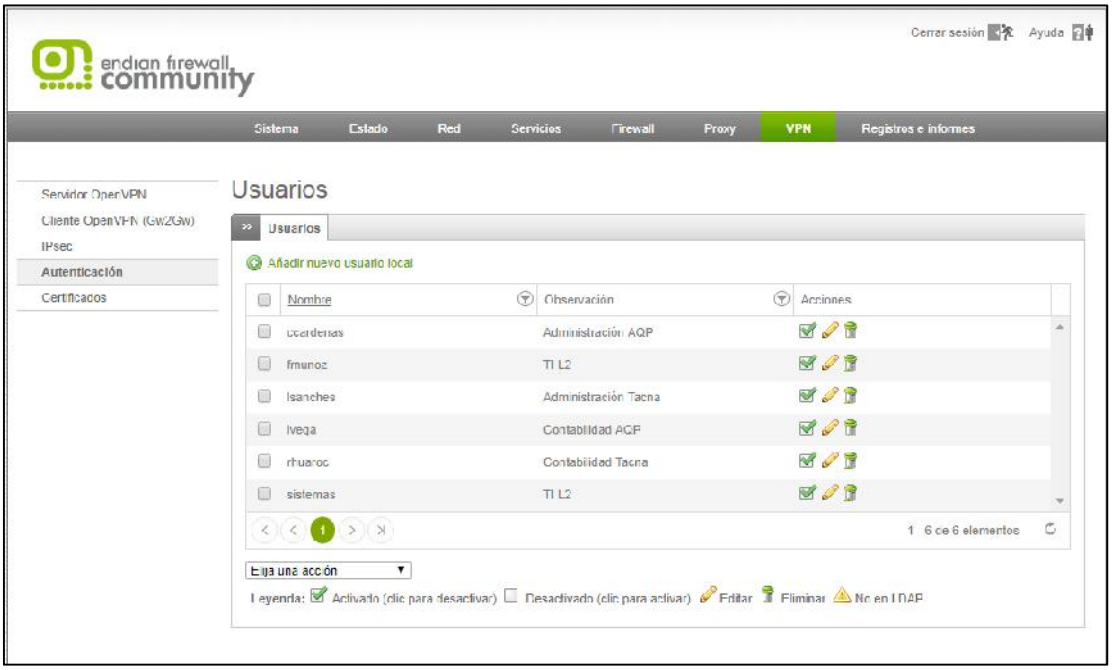


Figura 28. Usuarios VPN

3.3.3.4. Cableado a utilizar

Los tipos de red Ethernet que se han empledo para mejorar la infraestructura de red de la empresa Junefield Group S.A., será Giga Ethernet (1000Base-TX/100BASE-TX/10Base-T), debido a su compatibilidad con los dispositivos que cuenta actualmente la empresa. Por otro lado, Ethernet permite una plataforma bien equilibrada entre la velocidad y confiabilidad, estos puntos sumados a la adaptabilidad de soportar virtualmente todos los protocolos de red existentes en la actualidad hacen a Ethernet la tecnología ideal para diseñar e implementar infraestructuras de red LAN.

3.3.3.5. Equipos a utilizar

Luego de conocer el tipo de tecnología, se comenzó a enumerar los distintos dispositivos que se han utilizado para el diseño de la red, las cuales se detallan en la tabla 36.

Tabla 36. Dispositivos para la red de la empresa

Ítem	Dispositivos	Cantidad
01	Servidor IBM X3200 M3	01
02	HDD 146 GB SAS 15000 RPM	02
03	Tarjeta de red 10/100/1000 D-Link	02
04	Swich D-Link 48 Puertos GB	01
05	Ubiquiti Unifi UAP – LR	01
06	UPS APC 1400 VA – 220V	01
	Total	08

Así mismo se realizó el presupuesto de los dispositivos a emplear en la implementación del servidor Endian para la mejora de la seguridad perimetral de la red local de la empresa Junefield Group S.A. como se aprecia en la tabla 37.

Tabla 37. Presupuesto de los dispositivos para la red de la empresa

Dispositivos				
Item	**Descripción**	**Cantidad**	**P. Unitario**	**P. Total**
01	Servidor IBM X3200 M3	01	S/. 1,980.00	S/. 1,980.00
02	HDD 146 GB SAS 15000 RPM	02	S/. 420.00	S/. 840.00
03	Tarjeta de red 10/100/1000 D-Link	02	S/. 70.00	S/. 140.00
04	Swich D-Link 48 Puertos GB	01	S/. 1,520.00	S/. 1,520.00
05	Ubiquiti Unifi UAP – LR	01	S/. 350.00	S/. 350.00
06	UPS APC 1400 VA – 220V	01	S/. 1,730.00	S/. 1,730.00
			SUB TOTAL	S/. 6,560.00
			IGV 18 %	S/. 1,180.00
			TOTAL	S/. 7,740.80

3.3.4. Fase IV: Prueba, optimización y documentación

3.3.4.1. Pruebas del diseño de red

En esta etapa se pretende probar las distintas características establecidas en el servidor Endian, en la figura 29, se observa el dashboard del sistema, mostrando un resumen de la configuración de las interfaces de red (red verde, red naranja, red roja), la versión del firewall, las actualizaciones de firmas (clamav antivirus, firmas IPS, URL filter balcklist) y por último los servicios que se encuentran activos, detección de intrusos, proxy HTTP, proxy POP3. En este caso la opción proxy SMTP no está activo, debido a que el servidor de correo se encuentra en la nube.

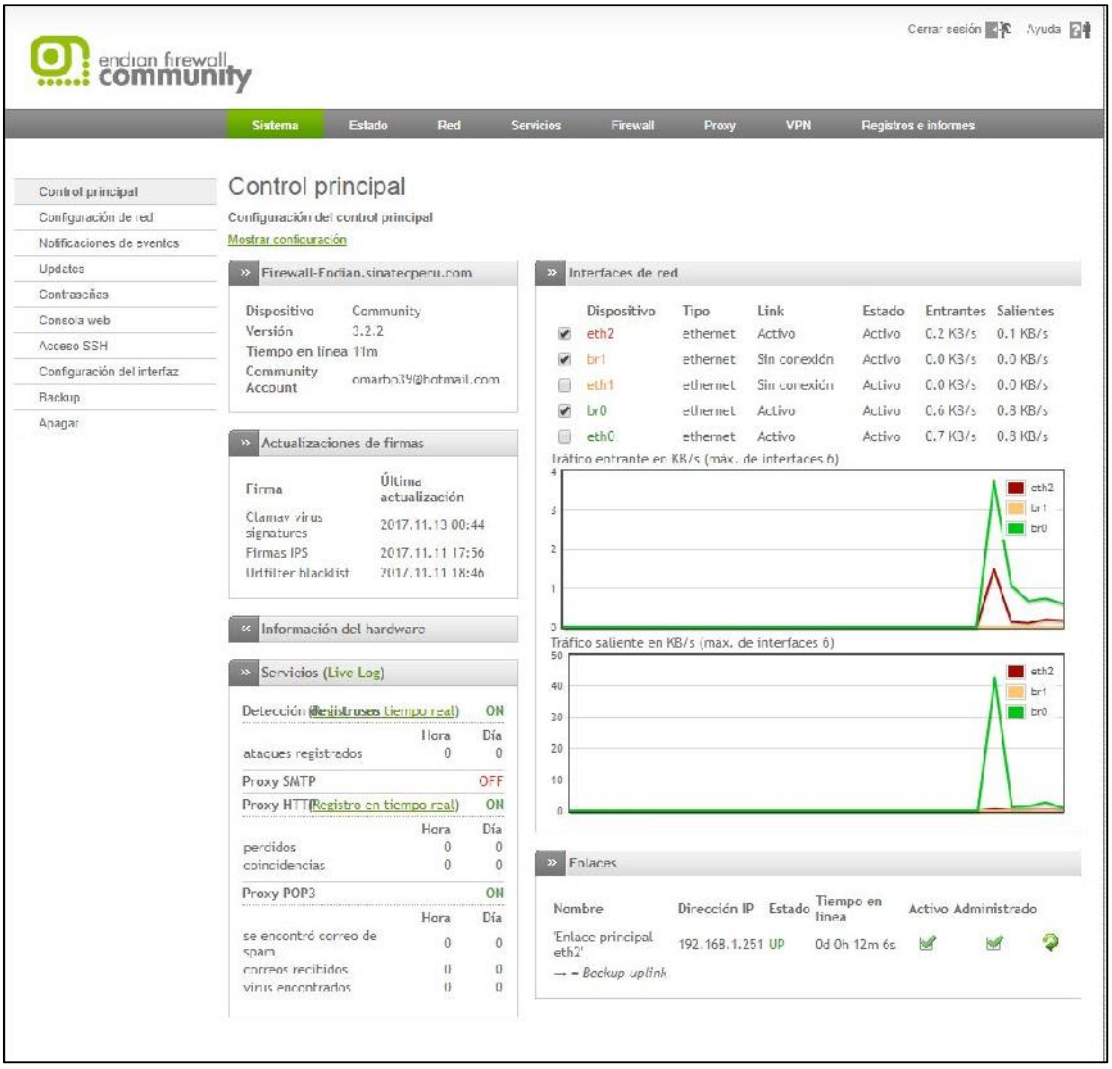


Figura 29. Dashboard del servidor Endian

En este sentido, se detalla las distintas pruebas que se realizó al servidor Endian, para corroborar la efectividad de sus procesos y si realmente cumple con el propósito deseado, que es la de preservar la seguridad perimetral de la red local, descritas en la etapa de diseño, para ello realizaremos las siguientes pruebas:

1) Autentificación de usuarios

Cada usuario cuenta con credenciales de autentificación único para comenzar a utilizar el servicio de internet, eso quiere decir que la primera

vez que el usuario abra el navegador, el servidor Endian automáticamente solicita las credenciales de acceso para permitir el uso del servicio (ver figura 30).

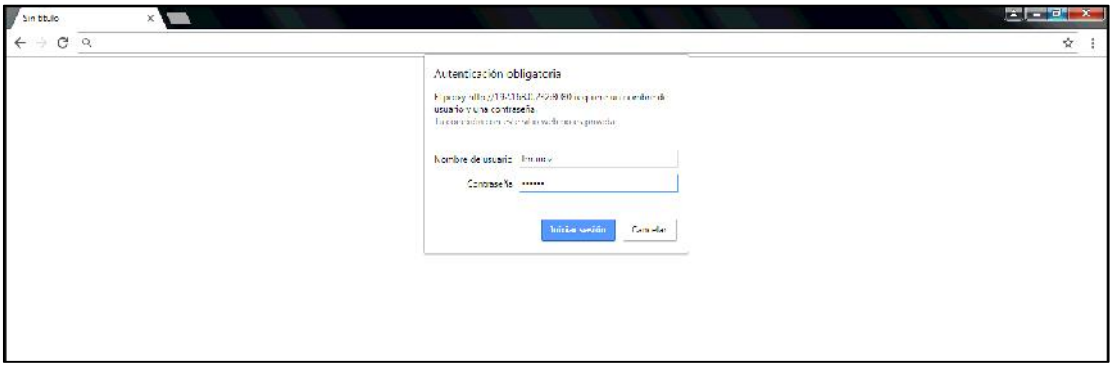


Figura 30. Autentificación de usuario válida

Según la figura 31, el usuario podrá navegar por internet siempre y cuando el servidor Endian valide las credenciales, por otro lado el usuario puede grabar las credenciales para que en el futuro no vuelva a ingresarla.

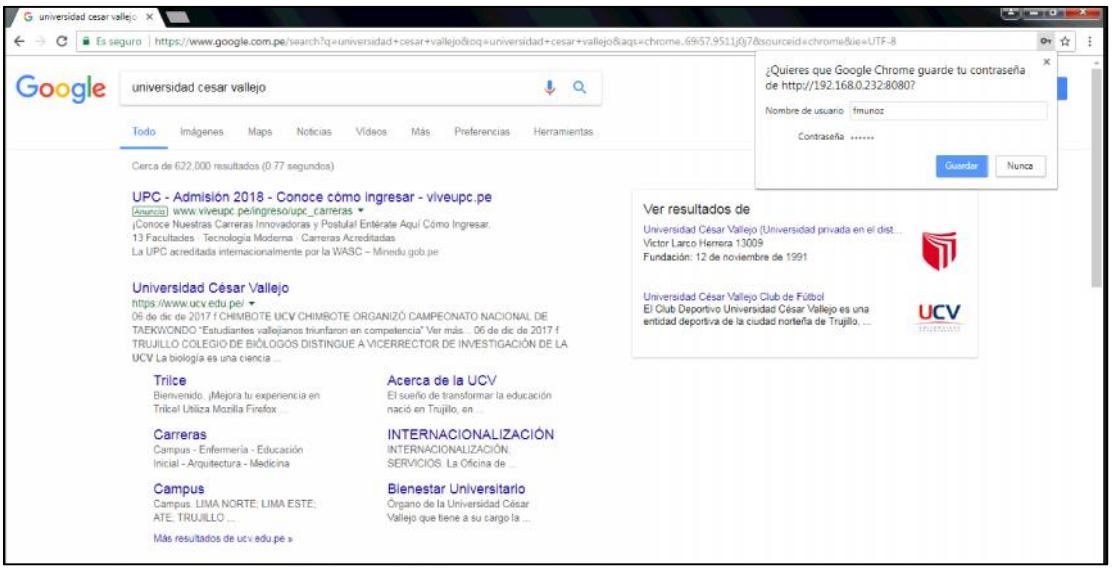


Figura 31. Acceso a internet

Si por algún motivo el usuario olvida su clave y/o usuario no podrá acceder a internet, ya que para el servidor Endian dicho usuario no existe y rechaza la petición denegando la utilización del servicio.

2) Proxy HTTP

El tipo de filtrado web dependerá de los perfiles establecidos (ver figura 32), se entiende como tipo de filtrado a los privilegios que se le brinda a cada usuario para acceder.

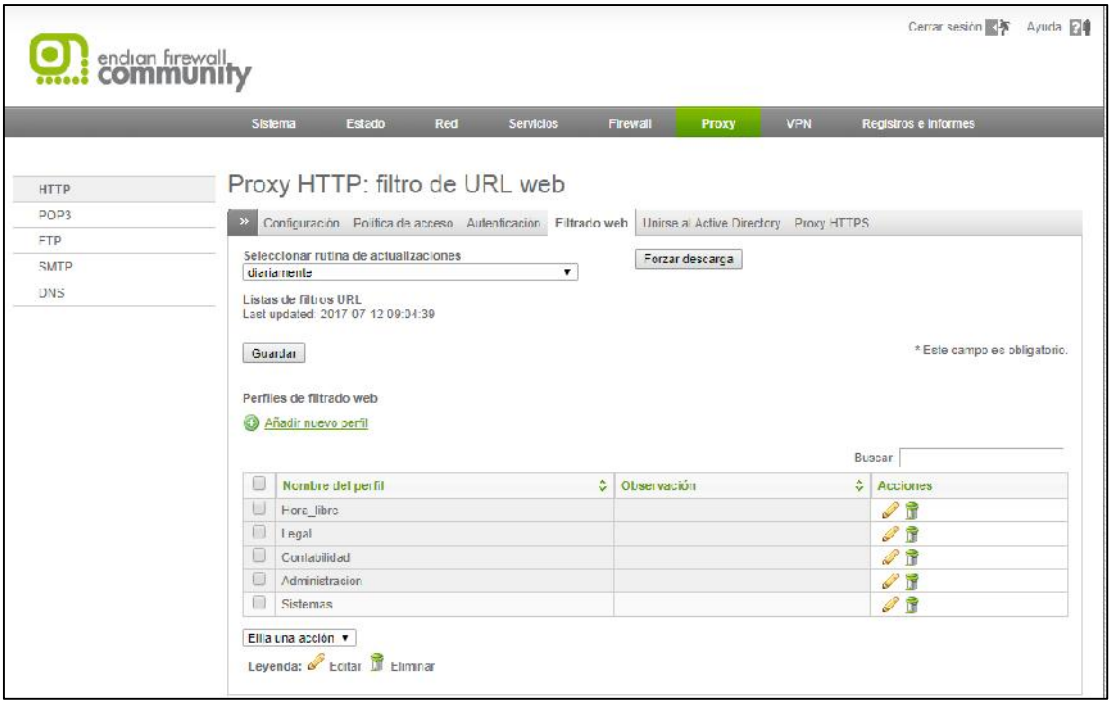


Figura 32. Perfiles de usuario

A continuación detallaremos las principales categorías bloqueadas según el tipo el tipo de perfil de usuarios:

a) Bloqueo de pornografía

Se estableció el bloqueo a páginas pornográficas para todos los usuarios de la empresa, en la figura 33 se observa que el filtrado web para denegar

el acceso a dichas páginas y otras categorías similares fueron bloqueadas con éxito por el servidor Endian.

Figura 33. Bloqueo de páginas pornográficas

b) Redes sociales

Las redes sociales (Facebook, Youtube, Instagram, etc) están bloqueadas para todas las áreas en el horario de oficina, solo el gerente de la empresa tiene acceso a ella, en la figura 34 se observa que el filtrado web para denegar el acceso a dichas páginas y otras categorías similares fueron bloqueados con éxito por el servidor Endian.

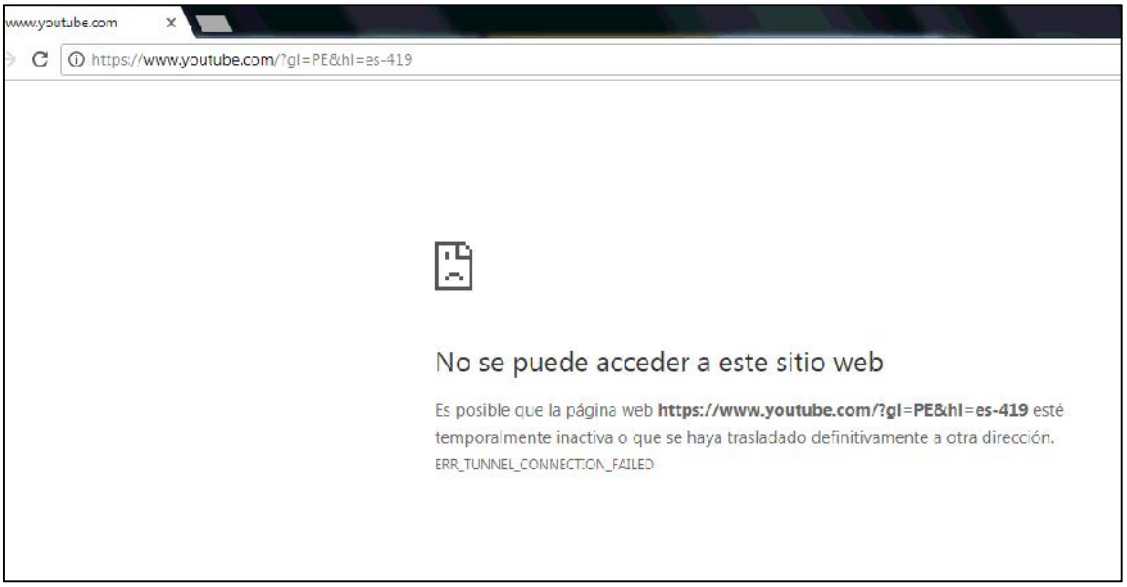


Figura 34. Bloqueo de redes sociales

c) Proxys

Las servidores proxy de la nube también están bloqueados para las áreas de administración, contabilidad y legal, en la figura 35 se observa que el filtrado web para denegar el acceso a dichas páginas y otras categorías similares fueron bloqueados con éxito por el servidor Endian.

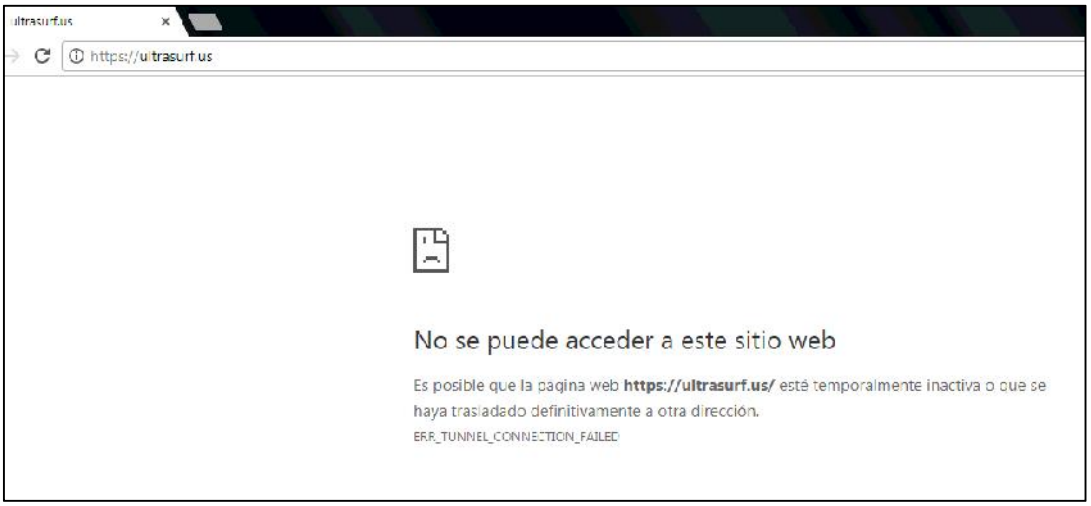


Figura 35. Bloqueo de proxy

d) Juegos

Las páginas web cuyo contenido son juegos online fueron bloqueados para las áreas de administración, contabilidad, legal y sistemas, en la figura 36 se observa que el filtrado web para denegar el acceso a dichas páginas y otras categorías similares fueron bloqueados con éxito por el servidor Endian.

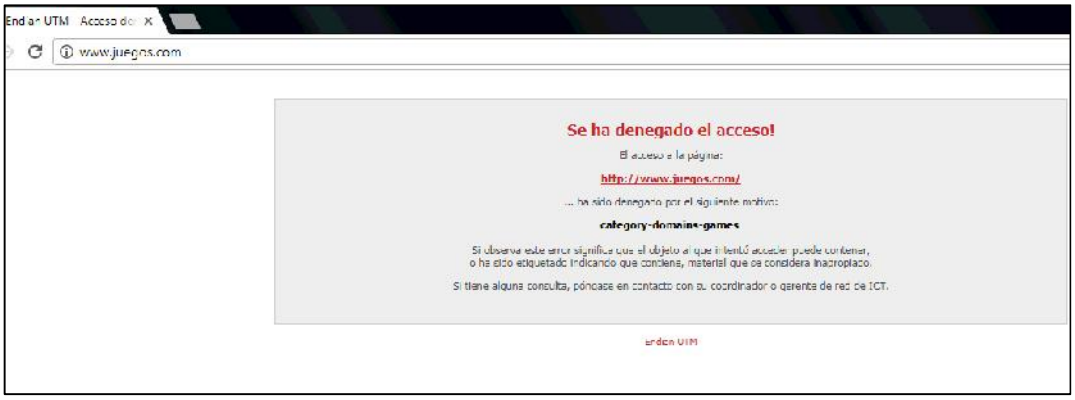


Figura 36. Bloqueo de juegos

e) Hora libre

Según la autorización de la gerencia, todo personal puede acceder a las redes sociales en horarios no laborables, como por ejemplo en la hora de refrigerio, después de las 18 horas, sábados y domingos, ya que en esos horarios no afecta la productividad y rendimiento del internet, en la figura 37 se observa el perfil configurado para cumplir dicha función.

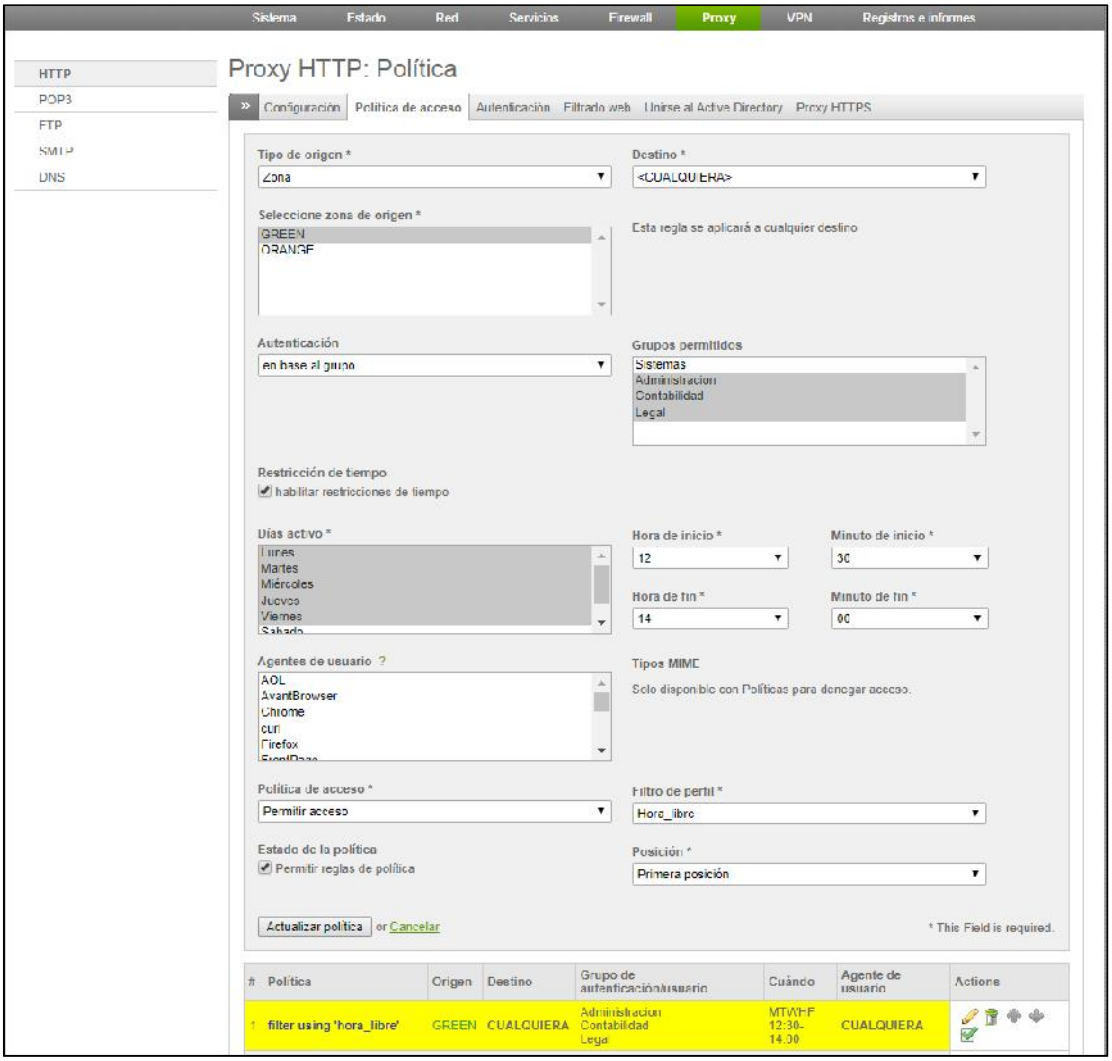


Figura 37. Configuración libre navegación

3) Proxy POP3

El escaneo de correos entrantes es muy importante para detectar riesgos de personas mal intencionadas que aprovechan el uso de correos electrónicos para enviar autoejecutables o enlaces de descarga con el propósito de infectar la red o en el peor de los casos al fraude electrónico, por tal motivo la implementación del filtro spam es muy importante para prevenir dichos ataques. En la figura 38, se observa que es posible determinar una lista de dominios (lista blanca) que pueden ser autorizados para llegar a las bandejas de correo de los usuarios.

Asimismo se puede determinar una lista negra de dominios, en este caso el firewall Endian identifica cualquier intento de ingreso de dichos dominios y bloquea automáticamente cualquier intento, sin dejar pasar el correo hacia la red interna.

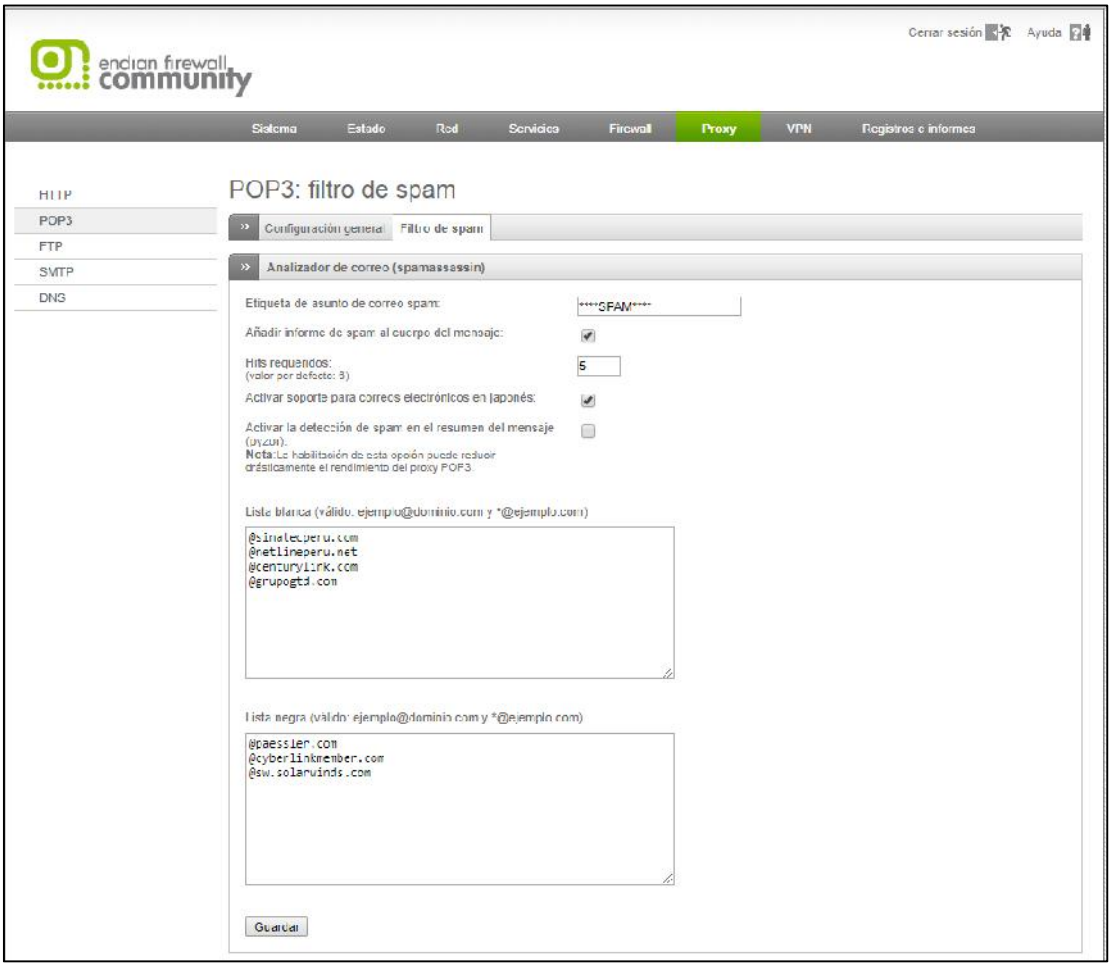


Figura 38. Configuración filtro spam

4) Pruebas de acceso remoto

El escritorio remoto es una tecnología muy utilizada en los últimos años, es por ello que no debemos prescindir de ella a la hora de diseñar una topología de red, en este caso la configuración se realiza en el firewall, para ello debemos tener en cuenta la dirección IP privada del equipo al cual

deseamos conectarnos, luego establecemos el puerto y protocolo de comunicación para establecer la conexión desde una red externa.

A continuación detallaremos los pasos que debe realizar el usuario cada vez que desee acceder a un equipo de la red local vía acceso remoto:

a) En la figura 39, se observa el campo donde se tiene que ingresar la dirección IP pública más el número de puerto a utilizar para establecer la conexión del servicio.

Figura 39. IP pública y puerto de conexión

b) En la figura 40, se observa las credenciales de autentificación para acceder al equipo, esta autentificación se dará siempre y cuando el firewall tenga configurado un DNAT (destination network address traslation) de la dirección IP interna y el puerto destino, caso contrario la petición será denegada.

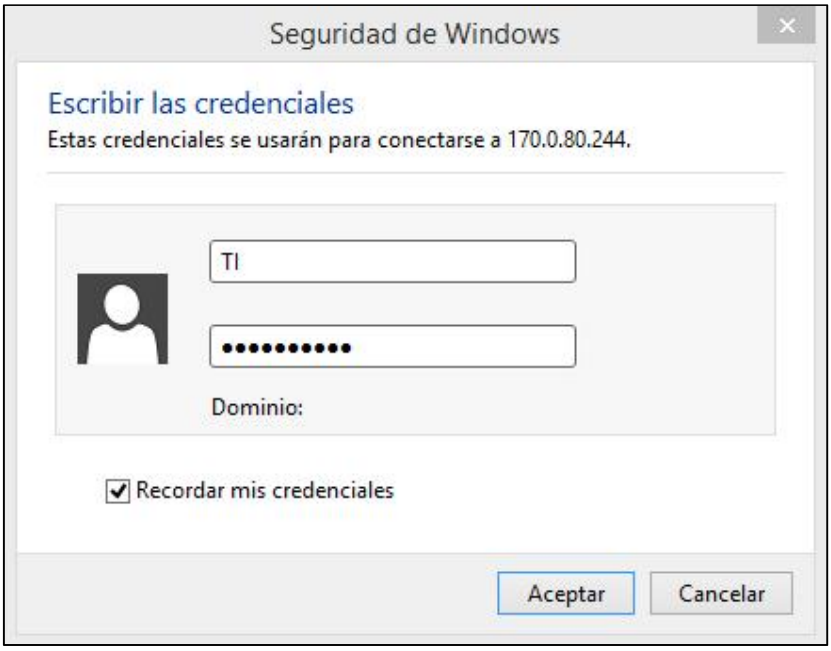


Figura 40. Solicitud de credenciales

c) En la figura 41, se observa que el firewall autentificó las credenciales y establece la conexión de escritorio remoto.

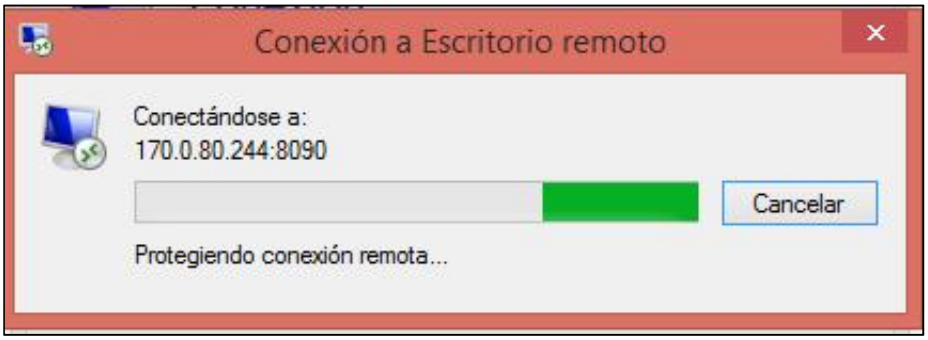


Figura 41. Estableciendo conexión

d) En la figura 42, se aprecia el ingreso vía acceso remoto al equipo de la red interna.

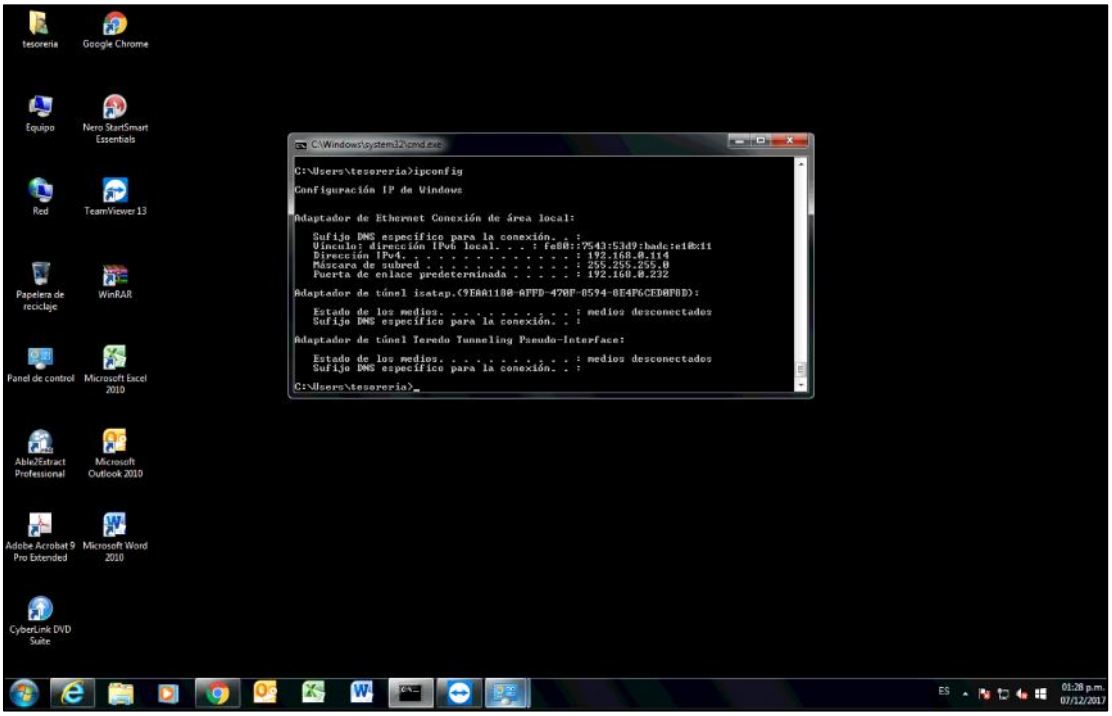


Figura 42. Ingreso a escritorio remoto

5) Pruebas de VPN

Según las nuevas políticas de seguridad, es necesario implementar tuneles VPN (red privada virtual), para el intercambio de información y/o acceso a los distintos servicios que se encuentran dentro de la red local, de forma segura.

Para proceder a crear las credenciales en el firewall Endian, es preciso que cada jefe de área designe los trabajadores que utilizarán dicha tecnología, luego procederemos a habilitar el servidor OpenVPN y crear la lista de usuarios que según la configuración a utilizar, será la autentificación de dos factores (certificado x.509 y PSK (usuario y contraseña)).

La acción que realiza la autentificación de dos factores, es validar además de las credenciales de usuario y contraseña (configuración usual), validar también las credenciales del certificado SSL que se encuentra creado en el servidor, es decir si un usuario desea acceder a la red interna

desde el exterior, deberá contar con ambas credenciales, de esa manera se logra que las conexiones entrantes hacia la red local sean más seguras.

A continuación detallaremos los pasos que debe utilizar cada usuario antes de acceder a la red local vía VPN, implementado en la empresa Junefield Group S.A.

a) En la figura 43, se observa los campos obligatorios que requiere la conexión VPN (dirección IP del servidor, tipo de autentificación, seleccionar la llave PKCS, contraseña de la llave PKCS, usuario y contraseña de la cuenta).

Figura 43. Autentificación de dos factores

b) En la figura 44, se observa la conexión establecida, es decir, si los datos ingresados son correctos, el firewall Endian autentificará las credenciales del usuario y establecerá la conexión.

Figura 44. Conexión establecida

c) En la figura 45, se aprecia las conexiones activas que se encuentran registrados en el firewall Endian, en ella se observa el nombre de usuario, fecha y hora de conexión, la dirección IP asignada, y la IP pública de donde se conecta el usuario.

Figura 45. Conexión VPN activas

3.3.4.2. Optimizar el diseño de red

En cuanto a la optimización de la red se debe tener en cuenta el crecimiento de host y los tipos de servicio que en el futuro se piense implementar, el diseño de red propuesto actualmente tiene las capacidades de soportar dicho cambio sin perjudicar el performance de la red.

Asimismo para la optimización de la red se utilizó equipos que soportan nuevas tecnologías para ser reutilizados sin perjudicar la economía de la empresa, de igual manera se identificó los servicios que se transmitirán a través de la red, realizando una priorización de tráfico y garantizar la calidad de servicio.

La implementación del servidor Endian para mejorar la seguridad perimetral de la red local es un proceso que va en paralelo con la evolución de la empresa, por lo que todo cambio en la configuración de las políticas del servidor se aprecia como mejora a la infraestructura de red del negocio.

Por otro lado, para tener una red segura y confiable se tiene que realizar constantemente un monitoreo a la red, el cual permitirá obtener una retroalimentación de los eventos ocurridos y realizar mejoras continuas a fin de evitar nuevas amenazas que van evolucionando a través del tiempo y la tecnología.

A continuación se observan las mejoras que se obtuvo al implementar el firewall Endian, el cambio fue notable, no solo en la eficacia de priorización de tráfico sino también en las políticas de filtrado web.

En la figura 46, se observa latencias muy altas el cual es originado por consumo excesivo del ancho de banda contratado, dichas latencias dificultaban las labores diarias de personal interno así como de las sedes remotas.

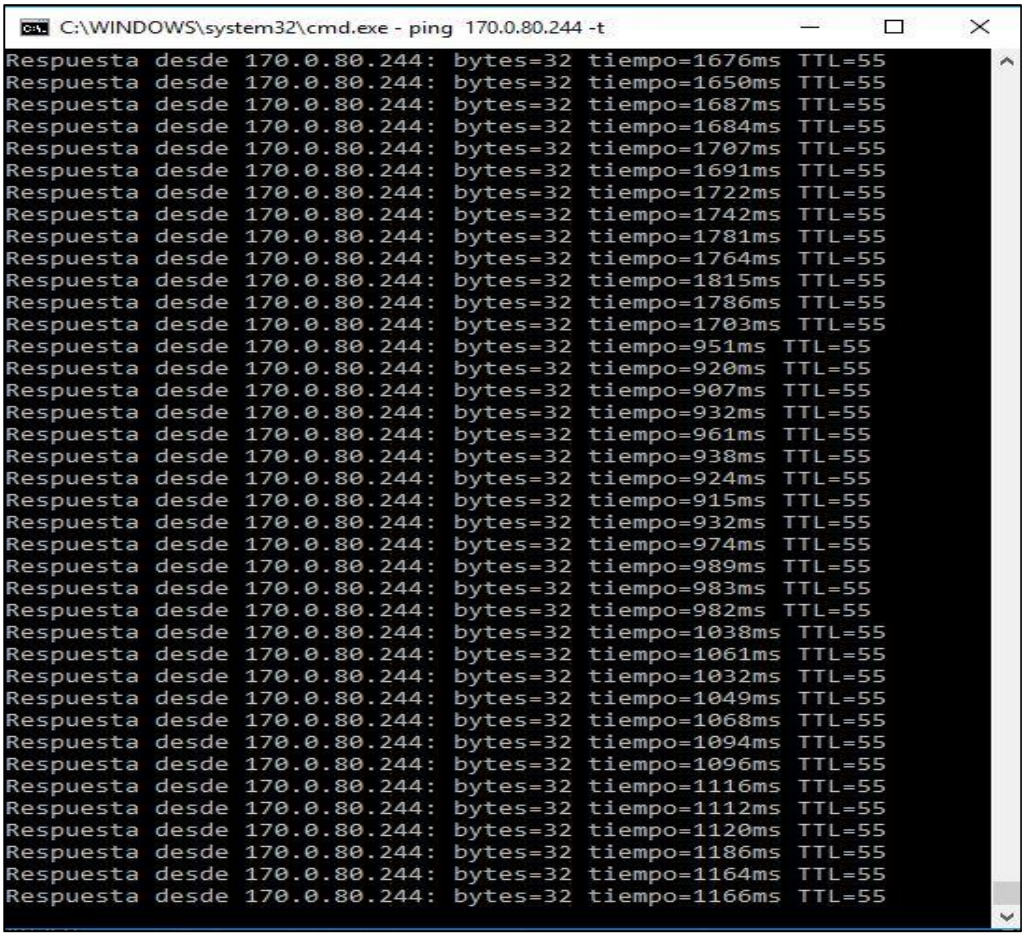


Figura 46. Pruebas de ping desde el exterior pre-test

En la figura 47, se observa mejora de las latencias, dicho cambio se originó debido a la implementación de políticas de filtrado y aplicaciones web, así como la priorización de tráfico.

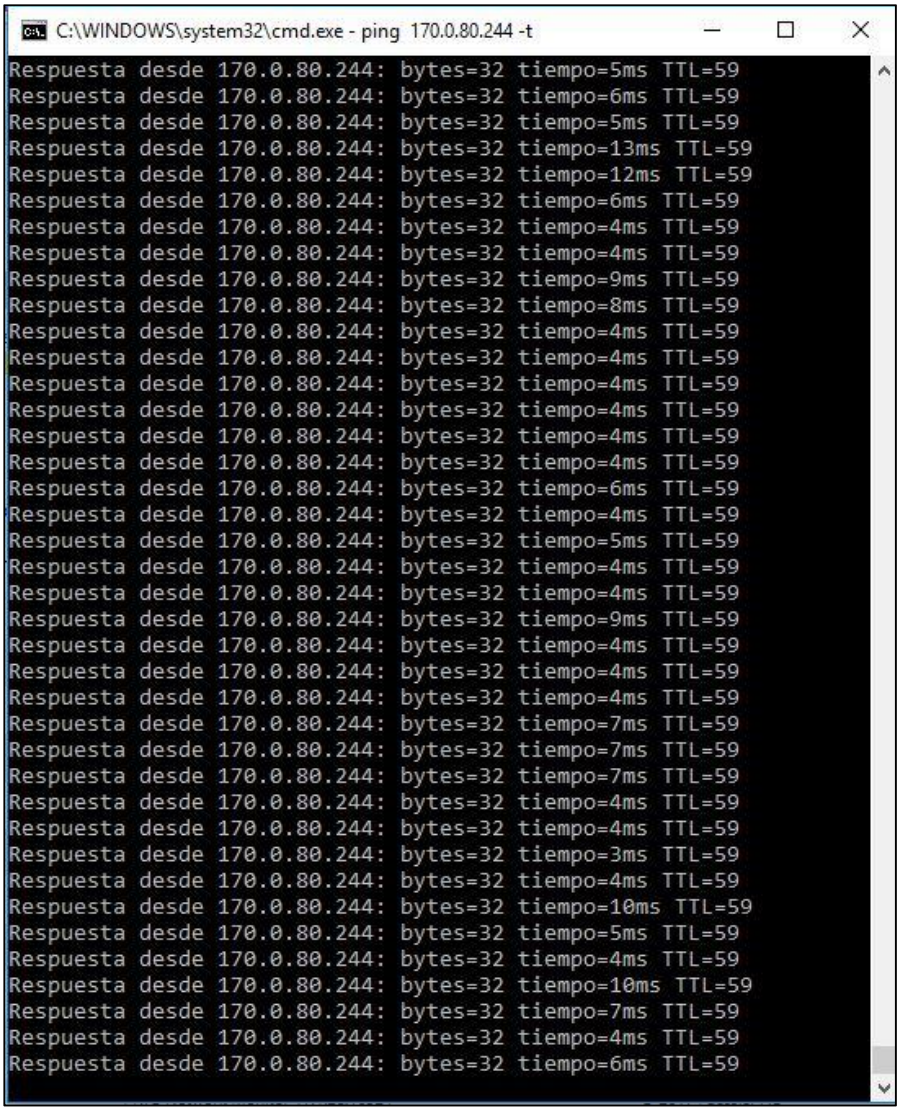


Figura 47. Pruebas de ping desde el exterior post-test

Por consiguiente, se pudo observar que la implementación del firewall Endian, mejora considerablemente la infraestructura y seguridad de la información, es por ello que este cambio garantiza la confiabilidad, integridad y disponibilidad de la red local de la empresa Junefield Group S.A.

IV. DISCUSIÓN

De los resultados conseguidos de la presente investigación como modelo de aplicación, se puede plante la siguiente discusión e interpretación:

1. Confidencialidad, para obtener los resultados de dicha dimensión se tuvo que cuantificar los indicadores que se muestran a continuación según la ficha de observación:

   - Nivel de políticas de seguridad, en la medición pre-test alcanzó un 32.8% y en la medición post-test alcanzo 91.0%.
   - Nivel de confidencialidad de los datos, en la medición pre-test alcanzó un 35.2% y en la medición post-test alcanzo 95.7%.

   Según los resultados obtenidos, se puede observar que la dimensión confidencialidad con sus indicadores “Nivel de políticas de seguridad” y “Nivel de confidencialidad” mejoró en un 63.96% y 63.2% respectivamente, por lo que se afirma que la implementación del firewall Endian, influye significativamente en la confidencialidad de la información de la empresa Junefield Group S.A.

2. Integridad, para obtener los resultados de dicha dimensión se tuvo que cuantificar los indicadores que se muestran a continuación según la ficha de observación:

   - Nivel de riesgo de los datos, en la medición pre-test alcanzó un 69.1% y en la medición post-test mejoró a un 11.3%.
   - Manipulación de datos, en la medición pre-test alcanzó un 66.4% y en la medición post-test mejoró a un 4.1%.

   Según los resultados obtenidos, se puede observar que la dimensión integridad con sus indicadores “Nivel de riesgo de los datos” y “Manipulación de datos” disminuyó el riesgo de los datos en -83.6% y -93.56% respectivamente, por lo que se afirma que la implementación del firewall Endian, influye significativamente en la integridad de la información de la empresa Junefield Group S.A.

3. Disponibilidad, para obtener el resultado de dicha dimensión se tuvo que cuantificar el indicador que se muestra a continuación según la ficha de observación:

   - Nivel de disponibilidad de los datos, en la medición pre-test alcanzó un 90.0% y en la medición pos-test alcanzó un 94.6%.

   Según los resultados obtenidos, se puede observar que la dimensión disponibilidad con su indicador “Nivel de disponibilidad de los datos” mejoró en un 5.25%, por lo que se afirma que la implementación del firewall Endian, influye significativamente en la disponibilidad de la información de la empresa Junefield Group S.A.

☞ Según la investigación realizada por Bravo, L. en la tesis: “Modelo diagnóstico y análisis de la red LAN para la mejora del rendimiento y seguridad en la red de salud Valle del Mantaro mediante la metodología CISCO”, el resultado obtenido fue la disminución de tráfico de red, de un 59.840% a 18.126% brindando disponibilidad total para los 93 usuarios y garantizando un correcto desempeño de las aplicaciones que se ejecuten sobre la red.

V. CONCLUSIONES

De acuerdo a los resultados obtenidos durante la experimentación se tienen las siguientes conclusiones, las cuales se describen en función a los objetivos específicos propuestos:

1. Se concluye que la confidencialidad de la información de la empresa Junefield Group S.A., sin el firewall Endian era 32.8% respecto al indicador “Nivel de políticas de seguridad” y con la implementación mejoró a un 91.0%, asimismo el “Nivel de confidencialidad de los datos” sin el firewall era de 35.2% y con la implementación mejoró a un 95.7%

   Según los resultados obtenidos, se puede observar que la dimensión confidencialidad con sus indicadores “Nivel de políticas de seguridad” y “Nivel de confidencialidad”, los porcentajes de variación mostraron un aumento de 63.96% y 63.2% respectivamente, por lo tanto, la implementación del firewall Endian influye favorablemente en la confidencialidad de la información de la empresa Junefield Group S.A.

2. Se concluye que la integridad de la información de la empresa Junefield Group S.A., sin el firewall Endian era 69.11% respecto al indicador “Nivel de riesgo de los datos” y con la implementación mejoró a un 11.3%, asimismo la “Manipulación de los datos” sin el firewall era de 66.4% y con la implementación mejoró a un 4.1%

   Según los resultados obtenidos, se puede observar que la dimensión integridad con sus indicadores “Nivel de riesgo de los datos” y “Manipulación de datos”, los porcentajes de variación mostraron una disminución en el riesgo de los datos de -83.6% y -93.56% respectivamente, por lo tanto, la implementación del firewall Endian influye favorablemente en la integridad de la información de la empresa Junefield Group S.A.

3. Se concluye que la disponibilidad de la información en la empresa Junefield Group S.A., sin el firewall Endian era 90.0% respecto al indicador “Nivel de disponibilidad de los datos” y con la implementación mejoró a un 94.6%.

Según los resultados obtenidos, se puede observar que la dimensión disponibilidad con su indicador “Nivel de disponibilidad de los datos”, los porcentajes de variación mostraron un aumento de 5.25%, por lo tanto, la implementación del firewall Endian influye favorablemente en la disponibilidad de la información de la empresa Junefield Group S.A.

- Según la investigación realizada por Bravo. L en la tesis “Modelo diagnóstico y análisis de la red LAN para la mejora del rendimiento y seguridad en la red de salud Valle del Mantaro mediante la metodología CISCO”, finalmente se concluye que el diseño de infraestructura de la red LAN y su implementación permitirá solucionar la problemática en cuanto a rendimiento y seguridad en la Red de Salud Valle del Mantaro.

VI. RECOMENDACIONES

- Para alcanzar el 99.5% de integridad de los datos, se recomienda implementar constantes políticas de seguridad, así como de filtrado y aplicaciones web, debido a la evolución constante de tecnología y por ende la aparición de nuevas amenazas, de esa manera se contribuirá a consolidar eficazmente las metas y objetivos trazados por la empresa.

- La empresa Junefield Group S.A., debe fortalecer las políticas de seguridad que se encuentran actualmente vigente, teniendo en cuenta que la información es un activo muy importante y debe ser resguardado de ataques enfocados al robo de información, modificación, entre otras.

- Se debe realizar monitoreo constante de las políticas de seguridad implementada ya sea lógico o físico, considerando siempre que debe existir mejoras continuas en toda implementación para garantizar la confidencialidad, integridad y disponibilidad de los datos.

- Debe existir constantemente capacitaciones a todo el personal que labora en la empresa Junefield Group S.A., respecto a la seguridad de la información.

VII. REFERENCIAS

AGUIRRE M., David A. Diseño de gestión de seguridad de información para servicios postales del Perú S.A. Trabajo de Titulación (Ingeniería en Informática). Lima: Universidad Católica del Perú, [en línea] Facultad de Ciencias e Ingeniería, octubre 2014. Disponible en Web:
http://tesis.pucp.edu.pe/repositorio/handle/123456789/5677

BALTAZAR G., José M. y CAMPUZANO R., Juan C. Diseño e implementación de un esquema de Seguridad Perimetral para redes de datos. Trabajo de Titulación (Ingeniería en Computación). México DF: Universidad Autónoma de México, [en línea] Facultad de Ingeniería, febrero 2011. Disponible en Web: http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/174/Version%20Final.pdf?sequence=17

BARRANTES P., Carlos E. y HUGO H., Javier R. Diseño e implementación de un sistema de gestión de seguridad de información en procesos tecnológicos. Trabajo de Titulación (Ingeniero de Computación y Sistemas). Lima: Universidad de San Martín de Porres, [en línea] Facultad de Ingeniería y Arquitectura, 2012. Disponible en Web:
http://www.repositorioacademico.usmp.edu.pe/bitstream/usmp/609/3/barrantes_ce.pdf

BARRIOS D., Joel. Implementación de Servidores con GNU/Linux. 3ra. Ed., México: junio 2014. Págs. 897.

BERMUDEZ M., Kelly G. y BAILON S., Edber R. Análisis en seguridad informática y seguridad de la información basado en la norma ISO/IEC 27001-Sistemas de Gestión de Seguridad de la Información dirigido a una empresa de servicios financieros. Trabajo de Titulación (Ingeniero de Sistemas). Guayaquil: Universidad Politécnica Salesiana sede Guayaquil, [en línea] Facultad de Sistemas Informáticos, marzo 2015. Disponible en Web:
https://dspace.ups.edu.ec/bitstream/123456789/10372/1/UPS-GT001514.pdf

BRAVO V., Liseth C. Modelo diagnóstico y análisis de la red LAN para la mejora del rendimiento y seguridad en la red de salud Valle del Mantaro mediante la Metodología CISCO. Trabajo de Titulación (Ingeniera de Sistemas). Huancayo: Universidad Nacional del Centro del Perú, [en línea] Facultad de Ingeniería de Sistemas, 2015. Disponible en Web: http://repositorio.uncp.edu.pe/handle/UNCP/1133

BUENO R., Juan J. Sistema de control y seguridad Endian Firewall para la empresa Frada Sport. Trabajo de Titulación (Ingeniero Informático). Quito: Universidad Tecnológica Israel, [en línea] Facultad de Sistemas Informáticos, Octubre 2013. Disponible en Web: http://repositorio.uisrael.edu.ec/bitstream/47000/493/1/UISRAEL-EC-SIS-378.242-261.pdf

CARRASCO D., Sergio. Metodología de la Investigación Científica. 1ra, ed. Lima: San Marcos, 2005. Págs. 474.

CHACON, Jaime. El 28% de empresas ha sufrido violaciones de seguridad perimetral en el último año. [en línea]. *El Comercio. PE.* 10 de setiembre de 2017. [Fecha de Consulta: 12 de noviembre de 2017]. Disponible en web: https://elcomercio.pe/economia/mundo/28-empresas-sufrido-violaciones-seguridad-perimetral-ano-noticia-456800

Endian S.P.A. [IT] Endian Community [en línea] [Fecha de consulta: 22 de diciembre de 2017]. Disponible en web: https://www.endian.com/community/

FABUEL D., Carlos M. “Implementación de un sistema de seguridad perimetral”. [Proyecto fin de carrera]. Universidad Politécnica de Madrid. [en línea] Escuela Universitaria de Ingeniería Técnica de Telecomunicación. 2013. Disponible en Web: http://oa.upm.es/22228/1/PFC_CARLOS_MANUEL_FABUEL_DIAZ.pdf

GELBSTEIN, Ed. La integridad de los datos: el aspecto más relegado de la seguridad de la información. [en línea]. *ISACA JOURNAL,* (6): 1-6. Suiza: 2011

[fecha de consulta: 18 noviembre de 2017]. Disponible en web: http://www.isaca.org/Journal/Documents/11v6-Data-Integrity-Information-Securitys-Poor-Relation-spanish.pdf

GONZALES-VALLE S., Guillermo. Todo sobre GNU/LINUX. Ventajas e Inconvenientes de Linux [en línea]. Madrid, 2014. [Fecha de consulta: 19 de febrero de 2017]. Disponible en Web: http://linux.ciberaula.com/articulo/ventajas_inconvenientes_linux/

GUEVARA P., Obed y MIRANDA Z., Arnold A. Diseño de una red de datos para el policlínico Señor de los Milagros S.R.L. usando Metodología Top Down Network Design y aplicando estándares ISO/IEC 27002. Trabajo de Titulación (Ingeniero de Computación y Sistemas). Trujillo: Universidad Privada Antenor Orrego. [en línea] Facultad de Ingeniería, 2014. Disponible en web: http://repositorio.upao.edu.pe/bitstream/upaorep/1044/1/GUEVARA_OBED_RED_DATOS_POLICLINICO.pdf

GUILLEN E., Montserrat, ALEA R., Ma. Victoria, MUÑOZ V., Ma. Carmen *et al.* Estadística con SPSS v.10.0. Barcelona: Edicions de la Universitat de Barcelona, 1ra. ed. 2001. Págs. 117. ISBN: 84-8338-257-1.

HERNANDEZ S., Roberto, FERNADEZ C., Carlos y BAPTISTA L., María. Metodología de la Investigación [en línea]. México DF: McGraw-Hill, 6ta. ed. 2014. [Fecha de consulta: 18 de octubre de 2016]. Disponible en Web: https://trabajosocialudocpno.files.wordpress.com/2017/07/metodologc3a3c2ada_de_la_investigacic3a3c2b3n_-sampieri-_6ta_edicion1.pdf

HURTADO DE BARRERA, Jackeline. Guía para la Comprensión Holística de la Ciencia. [en línea]. 3ra, ed. Caracas: Universidad Nacional Abierta – Dirección de Investigación y Postgrado, 2010. Disponible en Web: http://dip.una.edu.ve/mpe/017metodologiaI/paginas/Hurtado,%20Guia%20para%20la%20comprension%20holistica%20de%20la%20ciencia%20Unidad%20III.pdf

JARAMILLO R., Daniel D. Auditoría de Seguridad Informática para el Gobierno Autónomo Descentralizado de Santa Ana de Cotacachi, basada en la norma NTP-ISO/IEC 17799:2007 y la Metodología OSSTMM V2. Trabajo de Titulación (Ingeniero en Electrónica y Redes de Comunicación). Ibarra: Universidad Técnica del Norte. [en línea] Facultad de Ingeniería en Ciencias Aplicadas, Julio 2014. Disponible en web: http://repositorio.utn.edu.ec/bitstream/123456789/3774/1/04%20RED%20034%20TESIS.pdf

LEÓN B., Luis G. Diseño e Implementación de una infraestructura de servicios de red y resguardo de servidores Linux a través de Open Source en la empresa Proteco Coasin SA. Trabajo de Titulación (Ingeniero de Sistemas y Telecomunicaciones). Quito: Universidad Internacional SEK, Facultad de Sistemas y Telecomunicaciones, Mayo 2012. Disponible en web: http://repositorio.uisek.edu.ec/bitstream/123456789/534/1/TESIS%20FINAL%20LUIS%20GUILLERMO%20LE%C3%93N%20BUSTAMANTE.pdf

MENDEZ A., Carlos E. Metodología: Guía para elaborar diseños de investigación en ciencias económicas, contables y administrativas [en línea]. 4° ed. Bogotá: McGraw-Hill, 2011 [fecha de consulta: 10 de noviembre de 2017]. Disponible en Web: https://es.scribd.com/document/324262554/METODOLOGIA-DE-LA-INVESTIGACION-CARLOS-MENDEZ-1-pdf

OPPENHEIMER, Priscilla. Top-Down Network Design [en línea]. 3ra. ed. Indianapolis: Cisco Press, 2011 [fecha de consulta: 2 de diciembre de 2017]. Disponible en Web: http://www.valleytalk.org/wp-content/uploads/2013/01/top-down-network-design-3rd-edition.pdf

Ret Hat, Inc. [US] Ret Hat Linux [en línea] [Fecha de consulta: 22 de diciembre de 2017]. Disponible en web: https://www.redhat.com/es

STALLINGS, William. Fundamentos de Seguridad en Redes. Aplicaciones y Estándares. 2da. Ed. Madrid: Pearson Prentice Hall, Octubre 2004, Págs. 432

STALLINGS, William. Comunicaciones y Redes de Computadoras. 7ma. Ed. Madrid: Pearson Prentice Hall, Julio 2004, Págs. 896

TENORIO, Alonso. Algunas webs son atacadas por hackers peruanos. [en línea]. *El Comercio. PE.* 25 de mayo de 2017. [Fecha de Consulta: 12 de noviembre de 2017]. Disponible en web: https://elcomercio.pe/tecnologia/actualidad/web-atacadas-hackers-peruanos-ciberataque-peru-426122

The ISO 27000, Directory. [en línea] Enero 2013. [Fecha de consulta: 15 de octubre de 2017]. Disponible en web: http://www.27000.org/

VILLALÓN H., Antonio. Seguridad en UNIX y Redes [en línea]. V. 2.1 Red IRIS. Julio 2002. [Fecha de consulta: 15 de setiembre de 2017] Disponible en Web: http://www.rediris.es/cert/doc/unixsec/unixsec.pdf

ZAMBRANO, Fabián. Peligros en Redes Sociales: Digiware detectó que el Perú es el quinto país que recibe más ataques cibernéticos en Latinoamérica. [en línea]. *El Peruano. PE.* 30 de octubre de 2015. [Fecha de Consulta: 12 de noviembre de 2017]. Disponible en web: http://www.elperuano.com.pe/noticia-peligros-redes-sociales-35014.aspx

VIII. ANEXOS

Anexo I. Matriz de consistencia

<table>
<tr><td colspan="10">MATRIZ DE CONSISTENCIA</td></tr>
<tr><td>TITULO</td><td colspan="6">IMPLEMENTACIÓN DE UN SERVIDOR LINUX Y SU INFLUENCIA EN LA SEGURIDAD PERIMETRAL DE LA RED LOCAL DE LA EMPRESA JUNEFIELD GROUP SA</td><td>DISEÑO DE INVESTIGACION</td><td>Experimental de Tipo Pre Experimental</td></tr>
<tr><td colspan="2">FORMULACION DEL PROBLEMA</td><td colspan="2">OBJETIVOS</td><td colspan="2">HIPOTESIS</td><td colspan="2">VARIABLES</td></tr>
<tr><td>GENERAL</td><td>ESPECIFICOS</td><td>GENERAL</td><td colspan="2">ESPECIFICOS</td><td colspan="2">ESPECIFICOS</td><td>INDEPENDIENTE</td><td>DIMENSIONES</td></tr>
<tr><td rowspan="4">¿De qué manera la implementación de un servidor Linux influye en la seguridad perimetral de la red local de Junefield Group S.A.?</td><td>¿De qué manera la implementación de un servidor Linux influye en la Confidencialidad de la red local de la empresa Junefield Group S.A.?</td><td rowspan="4">Determinar la influencia del servidor Linux en la seguridad perimetral de la red local de la empresa Junefield Group S.A.</td><td colspan="2">Determinar la influencia del servidor Linux en la Confidencialidad de la red local de la empresa Junefield Group S.A.</td><td rowspan="4">La implementación de un servidor Linux influye significativamente en la seguridad perimetral de la red local de la empresa Junefield Group S.A.</td><td>Hi: La implementación de un servidor Linux influye significativamente en la Confidencialidad de la red local de la empresa Junefield Group S.A.</td><td rowspan="2">Servidor LINUX</td><td>Funcionalidad</td></tr>
<tr><td>¿De qué manera la implementación de un servidor Linux influye en la Integridad de la red local de la empresa Junefield Group S.A.?</td><td colspan="2">Determinar la influencia del servidor Linux en la Integridad de la red local de la empresa Junefield Group S.A.</td><td>Ho: La implementación de un servidor Linux no influye significativamente en la Confidencialidad de la red local de la empresa Junefield Group S.A.</td><td>Confiabilidad</td></tr>
<tr><td rowspan="2">¿De qué manera la implementación de un servidor Linux influye en la Disponibilidad de la red local de la empresa Junefield Group S.A.?</td><td colspan="2" rowspan="2">Determinar la influencia del servidor Linux en la Disponibilidad de la red local de la empresa Junefield Group S.A.</td><td>Hi: La implementación de un servidor Linux influye significativamente en la Integridad de la red local de la empresa Junefield Group S.A.</td><td>DEPENDIENTE</td><td>DIMENSIONES</td></tr>
<tr><td>Ho: La implementación de un servidor Linux no influye significativamente en la Integridad de la red local de la empresa Junefield Group S.A.</td><td rowspan="3">Seguridad Perimetral de la Red Local de la empresa Junefield Group SA.</td><td>Confidencialidad</td></tr>
<tr><td colspan="2" rowspan="2">Determinar la influencia del servidor Linux en la Disponibilidad de la red local de la empresa Junefield Group S.A.</td><td>Hi: La implementación de un servidor Linux influye significativamente en la Disponibilidad de la red local de la empresa Junefield Group S.A.</td><td>Integridad</td></tr>
<tr><td>Ho: La implementación de un servidor Linux no influye significativamente en la Disponibilidad de la red local de la empresa Junefield Group S.A.</td><td>Disponibilidad</td></tr>
<tr><td colspan="3">POBLACION</td><td colspan="2">MUESTRA</td><td colspan="2">Se tomará a un total de 11 trabajadores de la población.</td><td>TESISTA</td></tr>
<tr><td colspan="3" rowspan="2">La población adecuada para estudiar el problema y cumplir con los objetivos propuestos está conformada por todas las personas involucradas en el Proceso de Seguridad Perimetral de la Red Local de la empresa Junefield Group SA, para ello seleccionaremos un grupo de la población.</td><td colspan="2">CICLO</td><td>GRUPO</td><td colspan="2">ESPECIALIDAD</td><td rowspan="2">OMAR BAUTISTA PILLACA</td></tr>
<tr><td>27</td><td>X</td><td>12</td><td colspan="2">Ingeniería de Sistemas</td></tr>
</table>

Figura 48. Matriz de consistencia

Anexo II. Indicadores

VARIABLE DEPENDIENTE: Seguridad Perimetral de la red local de la empresa Junefield Group SA							
DIMENSIONES	**INDICADORES**	**TECNICA**	**INSTRUMENTO**	**UNIDAD DE MEDIDA**	**FORMULA**	**ITEM**	**CRITERIOS PARA MEDIR INDICADOR**
Confidencialidad	Nivel de políticas de seguridad	Observación	Ficha de Observación	Porcentaje	$NPS = \frac{\sum_{n=1}^{n=3} I_n}{3}$ Donde: I_n = Criterio de medición	I_1	Restricción para navegar por internet
						I_2	Complejidad de las contraseñas de los equipos que almacena información (laptop, pc, etc.)
						I_3	Politicas de seguridad para resguardar la información (control de acceso, filtrado web, etc.)
	Nivel de confidencialidad de los datos	Observación	Ficha de Observación	Porcentaje	$NCD = \frac{\sum_{n=4}^{n=6} I_n}{3}$ Donde: I_n = Criterio de medición	I_4	La información es clasificado según el nivel de criticidad
						I_5	El acceso a la información compartida es solo para personal que lo requiere
						I_6	Nivel de confidencialidad de la información que se encuentra dentro de la red local
Integridad	Nivel de riesgo de los datos	Observación	Ficha de Observación	Porcentaje	$NRD = \frac{\sum_{n=7}^{n=8} I_n}{2}$ Donde: I_n = Criterio de medición	I_7	La información se encuentra expuesto (vulnerable) en su estación de trabajo
						I_8	La información se encuentra expuesto (vulnerable) dentro de la red local
	Manipulación de datos	Observación	Ficha de Observación	Porcentaje	$NMD = \frac{\sum_{n=9}^{n=10} I_n}{2}$ Donde: I_n = Criterio de medición	I_9	Cambios no autorizados de la información (modificar o eleminar la información)
						I_{10}	Nivel de riesgo de los datos en la red
Disponibilidad	Nivel de disponibilidad de los datos	Observación	Ficha de Observación	Porcentaje	$NDD = \frac{\sum_{n=11}^{n=13} I_n}{3}$ Donde: I_n = Criterio de medición	I_{11}	Dentro de la red local, la información se encuentra disponible cuando se requiere
						I_{12}	Fuera de la red local, disponibilidad de la información entre sedes
						I_{13}	Servicios que se brinda en la red (internet, correo electrónico, etc.)

Figura 49. Indicadores

ISO/IEC 27002:2005. Dominios (11), Objetivos de control (39) y Controles (133)

CLIC SOBRE CADA CONTROL PARA MÁS INFORMACIÓN

Versión actualizada de esta lista en: http://www.iso27000.es/download/ControlesISO27002-2005.pdf

5. POLÍTICA DE SEGURIDAD.
- **5.1 Política de seguridad de la información.**
  - 5.1.1 Documento de política de seguridad de la información.
  - 5.1.2 Revisión de la política de seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- **6.1 Organización interna.**
  - 6.1.1 Compromiso de la Dirección con la seguridad de la información.
  - 6.1.2 Coordinación de la seguridad de la información.
  - 6.1.3 Asignación de responsabilidades relativas a la seg. de la informac.
  - 6.1.4 Proceso de autorización de recursos para el tratamiento de la información.
  - 6.1.5 Acuerdos de confidencialidad.
  - 6.1.6 Contacto con las autoridades.
  - 6.1.7 Contacto con grupos de especial interés.
  - 6.1.8 Revisión independiente de la seguridad de la información.
- **6.2 Terceros.**
  - 6.2.1 Identificación de los riesgos derivados del acceso de terceros.
  - 6.2.2 Tratamiento de la seguridad en la relación con los clientes.
  - 6.2.3 Tratamiento de la seguridad en contratos con terceros.

7. GESTIÓN DE ACTIVOS.
- **7.1 Responsabilidad sobre los activos.**
  - 7.1.1 Inventario de activos.
  - 7.1.2 Propiedad de los activos.
  - 7.1.3 Uso aceptable de los activos.
- **7.2 Clasificación de la información.**
  - 7.2.1 Directrices de clasificación.
  - 7.2.2 Etiquetado y manipulado de la información.

8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- **8.1 Antes del empleo.**
  - 8.1.1 Funciones y responsabilidades.
  - 8.1.2 Investigación de antecedentes.
  - 8.1.3 Términos y condiciones de contratación.
- **8.2 Durante el empleo.**
  - 8.2.1 Responsabilidades de la Dirección.
  - 8.2.2 Concienciación, formación y capacitación en seg. de la informac.
  - 8.2.3 Proceso disciplinario.
- **8.3 Cese del empleo o cambio de puesto de trabajo.**
  - 8.3.1 Responsabilidad del cese o cambio.
  - 8.3.2 Devolución de activos.
  - 8.3.3 Retirada de los derechos de acceso.

9. SEGURIDAD FÍSICA Y DEL ENTORNO.
- **9.1 Áreas seguras.**
  - 9.1.1 Perímetro de seguridad física.
  - 9.1.2 Controles físicos de entrada.
  - 9.1.3 Seguridad de oficinas, despachos e instalaciones.
  - 9.1.4 Protección contra las amenazas externas y de origen ambiental.
  - 9.1.5 Trabajo en áreas seguras.
  - 9.1.6 Áreas de acceso público y de carga y descarga.
- **9.2 Seguridad de los equipos.**
  - 9.2.1 Emplazamiento y protección de equipos.
  - 9.2.2 Instalaciones de suministro.
  - 9.2.3 Seguridad del cableado.
  - 9.2.4 Mantenimiento de los equipos.
  - 9.2.5 Seguridad de los equipos fuera de las instalaciones.
  - 9.2.6 Reutilización o retirada segura de equipos.
  - 9.2.7 Retirada de materiales propiedad de la empresa.

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.
- **10.1 Responsabilidades y procedimientos de operación.**
  - 10.1.1 Documentación de los procedimientos de operación.
  - 10.1.2 Gestión de cambios.
  - 10.1.3 Segregación de tareas.
  - 10.1.4 Separación de los recursos de desarrollo, prueba y operación.
- **10.2 Gestión de la provisión de servicios por terceros.**
  - 10.2.1 Provisión de servicios.
  - 10.2.2 Supervisión y revisión de los servicios prestados por terceros.
  - 10.2.3 Gestión del cambio en los servicios prestados por terceros.
- **10.3 Planificación y aceptación del sistema.**
  - 10.3.1 Gestión de capacidades.
  - 10.3.2 Aceptación del sistema.
- **10.4 Protección contra el código malicioso y descargable.**
  - 10.4.1 Controles contra el código malicioso.
  - 10.4.2 Controles contra el código descargado en el cliente.
- **10.5 Copias de seguridad.**
  - 10.5.1 Copias de seguridad de la información.
- **10.6 Gestión de la seguridad de las redes.**
  - 10.6.1 Controles de red.
  - 10.6.2 Seguridad de los servicios de red.
- **10.7 Manipulación de los soportes.**
  - 10.7.1 Gestión de soportes extraíbles.
  - 10.7.2 Retirada de soportes.
  - 10.7.3 Procedimientos de manipulación de la información.
  - 10.7.4 Seguridad de la documentación del sistema.
- **10.8 Intercambio de información.**
  - 10.8.1 Políticas y procedimientos de intercambio de información.
  - 10.8.2 Acuerdos de intercambio.
  - 10.8.3 Soportes físicos en tránsito.
  - 10.8.4 Mensajería electrónica.
  - 10.8.5 Sistemas de información empresariales.
- **10.9 Servicios de comercio electrónico.**
  - 10.9.1 Comercio electrónico.
  - 10.9.2 Transacciones en línea.
  - 10.9.3 Información públicamente disponible.
- **10.10 Supervisión.**
  - 10.10.1 Registros de auditoría.
  - 10.10.2 Supervisión del uso del sistema.
  - 10.10.3 Protección de la información de los registros.
  - 10.10.4 Registros de administración y operación.
  - 10.10.5 Registro de fallos.
  - 10.10.6 Sincronización del reloj.

11. CONTROL DE ACCESO.
- **11.1 Requisitos de negocio para el control de acceso.**
  - 11.1.1 Política de control de acceso.
- **11.2 Gestión de acceso de usuario.**
  - 11.2.1 Registro de usuario.
  - 11.2.2 Gestión de privilegios.
  - 11.2.3 Gestión de contraseñas de usuario.
  - 11.2.4 Revisión de los derechos de acceso de usuario.
- **11.3 Responsabilidades de usuario.**
  - 11.3.1 Uso de contraseñas.
  - 11.3.2 Equipo de usuario desatendido.
  - 11.3.3 Política de puesto de trabajo despejado y pantalla limpia.
- **11.4 Control de acceso a la red.**
  - 11.4.1 Política de uso de los servicios en red.
  - 11.4.2 Autenticación de usuario para conexiones externas.
  - 11.4.3 Identificación de los equipos en las redes.
  - 11.4.4 Protección de los puertos de diagnóstico y configuración remotos.
  - 11.4.5 Segregación de las redes.
  - 11.4.6 Control de la conexión a la red.
  - 11.4.7 Control de encaminamiento (routing) de red.
- **11.5 Control de acceso al sistema operativo.**
  - 11.5.1 Procedimientos seguros de inicio de sesión.
  - 11.5.2 Identificación y autenticación de usuario.
  - 11.5.3 Sistema de gestión de contraseñas.
  - 11.5.4 Uso de los recursos del sistema.
  - 11.5.5 Desconexión automática de sesión.
  - 11.5.6 Limitación del tiempo de conexión.
- **11.6 Control de acceso a las aplicaciones y a la información.**
  - 11.6.1 Restricción del acceso a la información.
  - 11.6.2 Aislamiento de sistemas sensibles.
- **11.7 Ordenadores portátiles y teletrabajo.**
  - 11.7.1 Ordenadores portátiles y comunicaciones móviles.
  - 11.7.2 Teletrabajo.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.
- **12.1 Requisitos de seguridad de los sistemas de información.**
  - 12.1.1 Análisis y especificación de los requisitos de seguridad.
- **12.2 Tratamiento correcto de las aplicaciones.**
  - 12.2.1 Validación de los datos de entrada.
  - 12.2.2 Control del procesamiento interno.
  - 12.2.3 Integridad de los mensajes.
  - 12.2.4 Validación de los datos de salida.
- **12.3 Controles criptográficos.**
  - 12.3.1 Política de uso de los controles criptográficos.
  - 12.3.2 Gestión de claves.
- **12.4 Seguridad de los archivos de sistema.**
  - 12.4.1 Control del software en explotación.
  - 12.4.2 Protección de los datos de prueba del sistema.
  - 12.4.3 Control de acceso al código fuente de los programas.
- **12.5 Seguridad en los procesos de desarrollo y soporte.**
  - 12.5.1 Procedimientos de control de cambios.
  - 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 12.5.3 Restricciones a los cambios en los paquetes de software.
  - 12.5.4 Fugas de información.
  - 12.5.5 Externalización del desarrollo de software.
- **12.6 Gestión de la vulnerabilidad técnica.**
  - 12.6.1 Control de las vulnerabilidades técnicas.

13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- **13.1 Notificación de eventos y puntos débiles de seguridad de la información.**
  - 13.1.1 Notificación de los eventos de seguridad de la información.
  - 13.1.2 Notificación de puntos débiles de seguridad.
- **13.2 Gestión de incidentes y mejoras de seguridad de la información.**
  - 13.2.1 Responsabilidades y procedimientos.
  - 13.2.2 Aprendizaje de los incidentes de seguridad de la información.
  - 13.2.3 Recopilación de evidencias.

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- **14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.**
  - 14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
  - 14.1.2 Continuidad del negocio y evaluación de riesgos.
  - 14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
  - 14.1.4 Marco de referencia para la planificación de la cont. del negocio.
  - 14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.

15. CUMPLIMIENTO.
- **15.1 Cumplimiento de los requisitos legales.**
  - 15.1.1 Identificación de la legislación aplicable.
  - 15.1.2 Derechos de propiedad intelectual (DPI).
  - 15.1.3 Protección de los documentos de la organización.
  - 15.1.4 Protección de datos y privacidad de la información de carácter personal.
  - 15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.
  - 15.1.6 Regulación de los controles criptográficos.
- **15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.**
  - 15.2.1 Cumplimiento de las políticas y normas de seguridad.
  - 15.2.2 Comprobación del cumplimiento técnico.
- **15.3 Consideraciones sobre las auditorías de los sistem. de información.**
  - 15.3.1 Controles de auditoría de los sistemas de información.
  - 15.3.2 Protección de las herramientas de auditoría de los sist. de inform.

Ver. 4.0, 16-1-2011

Figura 50. Norma ISO/IEC 27002:2005

Anexo IV. Ficha de observación

Figura 51. Ficha de observación – Pre-test

FICHA DE OBSERVACIÓN

UCV UNIVERSIDAD CÉSAR VALLEJO

"Implementación de un Servidor LINUX y su influencia en la seguridad perimetral de la red local de la empresa Junefield Group S.A."

Ficha de Observación (Pre – Test): Variable Dependiente – Seguridad Perimetral
Esta ficha de observación evalúa la mejora de seguridad perimetral de la red local de la empresa Junefield Group S.A. (cuantitativamente)

DETALLES DE EQUIPOS Y APLICACIONES UTILIZADOS						
Hadware	Laptop	☐	Desktop	☐	Otros:	
	Celular	☐	Impresora	☐		
Software	Windows 8	☐	Windows 10	☐	Otros:	
	Office 2013	☐	Office 2016	☐	Otros:	
	Antivirus kaspersky	☐	Antivirus Nod 32	☐	Otros:	
	Otros programas:					
Servicios que utiliza en la red	Internet	☐	Impresora de red	☐	Otros:	
	Carpeta compartida	☐	Base de datos	☐	Otros:	
	ERP	☐	Intranet	☐	Otros:	

Dimensión: Confidencialidad

Indicador	Item	Criterios para medir indicador	Bajo(%) <1-25>	Regular(%) <26-50>	Alto(%) <51-75>	Muy alto(%) <76-100>	Promedio (%)
Nivel de Políticas de Seguridad	1	Restricción para navegar por internet					
	2	Complejidad de las contraseñas de los equipos que almacena información (laptop, pc, etc.)					
	3	Políticas de seguridad para resguardar la información (control de acceso, filtrado web, etc.)					
Nivel de confidencialidad de los datos	4	La información es clasificado según el nivel de criticidad					
	5	El acceso a la información compartida es solo para personal que lo requiere					
	6	Nivel de confidencialidad de la información que se encuentra dentro de la red local					

Dimensión: Integridad

Indicador	Item	Criterios para medir indicador	Bajo(%) <1-25>	Regular(%) <26-50>	Alto(%) <51-75>	Muy alto(%) <76-100>	Promedio (%)
Nivel de riesgo de los datos	7	La información se encuentra expuesto (vulnerable) en su estación de trabajo					
	8	La información se encuentra expuesto (vulnerable) dentro de la red local					
Manipulación de datos	9	Cambios no autorizados de la información (modificar o eleminar la información)					
	10	Nivel de riesgo de los datos en la red					

Dimensión: Disponibilidad

Indicador	Item	Criterios para medir indicador	Bajo(%) <1-25>	Regular(%) <26-50>	Alto(%) <51-75>	Muy alto(%) <76-100>	Promedio (%)
Nivel de disponibilidad de los datos	11	Dentro de la red local, la información se encuentra disponible cuando se requiere					
	12	Fuera de la red local, disponibilidad de la información entre sedes					
	13	Servicios que se brinda en la red (internet, correo electrónico, etc.)					

OBSERVACIONES:

	USUARIO	Personal de TI
Nombre		
Cargo		
Fecha / Hora		
Firma		

FICHA DE OBSERVACIÓN

UCV UNIVERSIDAD CÉSAR VALLEJO

"Implementación de un Servidor LINUX y su influencia en la seguridad perimetral de la red local de la empresa Junefield Group S.A."

Ficha de Observación (Post – Test): Variable Dependiente – Seguridad Perimetral
Esta ficha de observación evalúa la mejora de seguridad perimetral de la red local de la empresa Junefield Group S.A. (cuantitativamente)

DETALLES DE EQUIPOS Y APLICACIONES UTILIZADOS					
Hadware	Laptop	☐	Desktop	☐	Otros:
	Celular	☐	Impresora	☐	
Software	Windows 8	☐	Windows 10	☐	Otros:
	Office 2013	☐	Office 2016	☐	Otros:
	Antivirus kaspersky	☐	Antivirus Nod 32	☐	Otros:
	Otros programas:				
Servicios que utiliza en la red	Internet	☐	Impresora de red	☐	Otros:
	Carpeta compartida	☐	Base de datos	☐	Otros:
	ERP	☐	Intranet	☐	Otros:

Dimensión: Confidencialidad

Indicador	Item	Criterios para medir indicador	Bajo(%) <1-25>	Regular(%) <26-50>	Alto(%) <51-75>	Muy alto(%) <76-100>	Promedio (%)
Nivel de Políticas de Seguridad	1	Restricción para navegar por internet					
	2	Complejidad de las contraseñas de los equipos que almacena información (laptop, pc, etc.)					
	3	Políticas de seguridad para resguardar la información (control de acceso, filtrado web, etc.)					
Nivel de confidencialidad de los datos	4	La información es clasificado según el nivel de criticidad					
	5	El acceso a la información compartida es solo para personal que lo requiere					
	6	Nivel de confidencialidad de la información que se encuentra dentro de la red local					

Dimensión: Integridad

Indicador	Item	Criterios para medir indicador	Bajo(%) <1-25>	Regular(%) <26-50>	Alto(%) <51-75>	Muy alto(%) <76-100>	Promedio (%)
Nivel de riesgo de los datos	7	La información se encuentra expuesto (vulnerable) en su estación de trabajo					
	8	La información se encuentra expuesto (vulnerable) dentro de la red local					
Manipulación de datos	9	Cambios no autorizados de la información (modificar o eleminar la información)					
	10	Nivel de riesgo de los datos en la red					

Dimensión: Disponibilidad

Indicador	Item	Criterios para medir indicador	Bajo(%) <1-25>	Regular(%) <26-50>	Alto(%) <51-75>	Muy alto(%) <76-100>	Promedio (%)
Nivel de disponibilidad de los datos	11	Dentro de la red local, la información se encuentra disponible cuando se requiere					
	12	Fuera de la red local, disponibilidad de la información entre sedes					
	13	Servicios que se brinda en la red (internet, correo electrónico, etc.)					

OBSERVACIONES:

	USUARIO	Personal de TI
Nombre		
Cargo		
Fecha / Hora		
Firma		

Figura 52. Ficha de observación – Post-test

"Implementación de un Servidor Linux y su influencia en la seguridad perimetral de la red local de la empresa Junefield Group S.A., Lima 2017"

Escala de medición Pre-test: **1. Bajo <1%-25%>** **2. Tolerable <26%-50%>** **3. Alto <51%-75%>** **4. Muy alto <76%-100%>**												
Dimensiones	**Indicadores**	**MUESTRA**										
		M1	**M2**	**M3**	**M4**	**M5**	**M6**	**M7**	**M8**	**M9**	**M10**	**M11**
Confidencialidad	Nivel de políticas de seguridad	27	28.33	37	40	30	40	37	40	30	30	22
	Nivel de confidencialidad de los datos	17	37	37	58.3	10	47	27	37	27	47	43.3
Integridad	Nivel de riesgo de los datos	75	72.5	70	55	70	65	70	65	70	70	77.5
	Manipulación de datos	80	60	70	50	90	50	75	70	75	50	60
Disponibilidad	Nivel de disponibilidad de los datos	90	92	88.3	92	92	88.3	87	87	90	90	93

Escala de medición Post-Test: **1. Bajo <1%-25%>** **2. Tolerable <26%-50%>** **3. Alto <51%-75%>** **4. Muy alto <76%-100%>**												
Dimensiones	**Indicadores**	**MUESTRA**										
		M1	**M2**	**M3**	**M4**	**M5**	**M6**	**M7**	**M8**	**M9**	**M10**	**M11**
Confidencialidad	Nivel de políticas de seguridad	89.3	89	93.3	95	82	91	97	92	91	88.3	93.3
	Nivel de confidencialidad de los datos	94	95	96	97	96	96.3	97	94	96	96.3	95
Integridad	Nivel de riesgo de los datos	15	14	9	10	15	12.5	3.5	10	12.5	15	7.5
	Manipulación de datos	4	5	6	4	3	3	2.5	6	4	3	5

Disponibilidad	Nivel de disponibilidad de los datos	96	92	96	95	94	96	95	95	93.3	92.3	96.3

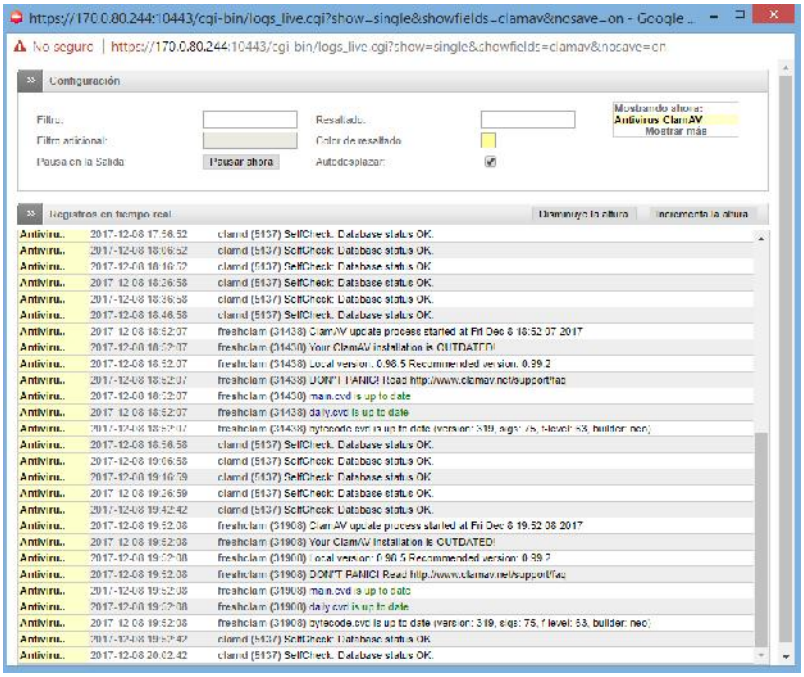


Figura 53. Registro de eventos de antivirus ClamAV

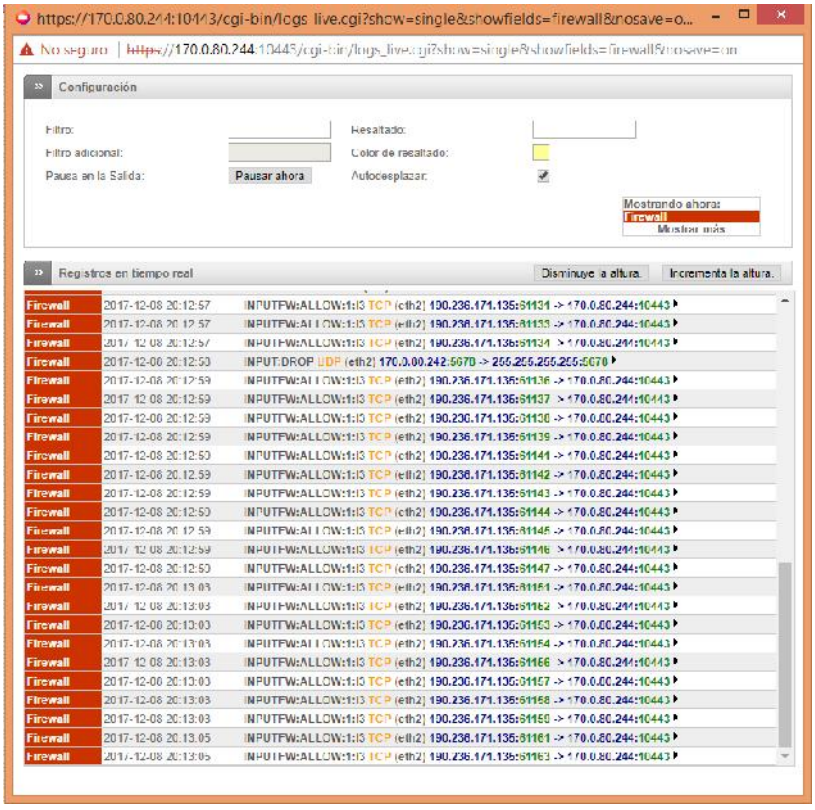


Figura 54. Registro de eventos de firewall

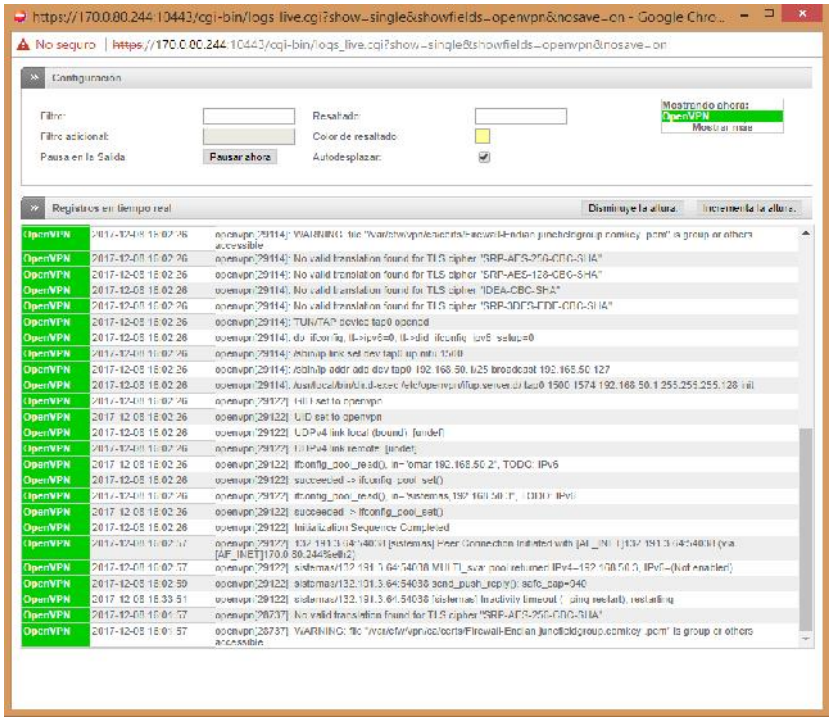


Figura 55. Registro de eventos Open VPN

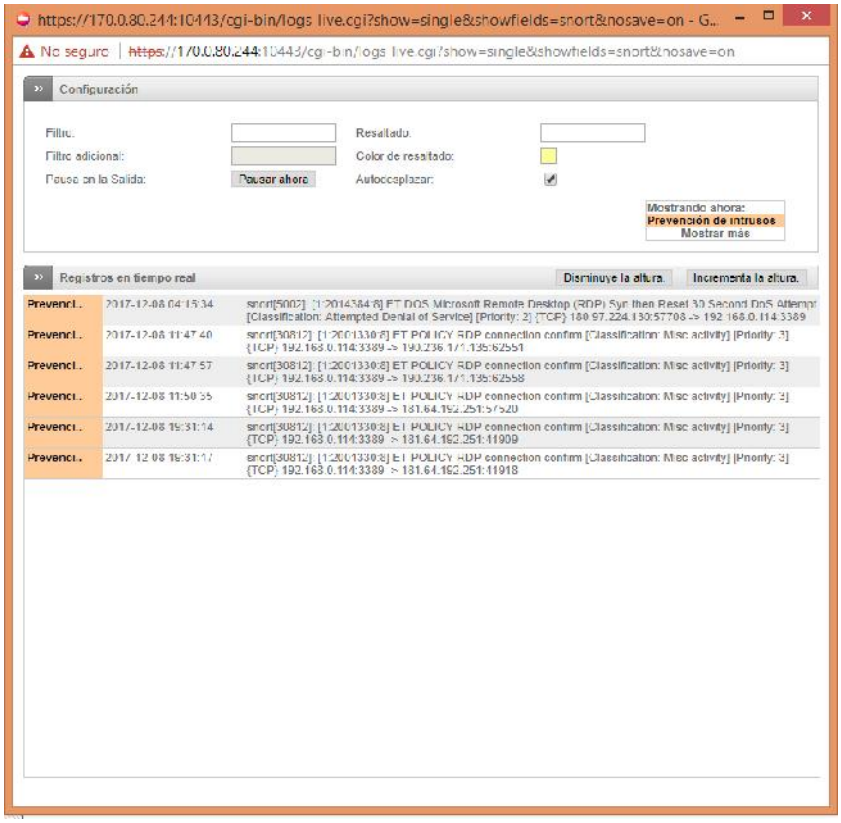


Figura 56. Registro de eventos de IPS

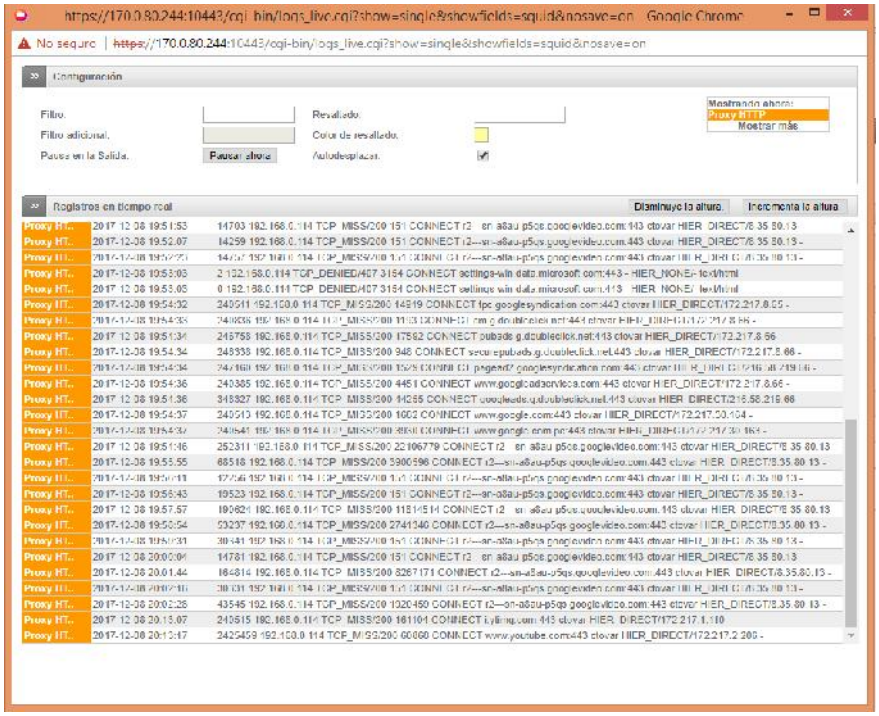


Figura 57. Registro de eventos de filtrado HTTS

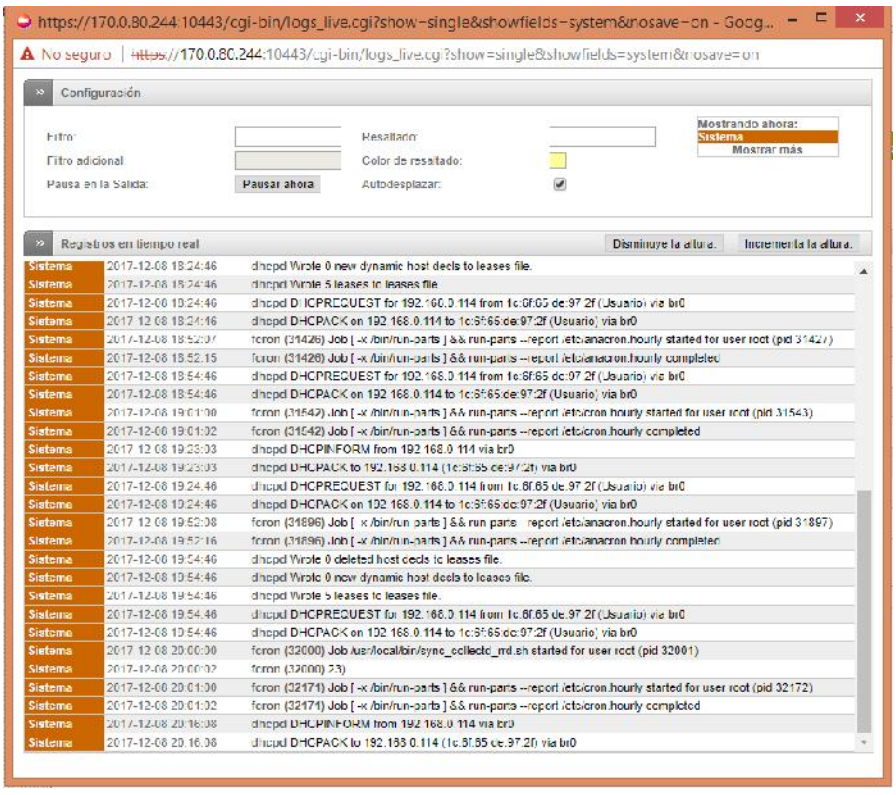


Figura 58. Registro de eventos de sistema

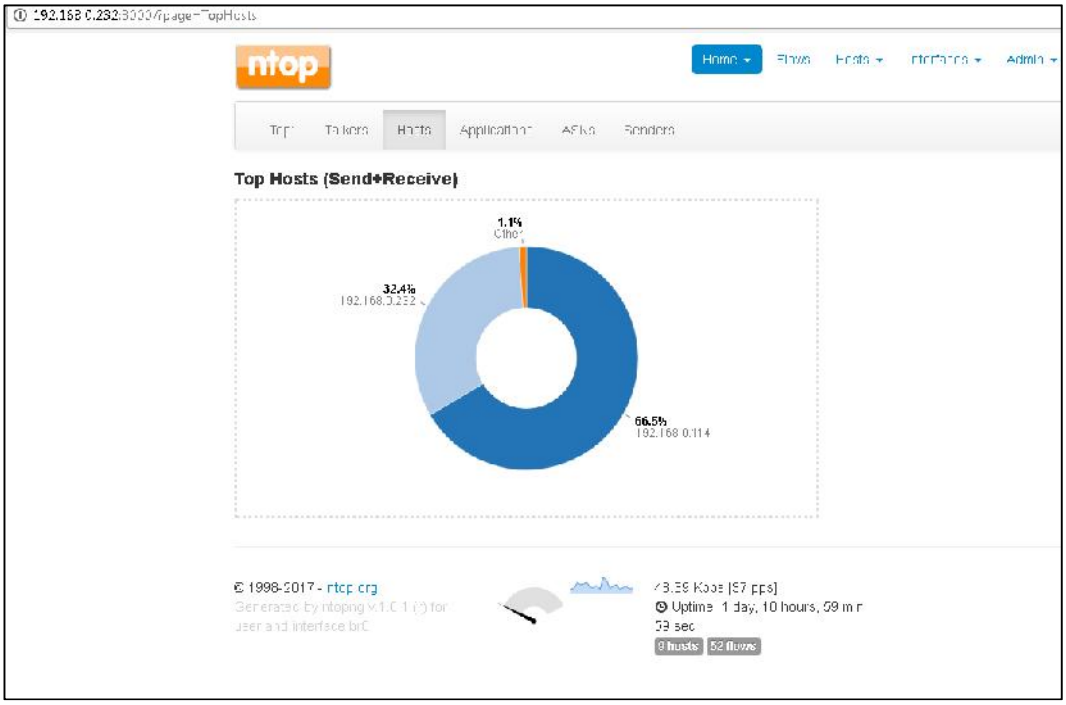


Figura 59. Registro de eventos por host

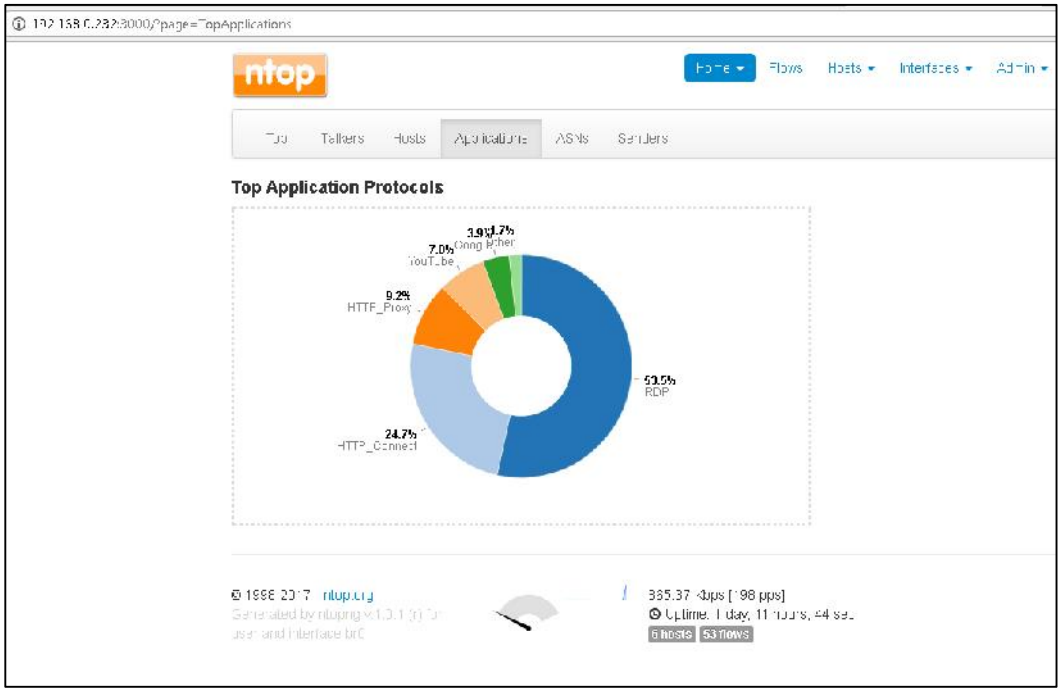


Figura 60. Registro de eventos por aplicaciones

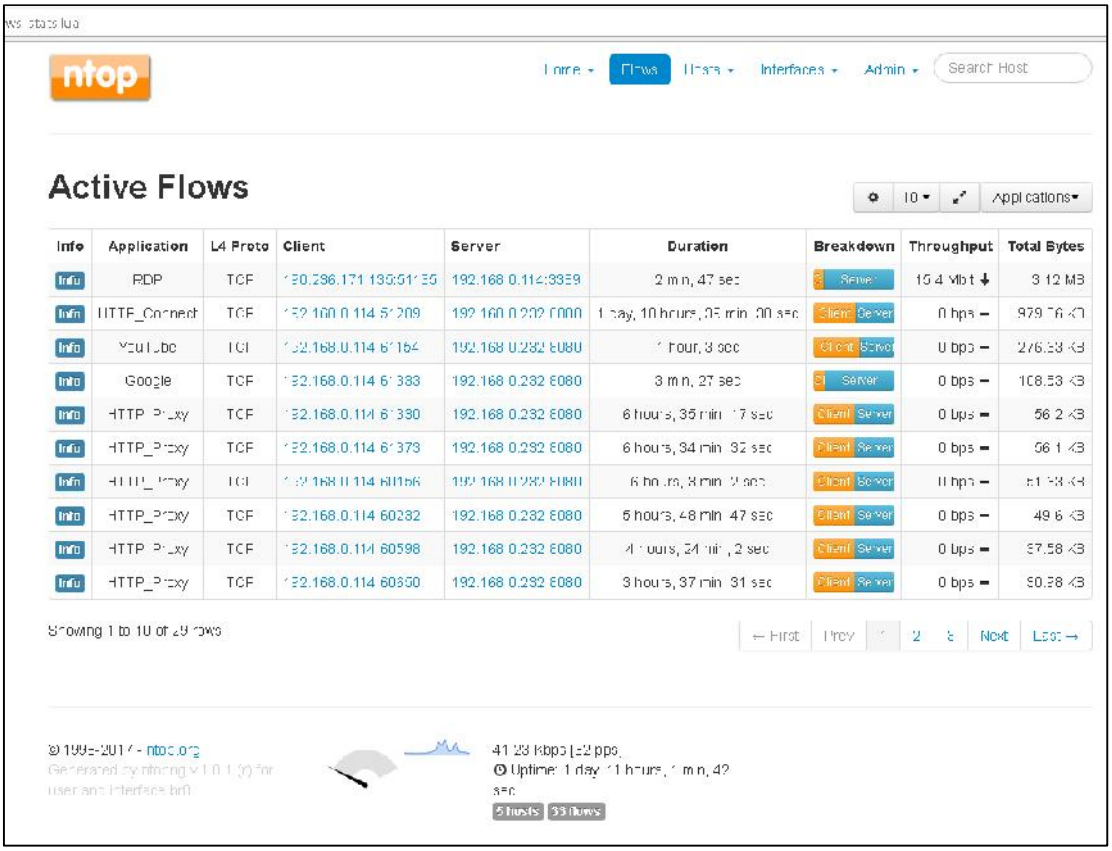


Figura 61. Registro de eventos netflow

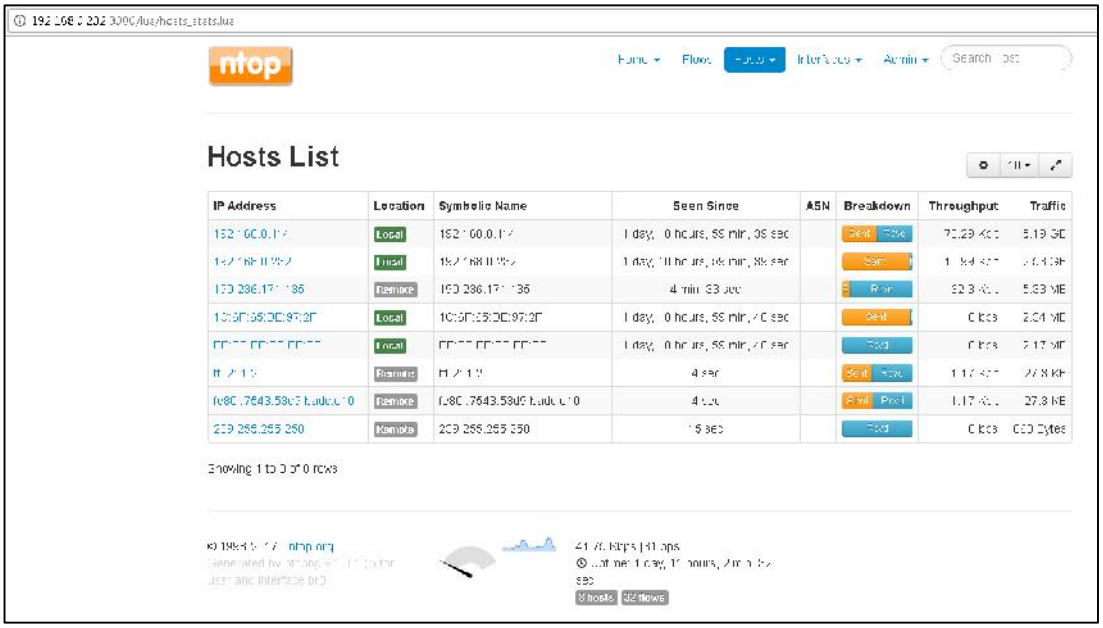


Figura 62. Registro de eventos por lista de host

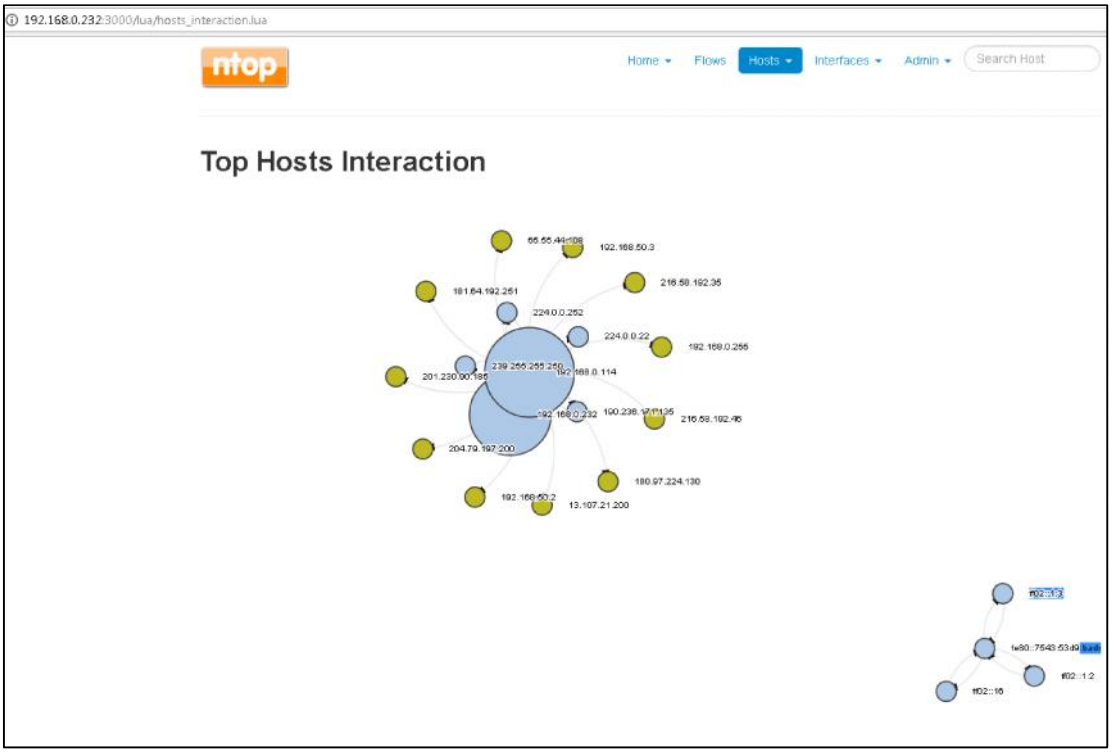


Figura 63. Registro de eventos por interacción de host

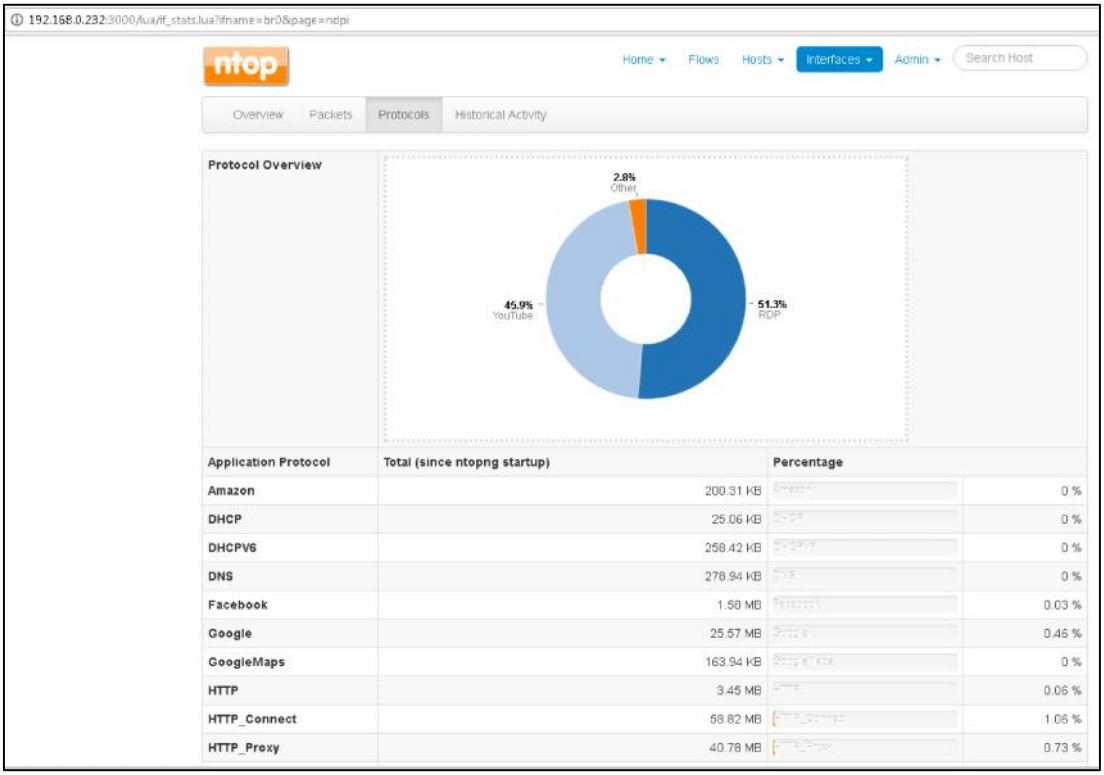


Figura 64. Registro de eventos por protocolo

Anexo VIII. Productos y características de firewall Endian

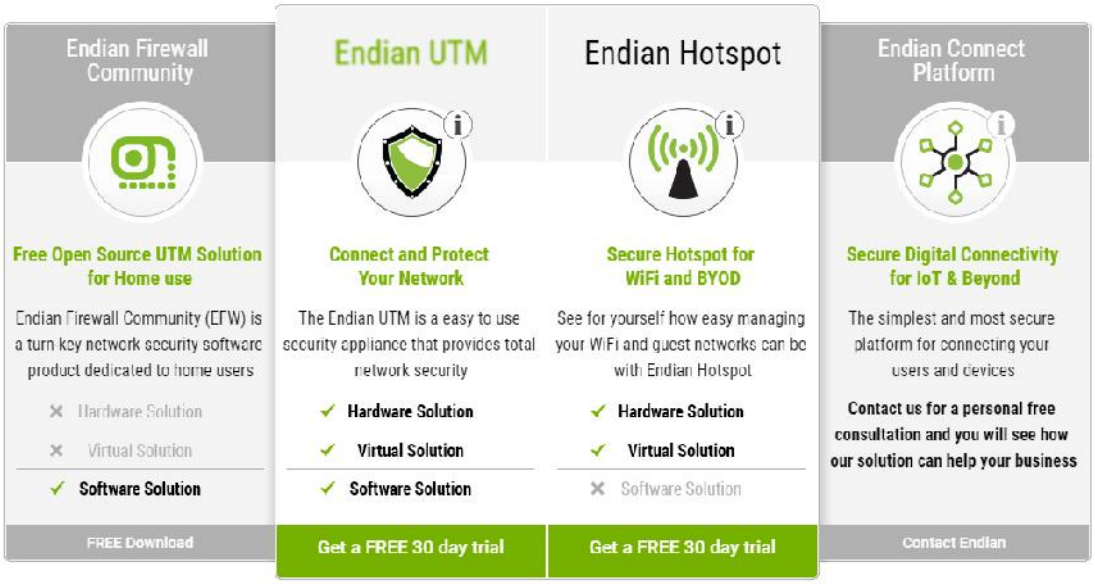


Figura 65. Soluciones disponibles Endian

*Figura 66. C*omunidad Endian (software libre). Endian UTM

General	Comunidad EFW	Dispositivo virtual	Dispositivo de software	Dispositivo de hardware
				
Licencia de código abierto (GPL)	Sí	Sí	Sí	Sí
Opciones de soporte comercial	No	Sí	Sí	Sí
Compatibilidad con el sistema de tickets	No	Sí	Sí	Sí
Asistencia directa de Endian	No	Opcional	Opcional	Opcional
Soporte telefónico	No	Opcional	Opcional	Opcional
Soporte en vivo / remoto (manos en mano)	No	Opcional	Opcional	Opcional
Reemplazo instantáneo de hardware	No	N / A	N / A	Opcional
Hardware de grado industrial	No	N / A	N / A	Sí
Soporte DynDNS	Sí	Sí	Sí	Sí

Figura 67. Características principales de los productos firewall Endian

Anexo IX. Costos de implementación de Linux Red Hat para seguridad perimetral

perúLiNUX

LA MEJOR ALTERNATIVA EN AHORROS DE LICENCIAS

Propuesta Seguridad Perimetral

Fecha: 22-12-2017

Datos del Cliente:

Señores: JUNEFIELD GROUP S.A
RUC:
Atención: Sr. Omar Bautista -
Correo: omarbp39@gmail.com
Teléfono: 948293399
Dirección: AV. REPUBLICA DE PANAMA NRO. 3545 DPTO. 1301 INT. A URB. LIMATAMBO LIMA - LIMA - SAN ISIDRO

Mediante la presente y de acuerdo a su solicitud hacemos llegar nuestra propuesta económica respecto a:

N°	CÓDIGO	CANT.	DESCRIPCIÓN	P. UNIT	P. TOTAL
1		1.00	**SERVICIO DE INSTALACION DE UN FIREWALL LINUX PFSENSE** INCLUYE: - Instalación de un Firewall con Pfsense. - Instalación del Certificado Digital. - Configuración del Servicio Proxy Server, Control de Navegación. - Configuración del Balanceo de Carga de Internet. - Configuración del Servicio Multiwan Gestor de 2 Proveedores de Internet. - Configuración Calidad de Servicio QoS, Reportes de Navegación por usuario, Via Web. - Habilitar la Red DMZ para servidores publicos. - Configuración del Forwarding, Nat, Routeos entre otras políticas de trabajo. - Capacitación Administrativa de 3 Hrs.	800.00	800.00
2	RH00004	1.00	**RED HAT ENTERPRISE LINUX SERVER, STANDARD (PHYSICAL OR VIRTUAL NODES) – 01 AÑO.** • Soporte Web y Telefónico RED HAT 8x5. Tiempo de respuesta 1 hora para casos críticos. • Actualización y Mantenimiento de Software vía Red Hat Network. Servicio de instalación y configuración Soporte 8x5	880.00	880.00
3		1.00	**SERVIDOR LENOVO THINKSERVER TS150** CARACTERISTICAS : Modelo Thinkserver TS150 Número de Parte: 70LU0013LD Procesador (GHZ) Intel Xeon E3-1245 v5 3.5GHz 4 Cores 8MB (80W) // Solo soporta 1 procesador Memoria: 8 Gb DDR4 2133 MHz; 4 ranuras DIMM // Máximo hasta 64GB Disco Duro (GB) 2TB 7.2K SATA CD-ROM DVD-RW Incorpora Video Intel HD Graphics RED 1 puerto RJ-45 GbE compartido para administraci□n Puertos Posterior: Serial (ES) : 1 RJ-45:1 - DB-15: 1 - USB 6 -Frontal: USB 2 Factor de Forma: Torre 4U Voltaje de Alimentación: Potencia de la Fuente (W) 250	1,073.83	1,073.83

SUBTOTAL:	2,753.83
DESCUENTO	
IGV (18%):	495.69
TOTAL (USD):	**3,249.52**

Términos y condiciones:

1. Garantía: 12 Meses.

AV. ARENALES 1912 - OFICINA 805 - LINCE | CENTRAL PBX (01) - 640-5800
VENTAS@PERULINUX.PE - WWW.PERULINUX.PE

Figura 68. Costo de servidor Red Hat para seguridad perimetral

Anexo X. Suscripción de licencia de Linux de Red Hat para seguridad perimetral

○ Premium (1 año)

COMPLEMENTOS

Elija los complementos para su (s) suscripción (es).

- ☐ Gestión inteligente
- ☐ Alta disponibilidad
- ☐ Almacenamiento Resilient
- ☐ Soporte extendido de actualizaciones

Order summary

Servidor Red Hat Enterprise Linux, Estándar (Nodos físicos o virtuales)
RH00004

Cantidad	Precio	Linea total
1	US $ 799	US $ 799

Subtotal: US $ 799

Anexo XI. Ventajas de la suscripción de la licencia de Linux Red Hat

redhat.

MODELO DE SUSCRIPCIÓN A RED HAT

Una suscripción a Red Hat

¿Qué es?

Para mantener una infraestructura de aplicaciones que cumpla con las exigencias de su organización que están en continuo proceso de expansión, necesita mucho más que un simple contrato de mantenimiento y soporte. Necesita una plataforma para empresas certificada, escalable y fiable. Además, necesita una relación de auténtica colaboración con su proveedor de tecnología.

Eso es exactamente lo que le ofrece su suscripción a Red Hat.

Sólida plataforma para empresas

La organización de ingeniería de Red Hat, reconocida a escala mundial, trabaja estrechamente con la comunidad de código abierto y con nuestros ingenieros para crear y probar soluciones innovadoras de tecnología capaces de proporcionar un nivel de disponibilidad, seguridad y escalabilidad sin precedentes.

Liderazgo en la comunidad

Red Hat es el colaborador comercial líder del kernel de Linux®, la comunidad de JBoss e innumerables proyectos de código abierto. Red Hat es el proveedor de código abierto líder del sector. Por ello, su suscripción le permite aprovechar nuestro compromiso e influencia.

Colaboración con el sector de TI

Red Hat mantiene relaciones con miles de proveedores de software independientes (ISV) y proveedores de hardware independientes (IHV). A través de estas relaciones, combinamos innovación del sector y de la comunidad con productos de la plataforma para empresas de Red Hat. El objetivo es brindarle soluciones sólidas en las que su empresa puede confiar en uno de los ecosistemas de certificación de tecnología más grandes del mundo.

Nuestra relación mutua

Su suscripción a Red Hat no solo le ofrece acceso a software y actualizaciones de gran calidad, sino que además le permite obtener información y servicios de soporte que abarcan toda la arquitectura, ciclo de vida e infraestructura de las aplicaciones. Le animamos a ponerse en contacto con nosotros para aprovechar al máximo nuestra experiencia en todas las etapas de planificación, verificación, implementación, mantenimiento y ampliación de la infraestructura o de las aplicaciones.

Más información

Documento técnico sobre el valor de una suscripción a Red Hat [PDF]
Guía de suscripción de Red Hat JBoss Middleware [PDF]
Preguntas más frecuentes sobre la renovación de la suscripción a Red Hat [PDF]

redhat.

MODELO DE SUSCRIPCIÓN A RED HAT

Una suscripción a Red Hat

Beneficios

Suscripciones a Red Hat, más que un simple servicio de soporte de gran calidad

Con una suscripción a Red Hat, dispondrá de acceso a la orientación, conocimientos y experiencia de Red Hat, lo que le permitirá centrarse en la creación de valor para su empresa. Podrá aprovechar la capacidad de Red Hat para trabajar con la comunidad del código abierto en la creación de una plataforma empresarial estable que se adapte a las necesidades de su organización. Todas las suscripciones a Red Hat ® incluyen lo siguiente:

Software empresarial

Su suscripción a Red Hat le brinda acceso continuo al software de Red Hat creado, probado y certificado por Red Hat y sus partners. Con una suscripción a Red Hat, dispondrá de acceso a todas las versiones compatibles en formato binario como fuente, además de toda la documentación de los productos para empresas. Actualizaciones de seguridad y corrección de errores.

Flexibilidad

Las suscripciones de Red Hat no están vinculadas a una versión específica. Con una suscripción a Red Hat puede actualizar el sistema instalando cualquier versión compatible del software de Red Hat y utilizarla fácilmente en servidores físicos, virtuales o basados en nube.

Gran seguridad

Mantenga la seguridad de sus sistemas gracias a nuestro equipo de respuesta de seguridad líder del mercado. Este equipo trabaja con nuestros clientes, partners, grupos de vigilancia de seguridad y la comunidad global de código abierto para identificar vulnerabilidades de seguridad. Hasta la fecha, ha solucionado más del 98 % de las vulnerabilidades críticas en el plazo de un día natural a partir de la identificación del problema. Obtenga más información sobre la gran seguridad que ofrece Red Hat.

Certificaciones de hardware y software

Red Hat mantiene relación con miles de proveedores de software y hardware para certificar el rendimiento de las aplicaciones de software de Red Hat y JBoss® de las que depende su empresa. Gracias a Red Hat, obtendrá acceso a uno de los ecosistemas de certificación de tecnología de mayor envergadura en el mundo, con más de 4000 certificaciones de productos hasta la fecha y más incorporaciones cada día. Ningún derivado de la tecnología de Red Hat disfruta de estas certificaciones y soporte de terceros. Obtenga más información sobre las certificaciones de productos de Red Hat.

Soporte para producción y desarrollo

Obtenga acceso al servicio de soporte técnico de Red Hat de manera ininterrumpida en todo el mundo. Red Hat no solicita a los clientes que reproduzcan ni justifiquen un problema para recibir soporte técnico. Puede tener la seguridad de que un ingeniero del servicio de soporte de Red Hat comprenderá rápidamente el problema. Obtenga más información sobre el servicio de soporte de Red Hat.

A través del galardonado Red Hat Customer Portal, obtendrá acceso integrado a todas las características de su suscripción:

- Acceda a la completa base de conocimiento de Red Hat.
- Busque casos prácticos y arquitecturas de referencia para aprovechar al máximo sus soluciones de Red Hat.
- Gestione sus suscripciones.
- Establezca contacto con Red Hat y nuestros partners.

Estabilidad

Reduzca los costos al adquirir una única plataforma estable, estándar y desarrollada por el proveedor de código abierto líder en la industria.

redhat.

MODELO DE SUSCRIPCIÓN A RED HAT

Una suscripción a Red Hat

Cómo funciona

Adquiera y mantenga las suscripciones más adecuadas para su entorno de Red Hat

Su suscripción le permitirá disfrutar de las soluciones empresariales de código abierto empresarial de Red Hat y cualquier aplicación que precise para utilizarlas de forma eficaz. Las suscripciones a Red Hat® funcionan sin licencias de acceso de cliente. Sin límites en cuanto al número de incidencias atendidas. Sin costos de actualización no presupuestados. Sin cargos ocultos.

¿Cómo se clasifican las suscripciones a Red Hat?

Los productos de Red Hat se distribuyen bajo suscripción por instancia o por instalación, lo que le permite acceder a todas las ventajas de la suscripción durante su periodo de vigencia. Aquí se incluye el acceso a las siguientes ventajas de Red Hat:

- Software
- Novedades
- Actualizaciones
- Soporte técnico
- Correcciones de seguridad
- Base de conocimiento
- Programa Open Source Assurance
- Soluciones probadas y listas para empresas

¿Qué suscripciones a Red Hat debo mantener?

Las suscripciones a Red Hat proporcionan un valor continuo, gracias a la fiabilidad y disponibilidad del servicio de soporte técnico y de mantenimiento de software, sus certificaciones y el programa Open Source Assurance.

Algunos recursos necesitarán recurrir a más ventajas que otros, por lo que Red Hat calcula el valor total de las suscripciones contando el número de instancias o instalaciones del software de Red Hat que utiliza. Mientras cuente con alguna suscripción a un producto de Red Hat, deberá mantener una suscripción por cada instancia o instalación del software de Red Hat que utilice en su entorno.

¿Cómo se determina el tamaño de la suscripción de Red Hat JBoss Middleware?

Las suscripciones a los productos de Red Hat JBoss® Middleware se ofrecen en un modelo de fácil virtualización, consumido en incrementos de 16 o 64 bandas centrales del procesador, y respaldado por una amplia selección de niveles de servicios para empresas que admiten todo tipo de implementación esencial.

Algunas de las características claves del modelo de consumo de Red Hat JBoss Middleware:

- Los núcleos de procesadores pueden ser virtuales o físicos, lo que los convierte en la opción ideal para la tendencia generalizada de virtualizar las cargas de trabajo de middleware.
- Como cliente, podrá elegir el tipo de núcleo de procesador que mejor se adapte a su entorno. Los núcleos de procesadores se tratan por igual, independientemente de su tipo.
- El soporte técnico abarca todos los problemas que pueden surgir durante todo el ciclo de vida de la aplicación, desde el desarrollo a la administración de implementaciones y en cualquier entorno compatible.
- Una suscripción a cualquier producto individual de Red Hat JBoss Middleware incluye el uso como desarrollador de todos los productos de la cartera de Red Hat JBoss Middleware.
- Obtenga más información sobre cómo ajustar el tamaño de su entorno de Red Hat JBoss Middleware

¿Quién puede proporcionarme el software de Red Hat?

Solo Red Hat y sus partners comerciales autorizados pueden brindarle acceso al software probado y certificado para empresas de Red Hat. Este acceso se proporciona a través de suscripciones, disponibles directamente a través de Red Hat o de un partner empresarial de Red Hat autorizado.

¿Cómo puedo aprovechar las ventajas de las suscripciones a Red Hat?

Puede adquirir una suscripción a Red Hat y disfrutar de todas sus ventajas (incluido el acceso al software) directamente a través de Red Hat o de un socio comercial de Red Hat autorizado.

Red Hat también trabaja con miles de integradores de sistemas (SI), proveedores de software independientes (ISV) y socios proveedores de hardware independientes (IHV) para crear, optimizar, vender y ofrecer soluciones completas a nuestros clientes. Algunos de estos partners, entre ellos, los fabricantes de equipos originales (OEM, por sus siglas en inglés) que estén autorizados, le podrán brindar soporte técnico.

Estos socios y sus clientes pueden confiar en su relación con Red Hat para aprovechar la tecnología más reciente de Red Hat y la experiencia del proveedor líder de código abierto de la industria.

¿Qué ocurre cuando se termina mi suscripción?

Para seguir beneficiándose de las suscripciones a Red Hat, debe renovarlas de manera que todas las instancias e instalaciones de software de Red Hat conserven una suscripción activa.

Si deja que caduquen todas las suscripciones y no cuenta con más suscripciones activas en su empresa, puede seguir utilizando el software, pero el entorno dejará de beneficiarse de las ventajas de la suscripción como, por ejemplo:

- Las últimas versiones de software certificado.
- Parches de seguridad y corrección de errores.
- Soporte técnico de Red Hat.
- Acceso al galardonado Portal de clientes.
- Garantía de código abierto de Red Hat.

Anexo XII. Acta de aprobación de originalidad de tesis

UCV UNIVERSIDAD CÉSAR VALLEJO	ACTA DE APROBACIÓN DE ORIGINALIDAD DE TESIS	Código : F06-PP-PR-02.02 Versión : 09 Fecha : 23-03-2018 Página : 1 de 1

Yo, **FRANCISCO MANUEL HILARIO FALCON,** docente de la Facultad de Ingeniería y carrera Profesional de Ingeniería Sistemas de la Universidad César Vallejo campus Lima Este, revisor (a) de la tesis titulada:

"IMPLEMENTACIÓN DE UN SERVIDOR LINUX Y SU INFLUENCIA EN LA SEGURIDAD PERIMETRAL DE LA RED LOCAL DE LA EMPRESA JUNEFIELD GROUP S.A., LIMA 2017", del estudiante **OMAR IVO BAUTISTA PILLACA,** constato que la investigación tiene un índice de similitud de **28** % verificable en el reporte de originalidad del programa Turnitin.

El/la suscrito(a) analizó dicho reporte y concluyó que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

San Juan de Lurigancho, 19 de diciembre del 2017

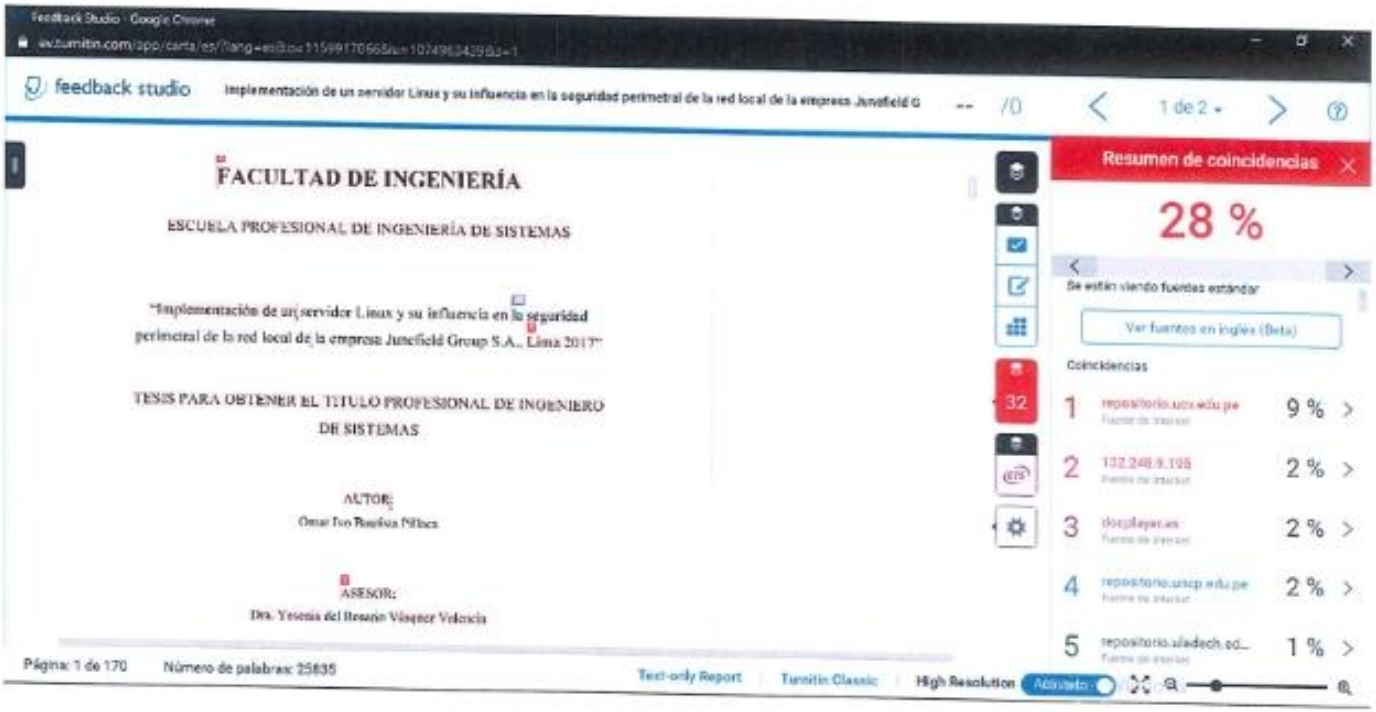
.....

FRANCISCO MANUEL HILARIO FALCON

DNI: 10132075

Elaboró	Dirección de Investigación	Revisó	Responsable del SGC	Aprobó	Vicedirectora de la Investigación

Pantallazo del Turnitin:



Anexo XIII. Autorización de publicación de tesis

UCV UNIVERSIDAD CÉSAR VALLEJO	AUTORIZACIÓN DE PUBLICACIÓN DE TESIS EN REPOSITORIO INSTITUCIONAL UCV	Código : F08-PP-PR-02.02 Versión : 09 Fecha : 23-03-2018 Página : 1 de 1

Yo **BAUTISTA PILLACA OMAR IVO**, identificado con DNI Nº **41868746**, egresado(a) de la Carrera Profesional de Ingeniería Sistemas de la Universidad César Vallejo, autorizo (**X**), no autorizo ( ) la divulgación y comunicación pública de mi trabajo de investigación titulado **"IMPLEMENTACIÓN DE UN SERVIDOR LINUX Y SU INFLUENCIA EN LA SEGURIDAD PERIMETRAL DE LA RED LOCAL DE LA EMPRESA JUNEFIELD GROUP S.A., LIMA 2017".** en el Repositorio Institucional de la UCV (http://repositorio.ucv.edu.pe/), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art. 23 y Art. 33

Fundamentación en caso de no autorización:

.....
.....
.....
.....
.....
.....
.....
.....

.....
OMAR IVO BAUTISTA PILLACA

DNI: **41868746**

Fecha: 19 de diciembre del 2017

Elaboró	Dirección de Investigación	Revisó	Responsable del SGC		Vicerrectorado de Investigación

Anexo XIV. Autorización de la versión final del trabajo de investigación

UNIVERSIDAD CÉSAR VALLEJO

AUTORIZACIÓN DE LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN

CONSTE POR EL PRESENTE EL VISTO BUENO QUE OTORGA EL ENCARGADO DE INVESTIGACIÓN DE

RIVERA CRISOSTOMO RENEE

A LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN QUE PRESENTA:

BAUTISTA PILLACA OMAR IVO

INFORME TÍTULADO:

"IMPLEMENTACIÓN DE UN SERVIDOR LINUX Y SU INFLUENCIA EN LA SEGURIDAD PERIMETRAL DE LA RED LOCAL DE LA EMPRESA JUNEFIELD GROUP S.A., LIMA 2017"

PARA OBTENER EL TÍTULO O GRADO DE:

INGENIERO DE SISTEMAS

SUSTENTADO EN FECHA: **19 DE DICIEMBRE DEL 2017**

NOTA O MENCIÓN: **(11) (ONCE).**

UNIVERSIDAD CÉSAR VALLEJO UCV LIMA - ESTE

RIVERA CRISOSTOMO RENEE