UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO

Facultad de Ingeniería

Escuela Profesional de Ingeniería Informática y de Sistemas

IMPLEMENTACIÓN DE FIREWALL ENDIAN COMUNITY PARA GESTIONAR LA SEGURIDAD PERIMETRAL EN LAS MYPES DE LA CIUDAD DE CAJAMARCA: CASO IMBYTE SOLUCIONES

Presentado por:

Bach. Chuquimango Mori, Jefferson Smith

Bach. Valera Cueva Arturo David

Asesor:

Dra. Ing. Diana Jakelin Cruzado Vásquez.

Cajamarca – Perú

2022

UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO

Facultad de Ingeniería

Escuela Profesional de Ingeniería Informática y de Sistemas

IMPLEMENTACIÓN DE FIREWALL ENDIAN COMUNITY PARA GESTIONAR LA SEGURIDAD PERIMETRAL EN LAS MYPES DE LA CIUDAD DE CAJAMARCA: CASO IMBYTE SOLUCIONES

Tesis presentada en cumplimiento parcial de los requerimientos para optar por el título profesional de ingeniero informático y de sistemas

Presentado por:

Bach. Chuquimango Mori, Jefferson Smith

Bach. Valera Cueva, Arturo David

Asesor:

Dra. Ing. Diana Jakelin Cruzado Vásquez.

Cajamarca – Perú

2022

UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO

FACULTAD DE INGENIERIA

CARRERA PROFESIONAL DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

APROBACIÓN DE TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO INFORMÁTICO Y DE SISTEMAS.

IMPLEMENTACIÓN DE FIREWALL ENDIAN COMUNITY PARA GESTIONAR LA SEGURIDAD PERIMETRAL EN LAS MYPES DE LA CIUDAD DE CAJAMARCA: CASO IMBYTE SOLUCIONES

Presidente: Dra. Luz Esther Chávez Toledo

Secretario: Dra. Lucía Milagros Esaine Suárez

Vocal: Dra. Diana Jakelin Cruzado Vásquez

Asesor: Dra. Diana Jakelin Cruzado Vásquez

DEDICATORIA

Este trabajo va dedicado principalmente a mis padres y a mi familia porque me han brindado todo el apoyo, tanto económico como también moral para seguir estudiando y lograr el objetivo trazado para un futuro mejor y ser el orgullo para ellos y de toda mi familia.

Arturo David Valera Cueva

Este trabajo va dedicado a Dios fuente de sabiduría y conocimiento, que ha sido mi guía en el proceso, también a mis padres y familia porque me han brindado todo el apoyo tanto económico como también moral para seguir estudiando y lograr el objetivo trazado para un futuro mejor y ser el orgullo para ellos y de toda mi familia.

Jefferson Smith Chuquimango Mori

AGRADECIMIENTO

A:

Nuestros maestros y asesora Dra. Ing. Diana Jakelin Cruzado Vásquez ya que siempre nos han guiado y apoyado durante toda la carrera, siempre han depositado su confianza en nosotros y su conocimiento en cada una de las enseñanzas que nos han brindado esto con el fin de desarrollarnos de la mejor manera posible en el ámbito profesional, así como en nuestra vida personal, agradecemos también a la UPAGU por permitirnos pertenecer a su casa de estudios.

RESUMEN

La presente investigación se llevó a cabo con la finalidad de identificar y evidenciar las principales virtudes y beneficios de la seguridad de la red perimetral en la modalidad de firewall en las MYPES o pequeñas empresas tomando como caso particular de esta investigación a la empresa Imbyte Soluciones, viendo las distintas perspectivas para las amenazas de seguridad, los grados de vulnerabilidad y la importancia de toda la información de cualquier entidad ya sea pública o privada, a través de la red de datos orientada por dispositivos de seguridad únicos y procesos que la empresa integra, son una parte elemental, ya que no solo corresponde a una herramienta de seguridad perimetral de este tipo , sino que también representa varios procesos de manera detallada y sistemática de diferentes ámbitos operacionales, además de modelos de desarrollo actuales mediante la implementación de un único sistema de seguridad y la protección de la red de datos cuidando el perímetro que esta abarca en la empresa. Así mismo brindar soluciones de seguridad estructuradas, estableciendo medidas como estabilidad, vigilancia, modelos de desarrollo y gestión altamente adecuada, perspicaz, metódica e intrínseca.

El presente estudio propuso una investigación de tipo aplicada – tecnológica de diseño Preexperimental de enfoque cuantitativo, la población estuvo conformada por 01 Gerente, 01 jefe administrativo, 01 jefe de sistemas, 07 colaboradores y la muestra fue conformada por 10 trabajadores, cuya unidad de análisis estuvo constituida por los 10 trabajadores, encargados de los procesos e información de la empresa Imbyte Soluciones de la ciudad de Cajamarca, para la recolección de

información, se utilizó la observación y como instrumentos de recolección de datos se utilizaron encuestas.

Se aplicaron cuestionarios pre y post implementación que nos permitieron recoger la información para validar y aceptar la hipótesis propuesta, con la aplicación de la prueba de normalidad de Shapiro-Wilk para determinar si los datos tienen distribución normal y el estadígrafo T-student obteniendo un valor de **0.001**.

Del análisis de los datos se logró observar resultados positivos como: la capacidad que tiene el firewall para proteger la red de datos, de los cuales 9 personas manifiestan que el firewall implementado no tiene la capacidad de proteger la red datos y 1 persona manifiesta que el firewall implementado si tiene la capacidad de proteger la red de datos. Del otro lado con la capacidad de protección del perímetro de la red datos las 10 personas encuestada nos dicen que el firewall implementado si cuenta con la capacidad de proteger el perímetro de la red de datos. De esta manera podemos concluir que la implementación de Firewall Endian comunity si influyo positivamente en la gestión de la seguridad perimetral en las MYPES de la ciudad de Cajamarca caso: Imbyte soluciones.

De acuerdo con los expertos de la empresa Imbyte Soluciones se concluyó que con la implementación del software propuesto se cumplió en su totalidad con la mejoría la seguridad perimetral de la red de la corporación. Así mismo, se tomó en cuenta los requerimientos de esta entidad. Además, se puede evidenciar que este elemento de seguridad informática permitió brindar mayor estabilidad y control a las amenazas de seguridad a la vez que contribuyo a la detección de vulnerabilidades no solo en la red de datos sino también en cada proceso que se realiza en la empresa.

Finalmente se evidencio la mejoría en el tráfico de la información que maneja Imbyte Soluciones, de este modo se cumplió con la protección de la red perimetral de la empresa. Mitigando posibles vulnerabilidades y brindando mayor seguridad a los servicios de red y de manejo de información, así como atención al cliente, que la entidad ofrece.

Palabras clave: Red perimetral, seguridad perimetral, amenaza de seguridad, detecciones vulnerables.

ABSTRACT

The present investigation was carried out with the purpose of identifying and demonstrating the main virtues and benefits of the security of the perimeter network in the form of firewall in the MYPES or small companies, taking as a particular case of this investigation the company Imbyte Soluciones, Seeing the different perspectives for security threats, the degrees of vulnerability and the importance of all the information of any entity, whether public or private, through the data network guided by unique security devices and processes that the company integrates, they are an elementary part, since it not only corresponds to the perimeter security tool as such, but to represent in detail and systematically different processes of different operational environments, as well as development models present through the implementation of a single security and protection system. of the data network taking care of the perimeter that it covers in the company. Likewise, provide structural security solutions and establish means of stability, surveillance, development models, highly adequate and insightful, organizational and essential control, among others.

The present study proposed an applied-technological research of e Pre-experimental design with a quantitative approach, the population was made up of 01 Manager, 01 administrative head, 01 head of systems, 07 collaborators and the sample was made up of 10 workers, whose unit The analysis was made up of the 10 workers, in charge of the processes and information of the company Imbyte Soluciones of the city of Cajamarca, for the collection of information, observation was taken and surveys were used as data collection instruments.

Pre- and post-implementation questionnaires were used to collect information to validate and accept the proposed hypothesis, with the application of the Shapiro-Wilk normality test to determine whether the data have a normal distribution and the student's t-statistic, obtaining a value of 0.001.

The analysis of the data showed positive results such as: the capacity of the firewall to protect the data network, of which 9 people said that the firewall implemented does not have the capacity to protect the data network and 1 person said that the firewall implemented does have the capacity to protect the data network. On the other hand, with regard to the capacity to protect the perimeter of the data network, the 10 people surveyed say that the firewall implemented does have the capacity to protect the perimeter of the data network. In this way we can conclude that the implementation of the Endian Community firewall did have a positive influence on the management of perimeter security in the MSEs in the city of Cajamarca, case: Imbyte Soluciones.

According to the experts of the company Imbyte Soluciones, it was concluded that the implementation of the proposed software was fully met with the improvement of the perimeter security of the company's network. Likewise, the requirements of this entity were taken into account. In addition, it can be shown that this element of computer security will provide greater stability and control to security threats while contributing to the detection of vulnerabilities not only in the data network but also in each process that is carried out in the company. Finally, the improvement in the information traffic handled by Imbyte Solucione was evidenced, in this way the protection of the company's perimeter network was fulfilled. Mitigating possible

vulnerabilities and providing greater security to the network and information management services, as well as to the client, that the entity offers.

Keywords: Perimeter network, perimeter security, security threat, vulnerable detections.

ÍNDICE

LISTA DE TABLAS

LISTA DE FIGURAS

IMPLEMENTACIÓN DE FIREWALL ENDIAN COMUNITY PARA GESTIONAR LA SEGURIDAD PERIMETRAL EN LAS MYPES DE LA CIUDAD DE CAJAMARCA: CASO IMBYTE SOLUCIONES

CAPITULO I: INTRODUCCIÓN

1.1. Planteamiento del problema

En la Actualidad las redes de datos en las entidades públicas y privadas han llegado a tener una mayor carga de tráfico de datos debido al uso de sistemas integrados, ERP'S, Bases de datos, Aplicaciones de gestión de datos o herramientas de gestión administrativa. Etc. Esto implica también tener una red que sea óptima y segura para controlar las diversas actividades que se realizan y llevan a cabo en estas entidades.

Como señala Vásquez (2018) "Se deben implantar controles de detección, prevención y recuperación para protegerse contra códigos maliciosos, junto con los procedimientos adecuados para concientizar a los usuarios "(pág. 210).

Uno de los principales problemas que presenta la empresa y que a la vez se considera un punto negativo es referente al manejo que dan los empleados a los equipos de computación y las tecnologías de información, algunos de los empleados visitaron varios sitios web que contenían información maliciosa y descargaron contenido o archivos multimedia, sin ser conscientes de los riesgos que estos suponían , resaltando la existencia de virus , troyanos correos electrónicos no deseados, Así que en incalculables hechos que se han dado dentro empresa, este tipo de virus no solo afecta a los equipos sino también provoca daños que afectan al rendimiento de los equipos, sino que también ponen en riesgo muy elevado la información que posee la empresa en cada uno de estos equipos, cabe precisar que dicha información es muy importante para la empresa y se debe tener en cuenta la seguridad de la información.

Haciendo un pequeño análisis de daños en los "dispositivos mencionados", considerando la infraestructura física, pero principalmente la lógica que tiene la empresa, es posible ver que su rendimiento ha disminuido provocando que el sistema se descomponga .Afectado al hardware y software gestionados por la empresa, identificando problemas con la funcionalidad de algunos programas , requiriendo reinstalación o incluso formateo de las computadoras afectadas perdiendo tiempo y reduciendo horas-hombre, productividad y costo para cada equipo.

El simple hecho de que descargue un archivo o programa a voluntad puede hacer que los virus infecten las computadoras y cause daños a esas computadoras. Por lo tanto, la empresa Imbyte Soluciones no cuenta con un control centralizado, ni motor antispam y filtros que brinden un mejor control a la hora de evitar riesgos informáticos

Es importante además mencionar que los controles de accesos de usuarios a la información importante son escasos, ya que la mayoría de veces se deja de lado los riesgos que se pueden originar si no se cumplen con la adopción de medidas de seguridad informática necesarias para controlar y mantener la eficiencia de los mismos, también de contrarrestar las vulnerabilidades, tener controles de accesos a la red, contar con controles físicos y lógicos que permitan evitar la actividad delictiva de las empresas tales como, la modificación de la información , robo de identidad , o la eliminación de la información , genera fundamentalmente la necesidad de buscar diversas opciones que permitan controlar la seguridad informática dentro de la red de datos de la empresa.

Se destaca además que existen usuarios que no cuentan con la experiencia necesaria en informática o seguridad de redes y esto puede ser incómodo o tedioso, generando la incomodidad al tener que gestionar las solicitudes y advertencias que dañan el dispositivo tales como: contenido publicitario, pornografía o sitios inseguros.

También hay que recalcar que el uso de controles de seguridad informática es sumamente importante para la organización por los procesos que se maneja, que son muy confidenciales y cuidadosos porque el negocio se hace por internet , con proveedores ,bancos, transacciones bancarias con esto en mente se tiene la posibilidad de que esta información sea vulnerable a atacantes modernos hoy conocidos como piratas informáticos, teniendo en cuenta la realidad en que vivimos y que los mismos acontecimientos tales como la pandemia por el COVID-19 han obligado a las empresas a aumentar de forma considerable el uso de internet y tecnologías de información para realizar sus actividades y procesos generando una brecha de inseguridad muy amplia, ya que a mayor uso de las tecnologías, mayor es el riesgo por consiguiente tiene que ser más alta la seguridad.

Teniendo en cuenta lo anterior , imbyte soluciones, no cuenta con firewalls , barreras o herramientas que pueda limitar o detener el tráfico no deseado o malicioso de los dispositivos infectados por lo que esta situación es irrelevante ya que se ha navegando por sitios web maliciosos , correos electrónicos que contienen virus o simplemente conectado un dispositivo USB , creando brechas de inseguridad y comprometiendo la integridad de la red e infraestructura de TI así como información corporativa importante.

1.2. Formulación del problema

¿De qué manera la implementación de firewall Endian Comunity influye sobre la gestión de seguridad en la empresa Imbyte Soluciones -Cajamarca?

1.3. Justificación de la investigación

Esta investigación tiene como objetivo crear una propuesta que trabaje en conjunto con el monitoreo y detección de riesgos o vulnerabilidades que se presenten y puedan generar un impacto negativo en la seguridad de la red en la Empresa Imbyte Soluciones. Para lograr los objetivos del estudio se acudió al empleo de técnicas de investigación como la observación, las encuestas y el procesamiento de estas. Mediante Software para poder medir la factibilidad o satisfacción, con ello se conoció el grado de factibilidad del firewall con los objetivos y procesos, así los resultados puedan apoyarse en técnicas de investigación válidas en el medio. Esto permitirá determinar controles de acceso a las herramientas gestionadas en un único dispositivo para su integración. Utilizando el control de acceso de usuarios para crear los medios y mecanismos para admitir y controlar el tráfico de la red.

De acuerdo con los objetivos de estudio el resultado permitió encontrar soluciones concretas a los problemas de la red de datos, software y hardware, que interfirieron en los procesos de la empresa, con tales resultados se tuvo también la posibilidad de realizar propuestas, o cambios en las políticas de seguridad de red con las que cuenta la empresa.

Por esta razón el presente proyecto se justifica de forma práctica con la propuesta de implementación de un firewall de seguridad en relación a otros dispositivos y en colaboración y apoyo del uso de software que no genere costos para la entidad en

este caso Endian Community (Open Source), ayudo a implementar controles para reducir ataques y riesgos , monitorear el tráfico de la red de la empresa en tiempo real, implementar controles de acceso a usuarios encaminados a mejorar y mantener el nivel de seguridad de la información relacionada con la red de datos, utilizar estas herramientas para crear políticas y controlarlas, como era la intención en la confirmación de mejoras en el nivel lógico de seguridad de la red corporativa y controles de usuarios para ayudar a proteger la información de la organización .

1.4. Objetivos de la investigación

1.4.1. Objetivo general

Implementar firewall Endian Comunity para gestionar la seguridad perimetral en las MYPES de la ciudad de Cajamarca: caso Imbyte Soluciones.

1.4.2. Objetivos específicos

- Determinar los aspectos más importantes para prevenir y corregir las vulnerabilidades de seguridad en la red perimetral y el cuidado y preservación de la información de la empresa Imbyte Soluciones, Cajamarca.
- Determinar la relación que existe en la seguridad de la red, la información de las tecnologías de información y la implementación de un firewall de seguridad en la empresa Imbyte Soluciones, Cajamarca.
- Demostrar las principales características del software Endian para brindar los servicios de seguridad de la información y protección de la red perimetral de la empresa Imbyte Soluciones, Cajamarca.

- Determinar las políticas de seguridad a implementar para el reforzamiento de la seguridad, de acceso y restricción con el filtrado de paquetes utilizando Endian Open Source en la empresa Imbyte Soluciones, Cajamarca.

CAPITULO II: MARCO TEÓRICO

2.1. Antecedentes

Si evaluamos en la actualidad la alta aceptación que tienen las soluciones a la seguridad, distribución, aplicación y sus aportes que brindan al aplicar sus funcionalidades correctamente, se ha presentado múltiples teorías de la utilización de este tipo de software, a continuación, se hace referencia a algunos proyectos enfocados a la utilización de software para proporcionar seguridad informática como aporte a la misma, así como conocimiento de distintas propuestas, Para garantizar resultados óptimos y triunfo del plan que se puso en marcha ha sido primordial consultar distintas fuentes o artículos de análisis involucrados con la solución planteada para la empresa Imbyte soluciones.

> Castillo Palomino, Domínguez & Sulca Galarza, (2017). En su tesis titulada: "Implementación de un Firewall TMG Forefront para la Seguridad Perimetral de la Red de Datos de la Clínica Aliada". En sus conclusiones nos dicen:

La utilización del firewall TMG Forefront está planificada para mejorar la administración de las políticas de estabilidad de conformidad con el ISO27001 (Seguridad de la información), otorga un estándar para la aplicación de políticas para los usuarios de la red de datos de la Clínica aliada.

Implementé el firewall Forefront TMG para optimizar los servicios de Internet de alta rapidez. Estas mejoras se reflejarán una vez que el firewall entre en producción. La utilización del firewall de Forefront TMG le posibilita brindar servicios VPN a

los usuarios que requieren hacer su trabajo a partir de cualquier sitio fuera de la organización.

Según Diaz Obando & Gonzales Torres (2017), En su proyecto de grado titulado: "Implantación un UTM basado en software libre para gestión de la seguridad lógica y perimetral para la alcaldía de restrepo valle". Concluyen:

Con el desarrollo de este proyecto de implantación de UTM basado en código abierto, se logró dar solución a la problemática que se tenía en la Alcaldía de Restrepo Valle, ya que por desconocimiento los usuarios internos tenían una muy baja defensa contra las vulnerabilidades actuales en la entidad. La implantación del UTM en la Alcaldía de Restrepo Valle podría llevar al inicio de un sistema de alertas tempranas en donde se podrían detener los riesgos informáticos antes de que ocurran. La falta de controles orientados a proteger la información que se maneja con terceros puede generar consecuencias graves para la entidad y afectar de manera negativa su imagen ante sus partes interesadas, por esa razón, es urgente que las entidades implementen mecanismos de cifrado con el objetivo de garantizar la integridad, confidencialidad y autenticidad de esta información sensible. Es necesario establecer cuanto antes el proceso de gestión de incidentes de seguridad para proveer en la entidad de un mecanismo para el reporte, evaluación y respuesta a los eventos e incidencias de seguridad de la información. Es necesario que se establezcan políticas de seguridad aprobadas por el gobierno, para garantizar su debida implementación, actualización y cumplimiento. Se requiere implementar controles adecuados y efectivos, además de fortalecer los existentes, con el objetivo

de asegurar que la seguridad de la información sea parte del día a día, en la entidad garantizando el inicio de buenas prácticas de manejo de información sensible.

Según Duván Mauricio & Moreno Ruiz (2015), Presentaron su monografía de tesis titulada: Seguridad Perimetral Pymes. Concluyen:

Se cumplieron los objetivos, el general y los específicos propuestos en el desarrollo del proyecto, realizando la implementación de seguridad perimetral en la empresa pyme. El aseguramiento de los servidores para los ataques más comunes desde la red interna y la red externa con bloqueos a 200 sitios sospechosos, permitió cumplir con la disminución de las vulnerabilidades y riesgos a los que estaba expuesta la seguridad informática de la pyme. Para cumplir con la restricción a sitios de Internet no deseado, fue necesario realizar el bloqueo de páginas no deseadas tales como páginas de adultos, logrando bloquear 30 sitios de esta categoría y en la categoría de streaming se bloquearon 50 sitios, esto gracias a la configuración de la fase 1 con el uso del servidor proxy. Posterior al bloqueo, el personal dejó de navegar en sitios web no deseados corporativamente, cumpliendo con las normas sobre protección de la información, además se reflejó un incremento en la productividad de los empleados. Para reemplazar los servidores Microsoft Windows la mejor opción de las validadas es zentyal. De acuerdo a las pruebas y las funcionalidades, pfsense solo puede compartir directorios, pero no puede llegar a tomar control de las estaciones de trabajo Windows, la cual puede ser administrada desde herramientas de escritorio de servidor remoto de Windows y no requiere licencia de servidor.

La empresa de ciberseguridad Eset (2014) Presentó un artículo titulado: "El desafío de privacidad en internet." Su objetivo es:

En 2012 la finalidad fundamental ha sido amenazar de manera directa a los aguantes móviles. Al siguiente año hubo un incremento destacable de los malintencionados para móviles, estas amenazas permanecen en constante incremento, sin embargo, el problema fundamental está enlazado con la privacidad en Internet.

En este sentido, casos como el acontecido con Edward Snowden y la Agencia Nacional de Seguridad de los Estados Unidos (NSA) acrecentaron la preocupación de la privacidad en Internet. Sin embargo, eso no disminuyó a los individuos que se vieron agraviados por algún tipo de código malicioso o amenaza informática. Está claro que esta preocupación es algo así como la iniciativa de los usuarios para con la informática y su seguridad, es primordial que las personas piensen en la Seguridad de la Información, si no es así, no se disminuirán los riesgos informáticos y todo lo relacionado a ellos. La situación es similar a alguien que le preocupa mucho la protección en su casa, pero no pone un sistema de alarma, deja pasar a desconocidos, deja puertas y ventanas abiertas, entonces así, hay muchas posibilidades de que ocurra algún episodio de riesgo.

Según Bueno Rosales (2013), En su tesis titulado: "Sistema de control y seguridad Endian Firewall para la empresa frada sport". Concluye:

El sistema Endian Firewall Security es una forma estratégica de controlar, proteger, poner a disposición, ejecutar y administrar su red de datos global. Este es el análisis de la empresa de observación directa, investigación descriptiva e investigación transversal, como se describe al principio. Consultar, identificar el eje principal del

problema empresarial y cubrir el proceso de desarrollo del enfoque. Poner en marcha un proceso de desarrollo basado en la investigación, analizar los distintos soportes vulnerables, los puntos clave, gestionar la información de cada departamento de la empresa, etc. y trazar el status con respecto a las diversas cuestiones comerciales como un proceso de diseño en el que estaré trabajando. Por tanto, la metodología de desarrollo en si d se basa en seis fases de mejora, cada una de las cuales incluye diferentes procesos de gestión de datos, control, seguridad, centralización y acceso. Además, es importante utilizar herramientas de entorno grafico para tareas complejas como la creación de reglas de filtro, políticas, servicios, registros, etc. Considerando todo el proceso, se puede decir que la empresa Frada Sport puede optar un sistema de seguridad de código abierto basado en costo mínimo de agencia de la empresa, toda la estructura física y lógica es controlada por el sistema de seguridad EFW. Esto se debe a que tiene muchas herramientas que ayudan a las empresas a enfocarse principalmente en la seguridad de alta disponibilidad, administrar y controlar adecuadamente todos los componentes de la red de datos.

Fabuel Diaz (2013), En su proyecto de tesis titulado: "implantación de un sistema de seguridad perimetral". Concluye:

En este proyecto se ha tratado de dar a conocer lo que es la seguridad perimetral, primero sentando unas bases teóricas, para posteriormente exponer las fases necesarias para la implantación de un sistema de seguridad perimetral. Para ello se ha partido de requisitos específicos, y una vez identificados, se ha ofrecido una solución que se adapte a dichos requisitos y cumpla en todo momento con un nivel

de seguridad y rendimiento óptimo. Además, se han incluido métodos de gestión y mantenimiento de la plataforma una vez implantada. En la definición de la arquitectura se ha optado por un modelo básico basado en dos niveles de cortafuegos. Actualmente este tipo de implementación garantiza un nivel de seguridad óptimo para las necesidades de la mayor parte de las organizaciones, pero no debemos caer en el error de delegar toda nuestra confianza en los cortafuegos como único elemento de seguridad informática. Un cortafuegos es un elemento fundamental en el diseño de cualquier topología básica de red, pero debe complementarse con otros componentes igualmente necesarios, como zonas de detección de intrusos, antivirus, gestores de ancho de banda, proxyes, etc. La integración de todos ellos de forma adecuada complementa un sistema fiable y robusto, reduciendo considerablemente los riesgos y permitiendo detectar comportamientos anómalos que puedan afectar al rendimiento de nuestra red. La situación actual en el campo de la seguridad perimetral ha evolucionado a un ritmo imparable en la última década. El número de amenazas ha crecido de manera exponencial en un entorno de seguridad perimetral que se convierte en algo imprescindible actualmente.

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 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. La previsión de aquí

a unos años en el campo de la seguridad perimetral es impredecible. El desarrollo de nuevos sistemas de seguridad es inevitable, y serán tan imprescindibles como los son actualmente los cortafuegos o antivirus. Será necesario adaptar nuestra infraestructura ya obsoleta a las nuevas tecnologías, bien ampliando los recursos existentes o sustituyéndolos por sistemas más avanzados. En cualquier caso, el campo de la seguridad perimetral no ha hecho más que comenzar su andadura y será necesario adaptarse a los continuos cambios para no quedarnos atrás.

> Según García (2012) en su tesis de título "Diseño e implementación de una red LAN (Local Área Network) y WLAN (Wireless Local Área Network con sistema de control de acceso AAA (Authentication, Authorization and Accounting)." menciona:

"En este Proyecto se definió todas las tecnologías que se emplearon en la implementación de la solución y cuál fue la evolución tecnológica para llegar a ellas".

Su análisis ha sido llevado a cabo de forma separada para LAN y para la WLAN ya que, al tratarse de redes con interfaces diferentes, cada una tiene forma determinada libre, y estándares de estabilidad para la entrada a la red.

Además se propuso un análisis del problema y se le ubico en un escenario real para especificar las exigencias y necesidades de la organización, la cual necesita una solución de una red LAN y WLAN que garantice la estabilidad de la información y la utilización correcta de los recursos de la red.

Posteriormente se diseñó la solución, realizando el análisis de los requerimientos propuestos en el segundo capítulo. Una vez terminado el análisis se decidió cuáles de los métodos y estándares estudiados se usaría en la implementación.

Finalmente se muestran los resultados y el análisis de la implementación de la solución diseñada en el laboratorio de redes de la especialidad.

> Valenzuela Gonzales (2012), Presentó su trabajo de tesis: "Diseño de una arquitectura de seguridad perimetral de una red de computadoras para una empresa pequeña" nos menciona:

"En este proyecto se presentó una solución de seguridad perimétrica que cubra los requerimientos de una red de computadoras de una empresa pequeña. mostrando además una simulación del diseño propuesto en un ambiente de pruebas controlado".

En un principio se muestra el estado real y peligros de la información y el valor de la misma.

Después se muestra en detalle y de forma técnica, los peligros, amenazas contra la totalidad de una red de pcs de una compañía pequeña y las contramedidas que tienen la posibilidad de ser adoptadas.

Se muestran los criterios que fueron tomados en importancia para la selección de la solución más correcta para el escenario propuesto en el tercer capítulo. Por último, se desarrollan políticas de seguridad que debe ser aplicada en la solución seleccionada.

2.2. Bases teóricas

2.2.1. Fundamentos de redes de datos

Desde que las computadoras se empezaron a utilizar de manera esencial en empresas, hogares, negocios, etc., surgió la necesidad de conectarlas entre sí para compartir información o datos de manera más segura y rápida. Debido a ello surge la necesidad de conocer e implementar las redes de datos, como el manejo y funcionalidad de las mismas, así como también a trabajar de manera unificada es decir compartir en una sola red de trabajo los programas, discos duros, servidores, impresoras, scanner, etc. Entre los diversos usuarios que puedan existir en estas.

De esta forma, una red de datos, además llamada red de telecomunicaciones es un grupo de dispositivos informáticos y TI que permanecen conectados entre sí y cuyo fin es mandar y recibir paquetes de información específicos destinados a repartir esta información y recursos informáticos y prestar servicios en beneficio del cliente..

2.2.2. Finalidad de una red de datos

"El fin de una red de datos es conectar usuarios entre ciertas distancias, que tienen la posibilidad de ser pequeñas o de manera considerable monumentales, dándoles la probabilidad de hacer un trueque de información preciso y confiable por medio de una red que es común entre ellos, o sea, que conecta a dicho cliente con el otro". (Suárez & Pinto, 2014) o en una empresa en su totalidad Dichas redes están basadas en:

- **Centros de telecomunicaciones**, donde se interconecta con hubs, patch panels.
- **Servidores** propios que se encuentran disponibles. (Sistemas base)
- **Hubs**, amplifican señales, se encuentra conectada entre nodos, la cual utiliza cable UTP, fibra óptica, entre otros.
- **Patch Panel**. - se basan en organizar los puntos de control
- **Patch core**. - son cables de comunicación, las cuales están inter conectadas con los puntos de acceso o terminales pcs, en donde los elementos principales de una red son: Servidores, cliente, medio, datos compartidos, recursos.

2.2.3. Conectividad

La conectividad de red es la capacidad de establecer una comunicación directa o crear un vínculo entre diferentes dispositivos informáticos, esto puede realizarse a través de dispositivos que se conectan mediante cables como también de manera inalámbrica, siendo esta una de las formas más comunes en la actualidad.

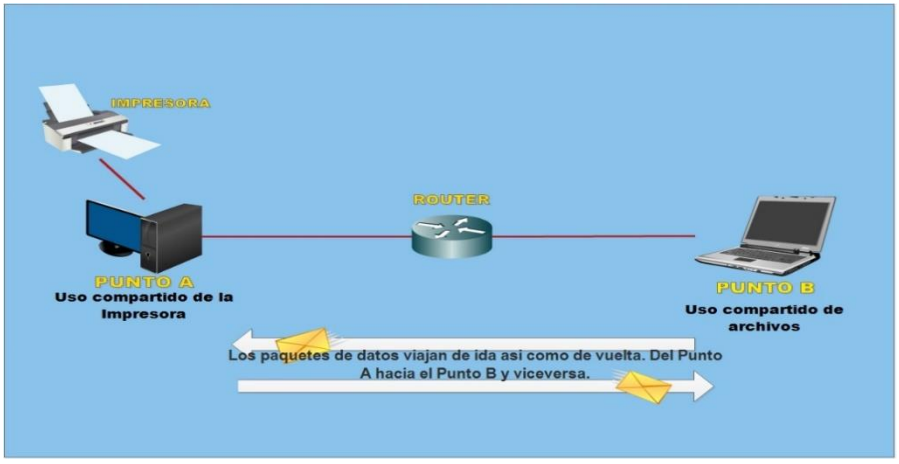
Según lo mencionado líneas arriba existen diferentes dispositivos que permiten a empresas, hogares, oficinas y negocios en general contar con una red a Internet y no siempre suelen ser las mismas.

Bien ahora, se revisarán los diferentes tipos de redes reales que son utilizadas para el envío de paquetes de datos que comprenden la información, empezando con la tecnología simple denominada punto a punto hasta las redes WAN.

- **Red de punto a punto**

"Las redes punto a punto implican nada más que la interconexión de dos puntos de red tal y como su nombre lo dice, se conectan dos equipos y son relativamente simples de establecer y pueden emplear ya sea líneas digitales, líneas analógicas o módems. Siempre y cuando los protocolos en ambos extremos del enlace concuerden, los equipos terminales de datos (ETD) dialogan fácilmente" (Bernal Kaiser & López Escoba, 2012, pág. 466) .es decir establecen una conexión directa en la que la información envía paquetes de datos de ida y de vuelta.

Figura 1 *Redes de Punto a Punto*



Nota: Esta figura representa la conexión punto a punto de la red de datos

- **Redes LAN**

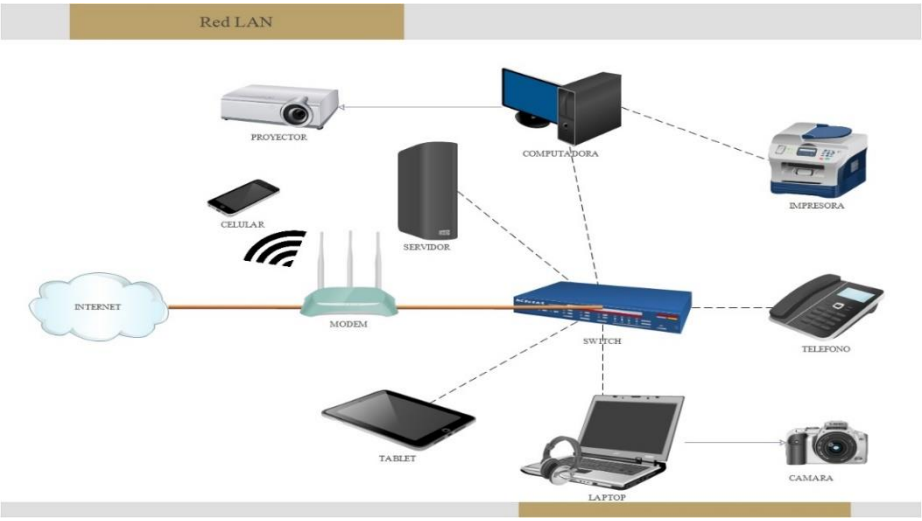
Por sus siglas en ingles se conoce a una red LAN como Local Área Network, cuya traducción es: Red de Área Local. Es una red informática cuyo alcance se limita a un espacio físico reducido, como una casa, un departamento o un edificio.

A través de una red LAN se pueden compartir recursos o datos entre distintos tipos de aparatos electrónicos tales como: "computadoras y aparatos informáticos (como laptops, teléfonos celulares, tabletas, etc.), además de periféricos (impresoras,

proyectores, etc.), información almacenada en el servidor (o en los computadores conectados) e incluso puntos de acceso a la Internet, a pesar de hallarse en habitaciones o incluso pisos distintos.

Este tipo de redes son de uso común y cotidiano en negocios, empresas" (Gilda, 2021), entidades públicas o privadas según sea la necesidad.

Figura 2 *Redes de datos LAN*



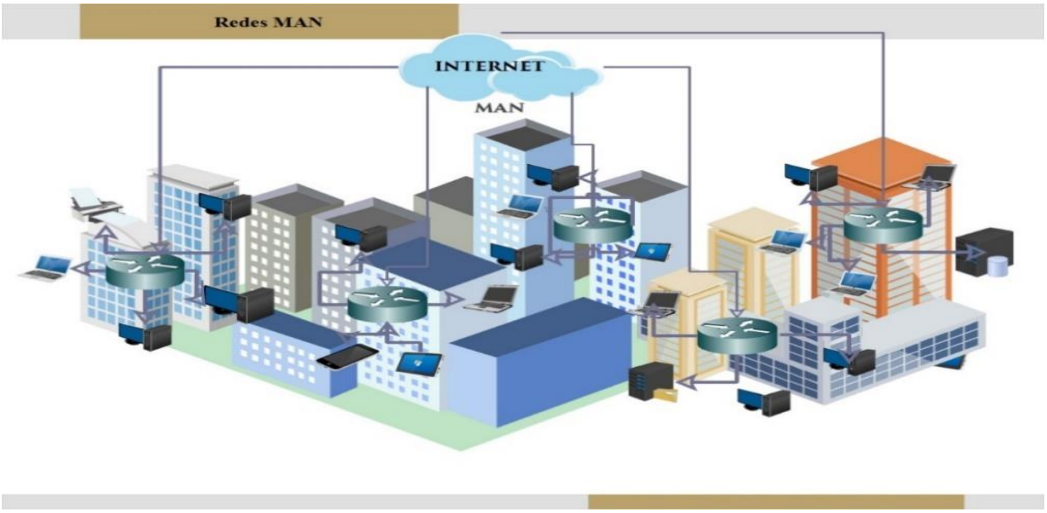
Nota: Esta figura representa la red de datos LAN.

- **Redes MAN**

Por sus siglas en inglés se conoce a una red MAN como Metropolitan Área Network, cuyo significado es Red de Área Metropolitana esta es una red de alta velocidad (banda ancha) que, dando cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y video, sobre medios de transmisión tales como fibra óptica y par trenzado. Esta ofrece cobertura amplia a una ciudad o un municipio.

Estas redes pueden se “públicas o privadas y se desarrollan con dos buses unidireccionales, esto quiere decir que cada uno actúa independientemente del otro respecto a la transferencia de datos. Cuando se utiliza fibra óptica, la tasa de error es menor que si se usa cable de cobre, siempre que se comparen dos redes de iguales dimensiones. Cabe mencionar que ambas opciones son seguras dado que no permiten la lectura o la alteración de su señal sin que se interrumpa el enlace físicamente”. (Gilda, 2021)

Figura 3 *Redes de datos MAN*



Nota. Esta figura representa la Red de datos MAN

- **Redes WAN**

Por sus siglas en ingles se conoce a una red WAN como Wide Área Network, cuyo significado es: Red de Área Amplia es decir son las redes que generan conexiones informáticas de mayor envergadura, es decir, las más extensas y que abarcan mayor rango y alcance además que cuentan con mayor velocidad, que cubren una extensa porción geográfica.

Estas incorporan gran cantidad de redes de menor tamaño en una sola, interconectando así a diversas cantidades de usuarios separados por enormes distancias, con mayores tasas de transmisión y con diversos niveles (capas) de datos.

Esto implica la necesidad de máquinas dedicadas por completo a la ejecución de programas de usuario (hosts), la presencia de tecnologías de información, enrutadores y conmutadores, o la utilización de máscaras de subred para conectar varios hosts.

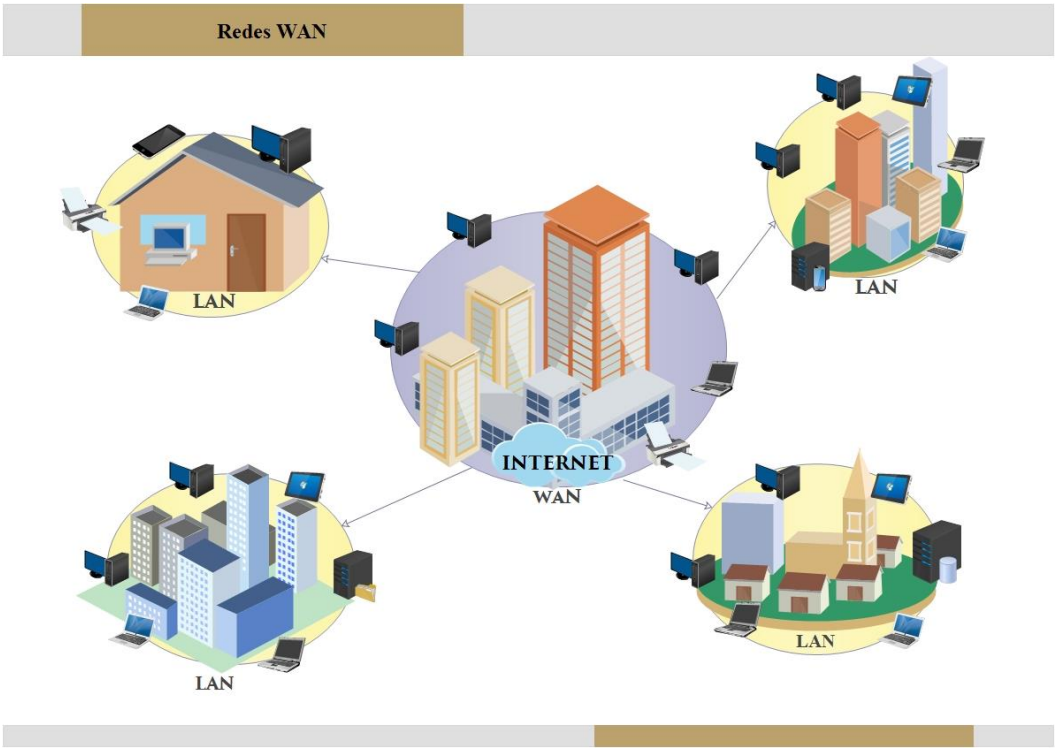
- **Tipos de redes WAN**

Las redes WAN suelen ser de diferentes tipos de acuerdo a la necesidad de comunicación que se quiera cubrir.

- ✓ **Red WAN por circuitos.** Se trata de redes de discado telefónico, que reciben la dedicación plena del ancho de banda mientras se emplea la línea telefónica, pero son lentas y ocupan la línea telefónica.
- ✓ **Red WAN por mensaje.** Se compone de ordenadores (conmutadores) que aceptan el tráfico de cada una de las terminales de la red y administran el flujo de la información mediante mensajes (e información en la cabecera de los mismos) que pueden ser borrados, redirigidos o respondidos automáticamente.

- ✓ **Red WAN por paquetes.** La información en estos casos es fraccionada en partes pequeñas (paquetes) y una vez que llegan a su destino son nuevamente integradas en el mensaje.

Figura 4 *Redes de Datos WAN*



Nota: Esta imagen representa la red de datos WAN.

2.2.4. Seguridad Informática

Según System (2018) define “Podemos definir "seguridad informática" o "ciberseguridad" como el área que se encarga de proteger las redes, equipos e información sensible de una empresa al identificar y eliminar amenazas que pueden difundirse en la red de dispositivos. Con la seguridad para las tecnologías de la información se busca a su vez minimizar el mantenimiento de la infraestructura y mejorar su seguridad en todos los niveles.”

Sebastián (2017), dice : En la actualidad es muy usual encontrar que al hablar de seguridad se entienda esta con certeza total de la falta de riesgo o contingencia, sin embargo no es posible tener la certeza total de dicha seguridad, el riesgo es algo que siempre está presente independientemente de las medidas que se tomen, es por ello que es de vital importancia establecer niveles de seguridad, de esta manera la seguridad informática es un conjunto de técnicas o estrategias que buscan obtener altos niveles de seguridad en los sistemas informáticos, lo cual a su vez, requiere un nivel organizativo(p21).

De igual manera, es importante mencionar que la seguridad informática también consiste en asegurar que los recursos del sistema de información (material informático o programas) es decir, garantizar que la información de una organización o empresa sean utilizados, modificados o tratados por el personal que está acreditado y autorizado para hacerlo.

Como se mencionó anteriormente, la seguridad informática es una de las divisiones o niveles de la seguridad de la información, esta parte de la seguridad de la información busca proteger dos aspectos esenciales: la seguridad física y la seguridad lógica, donde la seguridad física enmarca la protección de los medios de distribución y almacenamiento de la información frente a los desastres asociados a daños eléctricos, robos, inundaciones, etc. Y por otra parte La seguridad lógica busca proteger todo aquello comprendido como lógico ya sea sistemas operativos, aplicaciones y datos mediante componentes que reduzcan el riesgo de pérdida de información.

2.2.5. Seguridad perimetral

Para (Martín, 2020), define Seguridad Perimetral como: Este concepto relativamente emergente comprende la integración de los elementos y sistemas para proteger los perímetros físicos y detectar cualquier intento de acceso a las instalaciones. Se define al perímetro informático de una entidad o empresa como el límite entre la parte controlada de un ambiente en el cual se usan, almacenan y procesan datos y los otros entornos informáticos no controlados por una empresa.

Es decir, el límite entre lo que la seguridad de la información de una empresa puede administrar y lo que no. Dentro del perímetro de seguridad informática de la misma. En esta debería estar toda la información que se desea proteger con los distintos niveles de seguridad necesarios requeridos para cumplir con esa tarea.

La seguridad se convierte continuamente en una parte más destacada en la base de TI de cualquier asociación y es una tendencia general a diseñar estrategias que salvaguarden sus marcos de datos.

La seguridad fronteriza o perimetral construye su lógica con respecto a la seguridad de toda la organización de PC de una organización "considerando todo", es decir, estableciendo un caparazón que asegura cada componente sensible contra diferentes peligros, por ejemplo, infecciones, gusanos, troyanos, rechazo de asaltos de la administración, robo o aniquilación de información, pirateo de sitios corporativos, etcétera.

Esta tipología de peligros concebibles ha instigado una división del seguro de borde en dos inclinaciones: con respecto al sistema, en el cual podemos descubrir los

peligros que hablan de los asaltos de los programadores, las interrupciones o el robo de datos en las asociaciones remotas; y en el nivel de sustancias, que incorpora los peligros que son infecciones, gusanos, troyanos, spyware, phishing y diferentes tipos de malware, spam y contenido web que no se ajusta a las organizaciones. Esta división razonable, junto con la forma en que los peligros han avanzado últimamente, ha llevado al mercado de seguridad fronteriza a centrarse en la producción de artilugios dedicados a cualquiera de las dos razones.

Existen varias funciones fundamentales de la seguridad perimetral, ya que se trata de una primera línea de defensa, igual que las alarmas de una oficina o de una casa. La seguridad total no existe en el mundo informático y menos aún en el mundo físico como lo conocemos, pero reduce muchísimo el riesgo a que se roben los datos e información valiosa para una empresa o, incluso, que puedan desaparecer esta información. Por tal motivo se puede decir que para brindar la seguridad al perímetro informático deseado es necesario tomar en cuenta que se cumpla con las siguientes funciones:

- **Resistir** a los ataques externos.
- **Identificar** los ataques sufridos y alertar de ellos.
- **Aislar y segmentar** los distintos servicios y sistemas en función de su exposición a ataques.
- **Filtrar y bloquear** el tráfico, permitiendo únicamente aquel que sea absolutamente necesario.

2.2.5.1. Herramientas utilizadas para la Seguridad Perimetral

Existen diversos mecanismos para proteger la seguridad perimetral, los cuales veremos a continuación:

a) Cortafuegos

"Es un sistema de seguridad de red de computadoras que restringe el tráfico de Internet dentro o fuera de una red privada". (grupo atico 34, 2021)

Según (grupo atico 34, 2021) define: "Este software o unidad de hardware-software dedicada funciona bloqueando o permitiendo de forma selectiva paquetes de datos. Por lo general, su objetivo es evitar que cualquier persona, dentro o fuera de una red privada, participe en actividades web no autorizadas y ayudar a prevenir actividades maliciosas."

Según (grupo atico 34, 2021) define:" Los cortafuegos pueden verse como fronteras cerradas o puertas de enlace que gestionan el recorrido de la actividad web permitida y prohibida en una red privada. El término proviene del concepto de que las paredes físicas son barreras para frenar la propagación del fuego hasta que los servicios de emergencia puedan extinguirlo. De manera similar, los firewalls de seguridad de red son para la gestión del tráfico web, por lo general destinados a ralentizar la propagación de amenazas web".

Los cortafuegos se clasifican en función de la capa del protocolo de comunicaciones en la que actúan en:

- ✓ **Cortafuegos a nivel de red:** Se caracterizan por controlar las comunicaciones entre redes a nivel de capa de red. Implementan en tiempo real políticas de seguridad entre redes, estableciendo

diferentes niveles de confianza. Dentro de esta subcategoría están los routers con funcionalidad de filtrado de paquetes.

- ✓ **Cortafuegos a nivel de aplicación:** Estos operan por encima de la capa de red, a nivel de aplicación y son capaces de controlar protocolos específicos y aplicaciones, por ejemplo, los cortafuegos para mensajería instantánea o de aplicaciones web y P2P. Dentro de este tipo se incluyen los cortafuegos-proxy (filtran protocolos de nivel de aplicación HTTP, FTP, SMTP).

Otra forma de clasificarlos es según su ámbito de protección, es decir, si están destinados a proteger un área de trabajo o toda una organización:

- ✓ **Cortafuegos personales para uso particular:** Estos se usan en un ordenador personal o en un área de trabajo, generalmente vienen incorporados a los Sistemas Operativos.
- ✓ **Cortafuegos corporativos pensados para la protección completa de la red de una organización:** Se diferencian de los personales o de puesto de trabajo en la potencia y capacidad de proceso que incorporan, necesaria para controlar y gestionar miles de conexiones que entran y salen a diario de una red corporativa. Este tipo de cortafuegos puede trabajar tanto a nivel de red como de aplicación.

b) Red Privada Virtual o VPN

Una red privada virtual o VPN, es una conexión encriptada a través de Internet desde un dispositivo a una red. La conexión cifrada ayuda a garantizar que los datos confidenciales se transmitan de forma segura. Evita

que personas no autorizadas escuchen el tráfico y permite al usuario realizar el trabajo de forma remota. La tecnología VPN se usa ampliamente en entornos corporativos.

Una VPN extiende una red corporativa a través de conexiones encriptadas realizadas a través de Internet. Debido a que el tráfico está encriptado entre el dispositivo y la red, el tráfico permanece privado mientras viaja. Un empleado puede trabajar fuera de la oficina y aun así conectarse de forma segura a la red corporativa. Incluso los teléfonos inteligentes y las tabletas pueden conectarse a través de una VPN.

El tráfico en la red virtual se envía de forma segura al establecer una conexión encriptada a través de Internet conocida como túnel. El tráfico de la VPN de un dispositivo como una computadora, tableta o teléfono inteligente se cifra mientras viaja a través de este túnel. Los empleados externos pueden utilizar la red virtual para acceder a la red corporativa.

c) Sistema de detección y prevención de intrusos

La detección de intrusiones es el proceso de monitorizar los eventos que ocurren en la red y analizarlos en busca de señales de posibles incidentes, violaciones o amenazas inminentes a las políticas de seguridad. La prevención de intrusiones es el proceso de realizar la detección de intrusiones y luego detener los incidentes detectados. Estas medidas de seguridad están disponibles como un sistema de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS), que se vuelven parte

de su red para detectar y detener posibles incidentes (Seguridad perimetral que es y objetivos,et al 2021)..

Los sistemas de detección de intrusiones (IDS) y los sistemas de prevención de intrusiones (IPS) vigilan constantemente la red, identificando posibles incidentes y registrando información sobre ellos, deteniendo los incidentes e informándolos a los administradores de seguridad. Además, algunas redes utilizan IDS / IPS para identificar problemas con las políticas de seguridad y disuadir a las personas de lograr violar las políticas de seguridad (Seguridad perimetral que es y objetivos,et al 2021).

Los IDS / IPS se han convertido en una adición necesaria a la infraestructura de seguridad de la mayoría de las organizaciones, precisamente porque pueden detener a los atacantes mientras recopilan información sobre la red

Son dispositivos que monitorizan y generan alarmas cuando hay alertas de seguridad.

Su actuación se efectúa siguiendo estos pasos:

- ✓ Identificación de un posible ataque.
- ✓ Registro de eventos.
- ✓ Bloqueo del ataque.
- ✓ Reporte a los administradores y sistemas de seguridad.

d) Controles de identidad y acceso

El control de acceso es un método para garantizar que los usuarios sean quienes dicen ser y que tienen el acceso adecuado a los datos de la empresa.

En un nivel alto, el control de acceso, es una restricción selectiva del acceso a los datos. Consta de dos componentes principales: autenticación y autorización.

La autenticación es una técnica que se utiliza para verificar que alguien es quien dice ser. La autenticación no es suficiente por sí sola para proteger los datos. Lo que se necesita es una capa adicional, la autorización, que determine si un usuario debe tener acceso a los datos o realizar la transacción que está intentando realizar.

Cualquier organización cuyos empleados se conecten a Internet, en otras palabras, todas las organizaciones de hoy en día, necesitan algún nivel de control de acceso. Eso es especialmente cierto en las empresas con empleados que trabajan fuera de la oficina y requieren acceso a los recursos y servicios de datos de la empresa.

e) Honeyports

Un honeypot es un sistema de seguridad perimetral informática diseñado para detectar y contrarrestar el acceso o uso no autorizado de un sistema informático. El nombre "honeypot" se usa en referencia a la forma en que el sistema atrapa a usuarios no autorizados, como piratas informáticos o spammers, para que puedan ser identificados y evitar que causen más problemas.

Los honeypots son diferentes a las soluciones de seguridad típicas porque atraen intencionalmente a piratas informáticos o usuarios con intenciones maliciosas. Por ejemplo, una empresa puede crear deliberadamente un agujero de seguridad en su red que los piratas informáticos podrían explorar

para obtener acceso a su sistema informático. El sistema puede contener datos falsos que serían de interés para los piratas informáticos.

Al obtener acceso a los datos, el pirata informático podría revelar información de identificación, como una dirección IP, ubicación geográfica, plataforma informática u otros datos. Esta información se puede utilizar para aumentar la seguridad contra los ciberdelincuentes y usuarios similares.

f) Sistema anti DDOS

El software anti-DDOS se ejecuta sobre el hardware existente, analizando y filtrando el tráfico malicioso. Como regla general, el software Anti-DDOS es más rentable y más simple de administrar que las soluciones basadas en hardware. Sin embargo, las soluciones de software y secuencias de comandos solo pueden ofrecer protección parcial contra ataques DDoS, son propensas a falsos positivos y no ayudarán a mitigar los ataques DDoS basados en volumen. El software instalado localmente puede verse abrumado más fácilmente que los dispositivos o las soluciones basadas en la nube.

El hardware DDoS es una capa física entre los atacantes potenciales y la red. Aunque el hardware DDoS puede proteger de ciertos tipos de ataques, otros tipos, como los ataques DNS, no están influenciados en absoluto por el hardware, ya que el daño se hace bien frente a él.

2.2.6. ¿Para qué sirve la seguridad perimetral informática?

Los principales objetivos de la seguridad perimetral informática son:

- Soportar los ataques externos.
- Detectar e identificar los ataques recibidos y alertar acerca de ellos.

- Segmentar y brindar seguridad a los sistemas y servicios en función de su superficie de ataque.
- Filtrar y bloquear el tráfico ilegítimo.

2.2.7. ¿Por qué se debería proteger el área perimetral informática de una empresa?

Los sistemas de detección de intrusos y los sistemas de seguridad corrientes tienen al menos una cosa en común: es absolutamente esencial que todos sus componentes se integren en un todo sin fisuras. Por ejemplo, algunas empresas recomiendan sensores de movimiento montados en una cerca para proteger el perímetro de un área.

Desafortunadamente, los vientos fuertes y los animales pequeños tienden a activar estos sensores, lo que genera falsas alarmas, sin embargo, estos sensores no se activan en absoluto, lo que es mucho más grave cuando se trata de una situación de intrusión. En otras palabras, estos sensores a menudo no se integran bien con el resto del sistema.

La necesidad de la integración del sistema de protección del perímetro de la propiedad, para que el sistema funcione como un todo unificado, es parte de la razón por la que rara vez recomendamos que los clientes actualicen sus sistemas de manera gradual. Si bien eso puede parecer una opción monetariamente inteligente, a menudo puede tener un "coste" a largo plazo mucho mayor, que se mide en pérdidas económicas muy reales y en vidas humanas.

La información es uno de los bienes más preciados de una empresa, sobre todo de aquellas que tienen una raíz basada en procesos digitales o que se apoyan fuertemente en actividad informática.

Por eso es muy importante mantener a salvo la información interna que protege nuestra propiedad intelectual y toda la actividad de la que somos dueños, para evitar poner en riesgo la compañía a nivel legal, sobre todo si manejas información confidencial de terceros.

2.2.8. Firewall a nivel de red

Los Firewalls a nivel de red, adquieren las resoluciones basandose en la, dirección de destino y puertos, esto en paquetes individuales IP. Solo un router es un cortafuegos a nivel de red, específicamente, a partir del momento en que no resuelve situaciones sofisticadamente en ilación con la información o paquetes en este momento o desde donde llegue ahora.

Los modernos Cortafuegos a nivel de red ahora están perfeccionándose considerablemente, y tienen datos internos en relación a la situación de los enlaces que van por intermedio de ellos, la información de determinados datagramas y más cosas. Un matiz significativo que diferencia a los cortafuegos a nivel de red es que estos enrutan la circulación de modo directo a partir de ellas, de manera que un cliente cualquiera debe poseer un bloque válido de dirección IP asignado. Los cortafuegos a nivel de red procuran ser más rápidos y transparentes a los usuarios (Castillo Palomino, Dominguez Chavez, & Sulca Galarza, 2017).

2.2.9. Modelo OSI

El modelo OSI es el modelo de la interconexión de sistemas abiertos, y sus siglas provienen del inglés Model Open System Interconnection. Este es un modelo de referencia para los protocolos de red, este estándar fue desarrollado en 1980 por una federación global de organizaciones que representan aproximadamente a 160 países.

Esta normativa está formada por 7 capas que definen las diferentes fases por las que deben pasar los datos para viajar entre dispositivos sobre una red de comunicaciones. En los cuales los usaremos tanto en la parte de sistemas como para la parte de redes.

El modelo OSI no es la definición de una tecnología ni un modelo de red en sí mismo, lo que hace es definir la funcionalidad de ellos, para conseguir un estándar. Desde este modelo se han creado numerosos esquemas de protocolos de red.

Figura 5 *Modelo OSI*

Nota: Imagen que muestra la estructura del modelo OSI.

1. **Capa o nivel Físico:** Está dirigida y enfocada en la transmisión de bits, en forma seguida a lo largo del canal de comunicación, principalmente, destaca que, si llega un dato con valor 0 o 1, llega al otro lado de igual manera.

2. **Capa o nivel de Enlace de Datos:** Esta capa tiene como finalidad ofrecer a los niveles superiores un enlace libre de errores, proporcionando mecanismos para el control y la detección de errores. Por otro lado, ofrece medios para activar, mantener y desactivar este enlace.

Además, se encarga del control de enlaces de datos, realizando tareas como la delimitación de dichas tramas, reconocimiento de tramas, resolución de pérdidas de datos y duplicaciones, control de flujo y control del sentido de la transmisión.

Esta capa se ocupa, en resumen, de los siguientes aspectos:

- Direccionamiento físico
- Topología de la red
- División de los datos en tramas
- Acceso al medio
- Detección de errores
- Distribución ordenada de tramas
- Control de flujo.

3. **Capa o nivel de Red:** Esta capa tiene como finalidad ofrecer a los niveles superiores un enlace libre de errores, proporcionando mecanismos para el control y la detección de errores. Por otro lado, ofrece medios para activar, mantener y desactivar este enlace.

Además, se encarga del control de enlaces de datos, realizando tareas como la delimitación de dichas tramas, reconocimiento de tramas, resolución de pérdidas de datos y duplicaciones, control de flujo y control del sentido de la transmisión.

Esta capa se ocupa, en resumen, de los siguientes aspectos:

- Direccionamiento físico
- Topología de la red
- División de los datos en tramas
- Acceso al medio
- Detección de errores
- Distribución ordenada de tramas
- Control de flujo.

4. **Capa o nivel de Transporte:** Esta capa tiene como finalidad ofrecer a los niveles superiores un enlace libre de errores, proporcionando mecanismos para el control y la detección de errores. Por otro lado, ofrece medios para activar, mantener y desactivar este enlace.

Además, se encarga del control de enlaces de datos, realizando tareas como la delimitación de dichas tramas, reconocimiento de tramas, resolución de pérdidas de datos y duplicaciones, control de flujo y control del sentido de la transmisión.

Esta capa se ocupa, en resumen, de los siguientes aspectos:

- Direccionamiento físico

- Topología de la red
- División de los datos en tramas
- Acceso al medio
- Detección de errores
- Distribución ordenada de tramas
- Control de flujo.

5. **Capa o nivel de Sesión:** Esta capa tiene como finalidad ofrecer a los niveles superiores un enlace libre de errores, proporcionando mecanismos para el control y la detección de errores. Por otro lado, ofrece medios para activar, mantener y desactivar este enlace.

Además, se encarga del control de enlaces de datos, realizando tareas como la delimitación de dichas tramas, reconocimiento de tramas, resolución de pérdidas de datos y duplicaciones, control de flujo y control del sentido de la transmisión.

Esta capa se ocupa, en resumen, de los siguientes aspectos:

- Direccionamiento físico
- Topología de la red
- División de los datos en tramas
- Acceso al medio
- Detección de errores
- Distribución ordenada de tramas
- Control de flujo.

6. **Capa o nivel de Presentación:** Apunta a preservar el significado de la información recibida, su objetivo es codificar los datos de transmisión del flujo de bits, adecuada para la transmisión y después codificarlo para ser presentada en el formato del destino.

El objetivo de esta capa es encargarse de la representación de la información, de manera que distintos equipos puedan tener diferentes representaciones internas de caracteres y que los datos lleguen de manera reconocible. Principalmente trabaja en el contenido de la comunicación, cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas.

La capa de presentación es la encargada de:

- ✓ Definir el formato de los datos que se van a intercambiar entre las aplicaciones y ofrecer un conjunto de servicios de transformación de datos.
- ✓ Definir la sintaxis utilizada entre entidades de aplicación y proporcionar los medios para la selección y modificación de la representación utilizada.
- ✓ Codificar los datos en modo estándar (enteros, reales, caracteres, etc.) y realizar funciones de compresión y cifrado de datos.

7. **Capa o nivel de Aplicación:** Esta capa tiene como finalidad ofrecer a los niveles superiores un enlace libre de errores, proporcionando mecanismos para el control y la detección de errores. Por otro lado, ofrece medios para activar, mantener y desactivar este enlace.

Además, se encarga del control de enlaces de datos, realizando tareas como la delimitación de dichas tramas, reconocimiento de tramas, resolución de pérdidas de datos y duplicaciones, control de flujo y control del sentido de la transmisión.

Esta capa se ocupa, en resumen, de los siguientes aspectos:

- Direccionamiento físico
- Topología de la red
- División de los datos en tramas
- Acceso al medio
- Detección de errores
- Distribución ordenada de tramas
- Control de flujo.

2.2.10. Modelo TCP/IP

La definición de TCP/IP es la identificación del grupo de protocolos de red que hacen posible la transferencia de datos en redes, entre equipos informáticos e internet. Las siglas TCP/IP hacen referencia a este grupo de protocolos:

TCP es el Protocolo de Control de Transmisión que permite establecer una conexión y el intercambio de datos entre dos anfitriones. Este protocolo proporciona un transporte fiable de datos.

IP o protocolo de internet, utiliza direcciones en serie de cuatro octetos con formato de punto decimal (como por ejemplo 10.234.62.25). Este protocolo lleva los datos a otras máquinas de la red.

El modelo TCP/IP permite un intercambio de datos fiable dentro de una red, definiendo los pasos a seguir desde que se envían los datos (en paquetes) hasta que son recibidos. Para lograrlo utiliza un sistema de capas con jerarquías (se construye una capa a continuación de la anterior) que se comunican únicamente con su capa superior (a la que envía resultados) y su capa inferior (a la que solicita servicios)

Figura 6 *Modelo TCP/IP*

Nota: Esta imagen nos detalla la estructura del modelo TCP/IP

1. **Nivel de Enlace o Acceso a la red:** Es la primera capa del modelo y ofrece la posibilidad de acceso físico a la red (que bien puede ser en anillo, ethernet, etc.), especificando el modo en que los datos deben enrutarse independientemente del tipo de red utilizado.
2. **Nivel de Red o Internet:** La capa de Internet (también denominada capa de red) controla el movimiento de los paquetes alrededor de la red. proporciona el paquete de datos o datagramas y administra las direcciones IP. (Los datagramas son paquetes de datos que constituyen el mínimo de

información en una red). Esta capa es considerada la más importante y engloba protocolos como IP, ARP, ICMP, IGMP y RARP.

3. **Nivel o Capa de transporte:** La capa de transporte es la que proporciona una conexión de datos fiable entre dos dispositivos. Divide los datos en paquetes, hace acuse de recibido de los paquetes que recibe del otro dispositivo y se asegura de que el otro dispositivo haga acuse de recibido de los paquetes que recibe a su vez, permiten conocer el estado de la transmisión, así como los datos de enrutamiento y utilizan los puertos para asociar un tipo de aplicación con un tipo de dato.
4. **Nivel o Capa de aplicación:** La capa de aplicación es el grupo de aplicaciones que requiere comunicación de red. Es con lo que el usuario suele interactuar, como el correo electrónico y la mensajería. Como la capa inferior gestiona los detalles de la comunicación, las aplicaciones no tienen que preocuparse por ello.

   Esta capa se encuentra en la parte superior del protocolo TCP/IP y suministra las aplicaciones de red, IP, Telnet, FTP o SMTP, que se comunican con las capas anteriores (con protocolos TCP o UDP).

   Las capas del modelo TCP/IP coinciden con algunas capas del modelo teórico OSI, aunque tienen tareas muchas más diversas.

   La importancia del protocolo TCP/IP es muy elevada ya que permite que los datos enviados lleguen a su destino sin errores y bajo la misma forma en la que fueron enviados.

2.2.11. Descripción de protocolos y procesos de comunicación de una red de datos

- **LAN:** Red de Área local, la LAN, interconecta varios dispositivos de red apuntando a una red de distancia corta, su comunicación, trasciende cableado de comunicación coaxial, par trenzado, fibra óptica.
- **TCP:** Protocolo de control de Transmisión, establece y forma el núcleo del funcionamiento conjuntamente con la IP, se estructura a la capa 4 del Modelo OSI apunta a mantener confiabilidad, en la comunicación de datos.
- **IP:** Protocolo de Internet, es una etiqueta numérica que se establece de una manera lógica y ordenada de interfaces de comunicación de dispositivos de red, principalmente en una red de datos, se utiliza protocolos de internet que corresponde al nivel de red del protocolo TCP/IP.
- **FTP:** Protocolo de transferencia de archivos, además es un protocolo de transferencia de archivos, interconectados a la red TCP, para establecerse en una arquitectura cliente – servidor.
- **UDP:** Protocolo de Nivel de transporte, principalmente intercambia datagramas, establece la comunicación de enviar datagramas, su envió de datos, no confirma que los datos lleguen de manera fiable, correcta a los demás protocolos de comunicación.

- **DNS.** - Sistema de nombre de dominio, ejemplifica la traducción de dominio, ejemplo, https://ingenierosbyte.com/ a un direccionamiento IP.
- **SMTP. -** Protocolo Simple de Transferencia de Correo, pertenece a la capa de aplicación, este protocolo, se basa en el texto de utilización para intercambiar mensajes de correo electrónico entre pc, dispositivos en una red de datos.
- **POP3. -** Cuentas de email de correo electrónico, mensajes que se eliminan del servidor, es decir, los mensajes no se encuentran disponibles en un servidor correo.
- **ICMP. -**Es un protocolo de mensajes de control de internet, protocolo de control y notificaciones de errores, identificando que un servicio no esté disponible.

2.2.12. Utilidad de los protocolos

Tabla 1 Protocolos con los que trabaja Endian Firewall

Protocolos	Aplicación
IP	Usuarios en la red.
HTTP	Servidor Proxy (configuración proxy, políticas de acceso, autenticación, filtros, antivirus)
FTP	Subida y transferencia de archivos, segmentación red
UDP	Segmentación de red
SMTP	Servidor Proxy, Antivirus y Correo no Deseado
POP3	Filtros de Correo no deseado
ICMP	Sistemas de seguridad Snort

Nota: Descripción de la Aplicación de los Protocolos

2.2.13. Protocolos utilizados por el Firewall Endian Community

Tabla 2 *Protocolos que utiliza Endian firewall*

Nivel o Capa	Protocolo
Capa de Aplicación	HTTP, FTP
Capa de Transporte	TCP, UDP
Capa de Red	IP, ICMP
Capa de Enlace	Ethernet

Nota: Descripción de los protocolos que usa Endian Firewall, para realizar el filtrado de información.

2.2.14. Servidores Proxy

Un servidor proxy es una tecnología utilizada como puente entre un ordenador que se denomina (El origen) y la red de datos denomina (Internet). Generalmente se trata de un dispositivo u ordenador intermedio que nos permite conectarnos a Internet de manera indirecta.

Cuando utilizamos un servidor proxy, toda la información pasa primero a este ya que funciona como un filtro, el cual es el encargado de enviarlo al lugar de destino, impidiendo toda comunicación directa entre el ordenador destino e Internet (u otro ordenador).

- **Utilidad de los Servidores Proxy**

Por lo general un servidor proxy es utilizado para acceder a servicios que tienen bloqueado su contenido en un determinado país. Entre los servicios de los proxys

realizan: bloqueo de cookies y otros objetos alojados en las webs. Los dos son muy prácticos para proteger la privacidad y anonimato.

Un servidor proxy oculta únicamente la IP. Cualquier otro identificador adicional pudiera verse revelado, aunque tu IP esté oculta. Si alguien accede a la red, podría espiar el tráfico. Cuando se desea reforzar aún más la seguridad, es recomendable optar por herramientas más complejas como por ejemplo una VPN.

- **Funciones básicas de los Proxy**

Control de acceso: los administradores del servidor proxy permiten o no que sus usuarios se conecten a ciertos sitios.

Filtros de contenido: los administradores pueden bloquear sitios web específicos, así como categorías concretas.

Caché: tras acceder a una página, el proxy guarda toda la información de la web en su sistema. Para futuras solicitudes a la misma página no tendrá que volver a conectarse a Internet.

2.3. Hipótesis de la investigación

2.3.1 Hipótesis General

La implementación de Firewall Endian Comunity influye positivamente en la gestión de la seguridad perimetral en la empresa Imbyte soluciones, Cajamarca.

2.3.2 Operacionalización de variables

Variable independiente: Implementación de Firewall Endian Comunity

Variable dependiente: Gestión de la Seguridad perimetral en las MYPES

Cajamarca caso: Imbyte Soluciones

Tabla 3 *Operacionalización de Variables*

Variable	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Instrumento
Independiente - Implementación de firewall Endian Community	Implementación es llevar a cabo o poner en funcionamiento un software, o hardware que se está adquiriendo para una necesidad Según Quasar software: Endian es una distribución OpenSource de Linux, desarrollada para actuar no solamente como cortafuegos sino como solución integral para proteger su red de amenazas externas,	Brindar un componente de seguridad a los procesos de la empresa y también a la información de los clientes que adquieren los servicios.	- Eficiencia - Disponibilidad - Integridad - Confiabilidad de datos	- Nivel de Eficiencia - Nivel de Disponibilidad - Nivel de sensibilidad	- Encuesta - Ficha de observación

	ofreciendo todos los servicios.				
Dependiente - Seguridad perimetral en las MYPES Cajamarca caso: Imbyte soluciones	A nivel conceptual Cordero (2010) especialista en seguridad, señala que "la seguridad es vista como el conjunto de principios adecuados aplicados a un buen sistema de protección Unidos a una actitud de obrar en forma lógica y razonable para generar una situación, estado de tranquilidad real y asu vez un conjunto de normas adaptadas para prevenir un peligro riesgo o amenaza	La seguridad es la base para protección de la información y procesos de la empresa, así como también protección Contra el robo de información y/o infiltración ocasionada por personas ajenas a la empresa (ciberdelincuentes)	- Verificación de activos - Satisfacción de la empresa	Nivel de Satisfacción de los usuarios respecto al tiempo de respuesta. Tiempo promedio de reportes de incidencias delictivas	- Encuestas

CAPITULO III: METODOLOGÍA DE LA INVESTIGACIÓN

Se determinó que el enfoque de esta investigación será CUANTITATIVO porque se utilizarán encuestas para comprobar la relevancia que tendrá dicha investigación, así como nos dice:

Hernández, Fernández & Baptista (2014, pág. 4) "que utiliza la recolección de datos para probar hipótesis con base en la medición numérica y el análisis estadístico, con el fin de establecer pautas de comportamiento y probar teorías".

Se determinó que el tipo de esta investigación será TECNOLOGICA porque se realizará la implementación de firewall Endian Community.

Según (Arias, 2014, p.6). "Es la búsqueda y obtención de nuevos conocimientos prácticos y aplicados a corto plazo en la creación, producción o desarrollo de bienes y servicios innovadores, artefactos, materiales, prototipos o maquinarias que contribuyan a resolver problemas, satisfacer necesidades y mejorar la calidad de vida de la sociedad".

Se determinó que el diseño de esta investigación será PRE-EXPERIMENTAL "La investigación preexperimental es aquella en la que el investigador trata de aproximarse a una investigación experimental pero no tiene los medios de control suficientes que permitan la validez interna. (Campbell & Stanley, 1963)."

se produce una investigación pre-experimental cuando:

- Se compara un grupo de sujetos al que se aplica un tratamiento

experimental con otro grupo al que no se le aplica el tratamiento.

- Se mide el mismo sujeto o grupo de sujetos antes de la aplicación

de la variable independiente y después de la aplicación de la misma.

Se determinó que el alcance de esta investigación será CORRELACIONAL porque se basa en el estudio de 2 variables para la investigación; así como menciona:

Hernández, Fernández & Baptista (2014, pág. 81) "que los estudios correlacionales, al evaluar el grado de asociación entre dos o más variables, miden cada una de ellas (presuntamente relacionadas) y, después, cuantifican y analizan la vinculación. Tales correlaciones se sustentan en hipótesis sometidas a prueba".

3.1 Unidad de análisis, población y muestra

3.1.1. Unidad de Análisis

La unidad de análisis estuvo compuesta por los trabajadores de la empresa, encargados de la información de los clientes de la empresa Imbyte Soluciones. Por conveniencia y considerando el total de trabajadores que manejan la información de los clientes se tomó como muestra 10 trabajadores. Que se indican a continuación.

Tabla 4 *Trabajadores de la empresa Imbyte Soluciones*

Área	Cargo	N° de Trabajadores
Administración	Administrador	01

Sistemas	Jefe de Sistemas	01
Gerencia	Gerente	01
Soporte	Técnico	03
Ventas	Asesor de Ventas	02
Servicios	Asesor de Servicios	02

3.1.2. Población

Se consideró en este apartado de la investigación a los 10 trabajadores mencionados líneas arriba los cuales conforman la población que integra esta investigación.

3.1.3. Muestra

Dado que el tamaño de la población solo tiene 10 personas permitió al equipo determinar el muestreo no probabilístico por conveniencia a fin de obtener resultados más cercanos a la realidad.

> De acuerdo con Hernández, Fernández y Baptista (2003) nos dice: la investigación no experimental se realiza sin manipular deliberadamente variables, no varía en forma intencional las variables independientes, lo que se hace es observar tal y como da un fenómeno en su contexto natural para después analizarlos.
>
> Según (Ortega, 2018), nos Menciona: El muestreo por conveniencia es una técnica de muestreo no probabilística donde las muestras de la población se seleccionan solo porque están convenientemente disponibles para el investigador. Estas muestras se seleccionan solo

porque son fáciles de reclutar y porque el investigador no consideró seleccionar una muestra que represente a toda la población.

3.2 Métodos de investigación

Diseño de Estudio: INDUCTIVO: Esto se da debido a que este método se basará en las observaciones específicas, tal cual menciona:

> Bernal (2010, pág. 59): "que utiliza el razonamiento para obtener conclusiones que parten de hechos particulares aceptados como válidos, para llegar a conclusiones cuya aplicación sea de carácter general. El método se inicia con un estudio individual de los hechos y se formulan conclusiones universales que se postulan como leyes, principios o fundamentos de una teoría".

3.3 Técnicas de investigación

- **Observación:**

  Según Espinoza (2014), la observación es una técnica de recolección de datos que permite la acumulación y sistematización de información sobre el tema de investigación relacionada con el problema de investigación. Las observaciones pueden proporcionar datos cercanos al comportamiento actual del sujeto. Las herramientas utilizadas incluyen tarjetas de observación, formularios, guías de observación, listas de verificación, hojas de registro, cámaras y videocámaras, microscopios, escáneres, analizadores de gas, opacímetro, micrómetro y más.

Las fichas de Observación permitirán obtener y registrar información de diferentes fuentes sobre la información personal de los clientes, así también los diferentes servicios que brinda la Empresa. Dichas fichas serán aplicadas a expertos en los diferentes temas descritos anteriormente.

- **Instrumentos:**

Encuestas. - Las encuestas están enfocadas a las personas que conforman la muestra, quienes están diariamente atendiendo a los usuarios con el fin de conocer las opiniones y las sugerencias de los mismos.

3.4 Técnica de análisis de datos

Se realizarán fichas de observación para la estimación de la calidad del software así también para la evaluación de credibilidad de los contenidos configurados en el firewall, estas fichas serán puestas a disposición de expertos para su evaluación, para lo cual se considerará dos expertos para analizar y validar si las preguntas propuestas se alinean al interés del firewall en la ficha de evaluación y los objetivos e hipótesis planteadas. Para posteriormente aplicarlas y obtener resultados para luego procesarlos.

Las técnicas de análisis de datos consistirán en el desarrollo de operaciones en función de los objetivos de la investigación para el análisis de los datos, el análisis tendrá la siguiente estructura básica:

- Recopilación de datos cuantitativos.
- Procesamiento en SPSS 27 (tablas y gráficos estadísticos)

3.5 Aspectos éticos de la investigación

Para la presente investigación se tiene el consentimiento, la mayor discreción y compromiso que la institución ha podido brindar, así como la información donde se puede adaptar la investigación a sus políticas y reglas de la entidad.

> "La integridad y la disponibilidad aparecen como conceptos fundamentales tanto de normativa vigente relacionada con la protección de datos de carácter personal, como de códigos de buenas prácticas o recomendaciones sobre gestión de la seguridad de la información y de prestigiosas certificaciones internacionales, éstas últimas, relacionadas con la auditoría de los sistemas de información" López (2015).

Responsabilidad: con la finalidad de orientar la investigación de manera que se pueda obtener un beneficio social en el cual se evidencie que desde la elección del problema que ha de investigarse, el mismo que pasara los diferentes filtros metodológicos aplicados de forma ordenada y en cumplimiento de los mismos.

Veracidad: la investigación pretende además del resultado obtenido dar un beneficio de obtener nuevos conocimientos estos deben estar basados en la veracidad tanto en sus métodos como en sus resultados para poder obtener un impacto positivo en la sociedad.

Consentimiento consensuado y expreso: conforme se haga la investigación con personas, debe existir el respeto a la dignidad personal ya que es uno de los conceptos principales, lo que incluye información completa a los sujetos de lo referente a la investigación en la que participan. Tales personas deben estar de

acuerdo con lo informado, así como también con la información que se les pueda solicitar durante el proceso.

Respeto por el individuo, la sociedad y la vida: la adquisición de nuevos conocimiento y experiencias profesionales no debe transgredir los derechos individuales y sociales previamente establecidos de cualquier individuo además debe contemplar que la vida no debe ser vulnerada sin importar el beneficio que se pueda obtener de la investigación.

- **Validación del firewall**

Las encuestas realizadas para comprobar el funcionamiento del firewall serán validadas y evaluadas por expertos en redes y seguridad de la información y TIC'S, familiarizados con los servicios de la empresa Imbyte Soluciones Cajamarca. Se utilizará la herramienta estadística de IBM SPSS para analizar estadísticamente e interpretar los resultados gráficamente.

CAPITULO IV: IMPLEMENTACIÓN DEL FIREWALL

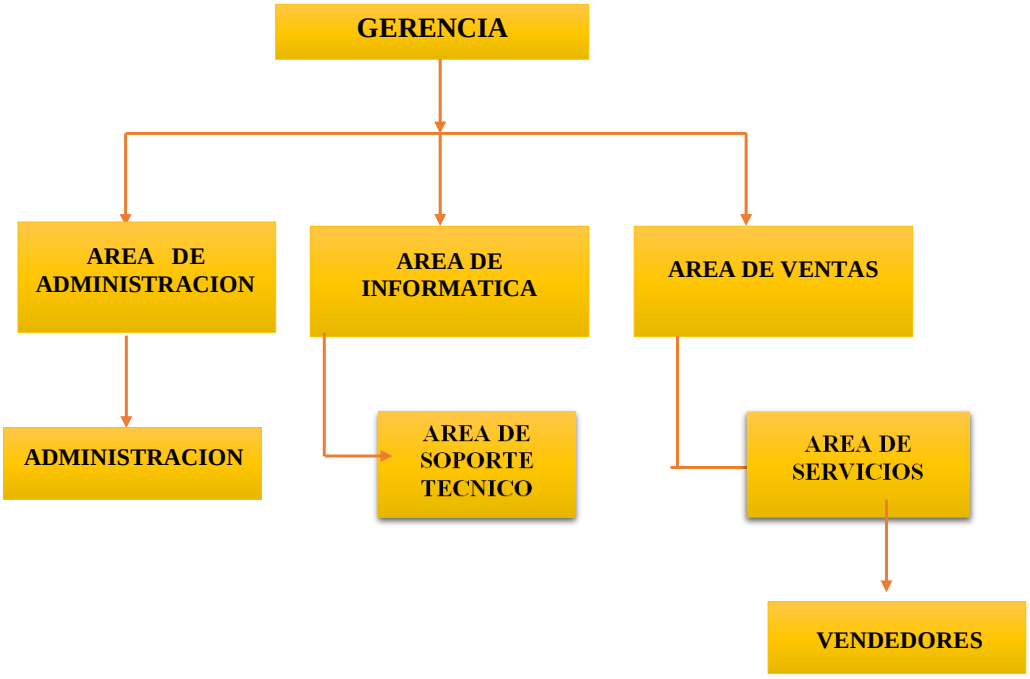
4.1. Etapas de la implementación

Figura 7 *Cronograma del desarrollo de actividades*

AÑO	2022																													
MESES	ENERO				FEBRERO				MARZO				ABRIL				MAYO				JUNIO				JULIO				AGOSTO			
SEMANAS	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
ACTIVIDADES																																
Analizar y verificar la distribucion de la red de Empresa																																
Analisis de las principales falencias y debilidades de la red de la Empresa																																
Definir las herramientas y dispositivos para la instalación del servidor Endian																																
Aplicación de encuestas y cuestionarios de la investigacion																																
Desarrollo e implenetacion de los diferentes filtros para proteccion de la red																																
Prueba del Firewal a niver de red y de usuario																																
Analisis de resutados y conclusiones de la investigacion																																
Presentacion de resultados y validacion del Firewal																																

4.2. Estructura general de la empresa

Figura 8 *Estructura general de la empresa*



Nota: La imagen muestra el organigrama general del Empresa Imbyte soluciones

4.3. Planeación de la seguridad de Imbyte Soluciones

La importancia de la conectividad en la empresa revela principalmente que se debe aplicar un mantenimiento de la seguridad de la red, esto debido a que lo primordial es brindar un acceso fácil a los datos por parte de los usuarios con privilegios y restringir el acceso a los usuarios mediante una segmentación de la red en la Empresa. Se puede evidenciar también, en cuanto a la seguridad de los datos, es una importante tarea administrativa, así como asegurar y prevenir, para que la red se mantenga fiable y segura, en pocas palabras, libre de cualquier amenaza.

En ese sentido, se define cómo está la estructura, o cómo funcionan los módulos o llamados métodos de prevención o protocolos inteligentes de alta disponibilidad Endian Firewall, permite, que se trace una estrategia para contrarrestar en lo

máximo posible las falencias de la red de datos. Los métodos inteligentes se basan en:

- ✓ Incorporar un sistema de Seguridad Open Source, reduciendo costos en la implantación y despliegue del mismo.
- ✓ Brindar un diagnóstico en el tráfico de red, mediante el sistema Endian firewall.
- ✓ Asegurar de forma eficiente el flujo de información es decir la información entrante y saliente mediante un sistema de seguridad.
- ✓ Mejorar el rendimiento de los equipos informáticos y de la red.
- ✓ Documentar toda la información que pasa a través de la red, permitiendo tener un mayor control y organización de los datos en la red.
- ✓ Tener un control y protección de los datos por medio de un antivirus y anti-spam, métodos inteligentes que brinden soporte a todo el perímetro de la empresa a nivel de red.

a) Importancia de la Seguridad Inalámbrica en la empresa

Es importante recalcar que toda la situación ya sea positiva o negativa en cuanto a la seguridad de las Tecnologías de Información que posee la empresa se manifiesta, gracias a los esquemas ineficientes y falta de políticas de seguridad. Ya que con las que cuenta Imbyte Soluciones no se garantiza la protección y resguardo de la información. Entonces el resultado consiguiente de una "violación" a los sistemas informáticos de la empresa, provoca una inestabilidad y una desorganización, que genera desconfianza además esto representa un daño con valor incalculable dentro de la misma.

b) Amenazas y vulnerabilidades de presenta Imbyte Soluciones

Es importante indicar que pese a que la empresa es pequeña y el tráfico de la información en la red de la misma no es muy excesivo es de suma relevancia mencionar que la vulnerabilidad es uno de los medios trascendentes en la empresa, ya que se establece como riesgo implícito, además existe diferentes riesgos que se manifiestan en los diferentes procesos que realiza la empresa, estos se manifiestan en distintas actividades y podremos evidenciarlos y clasificarlos, como:

- Spam
- Ataques de virus.
- No cuenta con control de usuario o accesos
- Manejo inadecuado de la información
- Desorganización del flujo de datos en la red.
- Baja preocupación en la seguridad informática.
- No se controla el acceso a páginas de dudosa procedencia

Es primordial tener en cuenta, el crecimiento de la comunicación y el uso de las tecnologías de información en la empresa, esto debido a que a nivel global el uso del internet, las redes de datos y las tecnologías de información incrementaron su demanda considerablemente a consecuencia de la pandemia y la emergencia sanitaria que golpeo a todo el planeta en el año 2020. En la empresa Imbyte Soluciones, se puede identificar que, así como se incrementó el uso de estas tecnologías pues los riesgos también han evolucionado y ahora, debe enfrentar a posibles ataques a los servicios o procesos de información, y diferentes amenazas.

Entonces es por ello que se puede apreciar los riesgos y amenazas que constantemente corre la empresa, la infraestructura de red y recursos informáticos, debe de estar protegidos bajo un esquema o una normativa de seguridad única, que reduzca los niveles de vulnerabilidad y mitigue los riesgos, permitiendo una eficiente administración de riesgos dirigido a los servidores de la empresa. De esta manera, se establece políticas de seguridad, las cuales empieza desde, formar y conocer el manejo de la información, así como el flujo de la misma, evidenciar niveles de riesgos, análisis y diseño de la infraestructura operativa y física de la red. Por último, contar con un sistema que brinde o ayude a la empresa ante posibles ataques o medidas de vulnerabilidad existentes.

En consecuencia, es importante plasmar que la seguridad de la información de la empresa Imbyte Soluciones debe estar basada en los siguientes parámetros:

- Integridad de la Información y Comunicación.
- Disponibilidad inmediata y segura de los sistemas de información.
- Organización y control de los sistemas informáticos.
- Confidencialidad de la información.
- Control de accesos y de usuarios.

4.4. Distribución de red de la empresa Imbyte Soluciones

Luego del análisis y la evaluación de la red se puede apreciar que la empresa Imbyte Soluciones, ubicada en la ciudad de Cajamarca, tiene una distribución de red que está estructurada de la siguiente manera: Posee un rack central, en el cual, esta interconectado con un switch de 16 puertos, un modem y el router que lo proporciona Claro. como su ISP, la señal de su ISP, llega a su router central con

fibra óptica, en donde llega la señal de internet a la empresa, el modem a su vez esta interconectado con los patchcore, distribuidos a todos los puntos de red o áreas de la empresa, esta corresponde:

- ✓ Área de Ventas
- ✓ Área de Contabilidad
- ✓ Área de Administración
- ✓ Área de Sistemas.

Entonces se puede evidenciar que primordialmente se destaca, la interconectividad empalmada del modem-router a los servidores propios de la empresa, estos son:

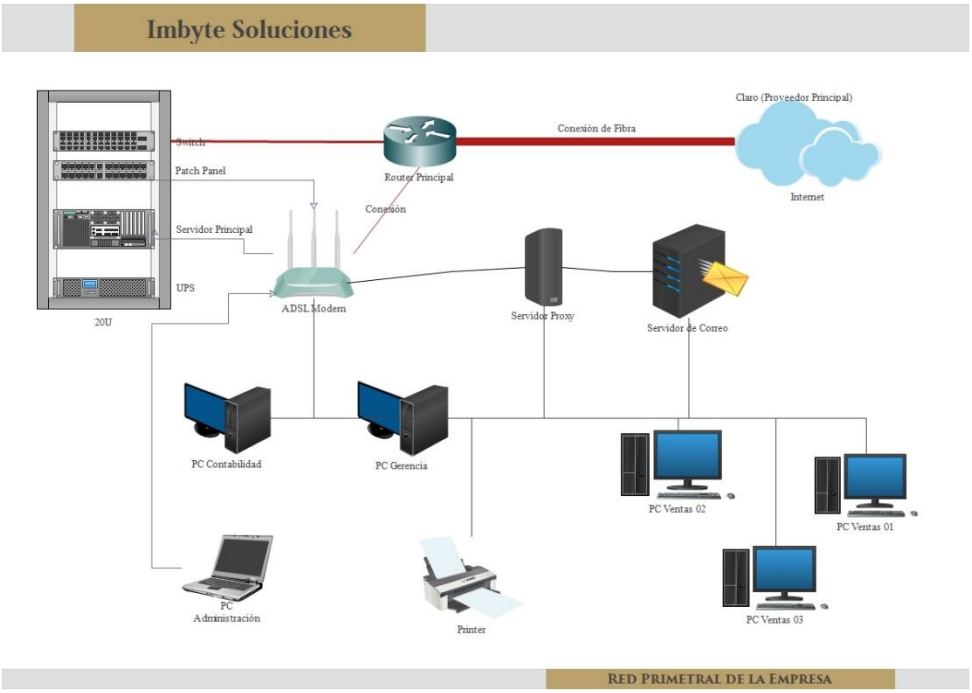
Servidor Dell (Sistema de la empresa Imbyte Soluciones Facturación, Servicios, Asientos Contables, etc.)

Servidor de Correo (Cuentas de los usuarios de la empresa.)

El proveedor de servicios de internet, proporciona, un ancho de banda de 100Mb, la cual es de cierta forma un poco bajo para el correcto funcionamiento y velocidad, pese a eso el servidor requiere de la protección es por ello que se está pensando en la implementación de este firewall, el cual tendrá la IP estática, redirigido con la IP asignada. Por otro lado el servicio proxy que orienta a las demás computadoras del área a crear políticas, reglas, filtros, a contar con un sistema centralizado de auto detección de intrusos, cabe mencionar que el proxy es un servidor a nivel de red el cual esta proporcionado por defecto a modo que se tiene que integrar conjuntamente con el Firewall para proporcionar el servicio de seguridad de red más adecuado,

además del control de virus y spam, y obtener estadísticas certeras de vistas del tráfico en la red, y manejo de conexiones, entre otros.

Figura 9 *Distribución de la red de datos – Imbyte Soluciones*



Nota: Esta imagen muestra la Distribución de la red de las áreas de la Empresa

4.5. Análisis de información y niveles de riesgo

Uno de los principales aspectos a tratar y que significa un riesgo considerable para la empresa es la filtración de la información es por ello que si analizamos los diferentes puntos por los que se puede identificar las características importantes en las que estas falencias se presentan.

a) Transferencias

El crecimiento del tráfico informático y el uso de las tecnologías de información se puede evidenciar, que el uso de las transferencias y transacciones se manejan en muchas oportunidades de manera online, se encuentran involucradas cuentas

de la empresa como, cuentas corrientes existentes en diferentes bancos, lo que genera un punto importante en cuanto al nivel de seguridad en la empresa debido a que la información de la empresa se ve expuesta sin tener en cuenta la baja presencia de seguridad.

b) Proveedores

En este aspecto es preciso mencionar que no existe comunicación formal con los proveedores es decir hay intercambio de información de productos y servicios de manera directa es decir sin llevar un control a los que se ve la necesidad de la utilización del correo corporativo ya que simplemente con recibir un email y responder a dicho mensaje, se tiene acceso a información importante es por ello que se ve la necesidad de darle uso correcto al servicio de correo para mantener el seguimiento correcto de toda la información de la empresa y de los proveedores.

c) Ventas

Se puede evidenciar que gran cantidad del flujo de datos y de información se ve reflejada en el área de ventas debido a que se tiene registro de ventas, precios, servicios, usuarios, además de datos de clientes. En tal sentido, se puedo verificar que los puntos de acceso del área de ventas no cuentan con contraseña o bloqueos de usuarios, es decir cualquier persona puede acceder a dichas máquinas, además que no se lleva un orden y un registro de los datos de clientes y de usuarios.

d) Administración

Es importante mencionar que el área de administración, cumple con unos de los roles de suma importancia y relevancia como alto cargo, se involucra en dar seguimiento a negocios, a los servicios y al de toda la información y actividad en la empresa por ellos que las máquinas y puntos de acceso a la red tienen que estar aún más seguros en estas áreas en donde tiene que existir mayor cuidado ya que esta área involucra al área administrativa y contable de la entidad es por ello que se detectó que es muy necesario el uso y aplicación del firewall además de un antivirus y bloqueos de usuario con contraseñas seguras y confidenciales de acceso solo del administrador y personal que el crea conveniente.

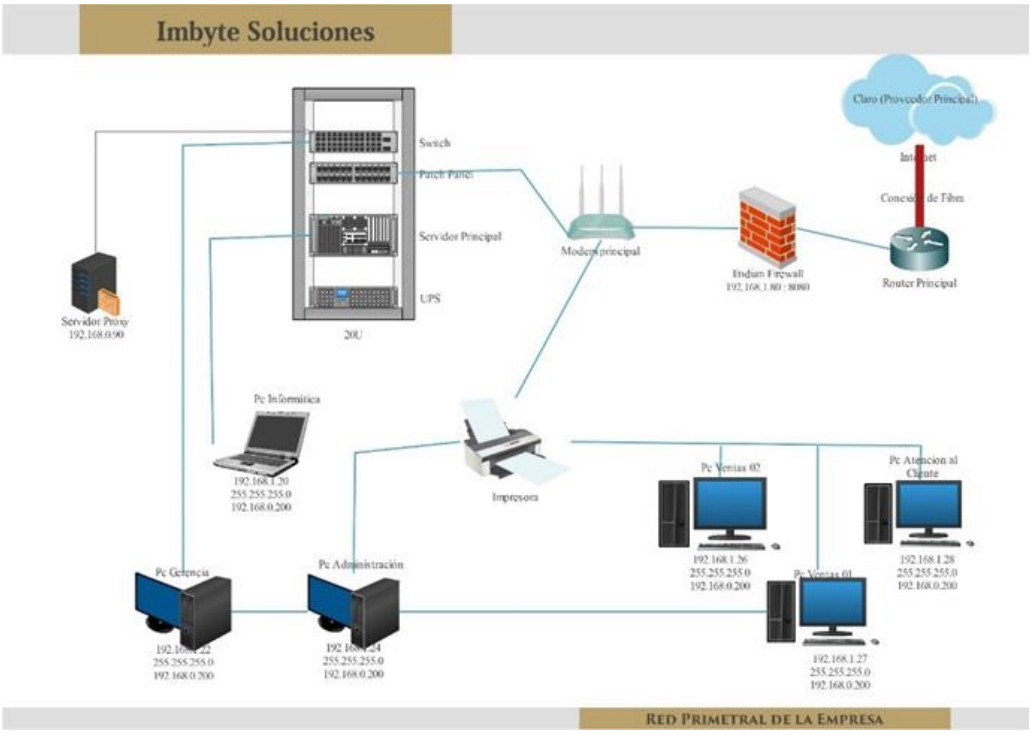
En este análisis es importante evidenciar que los empleados de la empresa Imbyte Soluciones, no poseen políticas de seguridad, lo que influye que muchos de los usuarios, manipulen a su conveniencia las configuraciones, las aplicaciones, etc. El acceso a internet y la facilidad para descargar, contenido malicioso o simplemente virus. Es una de las principales falencias. Esto se ve totalmente involucrado en el rendimiento de los equipos informáticos y principalmente de software, sistemas operativos y hardware.

Entonces es importante notar que el rendimiento y falla de los equipos, muchas veces se debe a estas razones o falencias identificadas, razones para crear otro nivel de seguridad, que ayude a la estabilidad y fiabilidad, además del desarrollo de sistemas de seguridad que mejoren el control, organización, seguridad y eficiencia de los diferentes procesos en cuanto al manejo de la información.

4.6. Diagrama de red final de la Empresa Imbyte Soluciones

El modelo sistemático que representa este diagrama es un punto primordial para esta investigación, ya que es el punto de partida para poder empezar a emprender y entender mejor el sistema de seguridad. Es de vital importancia configurar los equipos informáticos de la empresa de cada área, estas son: Todas las áreas de la empresa, que cuentan con un enlace o conectividad a la empresa o a la red, es decir,

Figura 10 *Diagrama final de red de la empresa Imbyte Soluciones*



Nota: Diagrama de Red completo de todas las áreas de la empresa, con sus respectivos IP.

cada equipo, presenta una IP, una máscara de red, una puerta de enlace y un DNS, para establecer conectividad entre usuarios y servidores, de ese modo brindar la mayor seguridad a la empresa y red en su totalidad resguardando la información que es muy importante para la entidad.

Es importante tener presente la configuración estática de los equipos informáticos, se procede a crear reglas o políticas de seguridad para la empresa.

Si bien es cierto, es una empresa pequeña y su infraestructura no es de las mejores, se puede resaltar que los equipos cuentan con buena configuración y mayor control del manejo de estos, pueden tener alta disponibilidad mediante el sistema de seguridad de alto rendimiento (firewall), que proporciona una ventaja competitiva y tecnológica, al aumentar la productividad, y la autonomía de los usuarios dependiendo de su área de trabajo. Pues será más rápido tomar decisiones y llevar un control de acuerdo a las necesidades de la empresa. Sin embargo, los beneficios han llegado una dependencia cada vez mayor de la infraestructura. Si una aplicación o mal manejo de la información, basada en su mal uso, entonces toda la empresa puede estar en constante riesgo. Los ingresos, los clientes, los sistemas de control, las ventas, pueden estar involucrados en constantes falencias en los sistemas, y poder perderse. Es muy importante examinar los factores que determinan la forma en que los datos son protegidos, sobre todo en ciertos manejos de la información, ser vulnerables y maximizar la disponibilidad para los usuarios, dependiendo de las funciones dentro de la empresa.

4.7. Proceso de aplicación e implementación

- Creación de reglas de acceso, mediante autenticación para cada usuario ya sea por medio de contraseñas o pin de acceso.
- Mejorar el rendimiento de los equipos y de la red, mediante el acceso y no acceso a internet, a los usuarios de la empresa, según el área en que se

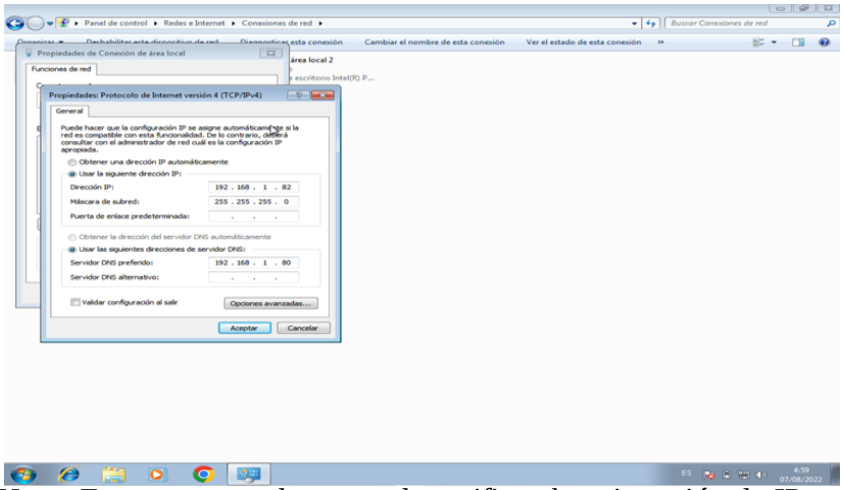
desempeñan. Permitir o denegar el acceso a internet, a los usuarios de la empresa según su área.

- Control y seguridad a la hora de realizar, compras por internet, mediante métodos inteligentes.
- Control organizativo a los usuarios de la empresa, basado en crear políticas de seguridad, mediante especificación del tamaño máximo para descargar y subir archivos.
- Revisión y valida dación de las páginas de ingreso de cada usuario sean de carácter laborar es decir asociados a labores que realiza la empresa. (registros. proxy).

4.7.1. Configuración de Endian Firewall en el Servidor

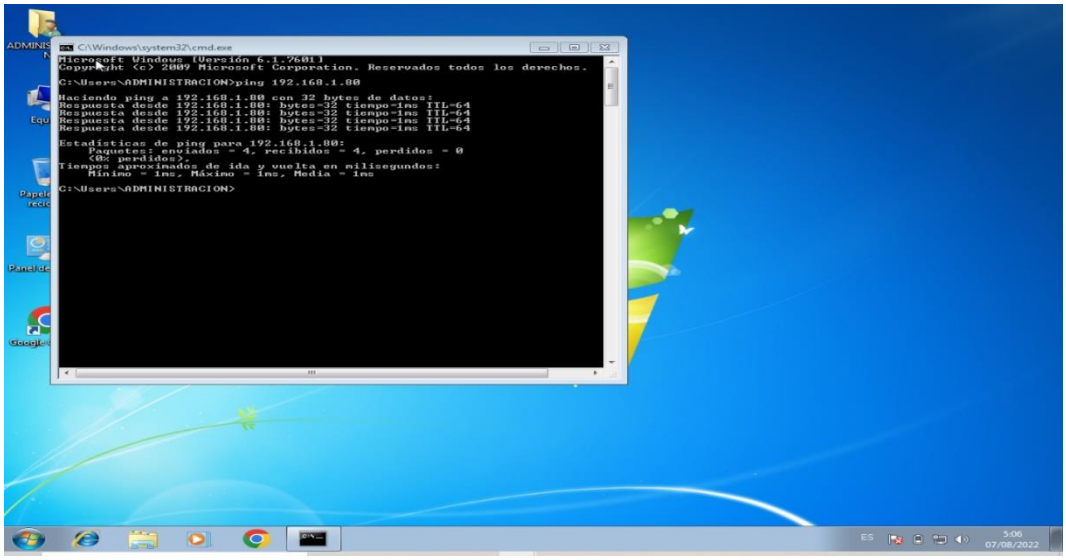
Configuramos los IP en la maquina servidor, IP :192.168.1.80 (IP asignada a Endian Firewall)

Figura 11 *Configuración de IP asignada en el Servidor*



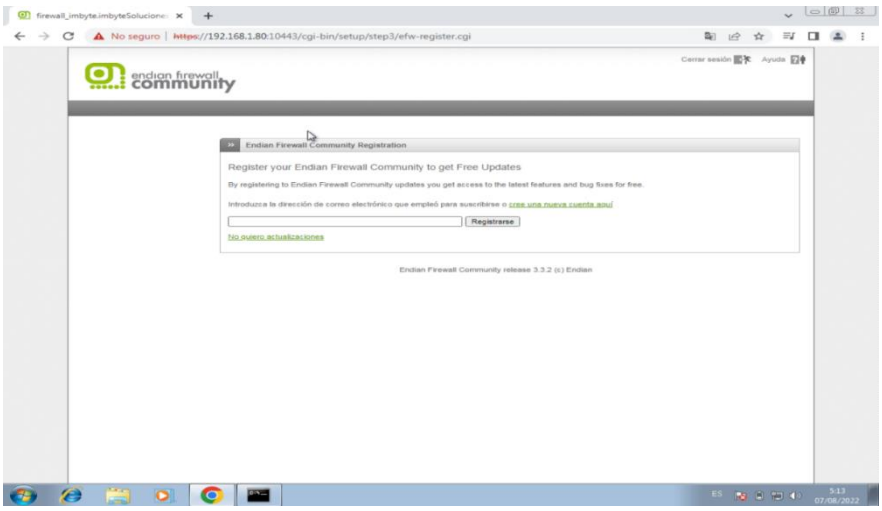
Nota: En este apartado se puede verificar la asignación de IP y configuración de la misma: 192.168.1.80 es la IP que se asignó a Endian Firewall para poder configurarlo en el servidor.

Figura 13 *Conexión con el Servidor*



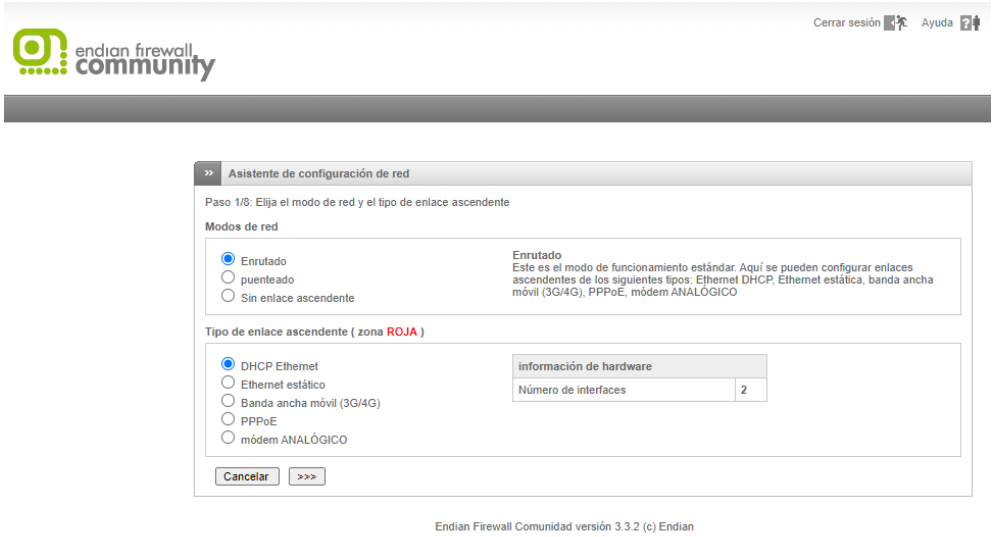
Nota: En este apartado se realizaron las pruebas de conexión respectivas del servidor hacia Endian Firewall a través del comando PING

Figura 12 *Verificación de conexión con Endian Firewall*



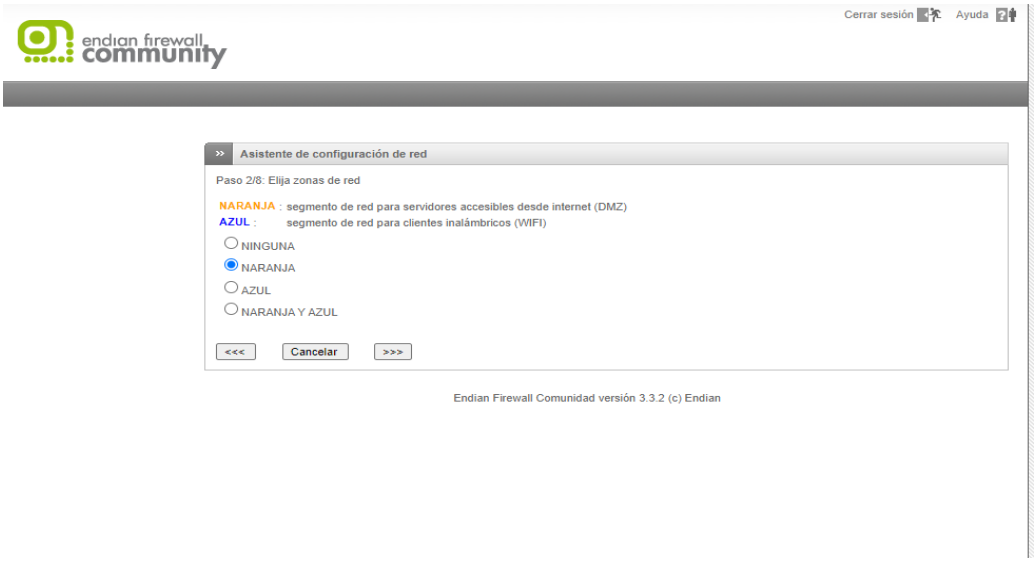
Nota: Comenzamos a configurar Endian Firewall en el servidor mediante interfaz web en este caso se usó Google Chrome para la configuración.

Figura 14 *Interfaz de configuración de red*



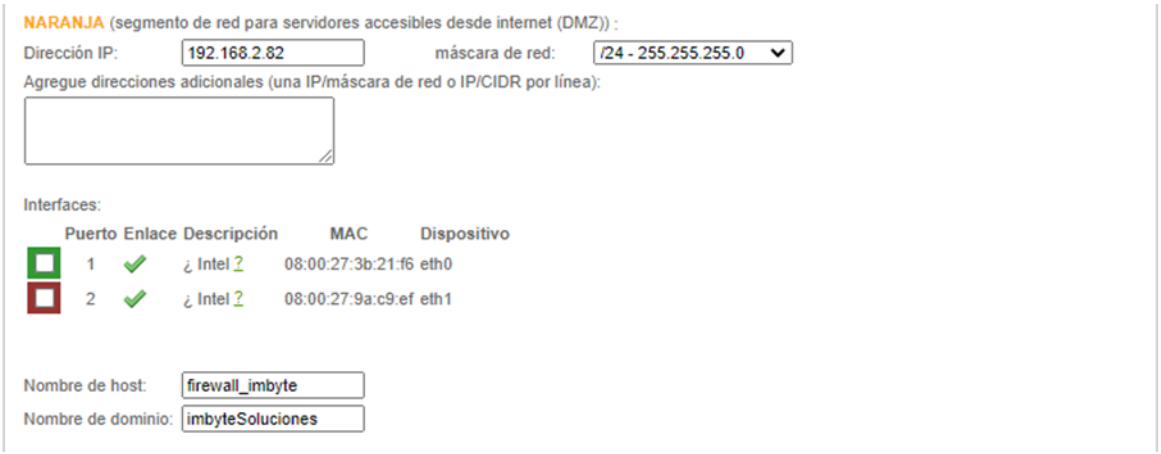
Nota: Se procedió a Elegir la interfaz de red, así como el enlace que se establecerá para la configuración.

Figura 15 *Elección de zona de Configuración*



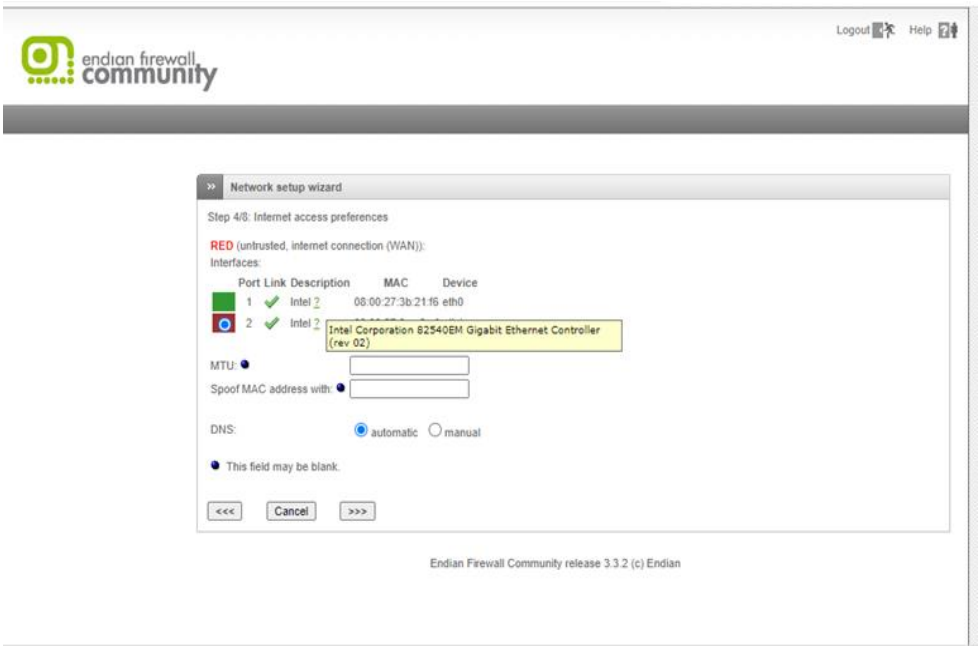
Nota: En esta parte elegimos la “Zona Naranja” que es el segmento de red para servidores accesible a nivel de red

Figura 16 *Elección del Gateway Zona Verde*



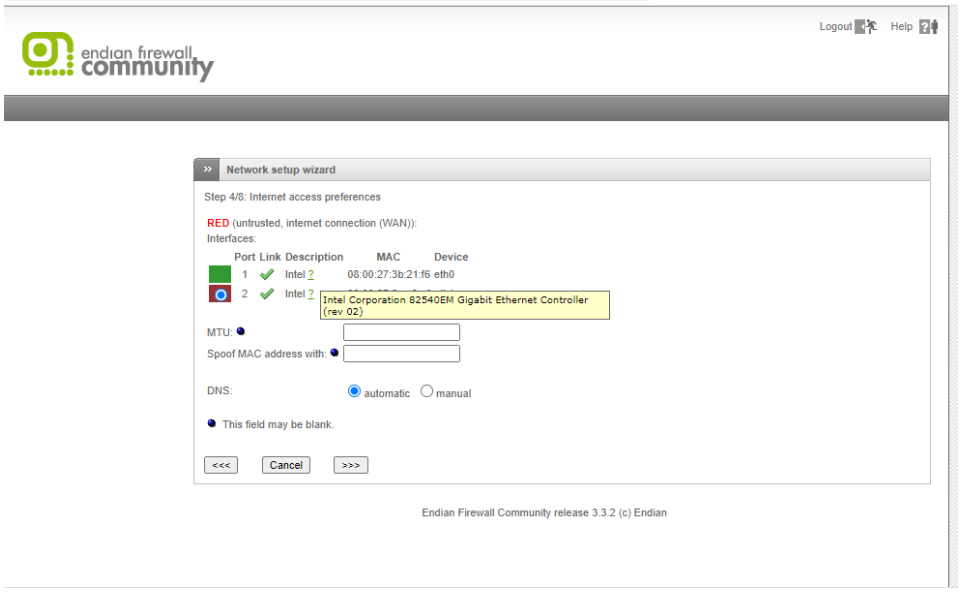
Nota: Se procedió a elegir el Gateway en la zona Naranja “incide” Asignado el host y el nombre asignado para el servidor de control de Firewall.

Figura 17 *Elección del Gateway Zona Naranja*



Nota: Elegimos el Gateway de la zona Naranja “DMZ”. Asignándole los parámetros de la red con la configuración automática de la misma.

Figura 18 *Elección del Gateway zona roja*



Nota: Elegimos el Gateway de la zona roja "outside"

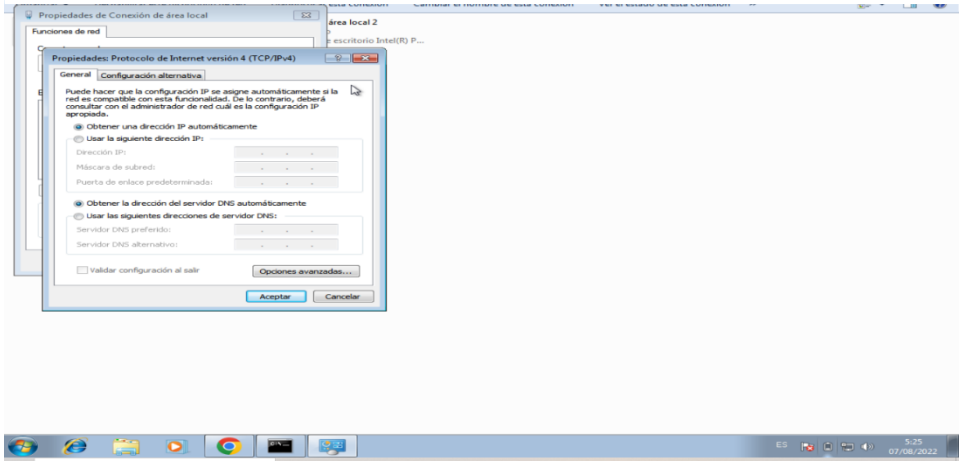
Figura 19 *Configuración del Correo electrónico*

Nota: Configuramos el correo, es opcional, en este caso si colocamos el correo esto para que la empresa pueda tener mayor control acceso seguro a través del mismo.

Figura 20 *Finalización del proceso de configuración*

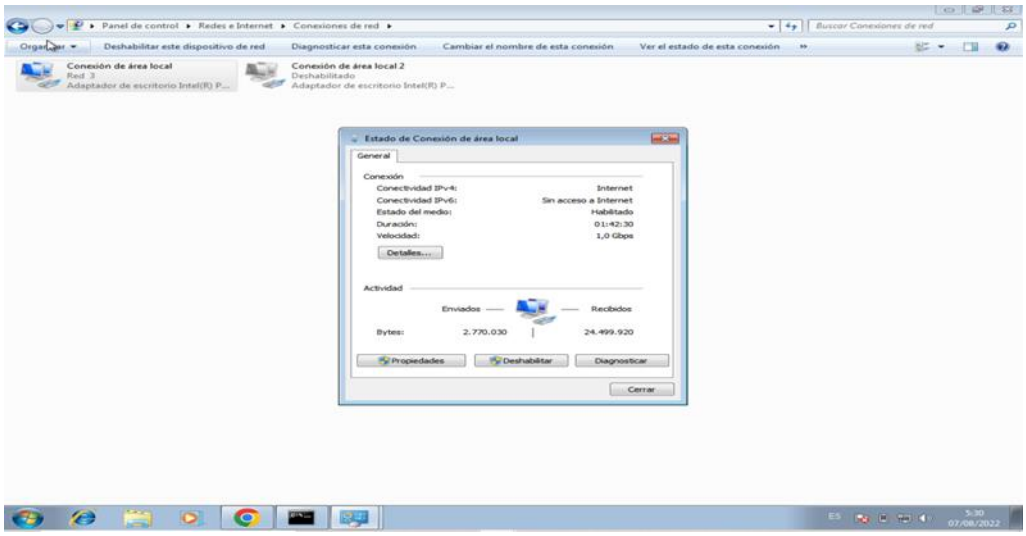
Nota: Luego de realizar toda la configuración inicial y verificar que los cambios realizados se han guardado con éxito se procede a finalizar con el proceso de configuración.

Figura 21 *Comprobación de funcionalidad de Endian firewall*



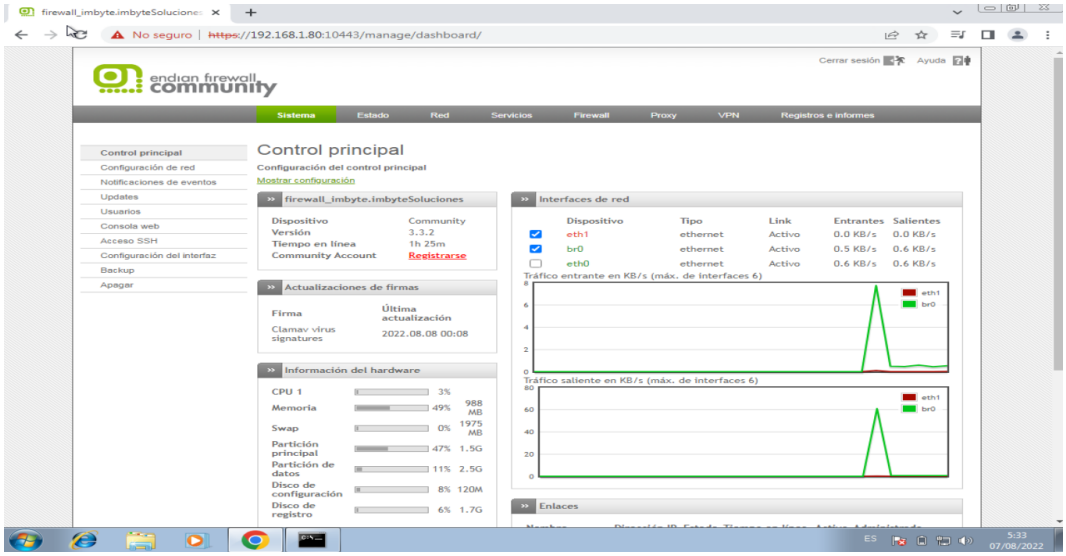
Nota: Para comprobar la configuración realizada, se realiza el cambio de DHCP a modo automático.

Figura 22 *Verificación de la conexión a la red de datos*



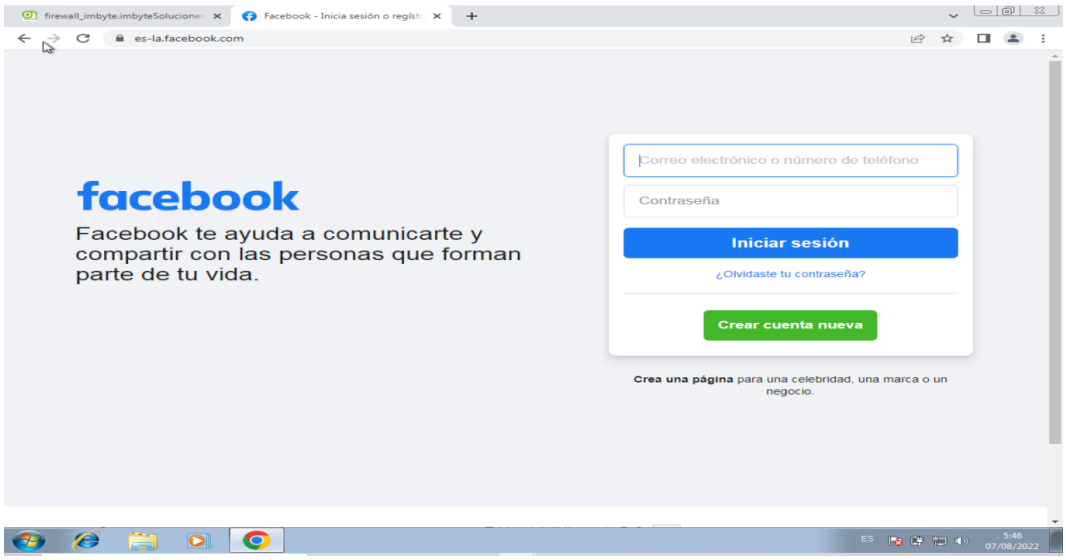
Nota: Se realizaron las pruebas pertinentes para comprobar que se tenga acceso a la red de interne normalmente.

Figura 23 *Pantalla principal del servicio de Endian*



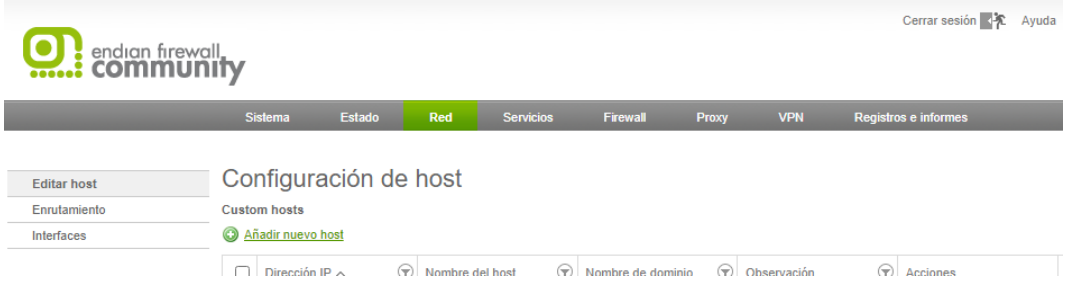
Nota: Aquí se puede apreciar la pantalla principal de Endian el mismo que ya cuenta con la configuración y parámetros asignados sobre la red y el servidor además se puede evidenciar que aún no cuenta con algún servicio activo.

Figura 24 *Prueba de navegación por la red*



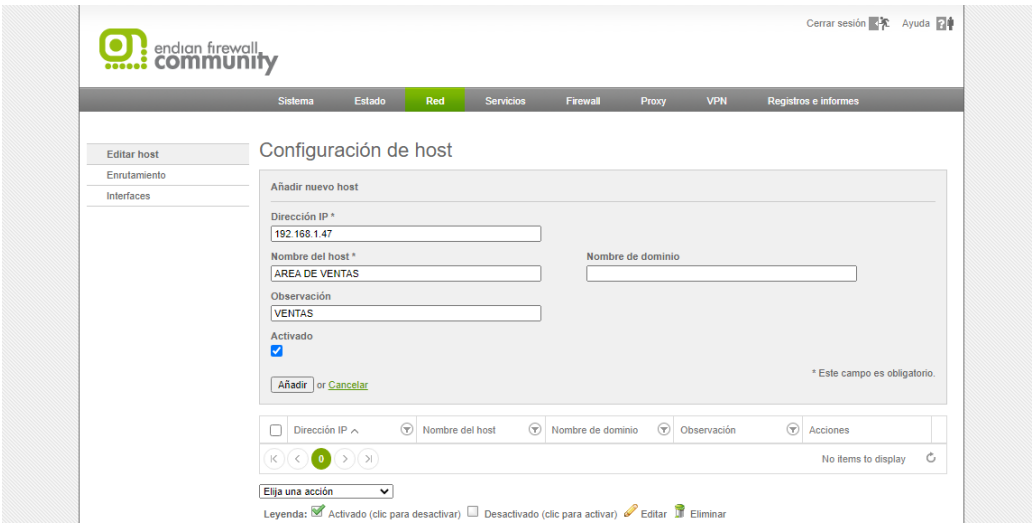
Nota: Comprobamos que podemos navegar libremente sin ninguna restricción, aun no realizado el filtrado. Esta es una prueba previa en la que se puede evidenciar que el acceso a paginas ajenas al trabajo que realiza la empresa es concedido sin ninguna restricción esto es previo a la creación de reglas y políticas de seguridad en el servidor.

Figura 25 *Configuración de equipos de red*



Nota: En el apartado de red se realizó las configuraciones de Host.

Figura 26 *Configuración de IP en el Host*

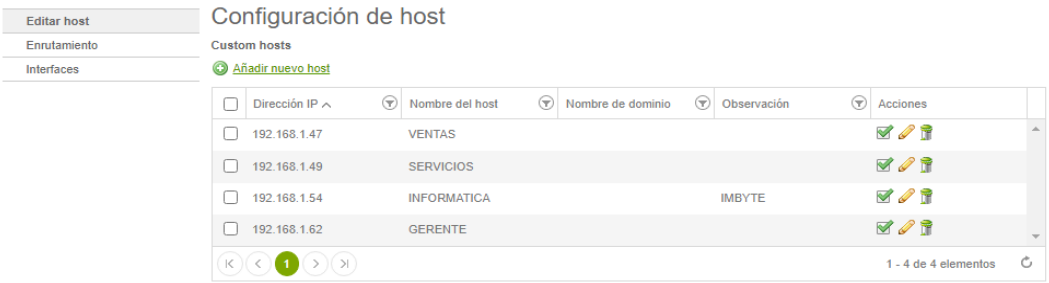


Nota: Aquí se añadió los IP de los equipos que existen en la red de la empresa. Asi mismo se establecerá los permisos de usuario asignando privilegios según el nivel de acceso.

Primeramente, se crea o se añade usuarios a los equipos informáticos basados en:

- ✓ Direcciones IP
- ✓ Nombre de Equipo
- ✓ Nombre de Usuarios

Figura 27 *Lista de equipos de la red*

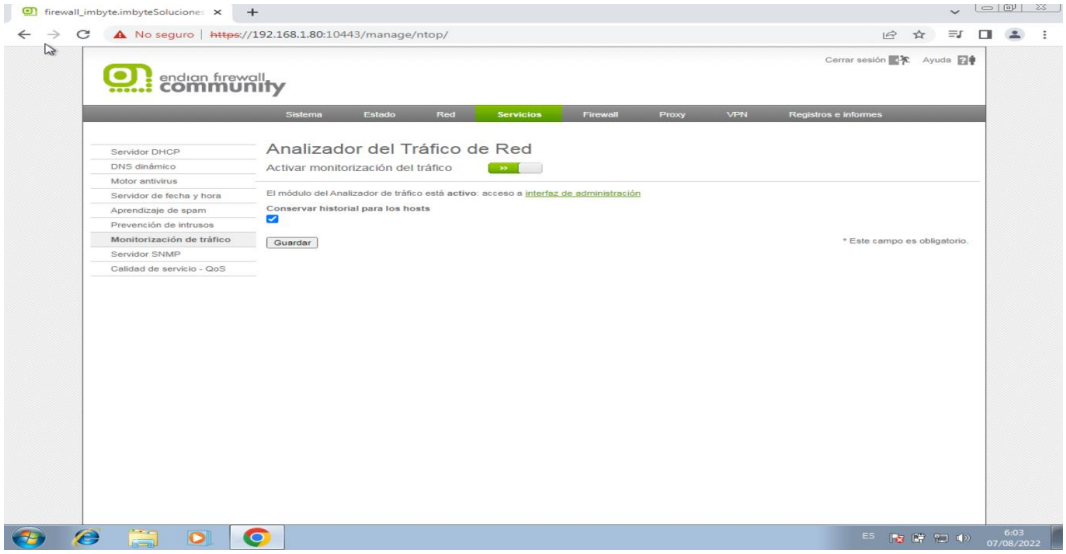


Nota: Se puede visualizar la lista de los equipos añadidos a la red de la empresa y configurados por nombre de usuarios de cada área.

4.7.2. Filtrado de páginas web restringidas

En este punto se inició con las pestañas de servicios, aquí visualizaremos el DHCP que hemos activado el cual se está utilizando y también el rango de IPS que se le asignó a las PC el cual también se puede modificar, ya que nosotros estamos en el PC servidor.

Figura 28 *Activación de trafico de red*

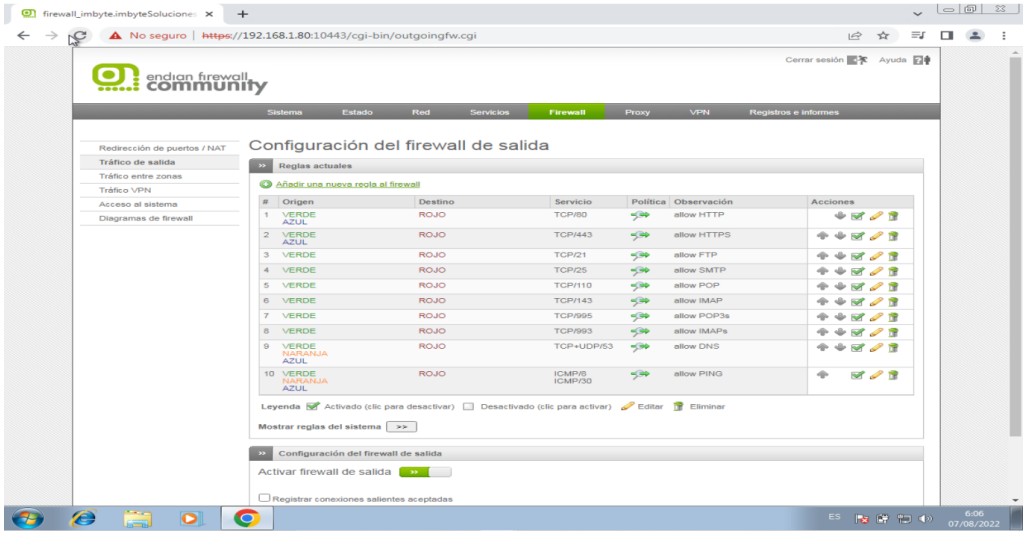


Nota: Tal y como se puede apreciar en la imagen procedemos a activar el analizador de trafico de red para poder medir el tráfico de la red de datos garantizando que este se encuentre en las mejores condiciones.

Figura 29 *Activación del servicio de prevención de intrusos*

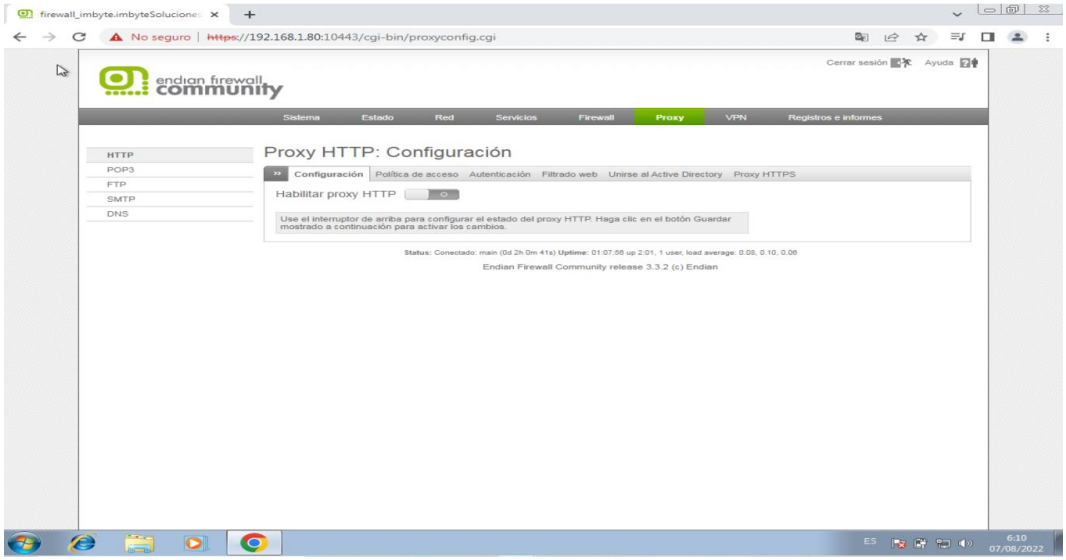
Nota: Ahora se puede evidenciar un paso importante para la protección de la red de datos de la empresa, se procedió a activar el filtro de intrusos para evitar que cualquier ciberdelincuente tenga acceso a los datos de la red de la empresa.

Figura 30 *Configuración de firewall de salida*



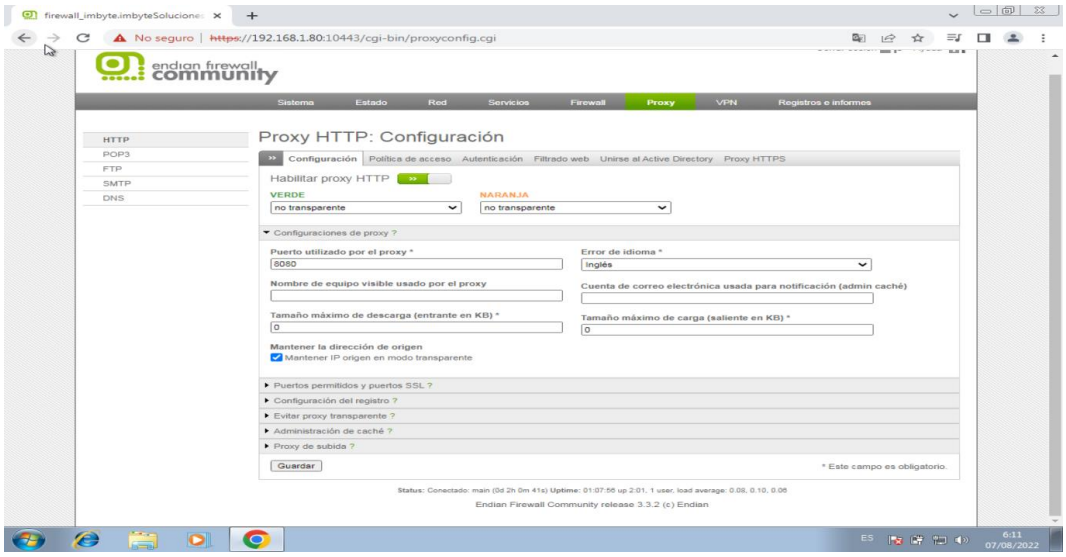
Nota: Ingresamos a la pestaña Firewall en la cual podemos revisar que en el tráfico de salida, todos los puertos están activos esta información será indispensable para el control de los accesos a la red de la empresa.

Figura 31 *Activación del protocolo HTTP*



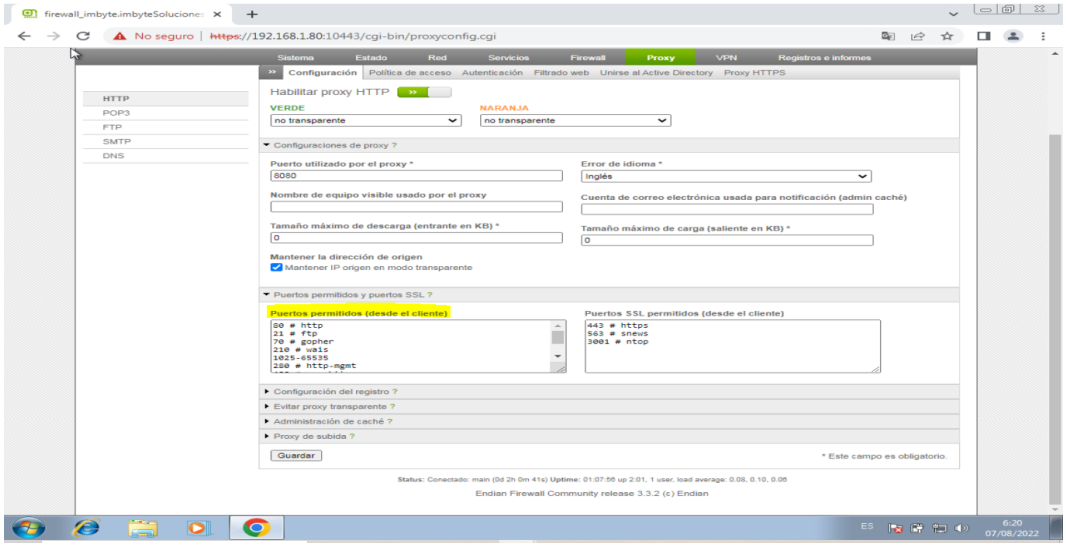
Nota: Ingresamos a la pestaña Proxy y activamos el Proxy HTTP, para poder empezar a realizar el Filtrado según los requerimientos de la empresa se realizara el filtrado de paginas para bloquear el acceso a páginas que no tengan que ver con las actividades que realiza la empresa.

Figura 32 *Configuración del servicio Proxy HTTP*



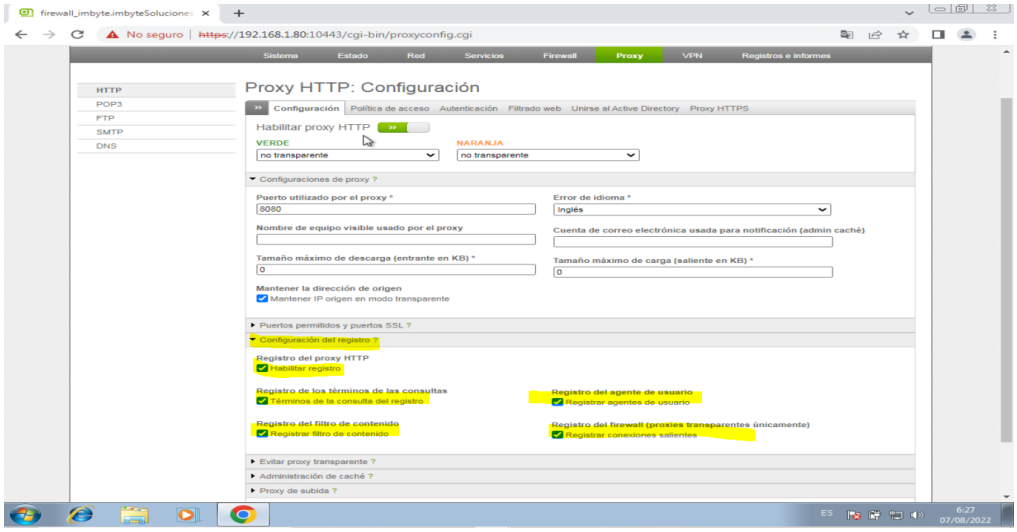
Nota: Aquí se realizó el cambio del modo y podemos visualizar que se uso el puerto 8080.

Figura 33 *Verificación de puertos permitidos en la red*



Nota: Aquí podemos visualizar los puertos con el que cuenta Endian Firewall.

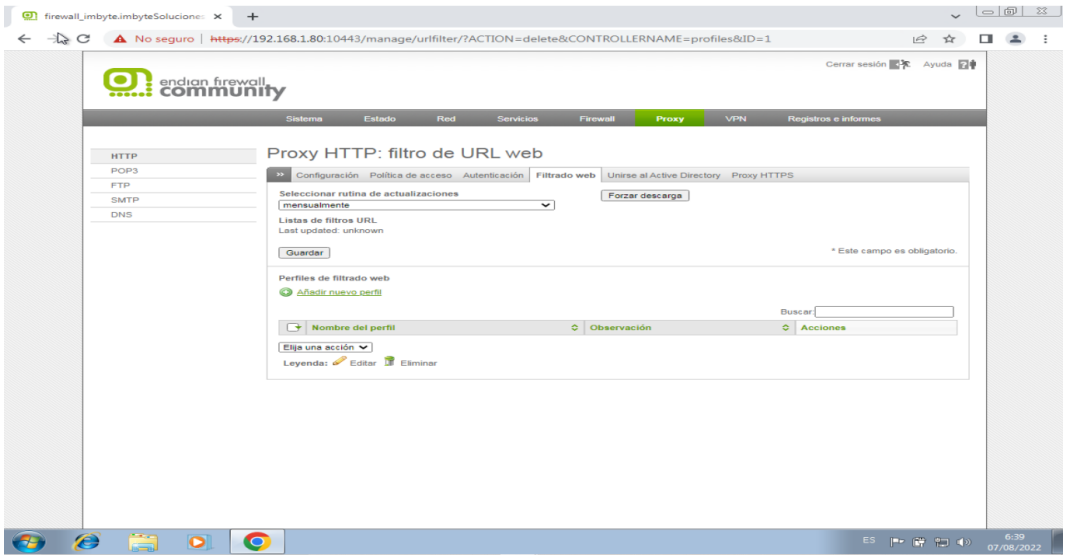
Figura 34 *Habilitación de registros de puertos*



Nota: En esta parte se procedió a habilitar los registros para posteriormente monitorear cual ha sido el registro del firewall como tal el mismo que se controlara para verificar el flujo de datos en el puerto seleccionado.

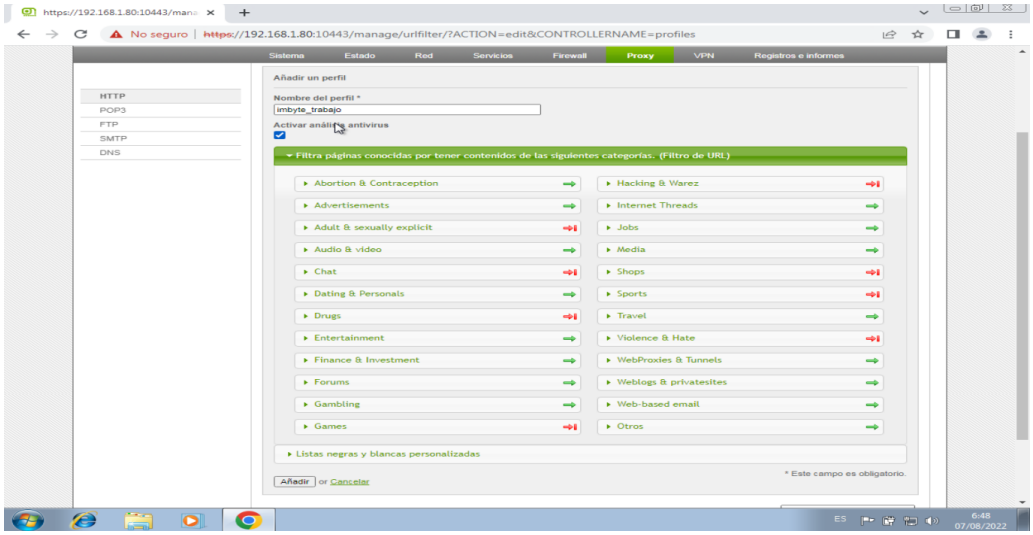
4.7.3. Filtro WEB

Figura 35 *Selección de la Rutina*



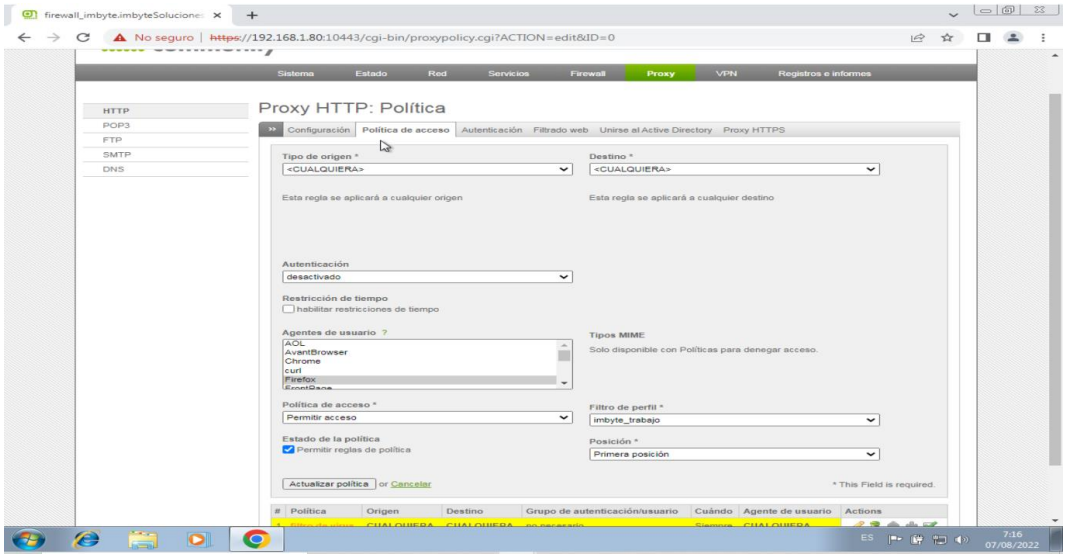
Nota: En esta parte Seleccionamos la rutina de actualización y agregamos un perfil

Figura 36 *Selección de filtros por categoría*



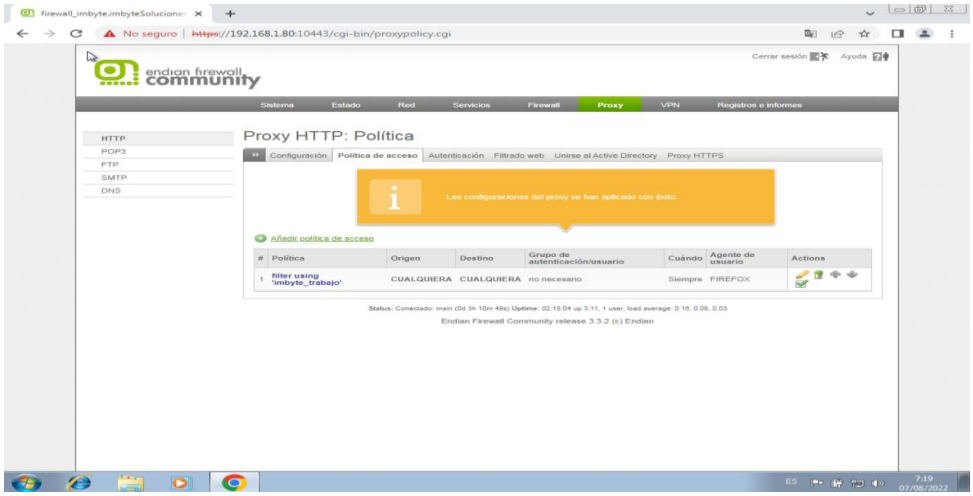
Nota: En este apartado se procedió a identificar y seleccionamos las categorías que deseamos filtrar, así mismo se asignó el usuario a cual se le aplicara el filtro.

Figura 37 *Configuración de políticas de acceso*



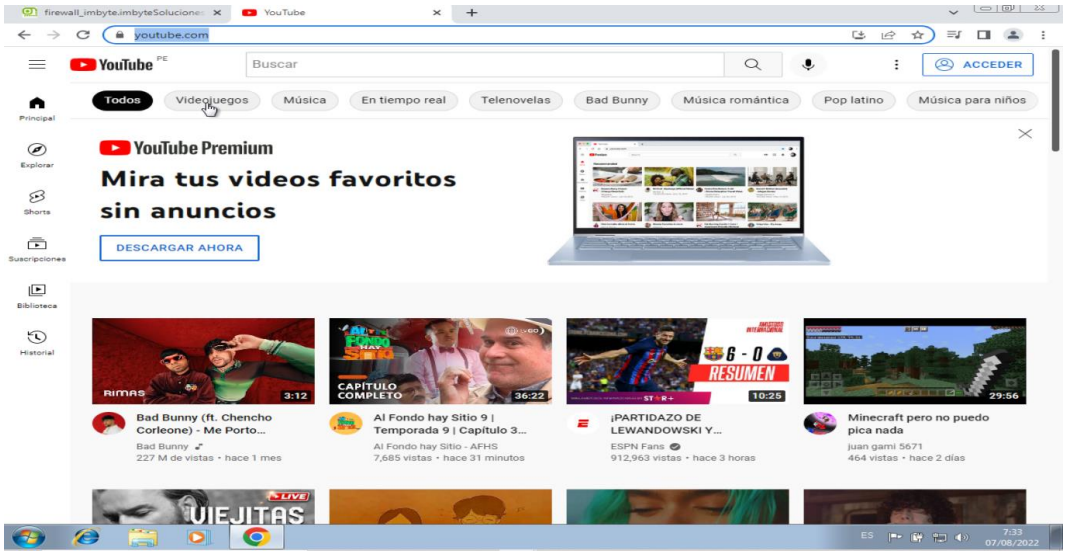
Nota: En esta parte en la pestaña políticas de acceso se editó la política para posteriormente añadir el perfil de filtro que se creó previamente.

Figura 38 *Visualización de políticas del servicio*



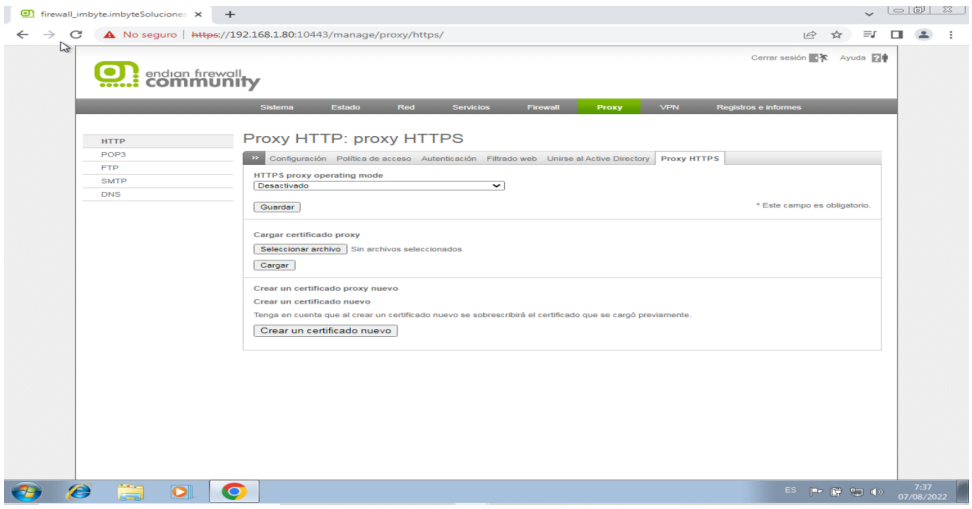
Nota: Como se puede apreciar en la imagen se han aplicado y guardado los cambios de las políticas que se añadieron, junto con todas las configuraciones de acceso de usuario a paginas no autorizadas por la empresa.

Figura 39 *Comprobación de filtros*



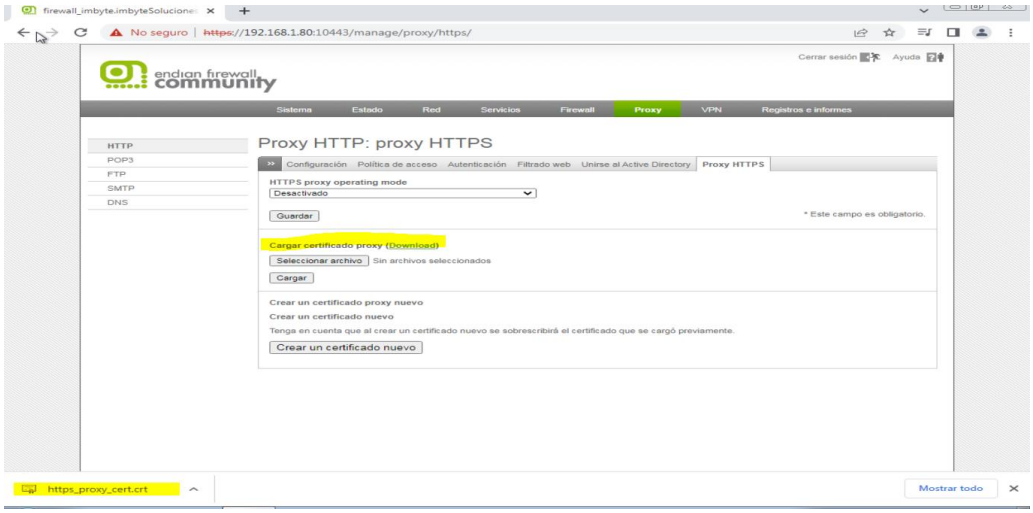
Nota: En esta parte se puede apreciar que se puede navegar con normalidad y sin restricción a pesar que hemos aplicado el filtro, en este caso es porque hemos filtrado el protocolo HTTP, lo cual estas páginas tienen protocolo HTTPS.

Figura 40 *Creación del certificado HTTPS*



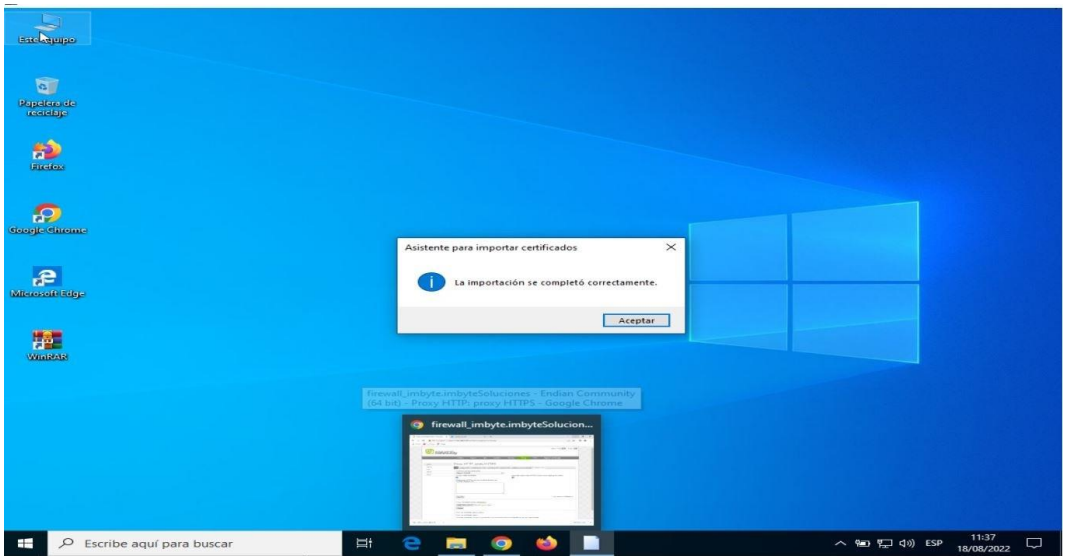
Nota: Se creo un certificado requerido el mismo que posteriormente será instalado en el equipo en el cual se aplicara el filtro.

Figura 41 *Descarga de Certificado creado*



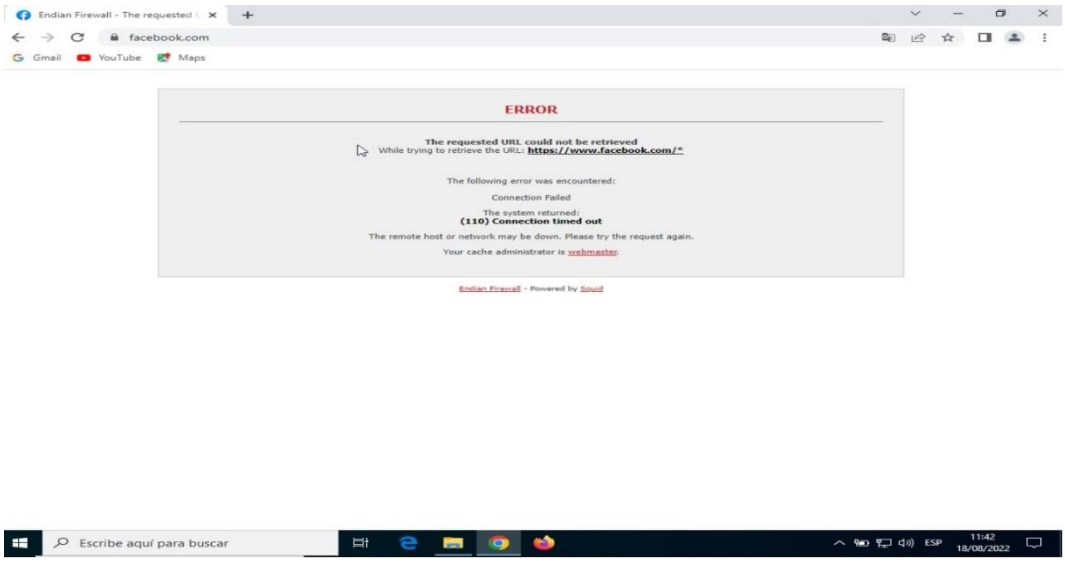
Nota: En este parte ya descargado el certificado se procedió a instalar en la el equipo en el cual se realizará el filtrado.

Figura 42 *Instalación del certificado*



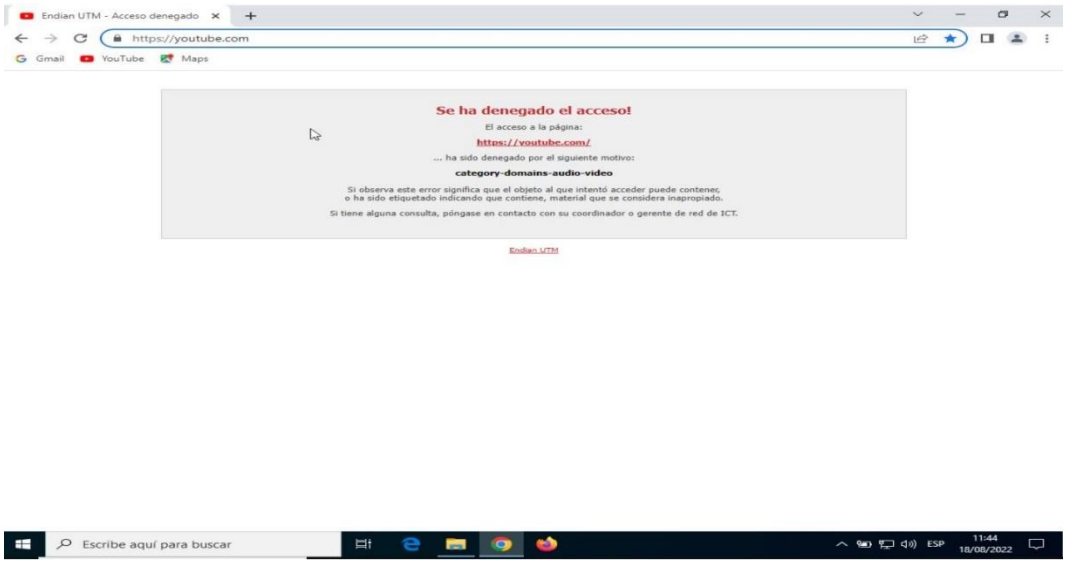
Nota: Como se puede apreciar la instalación del certificado creado se realizó satisfactoriamente.

Figura 43 *Filtro de red social Facebook*



Nota: Como se puede apreciar en la imagen se realizó la validación del certificado de filtro. Vemos que el filtrado de la red social Facebook, después de haber instalado el certificado, es exitoso.

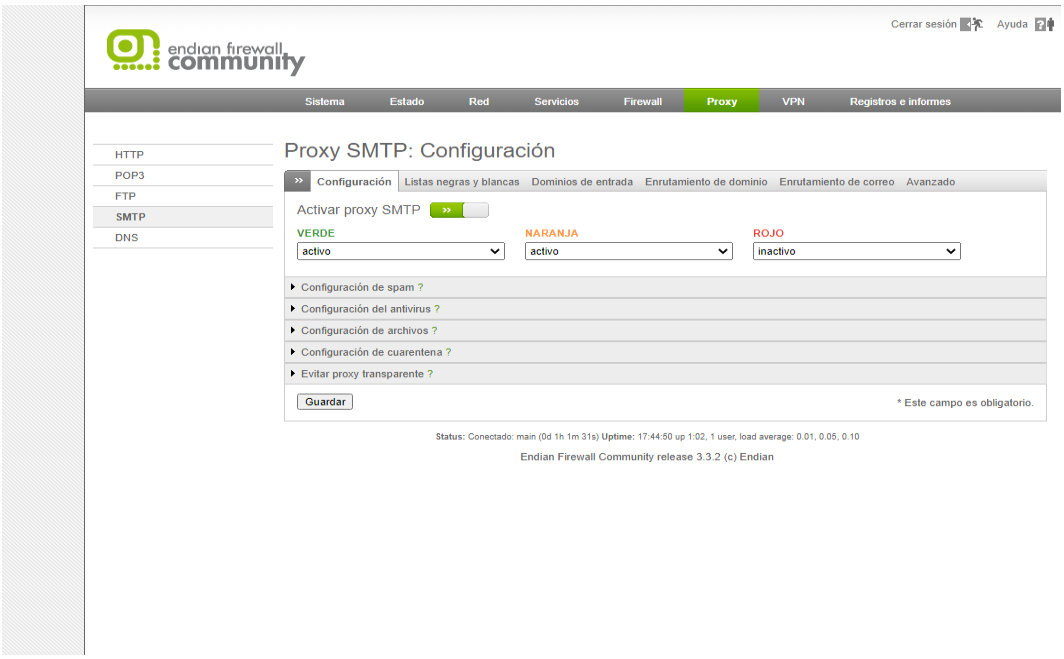
Figura 44 *Filtro de YouTube*



Nota: Como se puede apreciar en la imagen se realizó la validación del certificado de filtro. Vemos que el filtrado de la página de YouTube, después de haber instalado el certificado, es exitoso.

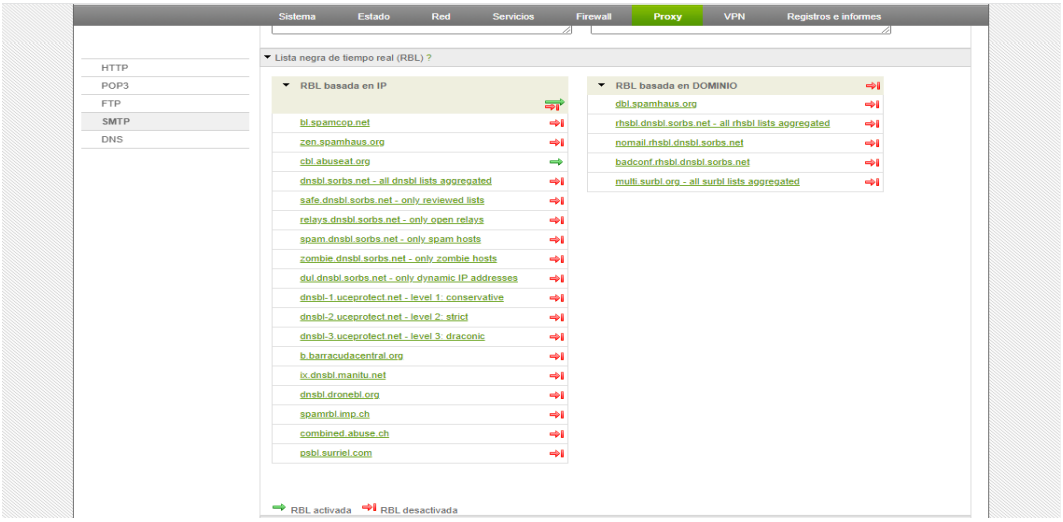
4.7.4. Configuración SMTP

Figura 45 *Configuración Proxy SMTP*



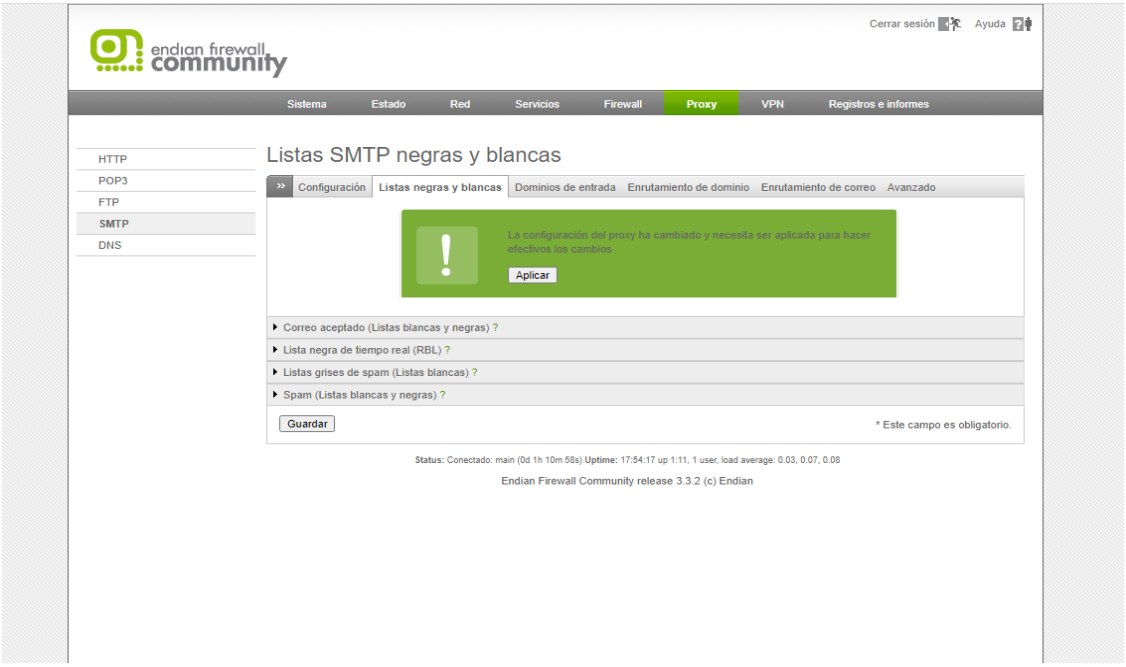
Nota: En este apartado se procedió a realizar la configuración del Proxy SMTP para validar según listas los accesos lo cual al momento que se activó la sección en verde.

Figura 46 *Referencia de listas*



Nota: Se hace referencia a los denominados Black & Write list, se despliega varias opciones, pero la más importante en este campo en tiempo real son las listas negras que se puede observar y contrastar que cada URL contiene registros de spam y los bloqueara.

Figura 47 *Validación y registro de cambios*



Nota: Como paso primordial para mantener esa configuración establecida se procedió a guardar y aplicar los cambios teniendo como resultado la imagen que se muestra anteriormente.

Entonces en este punto si el firewall llegara a detectar el control automático de spam por defecto, las acciones que se harán, será de bloquear el contenido, impidiendo y mostrando en pantalla, el acceso al contenido.

CAPITULO V: RESULTADOS Y DISCUSIÓN

5.1. Presentación, análisis e interpretación

En este capítulo se presentarán los resultados obtenidos después de haber aplicado todos los instrumentos de recolección de datos y se evidenciara la discusión de estos de acuerdo a la hipótesis planteada.

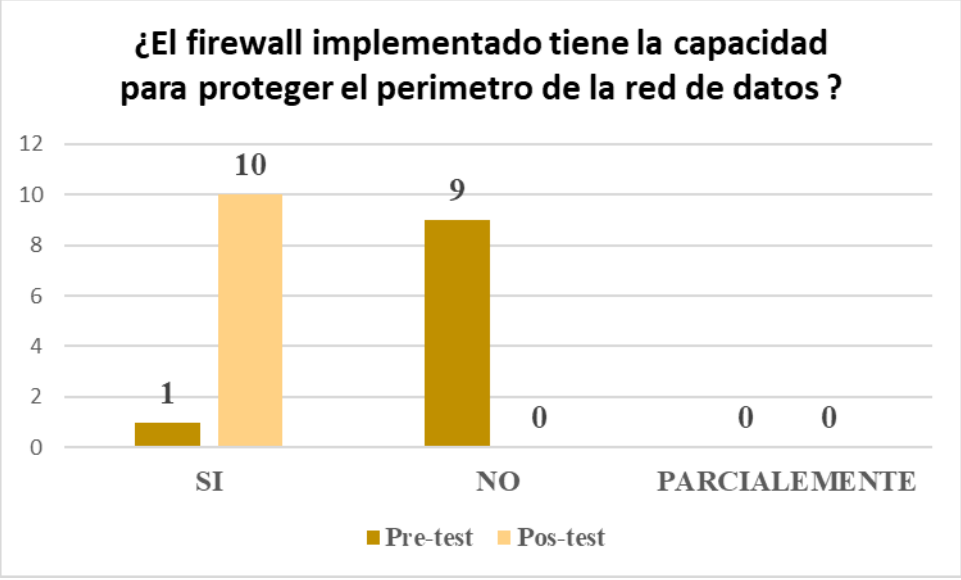
5.1.1. Resultados de la variable implementación de Endian Firewall

A continuación, presentamos los resultados obtenidos después de la aplicación del instrumento de medición, los mismos que se clasifican por dimensión.

5.1.1.1. Resultado de la dimensión Eficacia

A continuación, presentamos los resultados de la dimensión eficacia

Figura 48 *¿El firewall implementado tiene la capacidad de proteger el perímetro de la red de datos?*



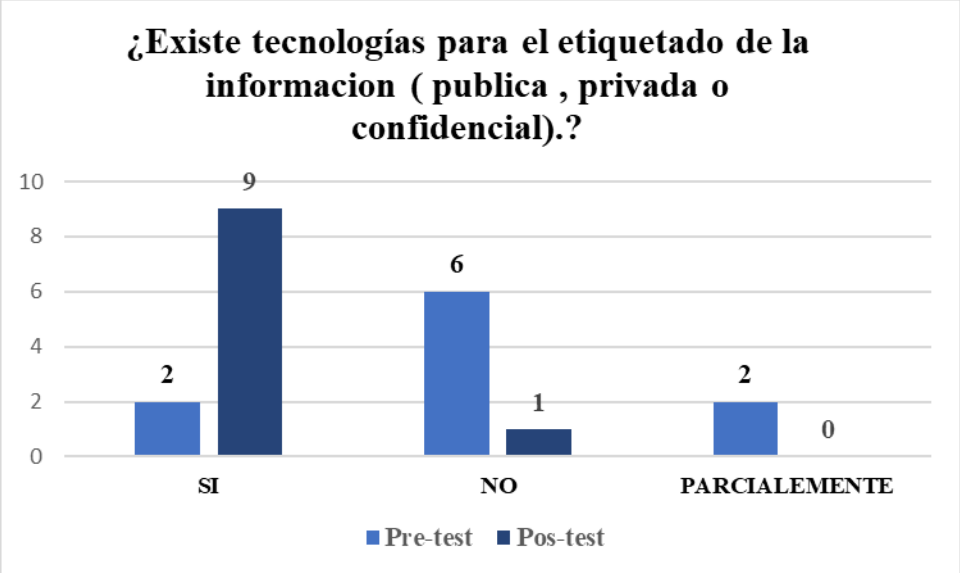
Fuente: Elaborado por los autores (2022). A partir de los datos recolectados de las encuestas aplicadas.

En la Figura 48, se muestran los resultados a la pregunta ¿El firewall Implementado tiene la capacidad de proteger el perímetro de la red de datos? En la cual el pre test las 9 personas manifiestan que, no cuentan con sistemas de protección de datos, mientras que una 1 de los encuestada dicen que si cuentan un firewall de protección de perímetro de la red de datos. En el post test las 10 personas encuestados manifestaron que el Firewall Implementado si cuenta con la capacidad para proteger el perímetro de la red de datos

5.1.1.2. Resultado de la dimensión Disponibilidad

A continuación, presentamos los resultados de la dimensión Disponibilidad

Figura 49 *¿Existe tecnología para el etiquetado de la información (pública, privada o confidencial)?*

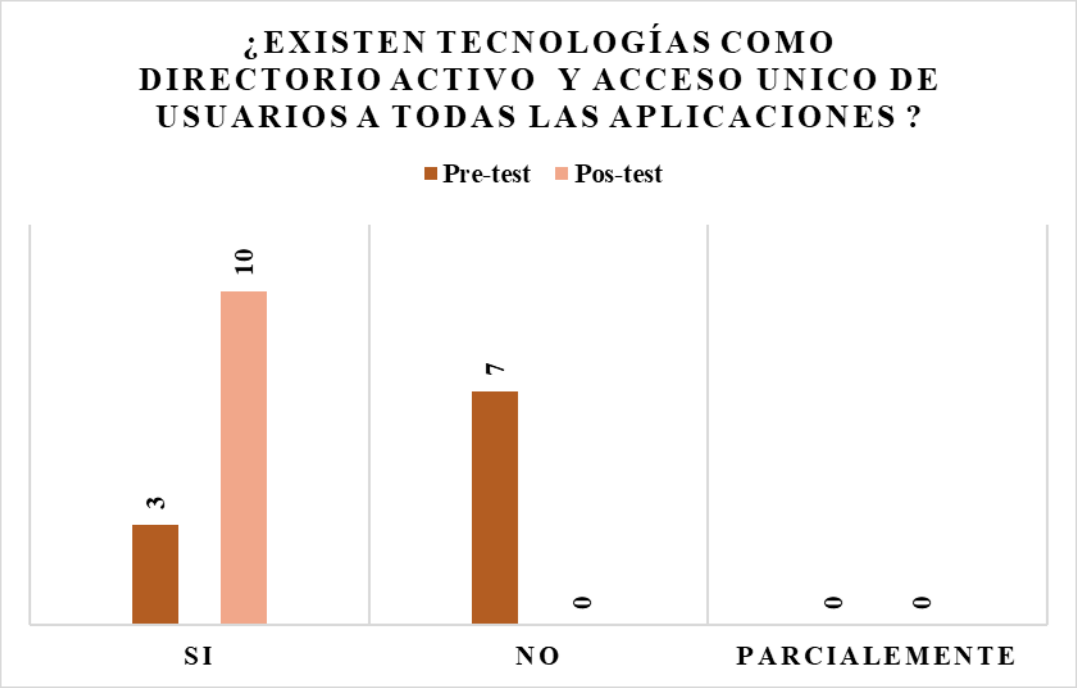


Fuente: Elaborado por los autores (2022). A partir de los datos recolectados de las encuestas aplicadas.

En la Figura 49, se muestran los resultados a la pregunta ¿Existe tecnología para el etiquetado de la Información (Pública, Privada o Confidencial)? En la cual el pre test las 2 personas encuestadas manifiestan que, si cuentan con una tecnología de

etiquetado de datos, mientras que 6 encuestados dicen que no cuenta con tecnología de etiquetado de datos y en las 2 personas encuestadas dicen que se cuenta parcialmente con tecnología de etiquetado de datos. En el post test 9 encuestados manifestaron que si se cuenta con un sistema de etiquetado de información mientras que 1 encuestado manifiesta lo contrario. Este gran cambio se debe al cifrado de la información.

Figura 50 *¿Existen tecnologías como directorio activo y acceso único de usuario a todas las aplicaciones?*



Fuente: Elaborado por los autores (2022). A partir de los datos recolectados de las encuestas aplicadas.

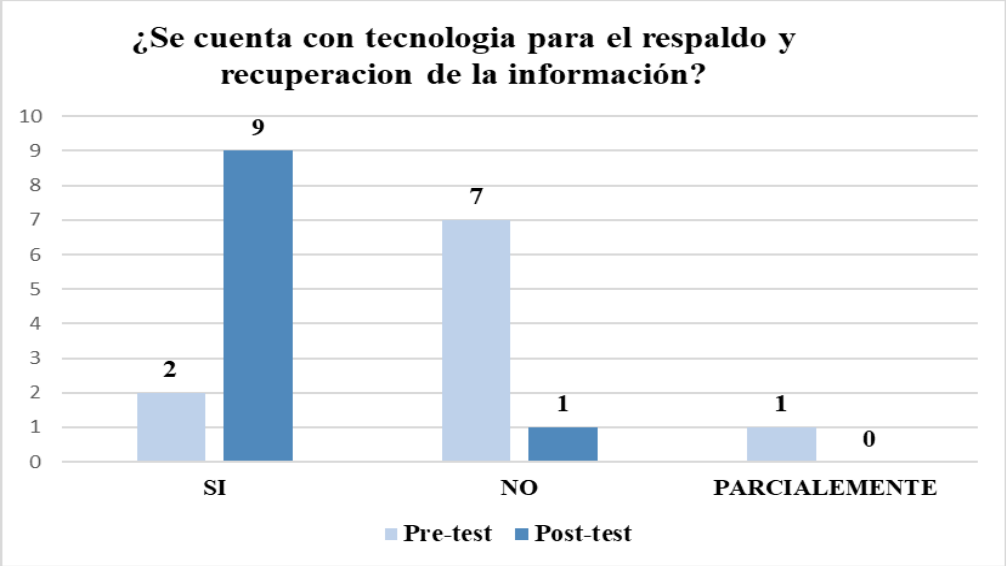
En la Figura 50, se muestran los resultados a la pregunta ¿Existen tecnologías como directorio activo y acceso único a usuarios a todas las aplicaciones? En la cual el pre test 3 personas encuestadas dicen, que, si cuentan con una tecnología como directorio activo y acceso único de usuarios, mientras que 7 personas encuestadas

manifiestan que no cuenta con tecnología como directorio activo y acceso único a usuarios. En el post test las 10 personas encuestadas manifestaron que si se cuenta con tecnologías como directorio activo y acceso único a usuarios.

5.1.1.3. Resultados de la dimensión Integridad

A continuación, presentamos los resultados de la dimensión Integridad

Figura 51 *¿Se cuenta con Tecnología para el respaldo y recuperación de la información*

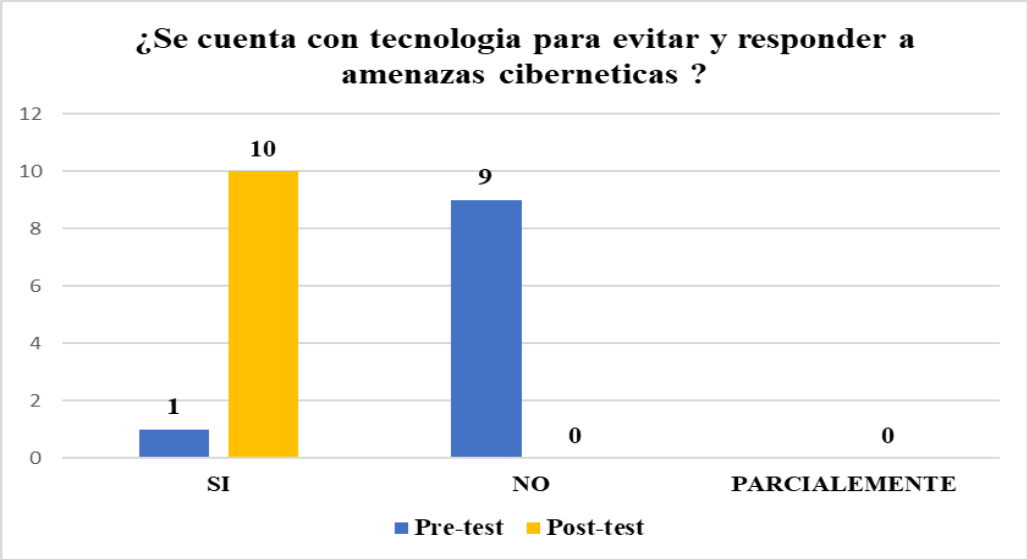


Fuente: Elaborado por los autores (2022). A partir de los datos obtenidos de las encuestas realizadas.

En la Figura 51, se muestran los resultados a la pregunta ¿Se cuenta con Tecnología para el respaldo y Recuperación de la Información? En la cual el pre test ,2 personas encuestadas dicen, que, si cuentan con tecnología para el respaldo y recuperación de la información, mientras que 7 personas encuestadas dicen que no cuenta con tecnología del respaldo y recuperación de la información, mientras que 1 persona encuestada dice que se parcialmente se cuenta con tecnología de recuperación y respaldo de información. En el post test las 9 personas encuestadas manifestaron

que, si se cuenta con tecnologías de respaldo y recuperación de información, mientras que 1 persona de los encuestados dice que no se cuenta con tecnología de respaldo y recuperación de datos.

Figura 52 *¿Se cuenta con tecnología para evitar y responder a amenazas cibernéticas?*



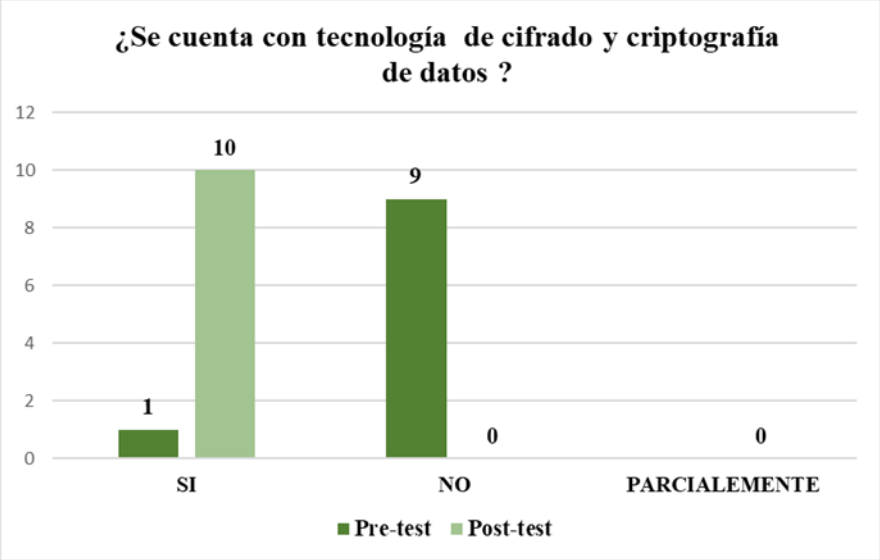
Fuente: Elaborado por los autores (2022*)*. A partir de los datos obtenidos de las encuetas realizadas.

En la Figura 52, se muestran los resultados a la pregunta ¿Se cuenta con tecnología para evitar y responder a amenazas cibernéticas? En la cual el pre test 9 personas de las encuestadas dicen, que, no se cuentan con una tecnología para evitar y responder a amenazas cibernéticas, mientras que 01 persona de las encuestadas menciona que si cuenta con tecnología para evitar y responder a amenazas cibernéticas. En el post test las 10 personas encuestados manifestaron que si se cuenta con tecnología para evitar y responder a amenazas cibernéticas.

5.1.1.4. Resultados de la dimensión confiabilidad de datos

A continuación, presentamos los resultados de la dimensión Confiabilidad de datos

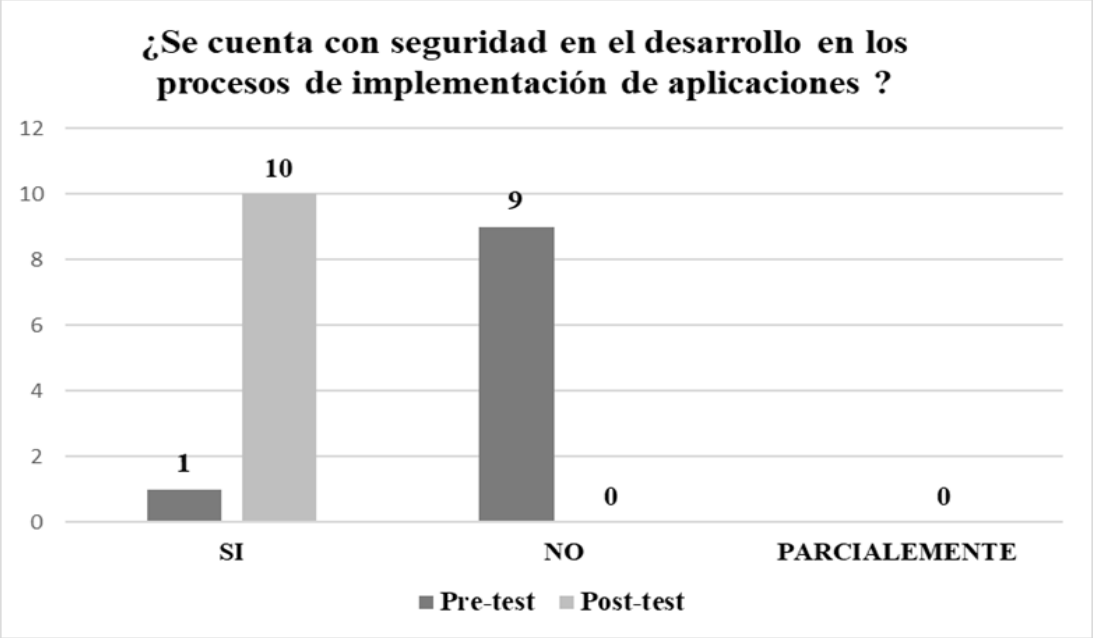
Figura 53 *¿Se cuenta con tecnología de cifrado y criptografía de datos?*



Fuente: Elaborado por los autores (2022). A partir de los datos recolectados de las encuestas aplicadas.

En la Figura 53, se muestran los resultados a la pregunta ¿Se cuenta con tecnología de cifrado y criptografía de datos? En la cual el pre test las 9 personas de las encuestadas dicen, que, no se cuentan con una tecnología de cifrado y criptografía de datos, mientras que 01 persona de las encuestadas menciona que si cuenta con tecnología de cifrado y criptografía de datos datos. En el post test las10 personas encuestados manifestaron que si se cuenta con tecnología de cifrado y criptografía de datos.

Figura 54 *¿Se cuenta con seguridad en el desarrollo y en los procesos de implementación de aplicaciones?*



Fuente: Elaborado por los autores (2022). A partir de los datos recolectados de las encuestas aplicadas

En la Figura 54, se muestran los resultados a la pregunta ¿Se cuenta con seguridad en el desarrollo y en los procesos de implementación de aplicaciones? En la cual el pre test, 09 personas encuestadas dicen, que, no se cuenta con seguridad en el desarrollo y en los procesos de implementación de aplicaciones, mientras que 01 de los encuestados dicen que si cuentan con seguridad en el desarrollo y en el proceso de implementación de aplicaciones. En el post test los 10 encuestados manifestaron que si se cuentan con seguridad en el desarrollo y en el proceso de implementación de aplicaciones

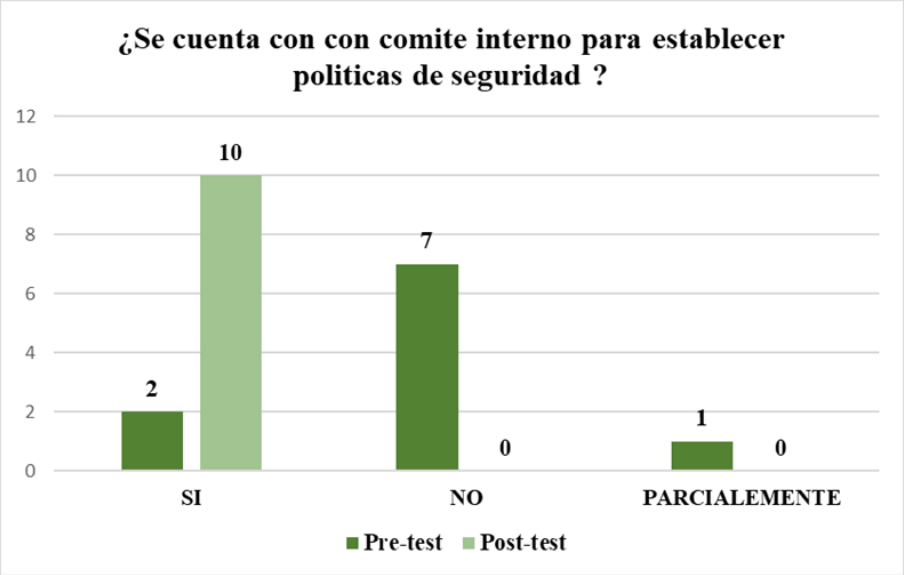
5.1.2. Resultados de la variable gestión de seguridad perimetral en las MYPES Cajamarca caso: Imbyte soluciones

A continuación, presentamos los resultados obtenidos después de la aplicación del instrumento de medición, los mismos que se clasifican por dimensión.

5.1.2.1. Resultados de la variable verificación de activos

A continuación, presentamos los resultados de la dimensión Verificación de activos

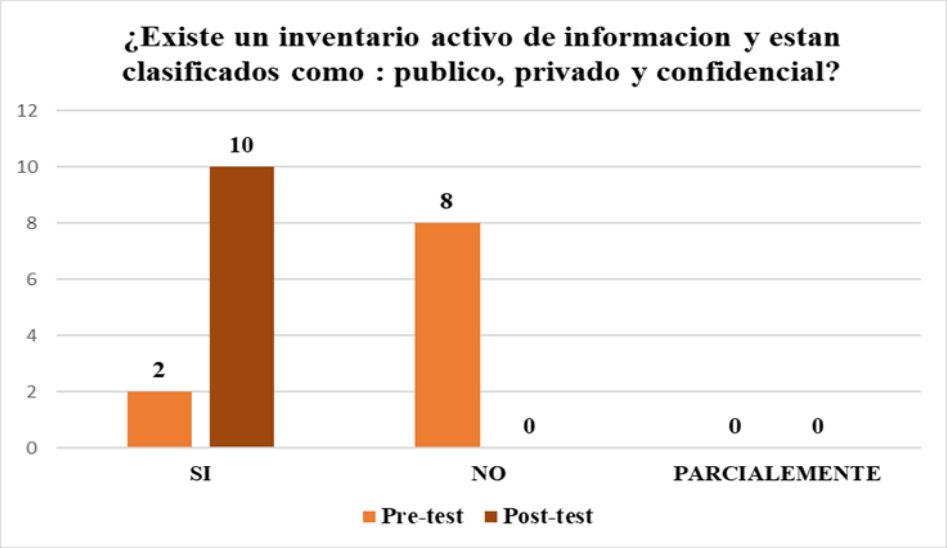
Figura 55 *¿Se cuenta con un comité interno para establecer políticas de seguridad?*



Fuente: Elaborado por los autores (2022*).* A partir de los datos recolectados de las encuestas aplicadas

En la Figura 55, se muestran los resultados a la pregunta ¿Se cuenta con un comité interno para establecer políticas de seguridad? En la cual en el pre test, 07 personas encuestadas dicen, que, no se cuenta con un comité para establecer políticas de seguridad, mientras,02 encuestados manifiestan que si cuentan con un comité para establecer políticas de seguridad y 01 encuestado dice que se cuenta parcialmente con comité interno para políticas de seguridad. En el post test los 10 encuestados manifestaron que si se cuentan con un comité para establecer políticas de seguridad.

Figura 56 *¿Existe un inventario de activos de información y están clasificados como público, privado y confidencial?*



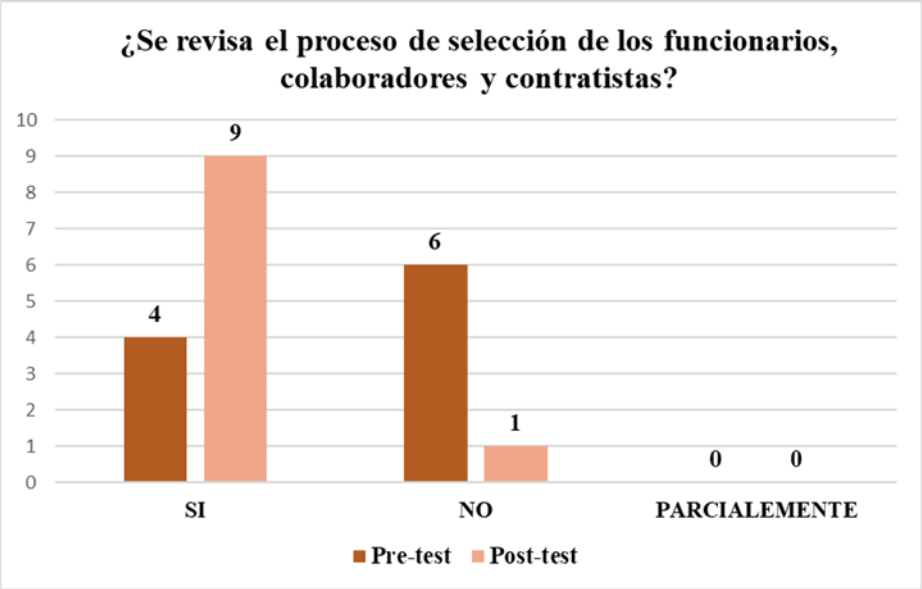
Fuente: Elaborado por los autores (2022). A partir de los datos recolectados de las encuestas aplicadas

En la Figura 56, se muestran los resultados a la pregunta ¿Existe un inventario de los activos de la información y están clasificados como, ¿Público, Privado y confidencial?, En la cual el pre test 08 personas encuestados dicen, que no existe un inventario de los activos de la información y no están clasificados como , público , privado y confidencial , mientras que 02 encuestados manifiestan que si Existe un inventario de los activos de la información y están clasificados como, Público, Privado y confidencial . En el post test las 10 personas encuestados manifestaron que, si Existe un inventario de los activos de la información y están clasificados como, Público, Privado y confidencial.

Resultado de la dimensión Satisfacción de la empresa

A continuación, presentamos los resultados de la dimensión satisfacción de la empresa.

Figura 57 *¿Se revisa el proceso de selección de los funcionarios, colaboradores y contratistas?*

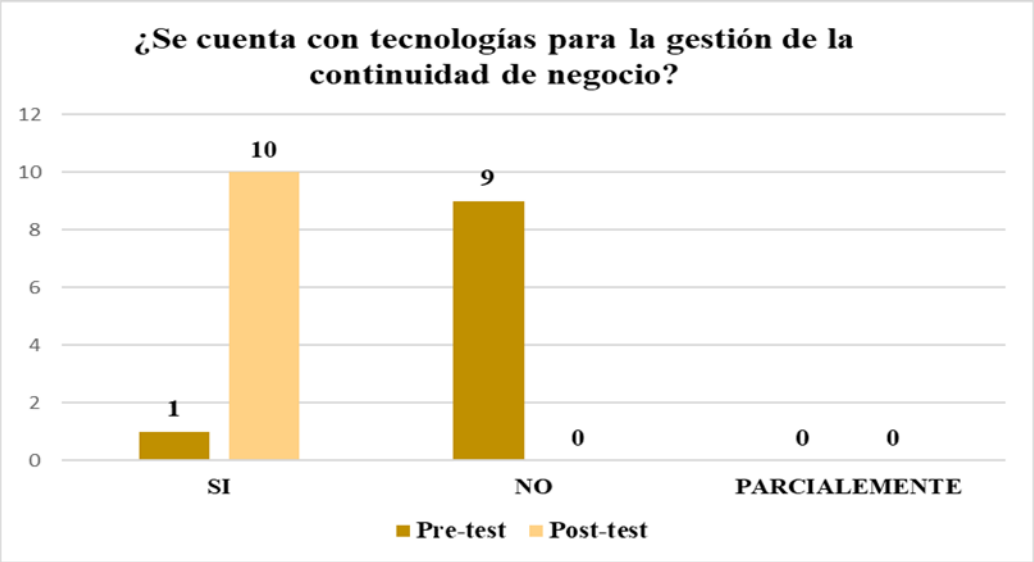


Fuente: Elaborado por los autores (2022). A partir de los datos recolectados de las encuestas aplicadas.

En la Figura 57, se muestran los resultados a la pregunta ¿Se revisa el proceso de selección de los funcionarios, colaboradores y contratistas ?, En la cual en el pre test ,06 personas encuestadas dicen, que no se revisa el proceso de selección de los funcionarios, colaboradores, y contratistas, mientras que 04 personas encuestadas manifiestan que si se revisa el proceso de selección de los funcionarios, colaboradores y contratistas. En el post test 09 encuestados manifestaron que, si se revisa el proceso de selección de los funcionarios, colaboradores y contratistas, mientras que 01 encuestado dice que no se revisa el proceso de selección de los

funcionarios, colaboradores y contratistas, este gran cambio debido a que se planteó políticas de seguridad de la información en la empresa.

Figura 58 *¿Se cuenta con tecnologías para la gestión de la continuidad de negocio?*



Fuente: Elaborado por los autores (2022). A partir de los datos recolectados de las encuestas aplicadas.

En la Figura 58, se muestran los resultados a la pregunta ¿Se con tecnologías para la gestión de la continuidad del negocio?, En la cual en el pre test, 09 personas encuestadas dicen, que no se cuenta con tecnologías para la gestión de la continuidad del negocio, mientras que 01 persona encuestadas manifiestan que si se cuenta con tecnologías para la gestión de continuidad del negocio. En el post test las 10 personas encuestadas manifestaron que, si se cuenta con tecnologías para la gestión de continuidad del negocio.

5.2. Contrastación de la hipótesis

En la presente investigación previo a la contrastación de la hipótesis se realizó una prueba de normalidad de los datos para poder identificar si los datos tienen una distribución normal o no normal en caso los datos tengan una distribución normal será necesario emplear una prueba Paramétrica, de lo contrario si los datos tienen una distribución no normal se elegirá una prueba estadística no paramétrica. Para esta investigación se aplicó la prueba de normalidad Shapiro-Wilk la misma que se aplica para estudios con una muestra menor o igual a 50, obteniendo el siguiente resultado.

Tabla 5 *Tabla de normalidad de Shapiro Wilk*

Prueba de normalidad Shapiro-Wilk			
	Estadístico	**gl**	**Sig.**
Pre-Test	0.871	10	0.102
Post-test	0.941	10	0.560

Nota: tabla de normalidad de Shapiro-Wilk realizada con los datos obtenidos de la empresa

Según los resultados obtenido se tiene una significancia (sig.) mayor a 0,05 indicando normalidad, por lo tanto, se afirma que los datos tienen una distribución normal, información importante para poder aplicar el estadígrafo T-Student así determinar la veracidad de la hipótesis "La implementación de Firewall Endian Comunity influye positivamente en la gestión de la seguridad perimetral en la empresa Imbyte soluciones, Cajamarca". y se obtuvo el siguiente resultado mostrado en la tabla.

Tabla 6 *Prueba t-student*

	Diferencias emparejadas					t	gl	Sig. (bilateral)
	Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
				Inferior	Superior			
Pre test-Post test	2.200	1.398	0.442	1.200	3.200	4.975	9	0.001

Nota: tabla de la Prueba t-Student aplicada con los datos de la empresa.

H1: La implementación de Firewall Endian Comunity influye positivamente en la gestión de la seguridad perimetral en la empresa Imbyte soluciones, Cajamarca.

H0: La implementación de Firewall Endian Comunity no influye positivamente en la gestión de la seguridad perimetral en la empresa Imbyte soluciones, Cajamarca.

Regla de Decisión

- Significancia =0.05 o 5%
- Si p>=0.05, Se Acepta H0 y se Rechaza H1
- Si p< 0.05, Se Rechaza H0 y Se acepta H1

Como "Sig" o valor "p=0.001" que es menor a 0.05; entonces se rechaza H0 y se Acepta H1.

En consecuencia, como el resultado de la significancia bilateral es 0,001 menor al 0,05, por lo tanto, se afirma la veracidad de la hipótesis propuesta, donde el pre y post test son significativamente diferentes, diciendo entonces que la implementación de Firewall Endian Comunity mejora la gestión de la seguridad perimetral en las MYPES de la ciudad de Cajamarca: caso Imbyte soluciones.

Se puede observar que la implementación del firewall Endian si influye en la seguridad perimetral de la empresa salvaguardando la información de los clientes, permitiendo tener una mejor gestión de la seguridad con la información de la empresa, también se percibe la relación entre ambas variables de la investigación, como aporte al conocimiento esta investigación queda como un precedente para futuras investigaciones.

5.3. Discusión de resultados

De acuerdo a los datos obtenidos, Según (Bueno Rosales, 2013). En su tesis de nombre: "Sistema de control y seguridad Endian Firewall para la empresa FRADA SPORT. Universidad tecnológica Israel. quito- ecuador", pudo demostrar que Endian Firewall brinda una manera de control , seguridad y disponibilidad , rendimiento y administración de la red de la empresa , que no genera ningún costro adicional , por nuestra parte con la implementación de Endian Firewall se pudo conocer la mejora y mayor seguridad en la red de datos y sistemas de las áreas de la empresa , con los resultados de las encuestas aplicadas se logró evidenciar un aumento del 80 % en la seguridad en la red de datos e internet , permitiéndonos afirmar que la implementación de Endian Firewall , si influye positivamente sobre la gestión de la seguridad en la empresa .

La tesis de (Alvarado,2018), tiene como nombre:" implementación de políticas de seguridad y control de navegación a través de un firewall basado en Linux para la empresa TRIBUTAX SERVICES S.A", que tuvo como propósito identificar las vulnerabilidades en los ataques y riesgos que

afectarían en la seguridad informática en la red de la empresa, tuvieron como muestra al encargado del área de tecnología.

Demostrando que una vez culminado el proceso de identificación de las vulnerabilidades se llevó a cabo la implementación de políticas de seguridad y control de navegación. Se llegó establecer muy satisfactoriamente las políticas de seguridad y control de navegación en la red interna del Área local de la empresa Tributax Services, brindando una mejor seguridad en acceso a internet y permitir minimizar el riesgo de algún posible ataque de algún intruso no autorizado, en relación a nuestra tesis tomamos como muestra 10 trabajadores, obteniendo resultados positivos donde se logró una protección de 90% de los datos e información de los clientes , estos resultados fueron obtenidos de acuerdo a las encuestas realizadas donde pudimos afirmar que la implementación de Endian Firewall mejoró la seguridad de los datos y la red de la empresa.

Según (Castillo Palomino y otros, 2017), en su tesis de título: Implementación de un Firewall TMG Forefront para la Seguridad Perimetral de la Red de Datos de la Clínica Aliada, Universidad Peruana de las Américas. Lima-Perú, su tesis tuvo como propósito conocer el desarrollo de la seguridad perimetral en la intranet de la clínica ALIADA , viendo las amenazas de seguridad desde perspectivas distintas , de esta manera se conoció los riesgos que pueden afectar a la clínica , siendo similar a nuestra tesis debido a que nuestro proyecto es gestionar la seguridad y el impacto que genera en las Mypes, permitiendo conocer sistemas de seguridad

actuales con los cuales pueden brindarle seguridad a sus sistemas de información y seguridad en los datos de sus clientes .

Según (Diaz Obando & Gonzales Torres, 2017) su tesis de título : "implantación un UTM basado en software libre para gestión de seguridad lógica y perimetral en la alcaldía de restrepo valle", Mediante la implantación de la UTM OPNsense se logró dar solución a la problemática que se tenía en el ámbito de la seguridad lógica y perimetral de la Alcaldía de Restrepo Valle, ya que se logró elevar el nivel de seguridad de la red interna, salvaguardando lo más importante la información digital, manteniendo su confidencialidad, integridad y veracidad.

Se logró demostrar al personal interno el estado de seguridad en el que se encontraba la Alcaldía de Restrepo Valle, de acuerdo a la cantidad de incidentes reportados por el área de informática de la alcaldía se llegó a la conclusión que la seguridad se incrementó en un 200% ya que al limitar el acceso de los usuarios a páginas web con alto grado de inseguridad y además de realizar un filtrado mediante re dirección del tráfico por proxy, se realiza análisis de la información mediante el antivirus configurado en el UTM OPNSense. En relación a nuestra tesis se logró incrementar en el 90% la seguridad de los datos, ya que limitando el acceso de los trabajadores a ciertas páginas web y/o plataformas y además de realizar un filtrado por proxy mediante Endian Firewall se restringió el acceso a paginas inseguras.

La tesis de (Mauricio Melo & Moreno Ruiz, 2015), titulada:" Seguridad Perimetral PYMES", De acuerdo a las pruebas realizadas en las diferentes distribuciones, se seleccionaron dos de estas que se presentaban como las

más fuertes candidatas con las necesidades expuestas por esta compañía, necesidades como seguridad perimetral y centralización de datos. Aunque la distribución que presentaba más bondades y características para ser elegida era zentyal 4.0 que tiene soporte para módulos "Gateway", el cual contiene firewall avanzado, VPN, proxy, filtro de contenido y balanceo de tráfico, en su última versión estable 4.1 no se encuentra soportado, se centran en la parte de soporte de usuario final como alternativa de controlador de dominio de Windows 2008 y 2012 server. En comparación con nuestra tesis, se logró filtrar 20 sitios web los cuales la empresa consideró como innecesarios o que generan distracción para los trabajadores ya que bajarían el rendimiento de su trabajo y pérdida de tiempo, así también evitando cualquier descarga de archivos malicioso o virus, salvaguardando los datos de la entidad y los clientes.

Según (Fabuel Días, 2013), En su tesis de título:" Implantación de un sistema de seguridad Perimetral. Universidad Politécnica de Madrid - España. En este proyecto se ha tratado de dar a conocer lo que es la seguridad perimetral, primero sentando unas bases teóricas, para posteriormente exponer las fases necesarias para la implantación de un sistema de seguridad perimetral.

Para ello se ha partido de unos requisitos específicos, y una vez identificados, se ha ofrecido una solución que se adapte a dichos requisitos y cumpla en todo momento con un nivel de seguridad y un rendimiento óptimo. Además, se han incluido unos métodos de gestión y mantenimiento

de la plataforma una vez implantada, En comparación con nuestra tesis se propuso las bases para poder realizar la implementación de Endian Firewall para la seguridad de la información y datos, aprobado por los expertos de seguridad informática de la empresa, así evitar que los ciberdelincuentes tomen control de los equipos y se adueñen de la información de los clientes.

Según (Valenzuela Gonzales, 2012), en su tesis de título: "Diseño de una arquitectura de seguridad perimetral de una red de computadoras para una empresa pequeña". Pontifica Universidad Católica del Perú, Lima-Perú, El servidor de correo, que compartía recursos con el antispam, presentaba un alto consumo de recursos debido a que cada correo entrante debe ser analizado por los motores de análisis del anti-spam para luego ser enviado al motor de los servicios de correo y finalmente depositado el correo en la casilla del usuario. En cada una de estas etapas, una copia temporal del correo es escrita en el disco duro. Esta es una razón adicional para justificar la implementación de una solución anti-spam fuera del servidor de correo electrónico. Una evaluación posterior realizada posteriormente a la implementación de la solución propuesta corroboró esta teoría, En acuerdo con nuestra tesis, se logró filtrar correos maliciosos, sospechosos de phishing que engañan al personal para que puedan abrirlos y posteriormente lograr robar información de los clientes.

CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

- Se logró implementar el Firewall Endian Community, con dicha implementación se pudo tener mejor gestión de la seguridad perimetral en la empresa.
- Se consiguió mejorar la gestión de las políticas de seguridad mediante la implementación de Endian Firewall Community, que nos proporcionó un estándar para aplicar políticas a los usuarios de la red de datos de la empresa Imbyte Soluciones.
- Una vez implementado el firewall y luego de haber realizado la evaluación pertinente para poder determinar la influencia sobre la gestión de seguridad, los resultados obtenidos fueron positivos afirmando que se mejoró la seguridad perimetral de la red de la empresa.
- Se determinó los servicios de Endian firewall, la cuales son; filtro de contenido web, antivirus, anti -phishing, anti-spam, filtro protocolos HTTP, HTTPS, y VPN, los cuales ayudaron a mejorar protección y la seguridad perimetral de la red y de los datos que maneja la empresa

6.2. Recomendaciones

- Se recomienda al personal administrativo de la empresa Imbyte Soluciones, mantener siempre el cuidado y mantenimiento del firewall debido a que representa una herramienta de uso bastante fiable para la seguridad de la información de la empresa como para los directivos.

- Realizar un correcto mantenimiento de la red global de datos, mediante el sistema de seguridad Endian Firewall Community.
- Disponer constantemente, del uso de la herramienta de seguridad, para determinar y registrar nuevas conexiones e interfaces.
- No compartir información de la empresa con terceras personas, como contraseñas o datos de clientes y / o trabajadores.
- No compartir contraseñas de las PC´S o sistemas que manejan en su área de trabajo ya que terceras personas, pueden substraer la información de la empresa
- Mantener el Antivirus activo en su PC, para realizar sus labores, también desinfectar las memorias USB o Discos duros una vez ingresados en la PC.
- No abrir correos electrónicos de remitente desconocidos o correos que no sean de interés personal o de interés de su área de trabajo en la empresa.
- Es importante que, en el caso de que la empresa no cuente con una persona especialista en seguridad de la información, se busque orientación por parte de un experto en el tema antes de adquirir y/o implementar alguna solución.
- Tanto la política de seguridad aplicada en los productos de seguridad lógica como los procedimientos de mantenimiento de la solución de seguridad y respuesta ante incidentes deben estar plasmados en un documento oficial de la empresa y que debe ser revisado constantemente.

REFERENCIAS BIBLIOGRÁFICAS

Bueno Rosales, J. J. (2013). Sistema de control y seguridad Endian Firewall para la empresa FRADA SPORT.

Castillo Palomino, R. G., Domínguez, C. M., & Sulca Galarza, C. I. (2017). Implementación de un Firewall TMG Forefront para la Seguridad Perimetral de la Red de Datos de la Clínica Aliada... lima: Universidad privada de las Américas.

Diaz Obando, F. J., & Gonzales Torres, C. E. (2017). IMPLANTACIÓN UN UTM BASADO EN SOFTWARE LIBRE PARA GESTIÓN DE SEGURIDAD LÓGICA Y PERIMETRAL EN LA ALCALDÍA DE RESTREPO VALLE. Bogotá: UNIVERSIDAD ABIERTA Y A DISTANCIA.

Erickson, T. (2012). SISTEMA DE SEGURIDAD PERIMETRAL INSTALACION Y CONFIGURACION DE ENDIAN FIREWALL. Bogotá: UNIVERSIDAD FRANCISCO DE PAULA SANTANDER.

Fabuel Días, C. M. (2013). MPLANTACIÓN DE UN SISTEMA DE SEGURIDAD PERIMETRAL. Madrid.

Frigo, E. (2019). Foro de seguridad. Foro de Profesionales Latinoamericanos de Seguridad: http://www.forodeseguridad.com/artic/discipl/4163.htm

Ivo, B. P. (2017). “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. Lima: Universidad Cesar Vallejo.

Jacob, B. R. (2013). SISTEMA DE CONTROL Y SEGURIDAD ENDIAN FIREWALL PARA LA EMPRESA FRADA SPORT. UNIVERSIDAD TECNOLÓGICA ISRAEL.

Luis, V. G. (2012). Diseño de una arquitectura de seguridad perimetral de una red de computadoras para una empresa pequeña. Lima: universidad Catolica del Perú.

Mauricio Melo, D., & Moreno Ruiz, R. F. (2015). Seguridad Perimetral para PYMES. UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS.

Mauricio Melo, D., & Moreno Ruiz, R. F. (2015). SEGURIDAD PERIMETRAL PYMES. Bogotá.

UNIR la universidad en internet. (30 de 07 de 2020). unir la universidad en internet: https://www.unir.net/ingenieria/revista/seguridad-perimetral-informatica/

Valenzuela Gonzales, J. L. (2012). DISEÑO DE UNA ARQUITEXTURA DE SEGURIDAD PERIMETRAL DE UNA RED DE COMPUTADORAS PARA UNA EMPRESA PEQUEÑA.

Víctor, A. J. (2018). "IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD Y CONTROL DE NAVEGACIÓN A TRAVÉS DE UN FIREWALL BASADO EN LINUX PARA LA EMPRESA TRIBUTAX SERVICES S.A.". quito: UNIVERSIDAD DE GUAYAQUIL.

Ortega, C. (2022, 22 septiembre). Muestreo no probabilístico: definición, tipos y ejemplos. QuestionPro. Recuperado 23 de septiembre de 2022, de https://www.questionpro.com/blog/es/muestreo-no-probabilistico/

System, A. (2018, noviembre 16). ¿Qué es Seguridad Informática? Arroba System. https://arrobasystem.com/pages/seguridad-informatica.

ANEXOS

Anexo01: CUESTIONARIO DIRIGIDO A LOS COLAORADORES

CUESTIONARIO PARA EL PRE Y POST TEST (ANTES Y DESPUES DE LA IMPLEMENTACION DE FIREWALL ENDIAN COMUNITY).

INSTRUCCIONES

- Se recomienda leer atentamente el enunciado de cada pregunta antes de marcar la alternativa
- La información recogida será de carácter anónimo y se utilizará para procesos estadísticos con fines de estudio.
- Se le agradece anticipadamente por su colaboración y participación.

I. RESPONDA LAS INTERROGANTES SEGÚN CREA CONVENIENTE:

1. ¿El firewall implementado tiene la capacidad de Proteger el perímetro de la red de datos?

SI ☐ NO ☐ PARCIALEMNTE ☐

2. ¿Existe tecnología para el etiquetado de la información (publica, privada o confidencial)?.

SI ☐ NO ☐ PARCIALEMNTE ☐

3. ¿Existen tecnologías como directorio activo y acceso único de todas las aplicaciones?

SI ☐ NO ☐ PARCIALEMNTE ☐

4. ¿Se cuenta con tecnología para el respaldo y recuperación de la información?

SI ☐ NO ☐ PARCIALEMNTE ☐

5. ¿Se cuenta con tecnología para evitar y responder a amenazas cibernéticas?

SI ☐ NO ☐ PARCIALEMNTE ☐

6. ¿Se cuenta con tecnología de cifrado y criptografía de datos?

SI ☐ NO ☐ PARCIALEMNTE ☐

7. ¿Se cuenta con seguridad en el desarrollo y en los posesos de implementación de aplicaciones?

SI ☐ NO ☐ PARCIALEMNTE ☐

8. ¿Se cuenta con comité interno para establecer políticas de seguridad?

SI ☐ NO ☐ PARCIALEMNTE ☐

9. ¿Existe un inventario activo de información y están clasificados como, público, privado y confidencial?

SI ☐ NO ☐ PARCIALEMNTE ☐

10. ¿Se revisa el proceso de selección de los funcionarios, colaboradores y contratistas?

SI ☐ NO ☐ PARCIALEMNTE ☐

11. ¿Se cuenta con tecnologías para la gestión de la continuidad de negocio?

SI ☐ NO ☐ PARCIALEMNTE ☐

ANEXO 02: VALIDACIÓN DEL CUESTIONARIO POR LOS EXPERTOS

UPAGU

VALIDACIÓN DE INSTRUMENTOS DE RECOLECCIÓN DE DATOS

TESIS:

IMPLEMENTACIÓN DE FIREWALL ENDIAN COMUNITY PARA GESTIONAR LA SEGURIDAD PERIMETRAL EN LAS MYPES DE LA CIUDAD DE CAJAMARCA: CASO IMBYTE SOLUCIONES.

I. REFERENCIAS (llenar datos)

1.1. Nombres y apellidos del experto: Jhovana Jacqueline Araujo Chuquirona

1.2. Grado académico: MBA. Ing

1.3. Tipo de Instrumento: Cuestionario

1.4. Lugar y fecha: Cajamarca, 20 de Julio del 2022

II. INDICACIONES:

2.1. En el anexo se presentan los formatos y el cuestionario, Instrumentos que deben evaluarse para determinar su validez y fiabilidad.

2.2. La evaluación consiste en asignar (colocar en el cuadro adjunto), un valor cada instrumento según los siguientes valores:
A: acuerdo, B: desacuerdo, C: no sabe no opina.

III. VALIDACIÓN

N°	ASPECTOS A VALIDAR	Instrumentos
		Técnica: Cuestionario
		Cuestionario dirigido a los colaboradores
1	**Pertinencia de indicadores**	A
2	**Formulado con lenguaje apropiado**	A
3	**Adecuado para el objeto de estudio**	A
4	**Suficiencia para medir las variables**	A
5	**Acorde al avance de la ciencia y la tecnología**	A
	TOTAL	A

Jhovana J. Araujo Chuquirona
INGENIERO DE SISTEMAS
CIP N° 134138

UPAGU

VALIDACIÓN DE INSTRUMENTOS DE RECOLECCIÓN DE DATOS

TESIS:

IMPLEMENTACIÓN DE FIREWALL ENDIAN COMUNITY PARA GESTIONAR LA SEGURIDAD PERIMETRAL EN LAS MYPES DE LA CIUDAD DE CAJAMARCA: CASO IMBYTE SOLUCIONES.

I. REFERENCIAS (llenar datos)

1.1. Nombres y apellidos del experto: Johan Geisel Vásquez Vega

1.2. Grado académico: INGENIERO DE COMPUTACION Y SISTEMAS.

1.3. Tipo de Instrumento: CUESTIONARIO

1.4. Lugar y fecha: 20 Julio 2022.

II. INDICACIONES:

2.1. En el anexo se presentan los formatos y el cuestionario, Instrumentos que deben evaluarse para determinar su validez y fiabilidad.

2.2. La evaluación consiste en asignar (colocar en el cuadro adjunto), un valor cada instrumento según los siguientes valores:
A: acuerdo, B: desacuerdo, C: no sabe no opina.

III. VALIDACIÓN

N°	ASPECTOS A VALIDAR	Instrumentos Técnica: Cuestionario Cuestionario dirigido a los colaboradores
1	**Pertinencia de indicadores**	A
2	**Formulado con lenguaje apropiado**	A
3	**Adecuado para el objeto de estudio**	A
4	**Suficiencia para medir las variables**	A
5	**Acorde al avance de la ciencia y la tecnología**	A
	TOTAL	A

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