UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TITULO DEL TRABAJO DE TITULIZACIÓN

REINGENIERÍA DE LA INFRAESTRUCTURA DE RED DE DATOS FÍSICA Y LÓGICA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL SANTA ELENA

AUTOR
BASTIDAS ORRALA ISMAEL JOAQUIN

PROYECTO DE UNIDAD DE INTEGRACIÓN CURRICULAR

Previo a la obtención del grado académico en
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR
ING. IVÁN CORONEL SUÁREZ, MSIA

Santa Elena, Ecuador

Año 2023

UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Ing. José Sánchez A. Mgtr.
DIRECTOR DE LA CARRERA

Ing. Iván Coronel S. MSIA.
TUTOR

Lsi. Daniel Quirumbay Y. MSIA.
DOCENTE ESPECIALISTA

Ing. Marjorie Coronel S. Mgti.
DOCENTE GUÍA UIC

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por BASTIDAS ORRALA ISMAEL JOAQUIN, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 17 días del mes de febrero del año 2023

Ing. Iván Coronel Suárez, MSIA

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **BASTIDAS ORRALA ISMAEL JOAQUIN**

DECLARO QUE:

El trabajo de Titulación, REINGENIERÍA DE LA INFRAESTRUCTURA DE RED DE DATOS FÍSICA Y LÓGICA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL SANTA ELENA previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

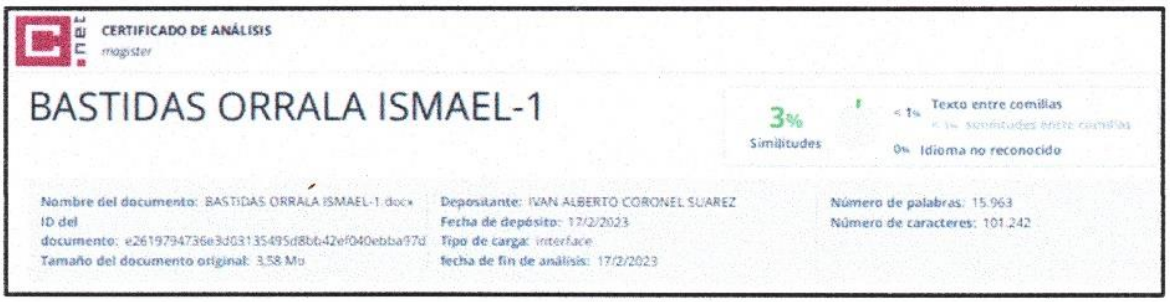
La Libertad, a los 17 días del mes de febrero del año 2023

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado REINGENIERÍA DE LA INFRAESTRUCTURA DE RED DE DATOS FÍSICA Y LÓGICA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL SANTA ELENA presentado por el estudiante, BASTIDAS ORRALA ISMAEL JOAQUIN fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 3%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.



CERTIFICADO DE ANÁLISIS
magister

BASTIDAS ORRALA ISMAEL-1

3% Similitudes

< 1% Texto entre comillas

0% Idioma no reconocido

Nombre del documento: BASTIDAS ORRALA ISMAEL-1.docx
ID del documento: e26197947736e3d03135495d8bb42ef040ebba97d
Tamaño del documento original: 3,58 Mb

Depositante: IVAN ALBERTO CORONEL SUAREZ
Fecha de depósito: 17/2/2023
Tipo de carga: interface
fecha de fin de análisis: 17/2/2023

Número de palabras: 15.963
Número de caracteres: 101.242

Ing. Iván Coronel Suárez, MSIA

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **BASTIDAS ORRALA ISMAEL JOAQUIN**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de artículo profesional de alto nivel con fines de difusión pública, además apruebo la reproducción de este artículo académico dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, a los 17 días del mes de febrero del año 2023

Bastidas Orrala Ismael Joaquin

AGRADECIMIENTO

Quiero expresar mi profundo agradecimiento a todas las personas que me han apoyado y acompañado en este largo y desafiante camino. En primer lugar, quiero agradecer a mi docente guía y tutor, quienes han sido unos mentores excepcionales, brindándome su experiencia y conocimientos, así como su paciencia y dedicación en la orientación de mi investigación.

También quisiera agradecer a los docentes de la facultad de Sistemas y Telecomunicaciones por compartir sus conocimientos y contribuir a mi formación académica. Además, quiero expresar mi gratitud a mis padres por su apoyo incondicional, motivación y orientación en la toma de decisiones.

Quiero expresar mi más profundo agradecimiento a mi esposa e hija por su apoyo y comprensión durante todo el proceso de elaboración de mi proyecto de unidad de integración curricular. Sin su amor, paciencia y aliento constante, no habría sido posible completar este proyecto.

Agradezco de todo corazón a mi abuelita Marina Pita. Gracias por ser mi fuente de inspiración y motivación.

Ismael Joaquin Bastidas Orrala

DEDICATORIA

Quiero dedicar este trabajo a las personas más importantes de mi vida: mi madre, mi esposa y mi hija, quienes han sido mi mayor apoyo y compañía en este proceso de investigación y aprendizaje. También quiero dedicarle un espacio especial a mi fiel acompañante de cuatro patas, cuyo amor incondicional y presencia siempre reconfortante ha sido una gran motivación para mí.

Agradezco infinitamente su confianza, su paciencia y su amor, que me han impulsado a seguir adelante y superar cualquier obstáculo en el camino. Cada uno de ustedes han sido una fuente inagotable de inspiración y motivación en todo momento, y sin su presencia y ayuda, este logro no habría sido posible.

Por todo ello, este proyecto de unidad de integración curricular también es suyo, ya que cada uno ha aportado su granito de arena en este proceso. Desde el fondo de mi corazón, les agradezco por ser parte de mi vida y por haberme acompañado en mi crecimiento académico. Les dedico este trabajo con todo mi amor y gratitud.

Ismael Joaquin Bastidas Orrala

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ITEM DESCRIPCIÓN PAG.

ÍNDICE DE TABLAS

ITEM DESCRIPCIÓN PAG.

ÍNDICE DE ANEXOS

ITEM DESCRIPCIÓN PAG.

RESUMEN

El presente proyecto de unidad de integración curricular tiene como finalidad la reingeniería del diseño actual de la red y la implementación de un Sistema de Seguridad Perimetral en la red de datos del GAD Municipal Santa Elena, con el propósito primordial de aumentar la seguridad de la información de dicha institución.

Dada la importancia de los datos institucionales y la información personal de los usuarios, resulta imperativo la búsqueda de soluciones informáticas innovadoras que permitan salvaguardar la información almacenada en los servidores. Por consiguiente, se va a implementar el firewall lógico "Pfsense", el cual será configurado utilizando la metodología top-down para garantizar una correcta instalación. Para llevar a cabo este proceso, se utilizará el software VMware y se configurará una red perimetral.

En esta red perimetral se definirán las políticas de acceso o restricción necesarias para proteger la red de posibles ataques externos. Es importante destacar que esta protección es esencial para garantizar la seguridad de la red y prevenir posibles ataques.

Palabras claves: reingeniería, firewall, red perimetral, protección.

ABSTRACT

The purpose of this curricular integration unit project is to reengineer the current network design and implement a Perimeter Security System in the data network of the Santa Elena Municipal Government, with the primary purpose of increasing the security of the institution's information.

Given the importance of the institutional data and the personal information of the users, it is imperative to search for innovative IT solutions to safeguard the information stored in the servers. Therefore, the logical firewall "Pfsense" will be implemented, which will be configured using the top-down methodology to ensure a correct installation. To carry out this process, VMware software will be used and a perimeter network will be configured.

In this perimeter network, the necessary access or restriction policies will be defined to protect the network from possible external attacks. It is important to highlight that this protection is essential to guarantee the security of the network and prevent possible attacks.

Keywords: reengineering, firewall, perimeter network, protection.

INTRODUCCIÓN

El progreso tecnológico y la conectividad de dispositivos con acceso a Internet de alta velocidad, como la fibra óptica, ha generado un gran volumen de tráfico de datos en empresas e instituciones. Esto implica una responsabilidad en asegurar la privacidad de la información para los usuarios, ya que la interactividad conlleva riesgos. Es por esto por lo que las instituciones deben garantizar la confidencialidad, integridad y disponibilidad de la información y tomar medidas necesarias para prevenir el acceso no autorizado o posibles ataques que puedan poner en peligro la información o la infraestructura que la respalda para garantizar una comunicación segura y disponible.

Es por ello por lo que se opta por implementar un firewall perimetral, ya que este puede brindar un nivel más elevado de protección para las instituciones que lo apliquen. El software para implementar es Pfsense, el cual es un sistema libre de licencias, robusto y confiable, que depende de las características del equipo que lo aloja, así como de una configuración y mantenimiento adecuados.

El primer capítulo presenta una exposición de la problemática, las justificaciones y los objetivos a alcanzar, así como también una descripción de la situación de la empresa, entre otros aspectos, y detalla con más precisión la teoría de lo presentado anteriormente.

El segundo capítulo incluye todas las bases teóricas relacionadas con los temas a ser estudiados durante la implementación, así como los detalles de los equipos que serán utilizados, el diseño de la propuesta, el desarrollo del mismo y, por último, los resultados que se obtuvieron luego de poner en funcionamiento dicho Firewall.

Al final del proyecto se establecen las conclusiones y recomendaciones obtenidas durante todo su desarrollo.

CAPÍTULO I

FUNDAMENTACIÓN

1.1. ANTECEDENTES

En la actualidad, la seguridad es un tema crucial en cualquier tipo de organización, por lo que es esencial tomar medidas para asegurar que los activos estén siempre disponibles [1]. Es importante destacar que la información es un elemento muy delicado que debe ser protegido cuidadosamente. Los principales aspectos de la seguridad son la confidencialidad, la integridad y la disponibilidad, aunque es difícil asegurar una seguridad absoluta[1].

El gobierno autónomo descentralizado (GAD) se encuentra ubicado en la provincia de Santa Elena. Esto implica ser responsable de la administración, gestión, facilitación y regulación de bienes y servicios públicos que sean permanentes, de alta calidad y que cuenten con eficiencia, cobertura y acceso, a través de procesos, programas y proyectos inclusivos, participativos y transparentes para la sociedad en general. Además, se debe aplicar principios como la solidaridad, el respeto, la responsabilidad y la equidad en el desempeño de las tareas [2].

Análisis de observación natural es la técnica que se utilizó (ver anexo 1), se pudo apreciar algunos de los problemas que tiene la red de datos lógica como lo son los conflictos con direcciones IP, esto es indicio de que no se está llevando un orden, el cual ocasiona problemas como que la navegación a internet sea lenta e inestable, dificultades al momento de imprimir, perdida de conexión y por ende no se podría navegar por Internet.

El malware también es uno de los motivos principales porque existen páginas maliciosas o archivos que pueden perjudicar no solo el rendimiento del computador, sino que puede crear conflictos a la red, el no tener restricciones al momento de navegar por Internet, provoca todos estos impactos negativos que no solo afectan a los trabajadores, ya que ellos ofrecen un servicio y el hecho de que el sistema este lento afecta de manera indirecta a sus usuarios.

Otro punto perjudicial es el tener varias aplicaciones operando en la red, el gestionar mal la red de datos conlleva a que casi siempre este saturado, esto no solo se ocasiona por los servicios que se estén ejecutando de manera predeterminada, también es porque los usuarios en sus computadores usan servicios externos como puede ser Spotify, YouTube, sitios de web de películas, etc.

En El Salvador se realizó un trabajo muy interesante llamado "reestructuración de la red informática del laboratorio de electrónica de la universidad tecnológica de El Salvador" y su objetivo primordial es el de lograr la reestructuración de la red de informática cumpliendo con los estándares básicos en un sistema de cableado estructurado. Para lograr dicho objetivo se dispuso a cumplir cuatro fases [3].

El autor Amada Feliz desarrollo el proyecto de "reestructuración en la red de comunicaciones física y lógica del gobierno autónomo descentralizado provincial de Imbabura". Se indica que el principal propósito es llevar a cabo la reorganización de la red de comunicaciones del GAD, tanto a nivel físico como lógico, utilizando el modelo de jerarquía de red. Este diseño constará de dos capas: la capa de núcleo reducido y la capa de acceso. La implementación de este modelo permitirá mejorar el rendimiento de la red.

En Santa Elena se llevó a cabo el trabajo de titulación denominado "planificación y ejecución de la instalación de un sistema de cableado estructurado en el laboratorio de electrónica que se encuentra en la facultad de sistemas y telecomunicaciones". El propósito del proyecto consistió en crear un plan para el diseño del cableado estructurado de la red de datos que se utilizará en el laboratorio de electrónica. El mismo que se compone de cinco fases. [5].

Por todo lo expuesto que se ha llevado a cabo, tanto internacional como nacional, podemos evidenciar que subsisten varias problemáticas, con estos estudios, proyectos, trabajos de titulación, etc. Se puede constatar que es necesaria una reestructuración de la red cada cierto tiempo, el presente proyecto se centra en mejorar y corregir vulnerabilidades que se pudiesen presentar, y con ello el poder proporcionar un entorno más confiable.

1.2. DESCRIPCIÓN DEL PROYECTO.

Debido a que toda red de datos puede ser susceptible a ataques informáticos y de que día a día se originan nuevos malware o surgen otras formas de acceder a las redes de datos. Este proyecto pretende realizar la reestructuración de la infraestructura de red de datos lógica, estableciendo nuevas medidas de seguridad en el GAD Municipal en la provincia de Santa Elena, con la finalidad de lograr que la información que circula por la red tenga niveles de seguridad más elevados, esto se lograra creando configuraciones locales en la red de datos, más conocido como DMZ, está enfocado en beneficiar a todos los trabajadores de dicha institución que utilicen la red de datos.

Se empleará la metodología de diseño de red Top-Down la cual está conformada por cinco fases, las cuales son:

Fase de recopilación y observación:

En esta primera fase consiste en recolectar información, con el fin de comprender la situación actual de la infraestructura de la red, tanto en sus aspectos físicos como lógicos, el principal objetivo a cumplir en esta fase es identificar la problemática y conocer la tecnología con la que dispone y su estructura, se visitará el GAD para realizar las entrevistas a los trabajadores del área de sistemas y realizar el levantamiento de información que sea necesaria, adicionalmente se hará observación directa sobre el funcionamiento de la red.

Fase de análisis:

En esta fase se analizará la información recopilada, el sistema de cableado estructurado (CE) de la red física, en el cual se deben considerar cuatro subsistemas principales: el área de trabajo, el cableado horizontal, el cableado vertical y la sala de equipos, y en el apartado de la red lógica de datos, se debe analizar los requerimientos técnicos que se debe cumplir con respecto a compatibilidad y funcionamiento de los nuevos proxys a implementar, el principal objetivo de esta fase de análisis es el diseñar el nuevo modelo de sistema de comunicación, cubriendo los fallas o problemáticas encontradas en la fase anterior.

Fase de desarrollo e implementación:

La fase de desarrollo e implementación debe plasmar los requerimientos iniciales definidos en la fase anterior en un diagrama detallado que cumpla con la funcionalidad deseada, aportando así a la confidencialidad, integridad, disponibilidad, escalabilidad y rendimiento. Una vez diseñado el modelo que se quiera emplear, se procederá a desarrollarlo, ya en funcionamiento se configuraran las reglas del firewall que se llevaran a cabo, una de ellas es implementación a los equipos proxys para el control de navegación en cada una de las VLAN's de la institución.

Fase de prueba:

En esta fase se incorporarán configuraciones y componentes a la red existente de acuerdo con las especificaciones del diseño propuesto, con el objetivo de mejorar el control en la navegación de los equipos de la institución, así mismo mitigar vulnerabilidades que presenta la infraestructura actual.

En este punto también se habilitan las interfaces de red adicionadas, se procede a configurar las políticas de seguridad del firewall perimetral y de cada proxy implementado mediante herramienta Pfsense, las reglas implementadas están en base a:

Punto de acceso: De los equipos de los usuarios finales, tomando el rol de un proxy secundario de salida de la VLAN asignada.

Reglas de control de acceso: Medidas de control de acceso para los activos que componen la red, estas contienen los siguientes aspectos: Se refiere a la necesidad de establecer un mecanismo de control, para el acceso a la red utilizada por los sistemas de información.

Restricciones y prohibiciones: Se controlan las siguientes actividades:

- Internet restringido, los usuarios solo podrán hacer uso de Internet aplicándose las políticas de seguridad y navegación según lo disponga la institución.

- La prohibición al acceso de páginas no autorizadas y que no tengan que ver con el quehacer diario de la institución.

Monitorización: Del uso correcto del ancho de banda por usuario de cada segmento en el que se encuentre ubicado, permitiendo localizar equipos que tengan comportamiento anómalo y saturen el servicio de Internet y posibles infecciones según sea necesario.

Esta es una de las fases más importantes y fundamentales, porque nos permite detectar los errores que se pudiesen presentar y de esta manera poder corregir los fallos.

Fase de implementación final:

La última fase consiste en implementación de la configuración de red establecida en las fases anteriores, habiendo pasado la fase de prueba y en caso de que se presente algún fallo inesperado en dicha fase, se aplicarán todos los correctivos necesarios con la finalidad de llegar a este punto con una infraestructura de red física y lógica, funcionando de manera eficaz, en todas las áreas a implementarse en el GAD.

Para la implementación de este proyecto se han considerado las siguientes herramientas, se recalca que los dispositivos a utilizar son los que nos proveen la institución para el cumplimiento del mismo.

- Organizador de cables
- Switches
- Patch Panel
- Patch Cord
- Jack RJ-45
- Pfsense
- Routers
- Conmutadores KVM de montaje en rack de 8 puertos
- Conversor de medios WDM
- VMware
- Diagrams.net

Este proyecto contribuye con la línea de investigación de la carrera de Tecnologías de Información, relacionada TSI en las organizaciones y en la sociedad, ajustándose a las nuevas tecnologías que nos permita llevar una mejor gestión de las redes de comunicación en la institución [6].

1.3. OBJETIVOS DEL PROYECTO

1.3.1. OBJETIVO GENERAL

Realizar la reingeniería de la infraestructura de red de datos lógica del GAD mediante la implementación de la red física, configuración de la estructura lógica y la DMZ con base en la metodología Top-Down, con el propósito de mejorar los niveles de seguridad.

1.3.2. OBJETIVOS ESPECÍFICOS

- Recopilar la información necesaria mediante entrevistas para conocer la situación actual de la red de datos lógica del GAD.
- Identificar los problemas de la red de datos actual y analizarlos para la elaboración del nuevo diseño de red mejorado.
- Generar el nuevo diseño de red en base a la metodología Top-Down para la correcta implementación de la red física, lógica y la DMZ.
- Establecer las políticas que se van a emplear a través de la configuración del Firewall Pfsense para la nueva infraestructura de red de datos lógica.

1.4. JUSTIFICACIÓN

Dado el valor crítico de la información y los beneficios que los ciberdelincuentes pueden obtener al acceder a ella, es común ver vulnerabilidades de seguridad que resultan en la filtración de información. En estos casos, se utilizan diversas técnicas de ataque con el objetivo de lograr sus objetivos malintencionados [7]. Un ejemplo de la gravedad de las filtraciones de información es el caso del malware Point of Sale que afectó a empresas como Target, Home Depot y UPS en 2014. Los atacantes lograron obtener más de 40 millones de números de tarjetas de crédito y débito de los usuarios. Además, empresas como eBay y Yahoo! han tenido que notificar a miles de usuarios que sus cuentas y contraseñas han sido comprometidas a través de ataques [8].

Miguel Ángel Mendoza dice que, en varios países, se han promulgado leyes cuyo objetivo es proteger los datos personales que manejan tanto el sector público como el privado. La protección de los datos es un derecho fundamental de las personas, que les permite ejercer control sobre la información privada que es recolectada, procesada o

transmitida por terceros [9]. Por consiguiente, los beneficiarios engloban tanto para las personas que se encuentran involucradas en la entidad y así mismo beneficia a la empresa porque no se verá afectada por problemas de filtración de datos.

Con la reestructuración de la infraestructura de la red física y lógica de datos, implementando el uso de una DMZ estaríamos protegiendo a la red interna de ataques externos que pueden ser muy graves, como el saber donde vive una persona, sus propiedades, sus deudas con dicha entidad, etc. Otro de los beneficios es el de poder establecer muro entre la red interna y la red exterior, haciendo esto nos ayudará a detectar si individuos no deseados pretenden ingresar a la red interna y de esta manera poder tomar las medidas necesarias para evitar este tipo de inconvenientes.

Un buen diseño y definición de las reglas de políticas de seguridad en la arquitectura de la red de datos de las instituciones, hace que los sistemas dentro de la red sean más confiables y robustas ante cualquier ataque cibernético.

Este proyecto está direccionado al plan de creación de oportunidades, haciendo relevancia al eje número 3, el cual es el siguiente:

Eje 3: Seguridad Integral [10].

Objetivo 9: Garantizar la seguridad ciudadana, orden público y gestión de riesgos [10].

Objetivo 10: Asegurar la independencia del país, preservar sus límites territoriales y proteger la estabilidad y protección del Estado [10].

1.5 ALCANCE DEL PROYECTO

Debido a que, en las distintas áreas del GAD ya sea de rentas, deportes, contable, etc. Presenta problemas en la gestión y organización de la infraestructura del cableado y la red lógica porque hay perdida de conexión, no se tiene los permisos necesarios en algunas áreas en específico, etc. Por lo cual se determina que es notable la implementación de una restructuración de la red física y lógica de dicho lugar.

Este proyecto es desarrollado para el GAD de Santa Elena y es dirigido para beneficiar a todos los trabajadores de dicha institución que utilicen la red de datos.

El mismo está comprendida en 5 fases:

- Fase de recopilación y observación.
  - Recolectar información para conocer la situación actual del GAD.
  - Identificar los problemas que tiene la infraestructura física y lógica de datos.
  - Conocer con la tecnología con la que dispone el GAD.
  - Realizar entrevistas a los trabajadores de área de sistema.

- Fase de análisis.
  - Analizar la información recopilada en su apartado físico y lógico.
  - Analizar los dispositivos con los que cuenta el GAD.
  - Analizar los requerimientos técnicos que se deben cumplir.
  - Diseñar el nuevo modelo de red a implementar.

- Fase de desarrollo e implementación.
  - Plasmar los requerimientos para su correcto desarrollo e implementación,
  - Implementación del nuevo diseño de red.
  - Implementación de equipos proxys.
  - Implementación de políticas al firewall de la red.

- Fase de prueba.
  - Incorporación de configuraciones y componentes a la red.
  - Reglas de control de acceso.
  - Restricciones y prohibiciones.
  - Monitorización.

- Fase de implementación final.
  - Implementación de la configuración de red en todo el GAD.

1.6. METODOLOGÍA

1.6.1. METODOLOGÍA DE INVESTIGACIÓN

La investigación de tipo exploratoria se realiza en torno a un tema u objeto que es desconocido o ha sido poco estudiado, lo que conduce a una comprensión superficial

del objeto de estudio y a resultados que son solo una aproximación del mismo [11]. Con este tipo de investigación se tiene objetivo principal el buscar trabajos similares o semejantes, con el propósito de que sirvan de ayuda para la realización del presente proyecto.

Para encontrar varios de los problemas de vulnerabilidades en la red de datos lógica del GAD y conocer un poco más sobre la seguridad de la misma y cuáles podrían ser los principales inconvenientes que se está teniendo, se empleara la metodología de investigación de tipo diagnóstica.

1.6.2. VARIABLE

Este proyecto tiene como prioridad aumentar el nivel de seguridad en la red interna porque las reglas creadas en el firewall Pfsense solo habilitan los puertos necesarios para el funcionamiento del servidor público de internet, de esta manera si los atacantes llegaran a ingresar al servidor no podrán acceder a la red internet de la institución.

1.6.3. TÉCNICAS DE RECOLECCIÓN DE LA INFORMACIÓN

Para la recolección de información se han usado dos tipos de técnicas que son de entrevista y recopilación documental y bibliográfica.

En entrevista se obtiene una opinión profesional, por parte de una persona experimentada en el funcionamiento de una red de datos por medio de un cuestionario, estableciendo preguntas referentes a la seguridad que se tiene en la red de datos. En recopilación documental y bibliográfica, se busca información de diferentes fuentes bibliográficas de acuerdo con el tema establecido, para poder tener una mejor idea con respecto a la implementación de la red física, configuración de la estructura lógica y la DMZ, y de proyectos similares.

1.6.4. METODOLOGÍA DE DESARROLLO

La perspectiva de la metodología top-down se centra en las redes empresariales y comienza por las capas de aplicación, presentación, sesión y transporte en lugar de las

capas inferiores (red, enlace de datos, física), ya que en estas capas se examinan: la situación actual de la red, los requisitos, las restricciones y su estructura lógica que es crucial para su desarrollo [12].

El enfoque de diseño de red top-down se basa en iniciar el diseño por las capas superiores del modelo de referencia OSI antes de avanzar a las capas inferiores, con el propósito de dar prioridad a las sesiones, aplicaciones, y transporte de datos. Posteriormente, se procede a seleccionar los dispositivos de red, como switches, routers, y medios, que operan en las capas inferiores [13].

Esta metodología de red consta de 5 fases que son las siguientes:

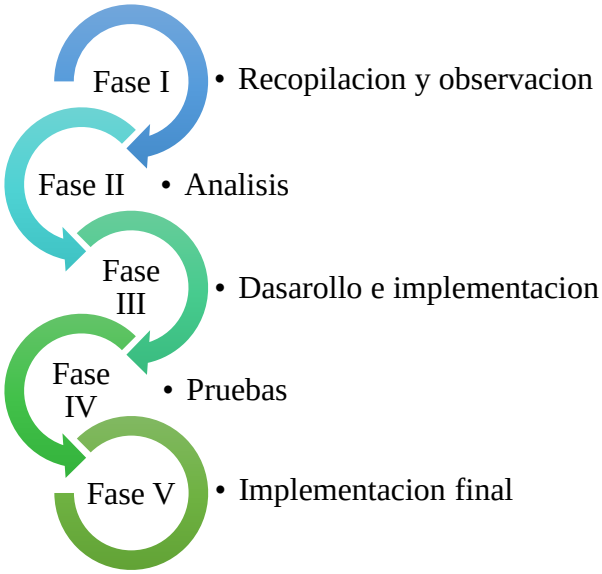


Figura 1. Fases de la Metodología Top-Down por: Autor

- Fase I: De recopilación y observación
- Fase II: De análisis
- Fase III: De desarrollo e implementación
- Fase IV: De prueba
- Fase V: De implementación final

CAPÍTULO II

LA PROPUESTA

2.1. MARCO CONTEXTUAL

2.1.1. GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL

Las entidades que integran la estructura territorial del Estado Ecuatoriano se conocen como Gobiernos Autónomos Descentralizados, y están sujetos a las disposiciones de la Constitución de la República del Ecuador y el Código Orgánico de Organización Territorial, Autonomías y Descentralización [14].

Los GAD son instituciones descentralizadas que gozan de autonomía política, administrativa y financiera, y están regidos por los principios de solidaridad, subsidiariedad, equidad, interterritorial, integración y participación social [14].

2.1.2. VISIÓN

El Gobierno Autónomo Descentralizado Municipal será una institución con capacidad administrativa, operativa y financiera, sólida e innovadora, generadora del desarrollo sostenible y sustentable del cantón, para los ciudadanos e inversionistas locales, nacionales y extranjeros, aplicando la gestión por resultados con transparencia, solidaridad, justicia y probidad.

2.1.3. MISIÓN

El Gobierno Autónomo Descentralizado Municipal tiene la responsabilidad de llevar a cabo la administración, gestión, facilitación y regulación de bienes y servicios públicos de alta calidad de manera eficiente, sostenible, amplia y accesible para todos los ciudadanos.

Para lograr estos objetivos, se emplean procesos, programas y proyectos que fomentan la inclusión y la participación de la ciudadanía, así como la transparencia en la toma de decisiones. Además, se aplican valores y principios tales como la solidaridad, la equidad, la responsabilidad y respeto.

2.1.4. OBJETIVOS INTITUCIONALES DE UN GAD

Componentes	Objetivos estratégicos
Biofísico	1. Promover acciones conjuntas en el territorio cantonal para la coordinación de políticas y estrategias comunitarias, de compromiso social y corresponsabilidad, que contribuyan a menorah la gestión ambiental y el desarrollo sostenible/sustentable urbano y rural. 2. Implementar acciones de mitigación del cambio climático, prevención y atención de desastres, recursos hídricos y biodiversidad orientados al bienestar humano a través de un desarrollo armonizado con el ambiente.
Sociocultural	3. Impulsar el desarrollo humano e identidad cultural, garantizando mejores condiciones de vida, en un entorno de convivencia sana, de seguridad ciudadana y conservacionismo patrimonial y cultural.
Económico-Productivo	4. Impulsar el desarrollo sostenible de la economía del cantón, basado en el turismo, la producción agropecuaria, la pesca, y el comercio, optimizando su capacidad productiva y la soberanía alimentaria. 5. Contribuir a los modelos productivos de los sectores agropecuarios y artesanales, mejorando su cadena de comercialización promoviendo el consumo local.
Asentamientos humanos, movilidad, energía y conectividad	6. Garantizar el acceso y suministro de agua potable a gran parte del cantón, además del saneamiento ambiental eficiente, la recolección y tratamiento de los desechos sólidos y aguas residuales basados en normas ambientales. 7. Garantizar la cobertura eficiente de los servicios relacionados con la conectividad, movilidad, energía, recreacionales y exequiales en el territorio cantonal. 8. Promover las buenas prácticas y convivencia entre los ciudadanos y ciudadanas del cantón, basados en el desarrollo de infraestructura y estructuras cerca de los asentamientos humanos.
Político institucional	9. Impulsar los procesos de gobernabilidad basados en los principios de participación, seguridad ciudadana y de inclusión, que produzca sinergias entre el GAD y las entidades públicas y privadas, garantizando la articulación y gestión de los procesos de planificación territorial y ordenamiento del cantón.

Tabla 1. Objetivos de un GAD [14].

2.1.5. ORGANIGRAMA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL.

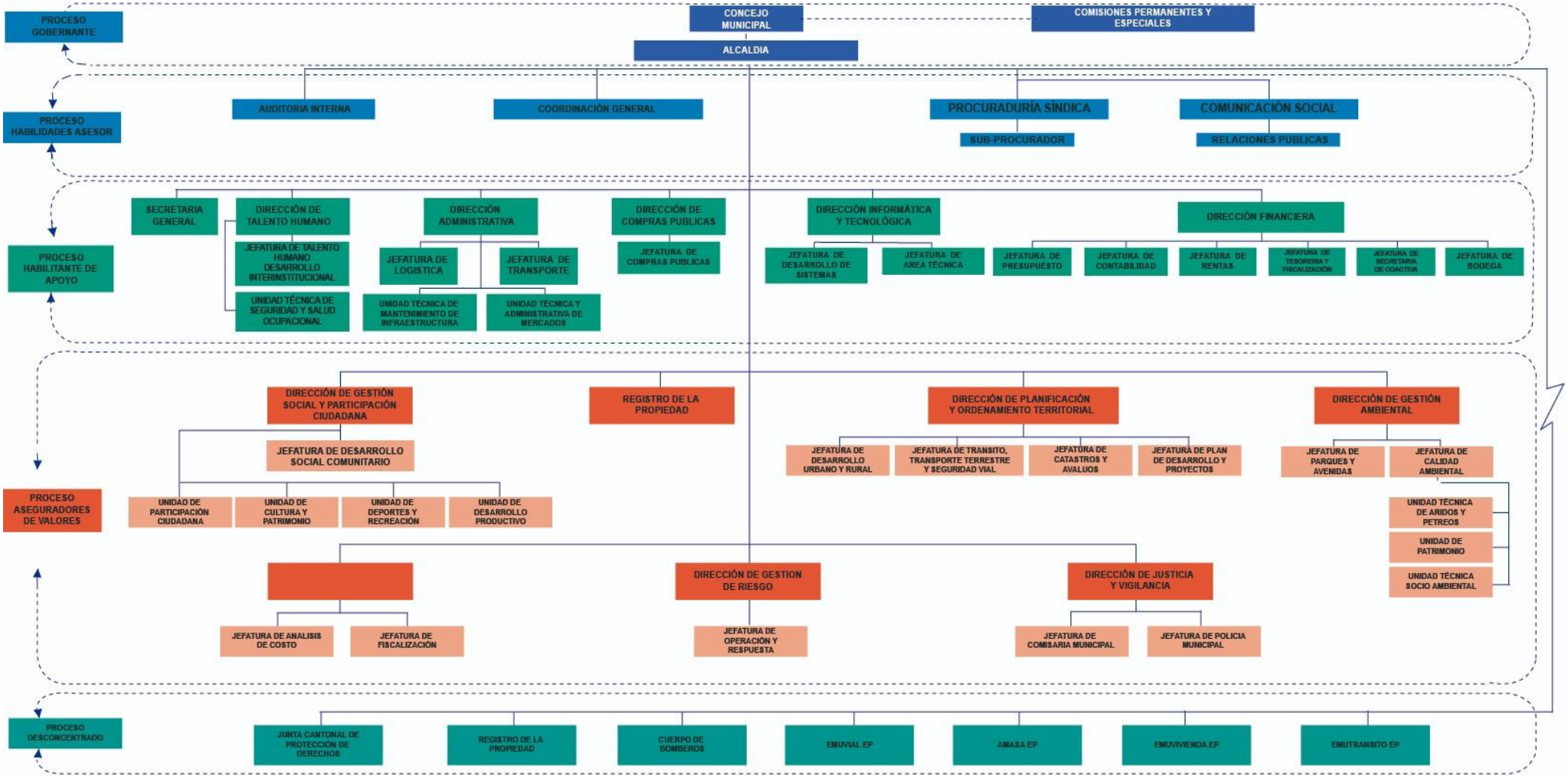


Figura 2. Organigrama del Gobierno Autónomo Descentralizado Santa Elena [15]

2.1.6. LEY ORGÁNICA DE PARTICIPACIÓN CIUDADANA Y LEY ORGÁNICA DEL CONSEJO DE PARTICIPACIÓN CIUDADANA Y CONTROL SOCIAL

La Ley Orgánica de Participación Ciudadana y Control Social (LOPC) y la Ley Orgánica de Consejos Provinciales y Municipales de Planificación y Coordinación de la Competencia Sectorial (LOCPCCS) tienen como propósito desarrollar los mandatos constitucionales relacionados con la rendición de cuentas, con el fin de garantizar su efectiva implementación y hacerla parte de los procesos diarios de la gestión institucional y de la participación ciudadana [15].

Estos objetivos se encuentran establecidos en los artículos siguientes de dichas leyes:

LEY ORGÁNICA DE PARTICIPACIÓN CIUDADANA	LEY ORGÁNICA DEL CPCCS	CONTENIDOS
	Art. 5 numeral 2	CPCCS establece mecanismos de Rendición deCuentas.
Art. 88		De ciudadano a la Rendición Derecho Cuentas.
Art. 89	Art. 9	Definición de Rendición de Cuentas.
Art. 90	Art. 11	Sujetos obligados a rendir cuentas.
Art. 91		Objetivos de la Rendición de Cuentas.
Art. 92	Art.10	Los elementos de la Rendición de Cuentas que se relacionan con el nivel político
Art. 93	Art.10	Contenidos de la Rendición de Cuentas correspondiente al nivel operativo y programático.
Art. 94		Mecanismos para rendir cuentas.
Art. 95		Periodicidad de la Rendición de Cuentas.
	Art. 11	Sanciones.
	Art. 12	Monitoreo.
Art. 96		El libre acceso a la información pública.
Art. 97		Principios generales del acceso a lainformación.
Art. 98		Transparencia de la administración pública.
Art. 60, N. 4		Funciones de las asambleas locales: organizar Rendición de Cuentas.

Tabla 2. Artículos De Participación Ciudadana y Ley Orgánica del CPCCS [15].

2.2. MARCO CONCEPTUAL

2.2.1. REDES DE COMPUTADORAS

Existen varios términos generales para describir las redes de computadoras, pero el concepto más preciso sería el siguiente: "Las redes de computadoras modernas son una combinación de dispositivos, técnicas y sistemas de comunicación que han surgido desde finales del siglo XIX, cuando se inventó el teléfono." En términos simples, una red de comunicaciones se refiere a un conjunto de tecnologías que permiten la comunicación a distancia entre dispositivos autónomos [16].

2.2.2. MODELO OSI

Cuando se trata de explicar la organización y operación de los protocolos de comunicaciones, se utiliza un modelo arquitectónico creado por la ISO. El modelo de este se diseñó para ser un punto de referencia fundamental, un marco que sirviera como base para establecer estándares que permitieran la plena interoperabilidad [17]. El modelo OSI se compone de siete capas que establecen las funciones que realizan los protocolos de comunicaciones. Cada capa del modelo cumple una función específica en la transferencia de datos entre aplicaciones que colaboran a través de una red intermedia. Este modelo se considera principalmente teórico, ya que se enfoca en explicar detalladamente las características y servicios de cada capa sin dejar de lado ningún aspecto importante [17].

2.2.3. TCP/IP

Se puede decir que estos protocolos son el conjunto de reglas de comunicación que rigen la transmisión de datos en Internet. Esta combinación incluye dos protocolos fundamentales, el Protocolo de Internet y el Protocolo de Control de Transmisión. Aunque existen otras normas importantes, estas dos son las más destacadas y esenciales para el funcionamiento de Internet. La combinación de estos dos protocolos se conoce comúnmente como la pila TCP/IP [18].

2.2.4. VMWARE

VMware es el líder mundial en virtualización e infraestructura de nube. Hoy en día, más de 190 000 clientes y 25 000 socios confían en las soluciones de VMware para lograr

sus objetivos empresariales. VMware ofrece un camino de evolución único a la computación en nube que reduce la complejidad de TI, disminuye significativamente los costos y habilita un suministro de servicios más flexible y ágil [19].

VMware suministra administración e infraestructura de nube, plataforma de nube para las aplicaciones y soluciones de computación para el usuario final que pueden acelerar el cambio de su organización a la computación en nube y permitir a su equipo obtener valor rápidamente a partir de este nuevo enfoque [19].

2.2.5. PFSENSE

Pfsense es una versión adaptada de FreeBSD diseñada para su uso en servicios de redes LAN y WAN como firewall, enrutador y servidor de balanceo de carga. También tiene la ventaja de contar con un gestor de paquetes integrado en su interfaz gráfica, lo que permite ampliar sus funcionalidades de manera sencilla y remota. Al seleccionar el paquete deseado, el sistema se encarga automáticamente de descargarlo e instalarlo en el sistema [20].

Es posible instalar Pfsense en cualquier tipo de ordenador PC o servidor, independientemente de su arquitectura, siempre y cuando cuente con un mínimo de dos tarjetas de red. Como se trata de un software de código abierto, existe una comunidad de desarrolladores que puede brindar soporte y asistencia técnica, aunque también se ofrece soporte de pago a través de BSD Perimeter. Además, cada usuario tiene la libertad de modificar el software y crear su propia distribución, siempre y cuando cumpla con ciertas condiciones [20].

2.2.6. REDES LAN

Una red de área local (LAN) es aquella que cubre un área limitada, como hogares, edificios, oficinas, entre otros. Es el tipo de red más utilizado y su característica principal es que los dispositivos están conectados a través de cables de cobre o fibra óptica. La velocidad de transferencia de datos en las redes LAN puede alcanzar hasta 10 Mbps (Ethernet) y 1 Gbps (Gigabit Ethernet) [21].

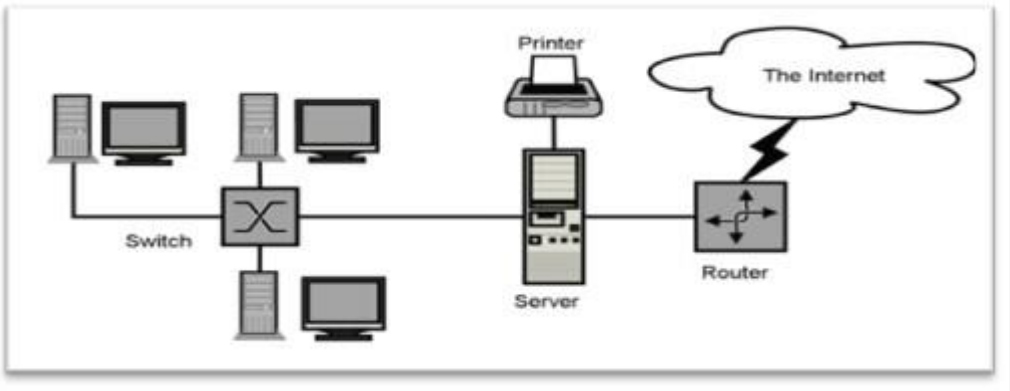


Figura 3. Estructura de Red LAN [21]

2.2.7. RED DE ÁREA METROPOLITANO (MAN)

Red MAN (Metropolitan Area Network, red de área metropolitana) conecta diversas LAN cercanas geográficamente (en un área de alrededor de cincuenta kilómetros) entre sí a alta velocidad. Por lo tanto, una MAN permite que dos nodos remotos se comuniquen como si fueran parte de la misma red de área local. Una MAN está compuesta por conmutadores o routers conectados entre sí con conexiones de alta velocidad (generalmente cables de fibra óptica) [22].

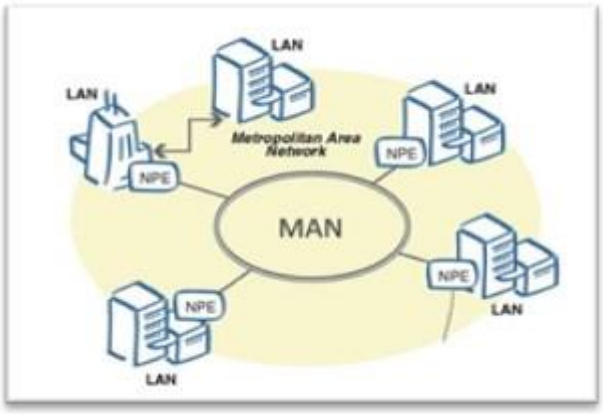


Figura 4. Estructura de Red MAN [22]

2.2.8. RED DE ÁREA EXTENSA (WAN)

Son redes punto a punto que interconectan ciudades, países y continentes. Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto y

continentes. Debido a la necesidad de cubrir grandes distancias, las redes WAN tienen velocidades más lentas que las redes LAN, pero tienen la capacidad de transportar una mayor cantidad de información. [22].

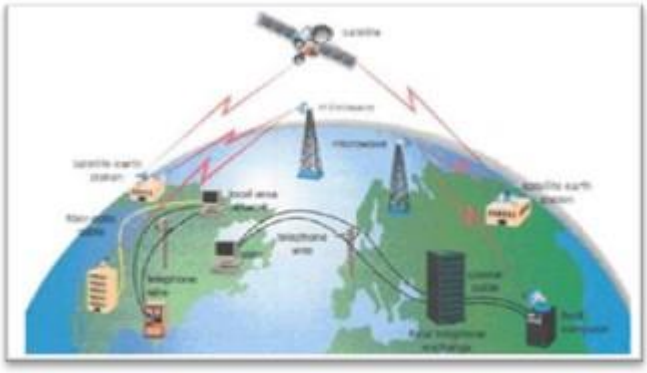


Figura 5. Estructura de Red WAN [22]

2.2.9. ELEMENTOS FÍSICOS DE UNA RED

- **Un hub: concentrador:** Es un equipo que posibilita la convergencia del cableado de una red, lo que permite el enlace de varios dispositivos y la comunicación entre ellos, creando un punto de consolidación para todas las conexiones de los equipos, lo cual facilita su ampliación y diseño está formado por una secuencia de puertos de entrada y salida que permiten la conexión de los dispositivos finales de la red [23].

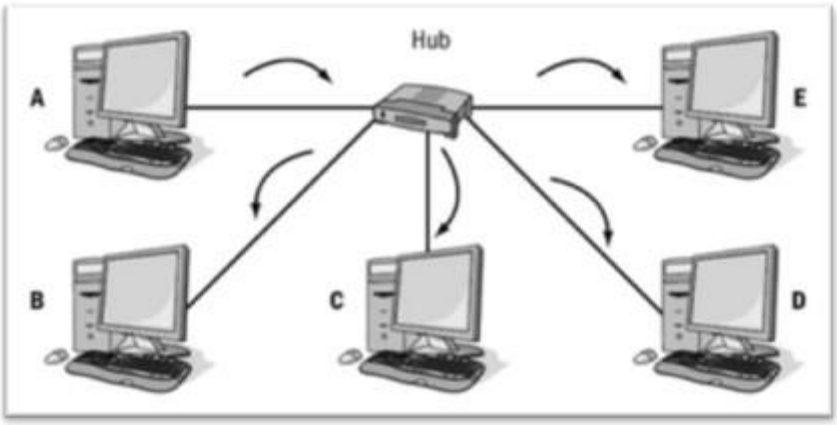


Figura 6. Estructura de un dispositivo Hub [23]

- **Switches o conmutadores:** Se incorporan de manera similar a un hub en la red, estos dispositivos filtran y dirigen de manera precisa las señales entre los equipos

conectados a él. A diferencia de un concentrador, un switch actúa de manera inteligente y tiene la capacidad de filtrar el tráfico y reconocer rutas de conducción separadas [23].

Figura 7. Dispositivo Switch [23]

- **Router:** Es un dispositivo que realiza varias funciones, una de ellas es la de ser una pasarela entre una red LAN e internet, la mayoría de ellos tienen una función de cortafuegos, reenviando el tráfico que debe pasar a través de él. [24]

Figura 8. Dispositivo Router [24]

- **Cables:** Representan todo el cableado de una red, son las líneas físicas utilizadas para transmitir información mediante impulsos eléctricos o lumínicos entre los equipos conectados a una red. Los cables más comunes en una red son:

- **Cable UTP o de par trenzado:** UTP es un tipo de cable que se usa en varias estructuras de conexión, hecho de cuatro pares de hilos trenzados. Los ocho hilos de cobre del cable están cubiertos con un material aislante de plástico para

protegerlos. Este posee pares de hilos trenzados que ayudan a cancelar las interferencias electromagnéticas y radioeléctricas que pueden degradar la señal. Además, se varía la cantidad de trenzas en los pares de hilos para reducir la interferencia entre ellos [25].

Figura 9. Estructura de un Cable UTP [25]

- Cable STP o par trenzado blindado: El cable de par trenzado con blindaje combina técnicas de blindaje y trenzado de cables. El STP reduce el ruido electrónico externo al cable, como la interferencia electromagnética (EMI) y la interferencia de radiofrecuencia (RFI). [25]

Figura 10. Estructura de un Cable STP [25]

- **Cable Coaxial:** El cable coaxial está compuesto por un conductor de cobre rodeado por una capa de plástico aislante y flexible. Sobre este aislante se coloca una malla u hoja metálica de cobre que actúa como segundo blindaje para el conductor interno. Esta capa reduce aún más la interferencia electromagnética externa. Por encima de estas capas, tiene un revestimiento exterior para darle un aspecto estético al cable. [26]

Figura 11. Estructura de un Cable Coaxial [26]

- **Fibra Óptica:** La fibra óptica es el medio utilizado para los enlaces de backbone (cableado vertical en un edificio o entre edificios), es capaz de soportar mayores distancias y una gran capacidad de tráfico. Por backbone o troncal se entiende que son las principales conexiones dentro de una LAN, llevando grandes volúmenes de datos. En los medios ópticos, se utiliza la luz para transmitir los datos a través de una fibra delgada de vidrio o materiales plásticos. Las señales eléctricas hacen que el transmisor de fibra óptica genere señales luminosas que son enviadas por el núcleo de la fibra. El receptor recibe las señales luminosas y las convierte en señales eléctricas en el extremo opuesto de la fibra. [26]

Figura 12. Estructura de un Cable de Fibra Óptica [26]

2.2.10. DIRECCIÓN IP

La dirección IP es un valor numérico que, expresado en formato de punto decimal, sirve para identificar lógicamente una interfaz de un dispositivo o la computadora del usuario dentro de una red. El componente fundamental que establece el límite entre la red interna

y externa es el router, y es importante asociar el direccionamiento IP o lógico con este dispositivo cuando se habla de él [27].

Las direcciones IP están divididas en 5 clases, que se diferencian entre sí por tener un rango de direcciones fijas asignadas; por ejemplo, las direcciones IP de clase A, B y C son utilizadas en empresas pequeñas, medianas y grandes. Las direcciones IP de clase D son usadas en ambientes de Multicast o envío de información a múltiples destinos, y las de clase E, para estudios en los campos de investigación y desarrollo. Las direcciones IP son asignadas por una entidad reguladora [27].

CLASES DE DIRECCIONES		
CLASE	**RANGO IP**	
A	0	127
B	127	191
C	192	223
D	224	239
E	240	255

Tabla 3. Clases de Direcciones IP por: Autor

2.2.11. PING

Ping es un comando de línea de comandos utilizado para medir la velocidad de respuesta (latencia) de una conexión de red. Es utilizado para comprobar la conectividad entre dos dispositivos en una red y para medir la calidad de la conexión. El comando "ping" envía un paquete de datos a otro dispositivo en la red y espera una respuesta. El tiempo que tarda en recibir una respuesta se conoce como el "tiempo de ida y vuelta" o "latencia". Un tiempo de ida y vuelta bajo indica una buena conectividad de red, mientras que un tiempo de ida y vuelta alto puede indicar problemas de red [28].

2.2.12. CABLEADO HORIZONTAL

El cableado horizontal tiene la función de llevar los datos desde el distribuidor de piso a los usuarios. La norma EIA/TIA 568A lo describe como la sección del sistema de

cableado de telecomunicaciones que va desde el área de trabajo hasta el cuarto de telecomunicaciones [29].

2.2.13. CABLEADO VERTICAL

El cableado vertical, también conocido como backbone o cableado troncal, es el encargado de crear conexiones entre los cuartos de equipo, cuartos de entrada de servicios y cuartos de telecomunicaciones. Este está compuesto por cables verticales, conexiones principales e intermedias cruzadas, terminaciones mecánicas y cordones de patching para conexiones cruzadas [29].

Para el cableado vertical se utiliza fibra óptica, la cual tiene como ventajas indiscutibles:

- Velocidad de navegación en Internet y transmisión de datos muy alta (hasta 500 MHz, dependiendo de la distancia).
- El cable de fibra óptica tiene la capacidad de resistir el ruido, las interferencias y la humedad. Además, puede ser instalado en proximidad de conductores que transportan altos niveles de energía sin ser afectado.
- La transmisión a través de un cable de fibra óptica es segura y no se interrumpe, ya que no hay pérdida de luz en el proceso.
- No tiene señales eléctricas, por lo que no hay riesgo de sacudidas ni otros peligros. Es adecuado para trabajar en ambientes propensos a explosiones.
- Tamaño y peso reducidos, pero capaz de transportar un gran número de señales.
- Fácil de instalar.
- Ancho de banda amplio.
- Compatibilidad con tecnología digital.
- Capacidad de transmisión superior.
- La fibra es una tecnología comprobada, sencilla, estandarizada y altamente confiable.

2.2.14. CABLEADO ESTRUCTURADO DE DATOS

Este sistema de cableado utiliza cables de categoría 5E que posibilitan la conexión de los equipos a la estructura vertical de datos. Para garantizar una red uniforme, se instalan puntos de red en cada piso según se describe a continuación.:

Planta Baja	**94 puntos de red**
Primer Piso	76 puntos de red
Segundo Piso	8 puntos de red
Total	178 puntos de red para datos

Tabla 4. Puntos de Red del GAD por: Autor

Armarios de Distribución

En el edificio principal de la GAD, se encuentran cinco armarios de distribución, dos gabinetes principales se encuentran en el departamento de sistemas del segundo piso, luego en el primer piso están los dos armarios de distribución intermedios y el último que se encuentra en la planta baja, cada uno de estos racks se han situado de forma estratégica, y en todos ellos se encuentran distribuidos los siguientes dispositivos:

- Conmutador KVM de montaje en rack de 8 puertos TK-801R
- HP Storageworks 1/8 G2 Tape Autoloader
- Servidor HP ProLiant DL380 Gen10
- Router Huawei - EG8247H
- Conversor de medios WDM - MC112CS
- Liebert NXR (30KVA)
- APC (NBRK0250) NETBOTZ RACK MONITOR 250
- Conmutador Grandstream Plataformas IP PBX
- Hikvision Digital Technology DS-9664NI-I8 Network Video Recorder 2U Black
- Switch TP-Link 48 PUERTOS

- Switch TP-Link TL-SG1024
- Signamax 24 Port 1U Patch Panel
- Cisco Reafacc 24-1000-PoE 370W-tot 4-SFP Console Catalyst Switch Admin
- 3com 3C16471-US Baseline Switch 2024
- Cisco - WS-C2960-24TT-L
- Switch con 16 puertos Gigabit TL-SG1016D

Armario de Distribución Principal – Segundo Piso

Se encuentra ubicado en el Departamento de informática, debido a que este es responsable de gestionar y supervisar el flujo de información. Como resultado de esto, se convierte en el centro de conexión en estrella para todo el municipio.

En los pisos restantes del edificio gubernamental, se utilizan switches con módulos de fibra óptica para interconectar todos los puntos de datos a la red global de cableado estructurado implementada en el municipio. La distribución de esta red se realiza de acuerdo con la siguiente configuración.

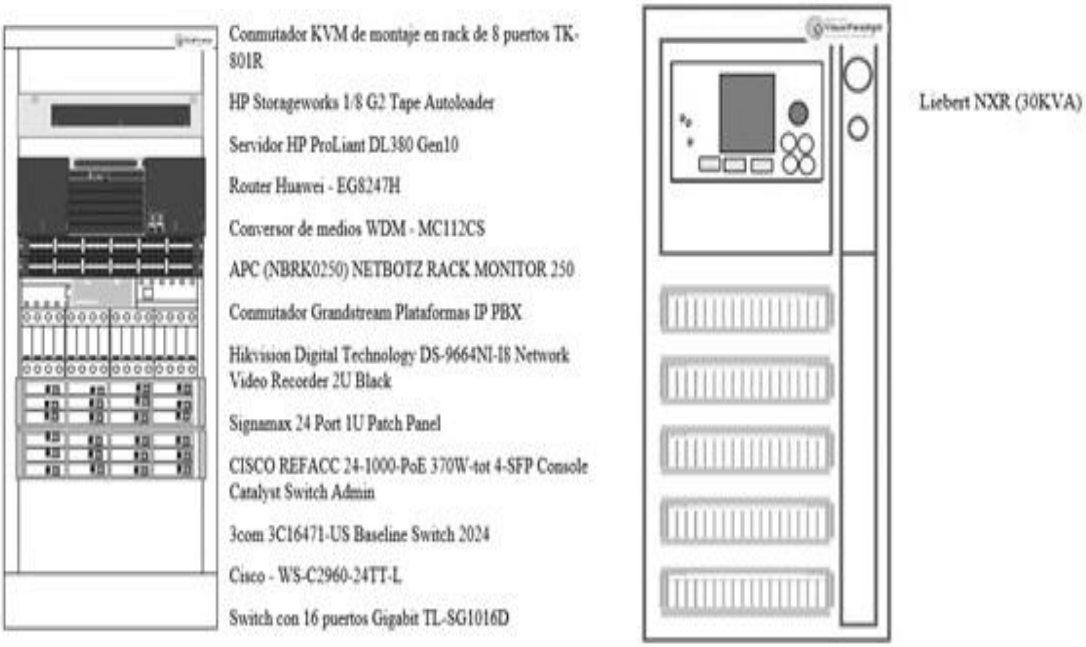


Figura 13. Armario de Distribución Principal – Segundo piso por: Autor

Armarios de Distribución Intermedios – Primer Piso

En el primer piso, se encuentra el segundo y tercer armario de distribución, el cual está situado en una posición muy central, justo enfrente del departamento de alcaldía. Esto permite una distribución óptima del cableado de red hacia todos los departamentos de este piso. La disposición de los dispositivos en su interior es la siguiente:

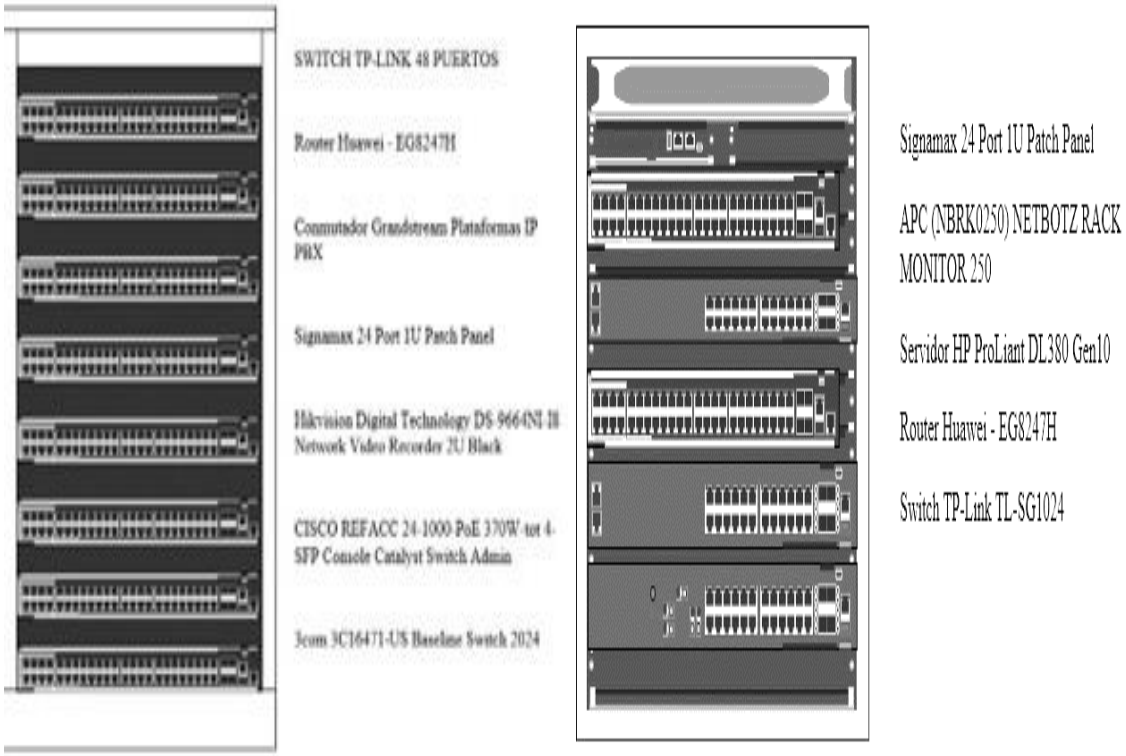


Figura 14. Armario de Distribución Intermedio – Primer piso por: Autor

Armario de Distribución Intermedio – Planta Baja

En la planta baja, se ubica el último armario de distribución al lado del ascensor. Al igual que en el primer piso, se encuentra en el centro de la planta para permitir una mejor distribución del cableado de red.

La organización interna de este armario de distribución es la siguiente:

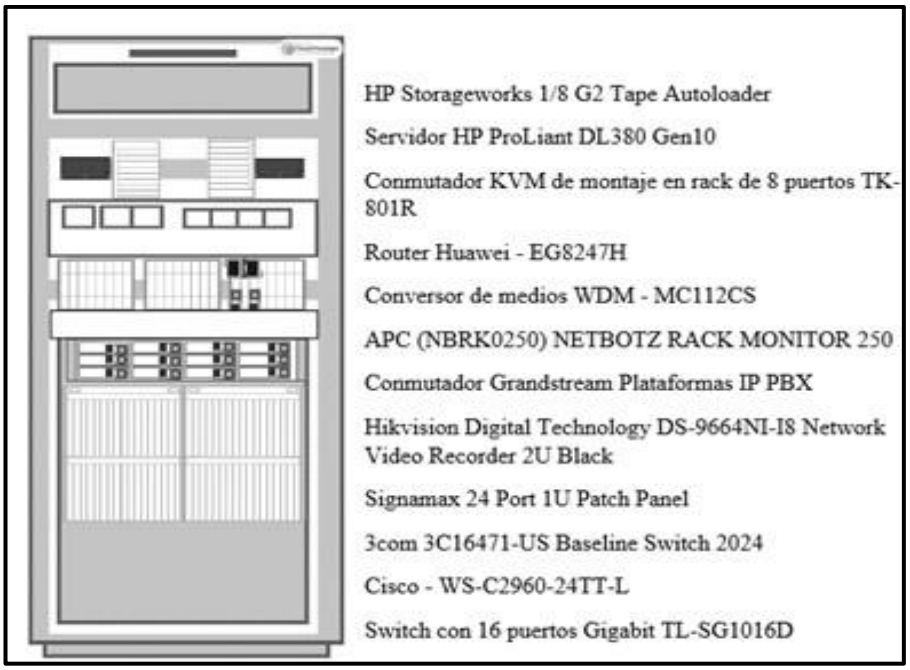


Figura 15. Armario de Distribución Intermedio – Planta baja por: Autor

El GAD dispone de equipos informáticos suficientes para llevar a cabo la reingeniería de la infraestructura de red de datos lógica, gracias a los requerimientos necesarios que se encuentran presentes en la planta baja, primer piso y segundo piso. En consecuencia, se halla en condiciones favorables para llevar a cabo esta tarea de forma efectiva

2.3. MARCO TEÓRICO

2.3.1. IMPORTANCIA DE LA IMPLEMENTACIÓN DE FIREWALL EN REDES EMPRESARIALES COMO MECANISMO PARA LA PROTECCIÓN DE INFORMACIÓN

Los firewalls son actualmente uno de los elementos clave de seguridad informática para las redes empresariales debido a las características y cualidades que ofrecen para proteger la información y los datos de estas. Estos son uno de los elementos estratégicos y operativos más importantes para cualquier organización que busque ser competitiva. Este trabajo investigativo se basa en una metodología de revisión de bibliografía y literatura, donde se investiga y se presenta información sobre las diferentes consideraciones relacionadas con los firewalls, sus características y tipologías, así como la implementación de estos, en diferentes organizaciones. Se presentan los resultados,

conclusiones y recomendaciones encontradas en relación con los firewalls, así como las perspectivas y consideraciones para futuros estudios [30].

La seguridad de datos y la protección de datos en redes corporativas, es actualmente una de las áreas más importantes de la informática, porque la cantidad e importancia de la información nunca ha sido tan importante para las empresas como lo es hoy, de manera similar, la misma exposición ante posibles acciones encaminadas a la obtención ilícita de información también presenta un desafío para los administradores de redes de comunicaciones por Internet. sus características, tipos y condiciones y los niveles de seguridad que brindan y la importancia de su implementación en las redes. para establecer un mecanismo efectivo para proteger la información de dichas organizaciones [30].

2.3.2. ARQUITECTURA DMZ PERIMETRAL: UNA IMPLEMENTACIÓN CORPORATIVA

La seguridad informática es esencial en el mundo empresarial. Contar con una infraestructura sólida y segura es un requisito importante debido a la naturaleza peligrosa de Internet. En este artículo se analizará uno de los modelos de arquitectura de red más conocidos y se verá cómo, mediante el uso de herramientas específicas, se puede mejorar la seguridad. Se propondrá una solución accesible para empresas emergentes que están dando sus primeros pasos en la red global [31].

La red está sujeta constantemente a muchos ataques, por lo que la seguridad de la información se ha convertido en una parte integral de los entornos tanto personales como empresariales. Los ataques son cada vez más complejos y numerosos, por lo que la respuesta es desarrollar métodos, plataformas y sistemas de seguridad cada vez más complejos y sofisticados para contener estas amenazas que se han vuelto características de la propia red. Estos ataques afectan a todas las empresas que cuentan con sus propias plataformas de red, por lo que parte de su presupuesto debe destinarse a la seguridad de la red. Aunque existen soluciones denominadas firewalls de aplicaciones web basadas en la nube que ofrecen seguridad como servicio, el costo puede ser alto para algunas empresas. Un diseño de red bien elegido, planificado y definido, que incluya varios dispositivos de seguridad, como firewalls, honeypots y sistemas de detección de

intrusos, puede proporcionar la seguridad de la información que necesitamos utilizando solo los recursos necesarios para implementar Internet [31].

2.3.3. VIRTUALIZACIÓN; EFICIENCIA Y ESCALABILIDAD

La virtualización se ha convertido en una tendencia popular entre las organizaciones, ya que ha demostrado ser una forma eficaz de reducir costos y aumentar la eficiencia en el uso de los recursos. Además, la virtualización permite una mejor escalabilidad en los centros de datos, lo que ayuda a adaptarse de manera más rápida a las necesidades de las organizaciones. Este documento presenta el concepto de virtualización y sus componentes, cómo mejorar la eficiencia y cómo permite una mejor escalabilidad. A medida que las empresas utilizan las tecnologías de la información y la comunicación para mejorar sus procesos, se han creado miles de centros de datos para albergarlos. La tendencia general es que la aplicación o servicio informático que se ofrece requiere de un servidor que lo soporte, aunque en algunos casos es posible agrupar algunos de estos servicios o aplicaciones en un único servidor [32].

Esto finalmente conduce a altos costos debido a varios factores: energía, mantenimiento, gestión, compra de componentes adicionales. Desarrollo y mejora de componentes de hardware, discutiendo la disponibilidad de arquitecturas de 6 bits, gigabytes de RAM, terabytes de almacenamiento, procesadores multinúcleo, servidores multiprocesador y velocidades de gigabit transmisión, podemos ver que tanto el procesamiento como el almacenamiento de los servidores aumentaron significativamente. Pero también hay estudios que muestran que gran parte de esta capacidad está infrautilizada, se dice que la utilización media de un servidor x86 suele ser del 10-15% de su capacidad real, porque en ocasiones puede llegar a un pico. valores máximos. En resumen, la virtualización es una herramienta que permite un uso eficiente de los recursos físicos en los centros de datos y ahorra energía y costos. Además de permitir escalabilidad y flexibilidad en la adición de nuevos servidores [32].

2.3.4. VIRTUALIZACIÓN DE REDES Y SERVIDORES EMULANDO INFRAESTRUCTURAS TECNOLÓGICAS

El desarrollo de habilidades en la tecnología de la información y comunicación es esencial en las empresas, así como también el aumento de la demanda de tecnologías de

virtualización en los centros de datos, como Xen Server, VMware, Proxmox, entre otros. La idea es formular escenarios tecnológicos que permitan la ejecución de prácticas profesionales en ambientes virtuales para mantener los conceptos actualizados y afrontar los desafíos de la industria tecnológica. La virtualización es una tecnología emergente que proporciona una gestión eficaz de los recursos de hardware y software, permitiendo la consolidación de servidores y la reducción de costos y espacio físico y humano en la infraestructura de TI. Como resultado, los escritorios virtuales pueden ser gestionados y protegidos de manera más efectiva. La implementación de los centros de datos ha aumentado debido a su capacidad de almacenamiento y procesamiento de grandes aplicaciones y servicios. La virtualización de servidores permite agrupar diferentes aplicaciones y servicios heterogéneos en un mismo hardware, lo que optimiza los costos de operación de las infraestructuras tecnológicas de los centros de datos [33].

La Zona Desmilitarizada (DMZ) es un conjunto de patrones de diseño de redes que aborda los problemas de seguridad y rendimiento de la red para los científicos. Incluye arquitectura de red, configuración del sistema, seguridad cibernética y herramientas de rendimiento que crean un entorno de red optimizado para la ciencia. El modelo DMZ dinámico responde en tiempo real a las demandas de tráfico de la red, optimizando tanto el rendimiento de la red como la seguridad. Este enfoque combinado permite a los científicos trabajar de manera eficiente y segura en un entorno virtual, sin preocuparse por la seguridad de sus datos y su información. De esta forma, los científicos pueden concentrarse en sus investigaciones y experimentos, en lugar de preocuparse por la seguridad de sus recursos tecnológicos [33].

2.4. DISEÑO DE LA PROPUESTA

2.4.1. OBSERVACIÓN DIRECTA

El método de recolección de datos por observación directa es una técnica para recolectar datos que implica la observación del sujeto de investigación en un contexto particular. Todo ello sin intervenir ni modificar el entorno en el que se despliega el objeto. De lo contrario, los datos obtenidos no serán válidos. Los métodos de recolección de datos se utilizan en los casos en que otros sistemas, como encuestas, cuestionarios, entre otros, no son tan efectivos.

Se recomienda la observación directa cuando se evalúa el comportamiento durante un período continuo de tiempo. En cuanto al problema de la observación directa, se puede proceder de dos formas, secretamente, cuando el sujeto no se da cuenta de que está observando, o cuando sabe que está siendo observado, en este caso se hizo de ambas maneras por lo que este método de recolección de datos fue dada cuando se estaba realizando el soporte técnico a los usuarios que manifestaban sus problemas y al momento de realizar inventario en cada departamento es donde se iba registrando los inconvenientes que presentaba el computador con la red de datos y los problemas que tenía el usuario con dicha red.

2.4.2. ANÁLISIS E INTERPRETACIÓN DE ENTREVISTA

1. ¿Cuál es su cargo dentro del departamento de Sistemas?

El conocer el cargo que dispone es muy relevante porque se tiene una idea clara del conocimiento que dicha persona tiene, en este caso se entrevistó al director de toda el área de informática y tecnologías, como director tiene mucho conocimiento en el área de redes y gracias a eso brindo una amplia información sobre el funcionamiento de la red de datos lógica.

2. ¿Cómo se encuentra estructurado el departamento de sistemas?

Gracias a que hay diversas áreas como lo es el área de desarrollo de sistemas, el área de soporte de atención al cliente y el área de servicio técnico. Es más sencillo identificar la persona correcta para realizar un tipo de consulta en específico, por ello al realizar la entrevista y conocer a fondo el funcionamiento de la red de datos se acudió al director de toda el área.

3. ¿Cómo está estructurada la red de datos?

El director manifestó que en cada piso está distribuida la red por VLANS y de esta manera llevar un control de la red por piso o por departamento, adicionalmente menciono que todo este proceso es llevado a cabo por router cisco y que dentro del GAD de Santa Elena se maneja una red interna la cual es la encargada de operar todos estos procesos, las IP son fijas manejándose por switch.

4. ¿**Cuentan con Firewall en la red y si es así, cuantos tienen y de qué forma está estructurado cada Firewall?**

Si se cuenta con un firewall el cual es un sistema que ayuda a proteger las redes privadas al no dar acceso a usuarios no autorizados, actualmente se está trabajando con un proxy el cual es un puente que usualmente es utilizado como un puente entre el origen y el computador, por el uso del proxy podemos tener acceso a internet y por medio de este elegir qué restricciones se impondrán al usuario.

5. ¿Cuántos proxys manejan?

El ingeniero encargado del área de sistemas nos mencionó que se está trabajando dos proxys cada uno de ellos funciona con distintos proveedores de Internet por lo que es una forma siempre mantener el servicio de internet, nos dijo que estos proxys suelen tener distintas políticas de seguridad para los usuarios en su computador por lo que el segundo proxy es más usado para el área de administración, finanzas y la gerencia.

6. ¿Qué políticas de seguridad se tienen implementadas actualmente?

Hay varias políticas de seguridad implementadas en el GAD de Santa Elena, una de ellas es el controlador de dominio el cual es manejado con el sistema de Windows Server, otra política es la del control de cuenta de usuario, el cual es usado para restringir el acceso a funciones del computador o para crear o unirse a una carpeta compartida, se aclara que todo funciona por cableado y no Wifi ni se cuentan con servicios como los Acces Point

7. ¿Cuentan con los planos de la estructuración de la red de datos?

Si se cuenta con los planos de toda la infraestructura de la red de datos lógica del GAD de Santa Elena, pero no disponen de este recurso en formato digital, ya que solo le tiene en formato físico y menciono que ya se encuentran desgastados por el uso que constantemente se les da, menciono que hace falta una nueva reestructuración del plano de la red porque existe el riesgo de que se pierda esa información.

2.4.3. REQUERIMIENTOS

Los requerimientos para la nueva infraestructura que se está planteando dentro de este proyecto, es necesario hacer un levantamiento de información sobre los equipos

informáticos que actualmente cuenta la municipalidad de Santa Elena, la última compra de registrada en el portal de la página oficial y los últimos cambios realizados fueron:

- El cableado estructurado utilizado para la transmisión de datos pertenece a la categoría 5E.
- El cableado estructurado utilizado para la transmisión de voz pertenece a la categoría 5E.
- Gabinetes de Distribución
- Estructura vertical de datos y voz (Backbone)
- Antenas de comunicación y un sitio central de comunicaciones
- Conmutadores KVM de montaje en rack de 8 puertos TK - 801R
- HP Storageworks 1/8 G2 Tape Autoloader
- Servidores HP ProLiant DL380 Gen10
- Routers Huawei-EG8247H
- Conversores de medios WDM-MC112CS
- Conmutador Grandstream Plataformas IP PBX
- Switch TP-Link 48 PUERTOS
- Switch TP-Link TL-SG1024
- Signamax 24 Port 1U Patch Panel
- Cisco Reafacc 24-1000-PoE 370W-tot 4-SFP Console Catalyst Switch Admin
- Cisco-WS-C2960-24TT-L
- Switch con 16 puertos Gigabit TL-SG1016D

La instalación del Sistema de Cableado Estructurado permitió la interconexión de todos

los dispositivos con servidores de alta tecnología, lo que permitió la implementación de sistemas centralizados para la gestión de datos.

La infraestructura consta de tres enlaces de cableado vertical o backbone y aproximadamente 361 puntos de telecomunicaciones. Los enlaces que se encuentran en la planta baja, primer piso y segundo piso se conectan con el Departamento de Sistemas.

2.4.4. DISEÑO DE RED

Los firewalls, ya sea en forma física o virtual, son dispositivos de seguridad que tienen la capacidad de filtrar el tráfico de red tanto de entrada como de salida, mediante el uso de reglas específicas. Su objetivo principal es permitir o denegar el paso a las comunicaciones que llegan a él, como una solicitud de acceso al servidor web de la empresa, dependiendo de cómo se hayan definido las reglas.

A continuación, se muestran el diseño de red actual y el nuevo diseño de red.

Nuevo diseño de Red

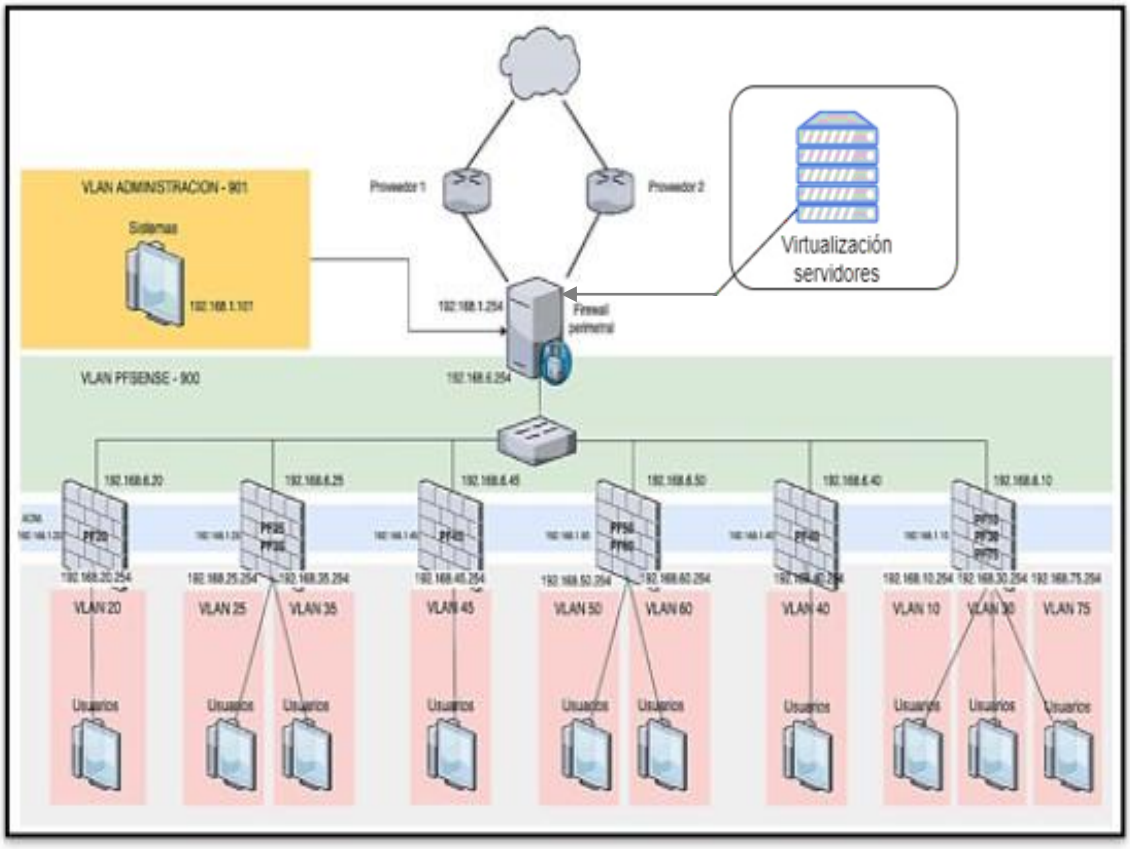


Figura 16. Diseño actual de la red del GAD por: Autor

Diseño Actual de la Red

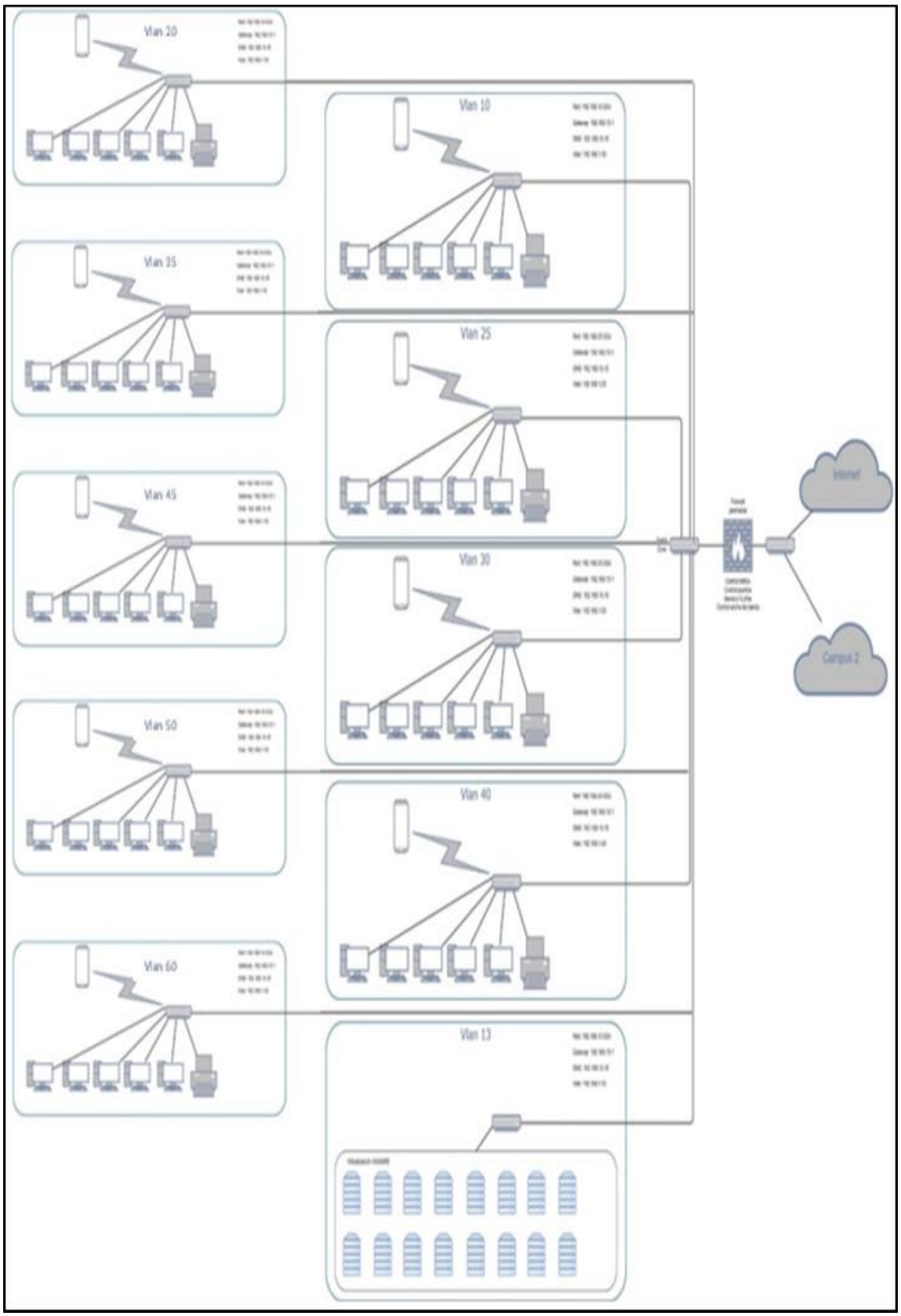


Figura 17. Diseño actual de la red del GAD por: Autor

2.4.5. CONFIGURACIÓN DE VMWARE

Para ingresar a la consola web de VMware ESXi, se necesita abrir un navegador web y escribir la dirección IP que se proporcionó en la ventana principal. Después, aparecerá una pantalla de inicio de sesión donde es necesario ingresar el nombre de usuario y la contraseña para poder acceder.

Es importante destacar que estos detalles de inicio de sesión son los mismos que ingresamos durante la instalación de VMware ESXi. Por lo tanto, es crucial recordar nuestro nombre de usuario y contraseña para poder acceder a la consola web y gestionar nuestro sistema virtualizado.

Una vez que hayamos ingresado nuestro nombre de usuario y contraseña, tendremos acceso a la consola web y podremos comenzar a trabajar con el software. Desde la interfaz gráfica de usuario, desde allí podremos crear y configurar máquinas virtuales, gestionar el almacenamiento y la red en nuestro sistema virtualizado, y realizar muchas otras tareas.

Figura 18. Pantalla de inicio de VMware por: Autor

Después de ingresar a la GUI web de VMware ESXi con nuestro nombre de usuario y contraseña, se nos presentará la ventana principal del host. Esta ventana es el centro de control y administración de nuestro sistema virtualizado.

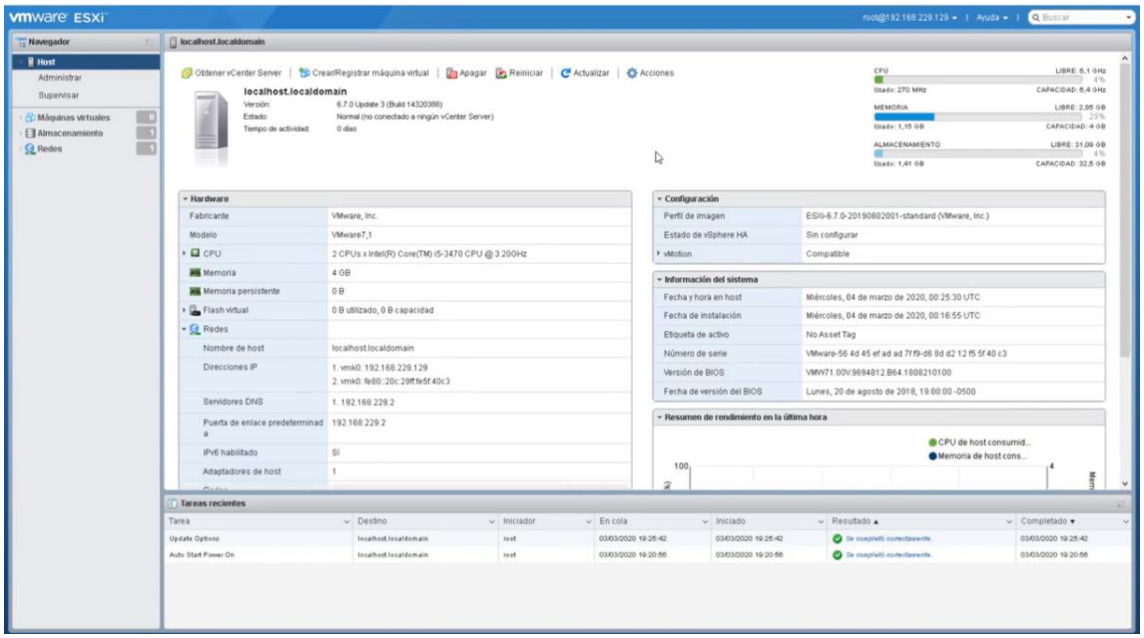


Figura 19. Vista general de la pestaña de Host de VMware por: Autor

Después de crear algunas máquinas virtuales en nuestro sistema virtualizado con VMware ESXi, la ventana principal del host se verá de una manera un poco diferente. En lugar de mostrar simplemente información general sobre el sistema, también mostrará información sobre cada una de las máquinas virtuales que hemos creado.

En la ventana principal, podremos ver una lista de todas las máquinas virtuales que hemos generado, incluyendo información sobre el uso de recursos, el rendimiento y el estado de cada máquina virtual. También tendremos acceso a opciones para gestionar y monitorear cada máquina virtual de forma individual.

Desde la pantalla principal, podremos realizar tareas importantes como la creación y configuración de nuevas máquinas virtuales, la gestión de almacenamiento, la configuración de la red y la realización de copias de seguridad para cada una de las máquinas virtuales que hemos creado.

También tendremos acceso a herramientas de diagnóstico y solución de problemas para resolver cualquier problema que pueda surgir en nuestras instancias virtuales

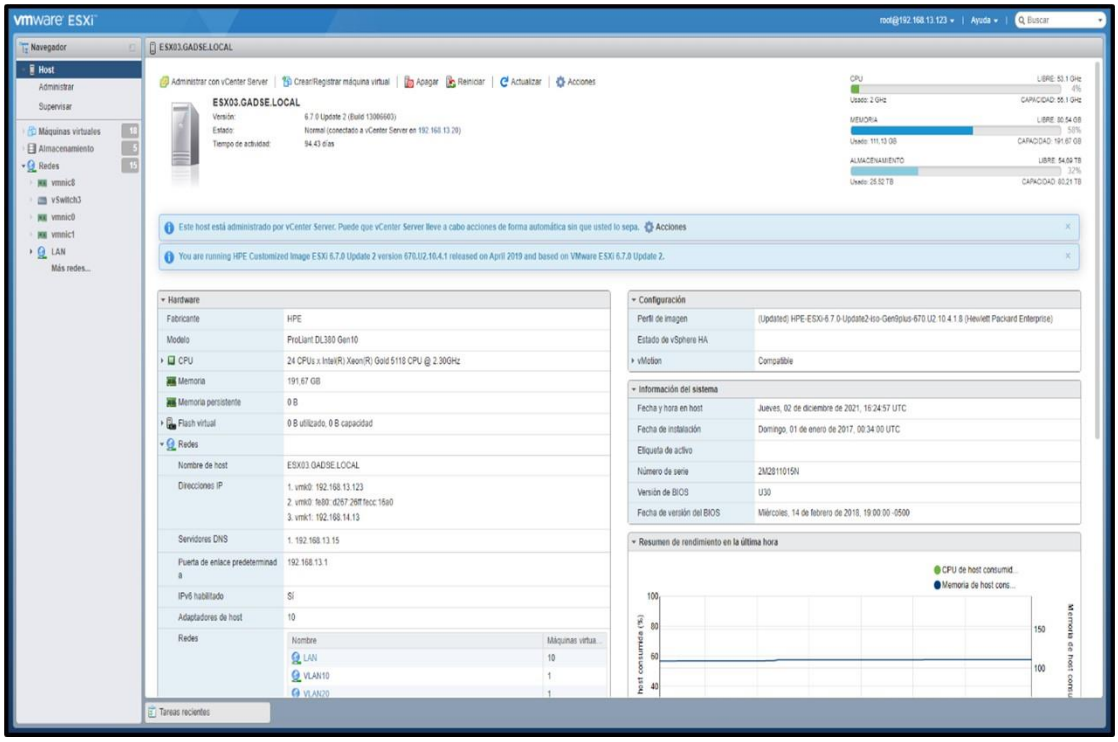


Figura 20. Vista general de la pestaña de Host ya con las configuraciones realizadas por: Autor

En la pestaña de redes en VMware ESXi es una herramienta muy útil para monitorear y gestionar las interfaces de red en nuestro sistema virtualizado. En esta sección, podremos ver información detallada sobre cada una de las interfaces de sistema de comunicación que tenemos disponibles, incluyendo información sobre el uso de recursos, el rendimiento y el estado de cada interfaz.

En particular, podemos ver la información específica sobre Vmnic0 y Vmnic1, las dos interfaces de red utilizadas en el GAD. Estas dos interfaces de red son responsables de proporcionar conectividad de red a nuestro sistema virtualizado, y es importante monitorearlas para asegurarnos de que están funcionando correctamente y proporcionando el rendimiento adecuado.

En la pestaña de redes, podremos ver información detallada sobre cada una de estas interfaces de red, incluyendo la dirección IP asignada, la cantidad de tráfico de red que está siendo enviado y recibido, y el estado de cada una de ellas. También podremos ver información sobre la configuración de conexión, incluyendo la subred, la máscara de subred y el Gateway.

Desde la sección de redes, también tendremos acceso a opciones para gestionar y configurar cada interfaz de red de forma individual. Por ejemplo, podremos cambiar la dirección IP asignada, configurar la conectividad VLAN, y modificar la configuración de seguridad para cada interfaz de red.

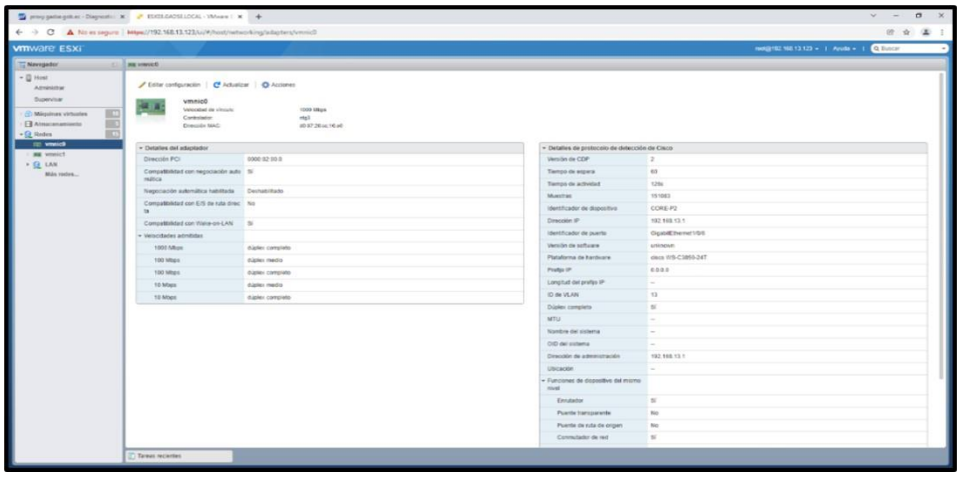


Figura 21. Vmnic0 y Vmnic1 las dos interfaces de red utilizadas en el GAD por: Autor

Ahora, al revisar la pestaña de redes, podemos ver información específica sobre LAN, que es la única interfaz de red a través de la cual entra y sale todo el tráfico de la red. Esta interfaz es esencial para el correcto funcionamiento de la red y es por ello que es importante monitorear y mantener su estado y configuración actualizados. Además, también es crucial asegurarse de que esté correctamente configurada y estable para garantizar un rendimiento óptimo y una buena conectividad.

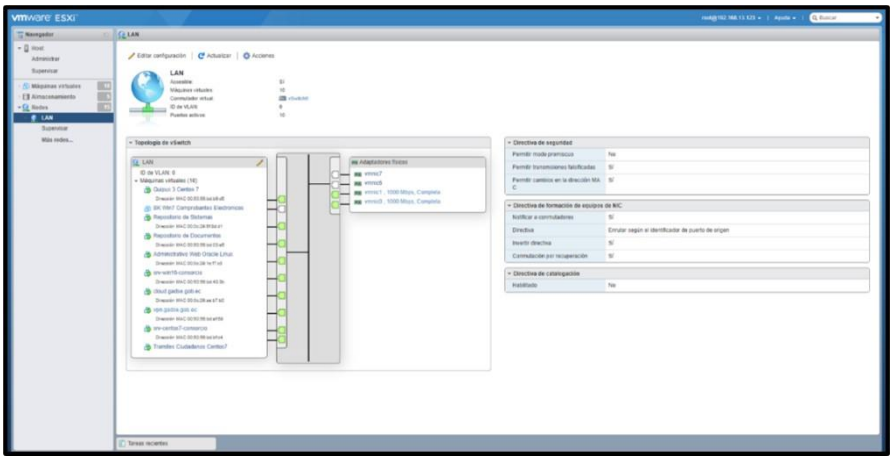


Figura 22. Interfaz única por la que sale e ingresa tráfico a toda la red por: Autor

2.4.6. INSTALACIÓN DE PFSENSE

Antes de comenzar con el proceso de instalación de Pfsense, es importante tener en cuenta que debemos leer y comprender los términos y condiciones de privacidad que se presentan. Estos términos establecen los límites y las responsabilidades de los usuarios con respecto al uso de la información y los datos que se manejan a través de la plataforma.

Después de haber leído cuidadosamente los términos y condiciones de privacidad, debemos hacer clic en el botón "Aceptar" para continuar con el proceso de instalación. Este paso es esencial para poder acceder a todas las funciones y opciones de Pfsense y utilizarlas de manera efectiva.

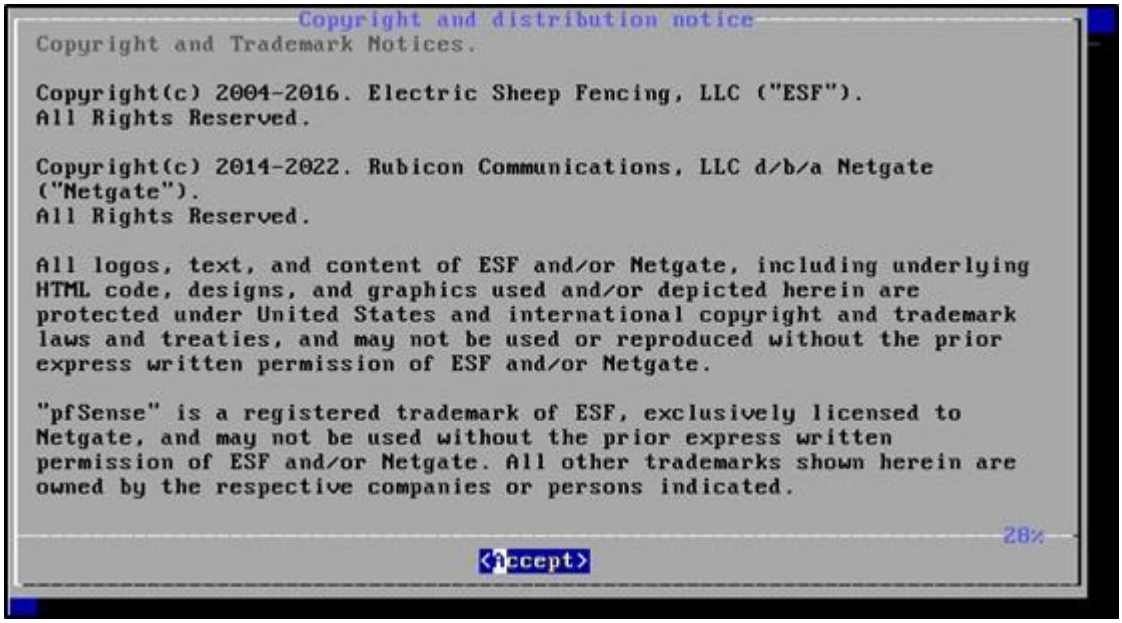


Figura 23. Primera ventana al inicializar Pfsense.

Después de aceptar los acuerdos de privacidad, se mostrará una nueva ventana. En esta ventana, tendremos la opción de seleccionar "Install Pfsense". Es importante elegir esta opción cuidadosamente, ya que esto iniciará el proceso de instalación del software. Una vez que hayamos seleccionado dicha opción, debemos hacer clic en el botón "OK". Es importante tener en cuenta que este es un paso crucial en este proceso, por lo que es necesario seguir adelante con precaución para asegurarse de que todo se haga correctamente.

Es fundamental tener en cuenta que esta ventana puede variar dependiendo de la versión de Pfsense que estemos utilizando, así que debemos asegurarnos de leer cuidadosamente todas las opciones y configuraciones que se presenten en ella. Algunas de las opciones que se nos presentarán incluyen la selección de una red, la configuración de la dirección IP, la selección de un disco duro para la instalación, entre otros.

Figura 24. Comienzo de la instalación de Pfsense por: Autor

En esta fase de la instalación de Pfsense, tendremos la opción de seleccionar el idioma del teclado que deseamos utilizar durante el proceso. Esta opción es importante, ya que nos permitirá ingresar los datos y las configuraciones de manera más fácil y precisa.

En mi caso, he decidido escoger la versión de teclado español. Esta opción es adecuada para mí, puesto que estoy familiarizado con las teclas del teclado en español, lo que me permitirá realizar mis ajustes de manera más eficiente.

Sin embargo, esta opción puede variar dependiendo de las preferencias y necesidades de cada usuario. Hay muchos otros idiomas disponibles, como inglés, francés, alemán, entre otros, por lo que cada consumidor puede seleccionar el que mejor se adapte a sus necesidades.

Figura 25. Selección de idioma de teclado en la configuración de Pfsense por: Autor

Después de seleccionar el idioma del teclado y hacer clic en la opción "Select", llegaremos a la siguiente ventana en la instalación de Pfsense. Se nos pedirá que escojamos el tipo de arranque correspondiente a nuestro equipo.

Es importante seleccionar la opción correcta, ya que esto afectará el proceso de instalación y configuración del Firewall en su equipo. Hay dos opciones disponibles: BIOS y UEFI. Cada una de estas opciones tiene sus propias ventajas y desventajas, por lo que debemos elegir cuidadosamente la opción adecuada para nuestro equipo, en mi caso escogeré la opción de BIOS.

Figura 26. Selección de tipo de arranque de Pfsense por: Autor

Después de seleccionar la opción de BIOS y presionar la tecla "Enter", comenzará instalación de Pfsense en su equipo. En esta fase, el Firewall será instalado y configurado para su uso.

Figura 27. Inicialización de la instalación de Pfsense por: Autor

Después de que la instalación de Pfsense haya concluido, aparecerá una ventana que nos preguntará si deseamos abrir una Shell para realizar una configuración avanzada. En este caso, he decidido escoger la opción de "No".

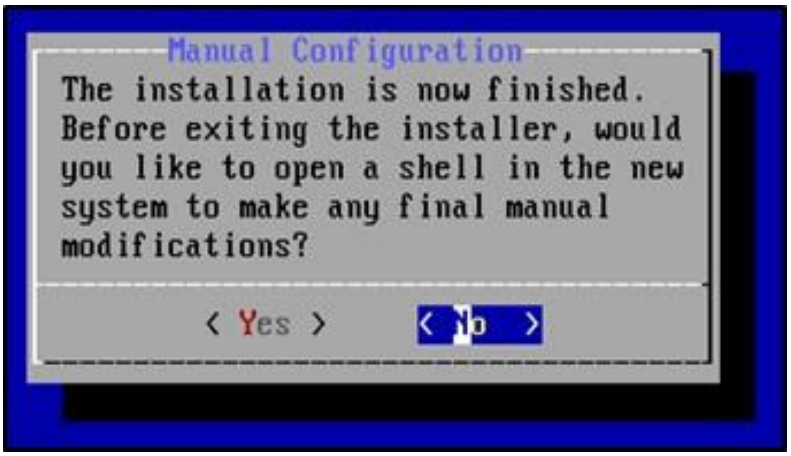


Figura 28. Abrir una Shell después de la instalación de Pfsense por: Autor

Después de reiniciar, tendremos acceso a la siguiente ventana, donde se indicará que el servicio ha sido iniciado con éxito.

Este es un paso importante en la configuración de Pfsense, ya que garantiza que todos los servicios necesarios para el correcto funcionamiento están en marcha. Desde aquí,

podremos acceder a la interfaz web de nuestro Firewall y comenzar a personalizarlo para nuestras necesidades específicas.

La GUI de este software es muy intuitiva y fácil de usar, lo que permite a los usuarios realizar una amplia variedad de tareas de ajustes con rapidez y eficacia. Podremos ajustar la configuración de red, establecer reglas de firewall, configurar políticas de seguridad y mucho más.

Figura 29. Servicio de Pfsense iniciado luego de su instalación por: Autor

Luego de todo el proceso anterior, ya es hora de dirigirnos a la máquina que queremos modificar. En este caso, se seleccionó una máquina con Windows 10.

El primer paso en la configuración de esta máquina será ejecutar un comando en la línea de comandos (CMD). Este comando es "ipconfig //all".

Este comando nos proporcionará información detallada sobre los ajustes de red de la máquina, la máscara de subred, la dirección IP, la puerta de enlace predeterminada y otros detalles importantes.

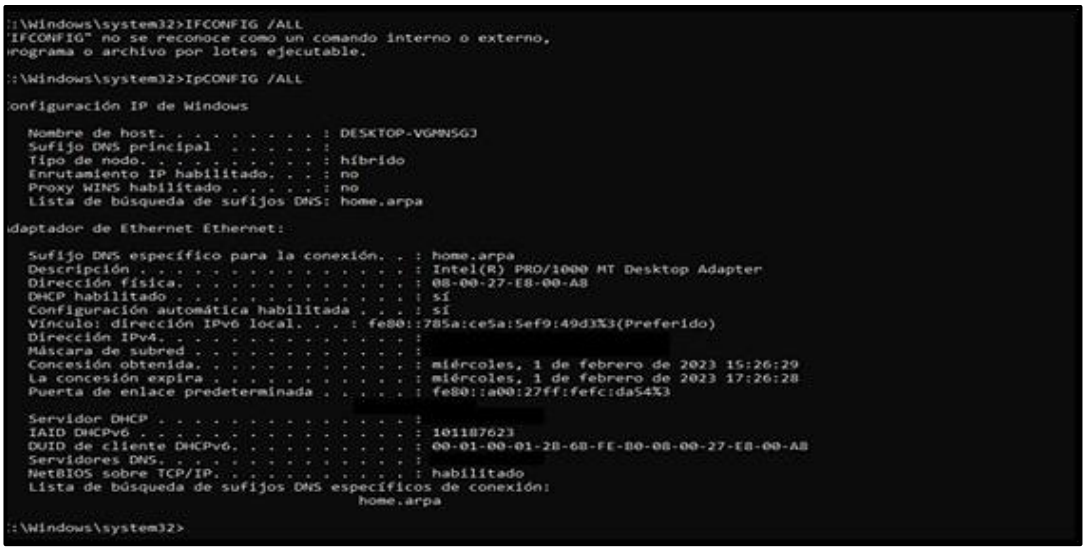


Figura 30. Comando ifconfig en Windows por: Autor

Después de haber verificado la configuración de la dirección IP de la máquina con Windows 10, es hora de probar la conexión con nuestro servidor Pfsense recién creado. Para hacer esto, utilizaremos el comando "ping".

Si la conexión es exitosa, condicho comando, este mostrará que la conexión está funcionando correctamente y que podemos comunicarnos con nuestro servidor Firewall.

Al asegurarnos de que los dispositivos estén trabajando correctamente y puedan comunicarse entre sí es una fase crucial en la configuración de Pfsense y la máquina con Windows 10.

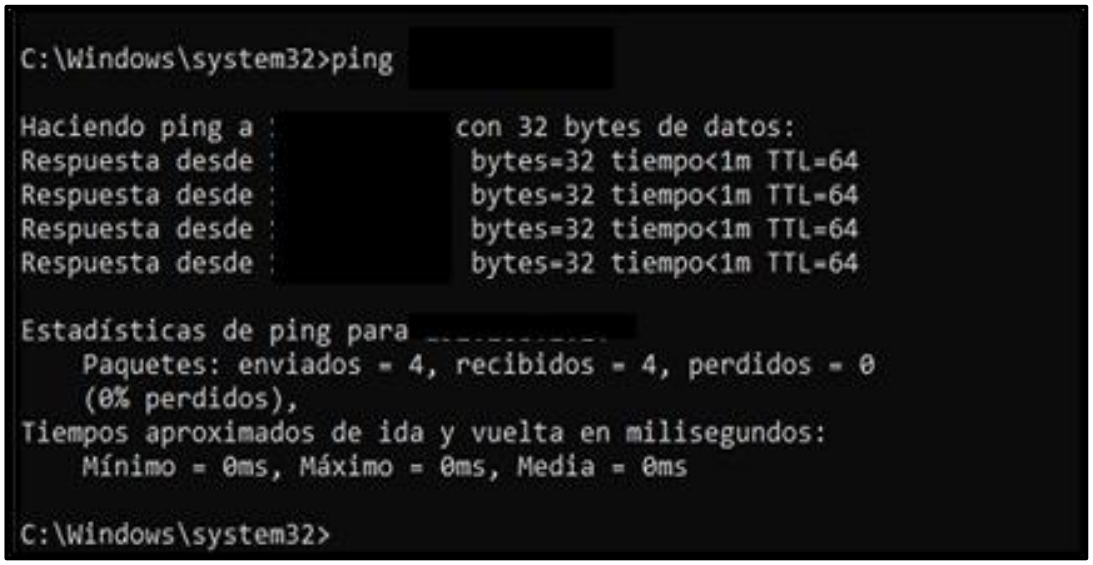


Figura 31. Verificación de conexión con el servidor Pfsense por: Autor

2.4.6. CONFIGURACIÓN DE PFSENSE

Después de haber verificado la conexión entre la máquina con Windows 10 y el servidor Pfsense a través del comando "ping", es hora de acceder a la interfaz web de nuestro Firewall. Esto se puede hacer a través de cualquier navegador web, desde cualquier dispositivo conectado a la misma red LAN.

Para acceder a la interfaz de gestión, simplemente abrimos explorador web y escribimos la dirección IP de la red LAN que nos proporcionó dicho servidor recién creado. Una vez que hayamos introducido la dirección IP en la barra de direcciones del navegador, presionamos "Enter" y se nos mostrará la página de una pantalla de inicio.

Esta página es la interfaz de gestión de Pfsense y es a través de ella que podremos configurar y gestionar nuestro servidor. Desde ahí podremos ver información importante sobre el sistema, gestionar reglas de firewall, configurar redes y servicios, y mucho más.

Es importante tener en cuenta que la dirección IP de la red LAN que nos proporciona el Firewall es única y solo es accesible desde dispositivos conectados a la misma red. Esto significa que no se puede acceder a esta GUI desde Internet o desde una red diferente.

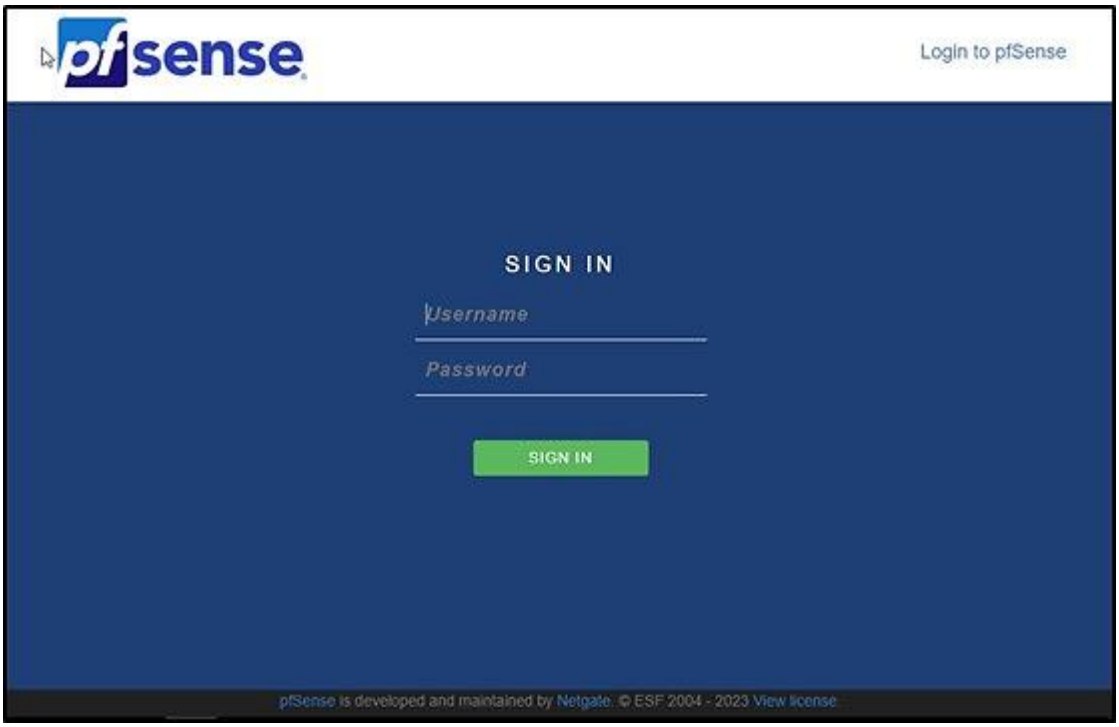


Figura 32. Pantalla de inicio de Pfsense por: Autor

Luego de ingresar las credenciales correctamente en la página de inicio de sesión, tendremos acceso a la interfaz de administración de Pfsense. Esta ventana de bienvenida es la primera que se muestra después de ingresar y es una forma de indicar que hemos iniciado sesión de manera exitosa y que tenemos acceso a todas las funciones y configuraciones del firewall. En esta GUI se nos muestran las opciones básicas y las más utilizadas para poder empezar a trabajar de manera efectiva.

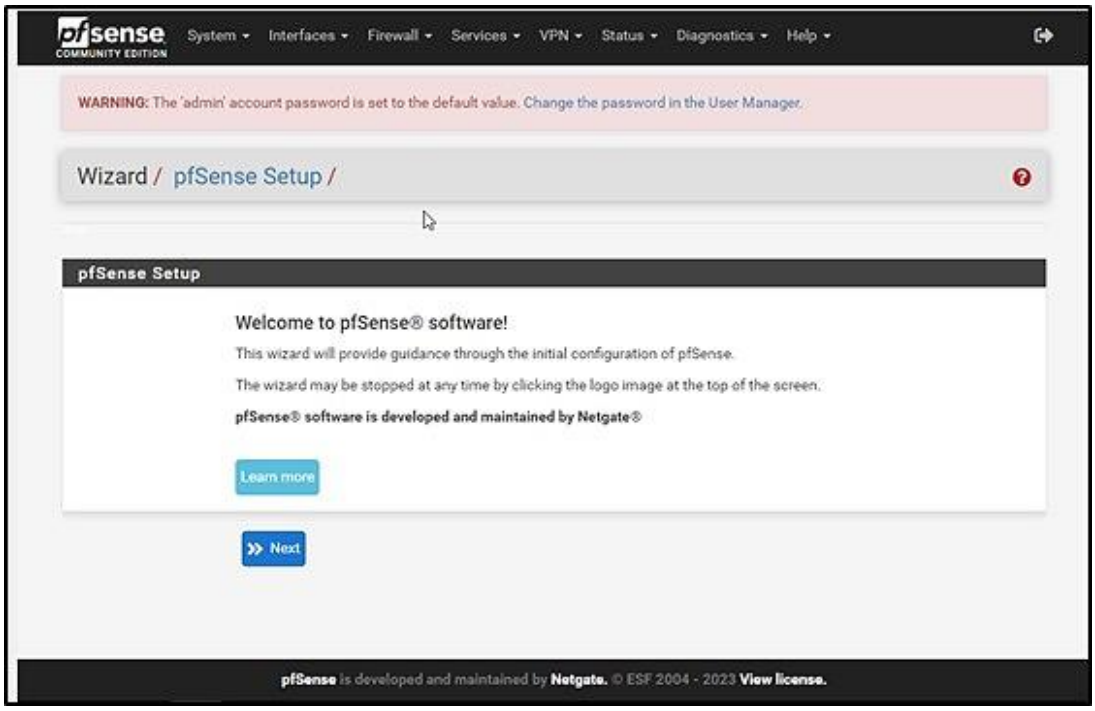


Figura 33. Pantalla de bienvenida de Pfsense por: Autor

Después de dar clic en "Next", llegaremos a una nueva ventana en la que podremos realizar la configuración avanzada de nuestro servidor. En ella podremos especificar detalles importantes como el hostname, que es el nombre que identifica a nuestro servidor en la red. También podremos configurar el dominio, que es una extensión que se agrega al final del nombre de la máquina y ayuda a identificar de manera más clara a qué organización o empresa pertenece el servidor.

Además de esto, también podremos especificar los servidores DNS primario y secundario que usaremos para resolver nombres de dominio a direcciones IP. Es importante configurar estos valores correctamente, ya que son esenciales para el funcionamiento adecuado de la red. Con esta información, podremos asegurarnos de

que todas las solicitudes de resolución de nombres de dominio se ejecuten de manera eficiente y segura.

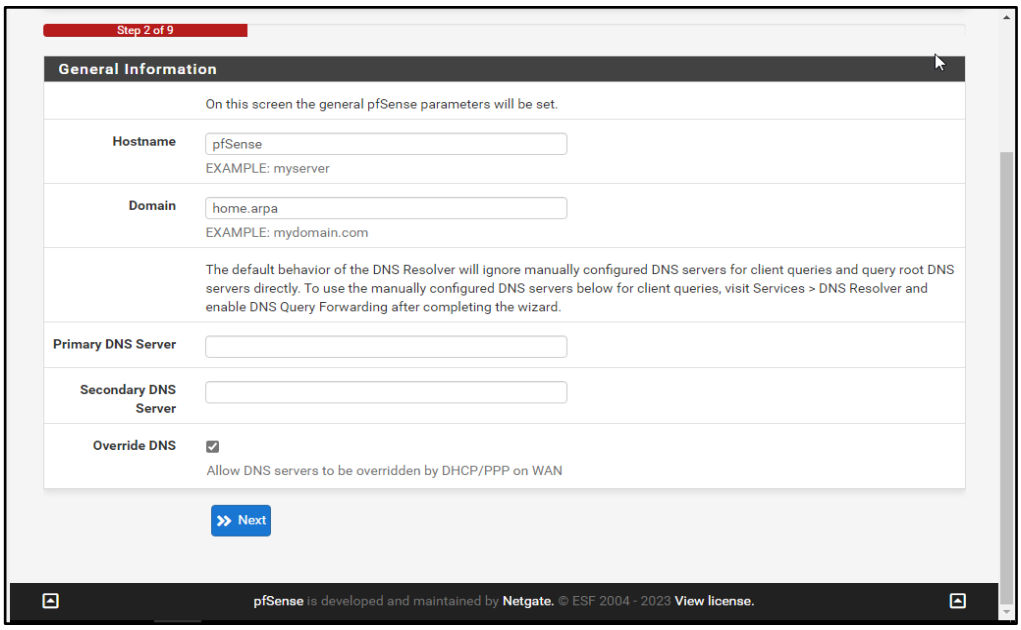


Figura 34. Pestaña de configuración avanzada de Pfsense por: Autor

Luego de dar clic en la opción "Siguiente", se abrirá una nueva ventana que nos permitirá configurar la sincronización del reloj con un servidor NTP específico. En este caso, hemos decidido escoger la opción "América/Guayaquil. Es importante tener en cuenta que sirve para garantizar la precisión de las fechas y horas en nuestro sistema, por lo que es un paso crucial en los ajustes de nuestro servidor Pfsense.

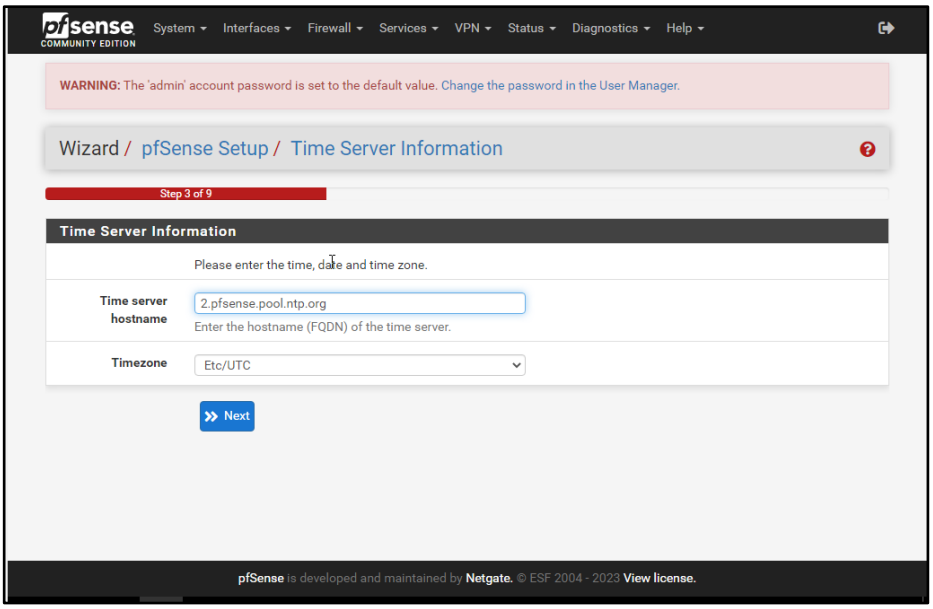


Figura 35. Configuración del reloj de Pfsense por: Autor

Después de hacer clic en "next", llegamos a la siguiente ventana en donde podremos configurar los detalles de nuestra interfaz WAN. Aquí podemos escoger cómo queremos que se conecte nuestro servidor a Internet, si queremos usar una dirección IP estática o dinámica, y otros detalles relacionados con la conexión a Internet.

Es importante tener en cuenta que los ajustes correctos en la interfaz WAN es crucial para el correcto funcionamiento de nuestro servidor Pfsense. Por lo tanto, es recomendable tomarse el tiempo necesario para configurar esta sección de manera adecuada.

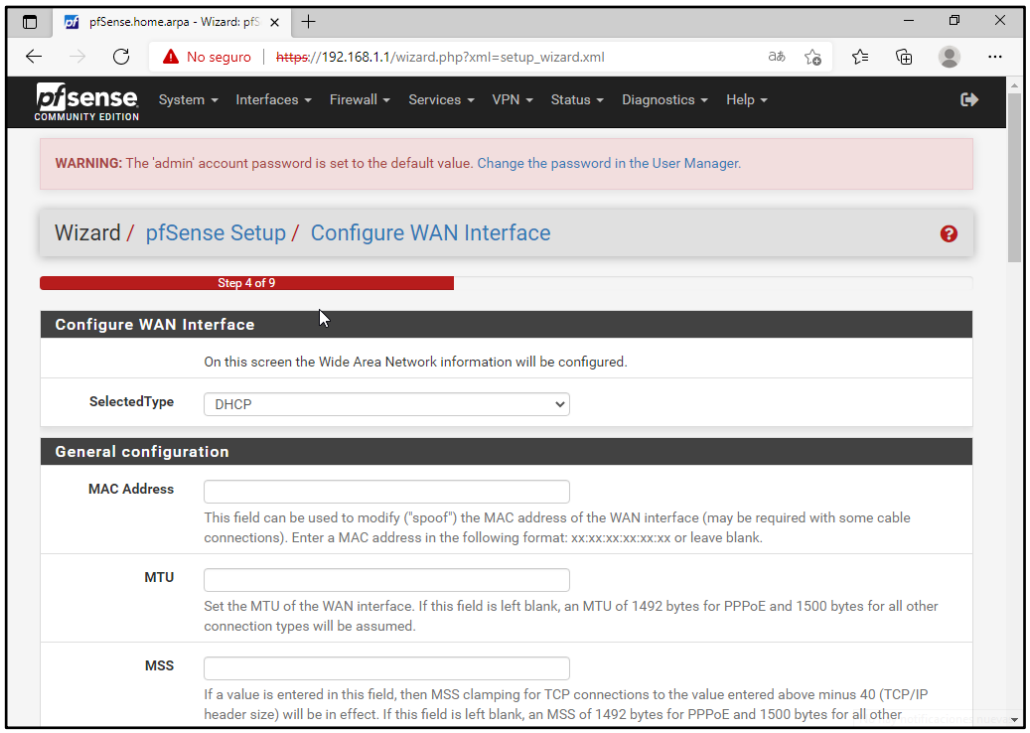


Figura 36. Configuración de la interfaz WAN de Pfsense por: Autor

Ahora en este apartado podemos cambiar la dirección IP LAN, es importante tener en cuenta que, al cambiar esta dirección, tendrás que realizar cambios en cualquier dispositivo o aplicación que esté utilizando la conexión de red interna anterior. Es por eso que es recomendable tener en cuenta esta decisión antes de realizar cualquier cambio. En caso de decidir hacer este ajuste, debemos asegurarnos de tener toda la información necesaria para reconfigurar los dispositivos y aplicaciones afectados de manera adecuada. De lo contrario, podríamos experimentar problemas en la conexión y en la configuración general de la red.

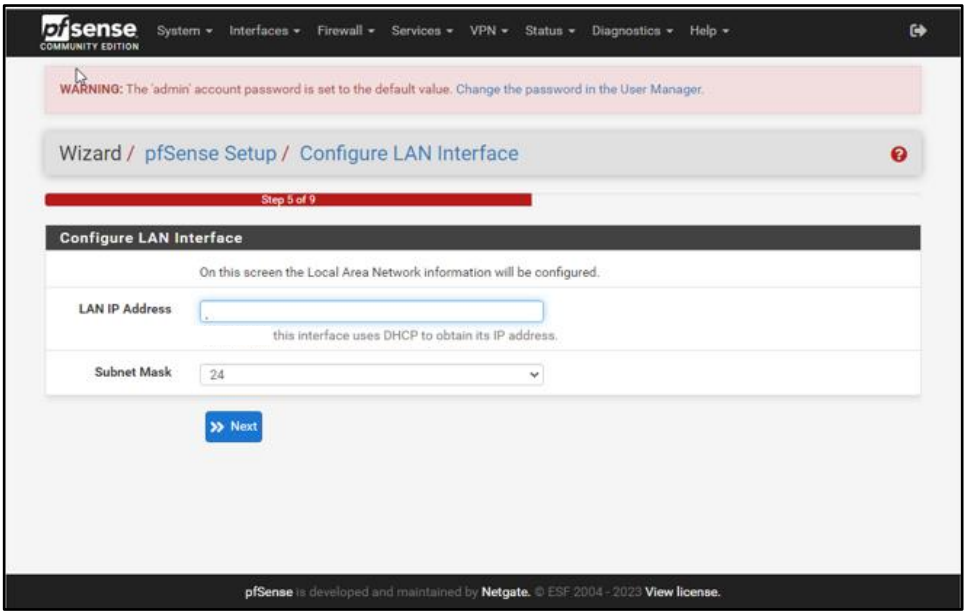


Figura 37. Configuración de la interfaz LAN de Pfsense por: Autor

Luego de dar clic en next, tendremos un apartado en el que podremos configurar una nueva contraseña para el administrador. Es importante tener en cuenta la importancia de tener una contraseña segura. Esto incluye caracteres variados, tales como letras mayúsculas y minúsculas, números y símbolos especiales. Es relevante evitar usar password común o fácilmente adivinables, como fechas de nacimiento o palabras comunes. Es recomendable usar una combinación larga de caracteres aleatorios para asegurarse que sea lo más segura posible.

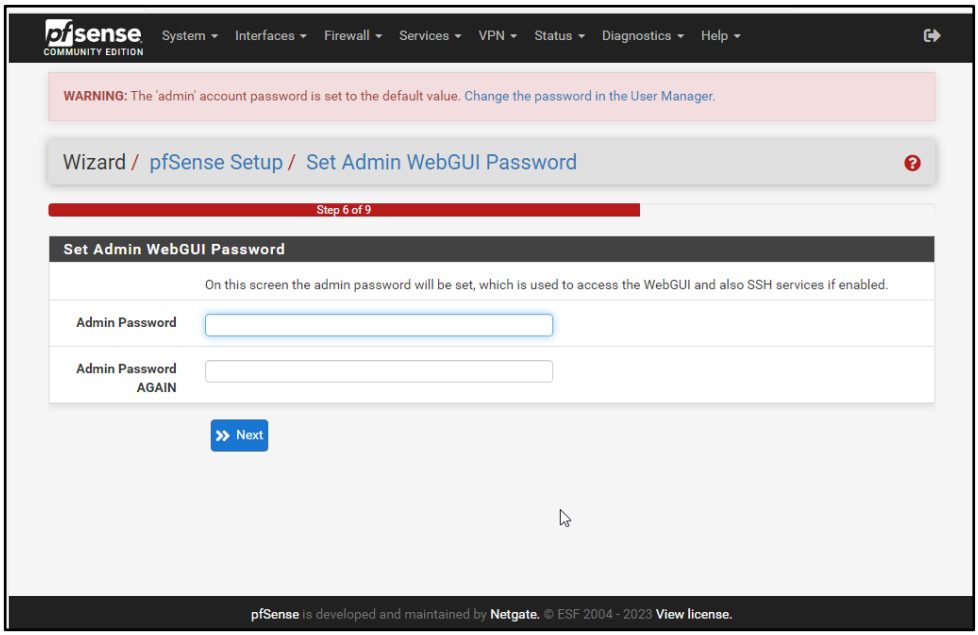


Figura 38. Configuración de nueva contraseña para Pfsense por: Autor

Luego de la recarga de Pfsense, tendremos una ventana que nos indica que hemos terminado con la configuración exitosamente. En este punto, podemos comenzar a utilizar dicha herramienta para proteger y administrar nuestra red. Sin embargo, es importante recordar que aún hay muchos otros ajustes adicionales disponibles, como son las reglas de firewall, ajustes de red, y la configuración de servicios adicionales como DHCP y DNS.

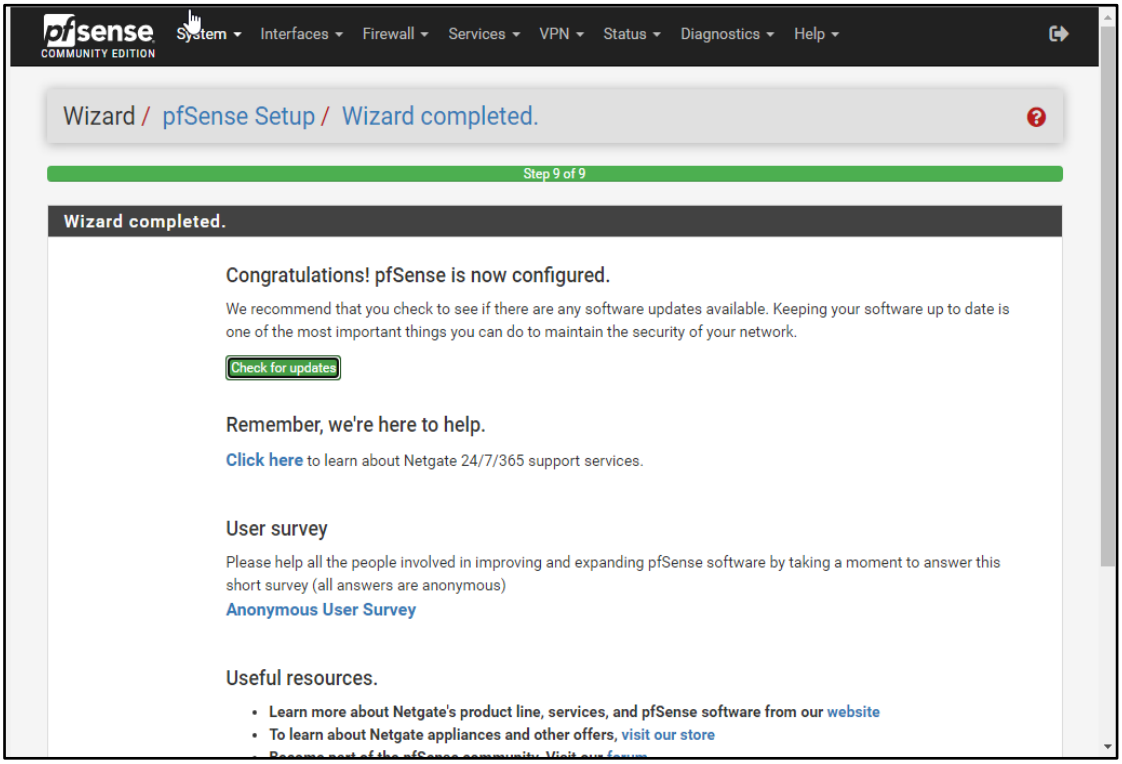


Figura 39. Culminación de la configuración básica de Pfsense por: Autor

Luego de finalizar la configuración de Pfsense, podremos acceder al Dashboard para ver una vista general de nuestro sistema. En esta pestaña podemos ver información detallada acerca del tráfico de red, la velocidad de conexión, el uso de la memoria RAM y el espacio en disco, entre otros aspectos relevantes para el correcto funcionamiento de nuestro servidor.

Además, se tiene acceso a diferentes módulos que nos permiten configurar y administrar diferentes aspectos de nuestro sistema, desde la gestión de usuarios hasta la configuración de reglas de firewall. En definitiva, esta pestaña es una herramienta fundamental para tener una visión clara y detallada de cómo está funcionando nuestro sistema Pfsense.

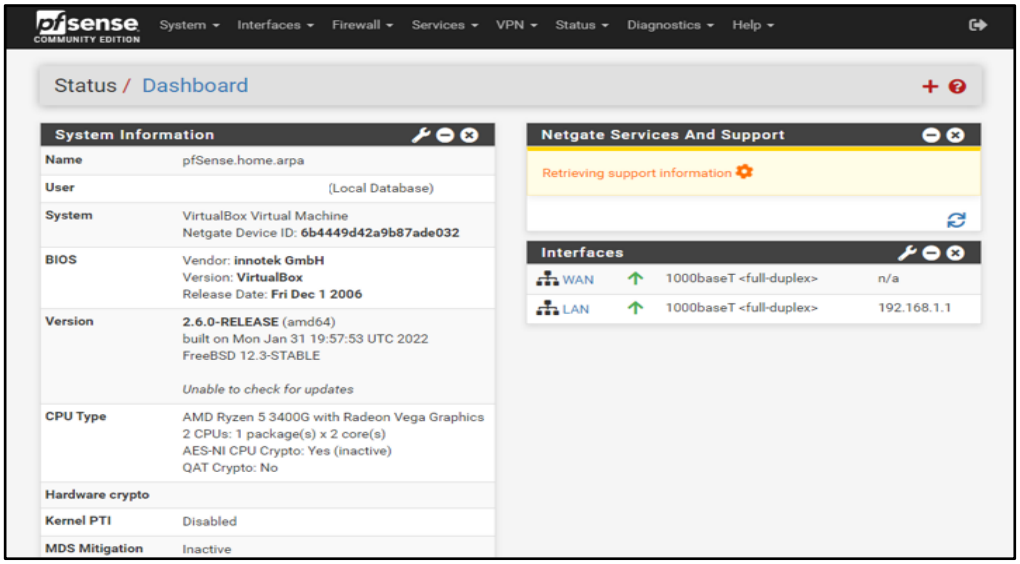


Figura 40. Pantalla general del Dashboard de Pfsense por: Autor

Ahora que hemos terminado con la configuración básica, podemos explorar aún más las opciones avanzadas que ofrece. Para ello, debemos dirigirnos a la sección de System y luego a Advance. En esta sección, tendremos acceso a una gran cantidad de configuraciones y opciones que nos permitirán personalizar aún más nuestro servidor.

Algunos de los apartados que podemos encontrar aquí incluyen los ajustes de seguridad, firewall, reglas, redes privadas virtuales (VPN), entre otros. Cada uno de estos apartados es importante y puede ser de gran ayuda para mejorar la funcionalidad de nuestro servidor, por lo que es recomendable tomarse el tiempo para entender cada una de ellas y cómo pueden aplicarse en nuestro caso particular.

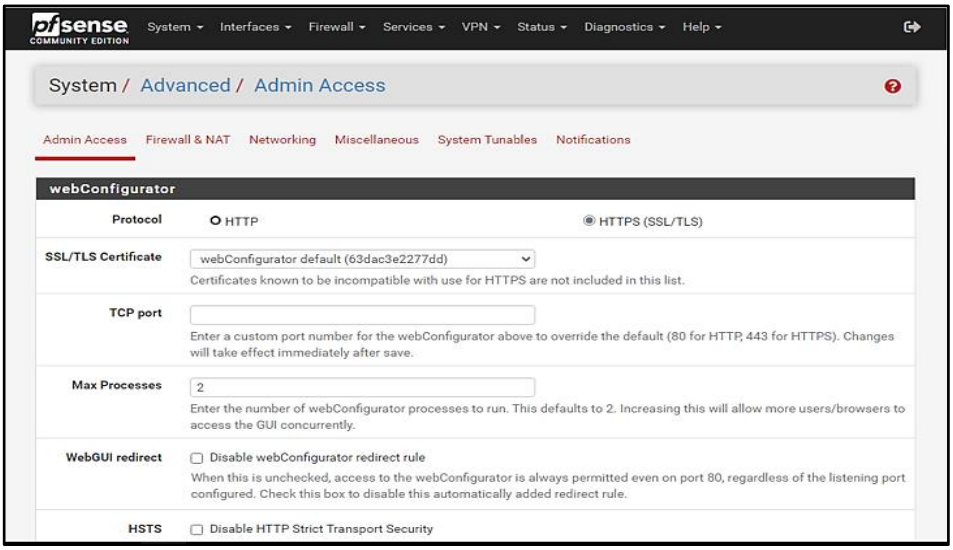


Figura 41. Configuración avanzada de admin access de Pfsense por: Autor

En este apartado es fundamental tener en cuenta la importancia de seleccionar la opción de proteger la contraseña de la consola. Esto significa que cada vez que queramos acceder a la consola de Pfsense para realizar cambios, primero tendremos que ingresar un usuario y contraseña válidos. De esta manera, se asegura la seguridad de los cambios y configuraciones realizados en el sistema.

Es importante tener en cuenta que esta medida de seguridad es esencial para mantener la integridad y confidencialidad de la información y ajustes guardados en nuestro servidor. Por lo tanto, es recomendable siempre seleccionar esta opción en el apartado de Sistema Avanzado.

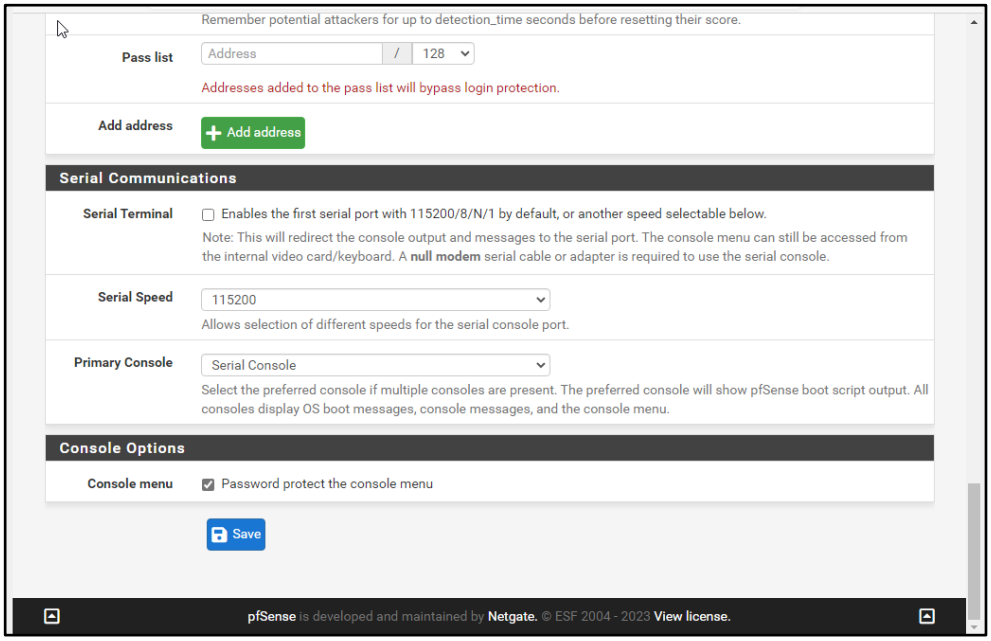


Figura 42. Configuración de contraseña para la consola de Pfsense por: Autor

En la pestaña de Firewall & NAT, es considerable tener en cuenta que la opción de “IP random id generation” puede ser una buena opción para aumentar la seguridad de nuestra red. Esta opción genera una identificación de paquete aleatoria para todos los paquetes que entran y salen de nuestra red, lo que dificulta a los atacantes realizar una acción maliciosa.

Es recomendable que luego de seleccionar esta opción, guardemos los cambios para que se vean reflejados. Finalmente, una vez hecho esto, podemos dirigirnos a la pestaña de Networking para continuar con la configuración de nuestra red.

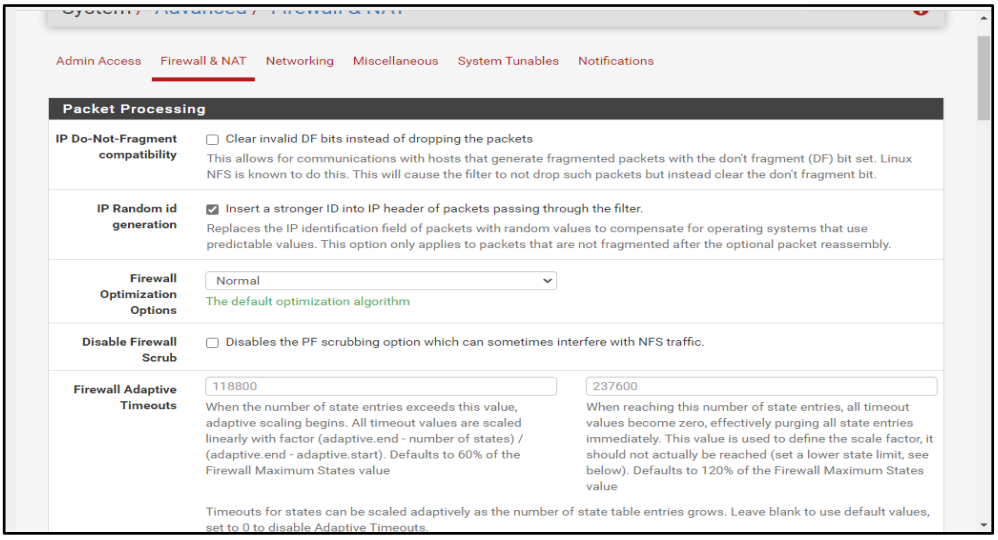


Figura 43. Configuración de la pestaña Firewall & NAT de Pfsense por: Autor

Además, en el apartado de Services, es importante asegurarse de que esté configurado de manera correcta. En este caso, al seleccionar la opción de DNS resolver, debemos asegurarnos de que las interfaces de red estén configuradas de manera adecuada. En este caso, se ha elegido la opción de LAN y localhost, ya que no es necesario que el DNS tenga acceso a todas las opciones disponibles.

Esto ayuda a mejorar la seguridad de la red, evitando posibles vulnerabilidades o accesos no autorizados a la información. Es relevante seguir los procedimientos recomendados para configurar de manera correcta los servicios de red, para asegurar un correcto funcionamiento y una mayor seguridad de los datos.

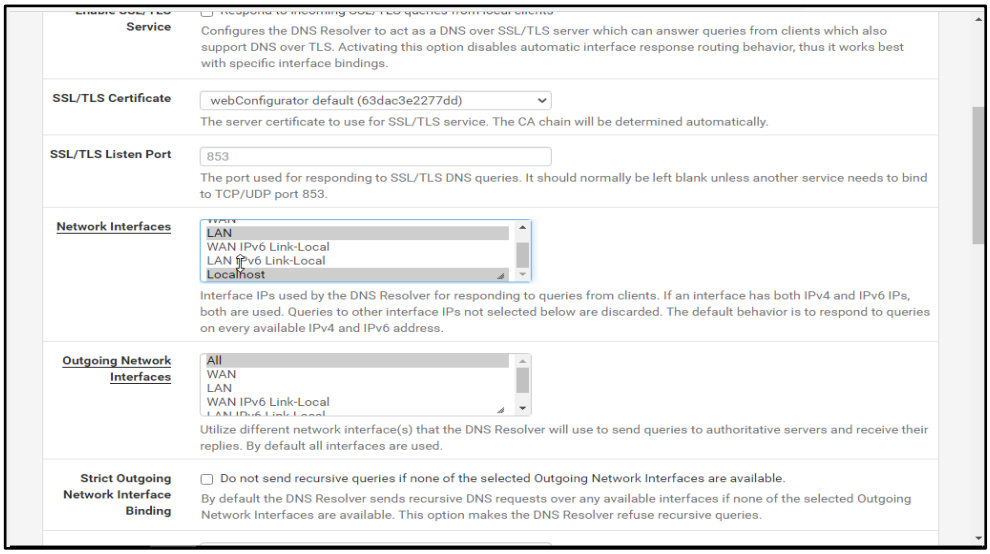


Figura 44. Configuración de la pestaña Services de Pfsense por: Autor

Además, en la opción de “Outgoing Network Interfaces”, es importante tener en cuenta que solo debemos seleccionar la interfaz WAN si es que queremos acceder a internet. Esto se debe a que la WAN es la interfaz que está conectada a internet y es la que nos permitirá acceder a la red global.

Es fundamental tener en cuenta que configurar correctamente la opción para que nuestra conexión a internet sea estable y funcione correctamente. Por lo tanto, asegurarse de seleccionar solo la WAN y no ninguna otra interfaz que pueda causar problemas en nuestra conexión a internet.

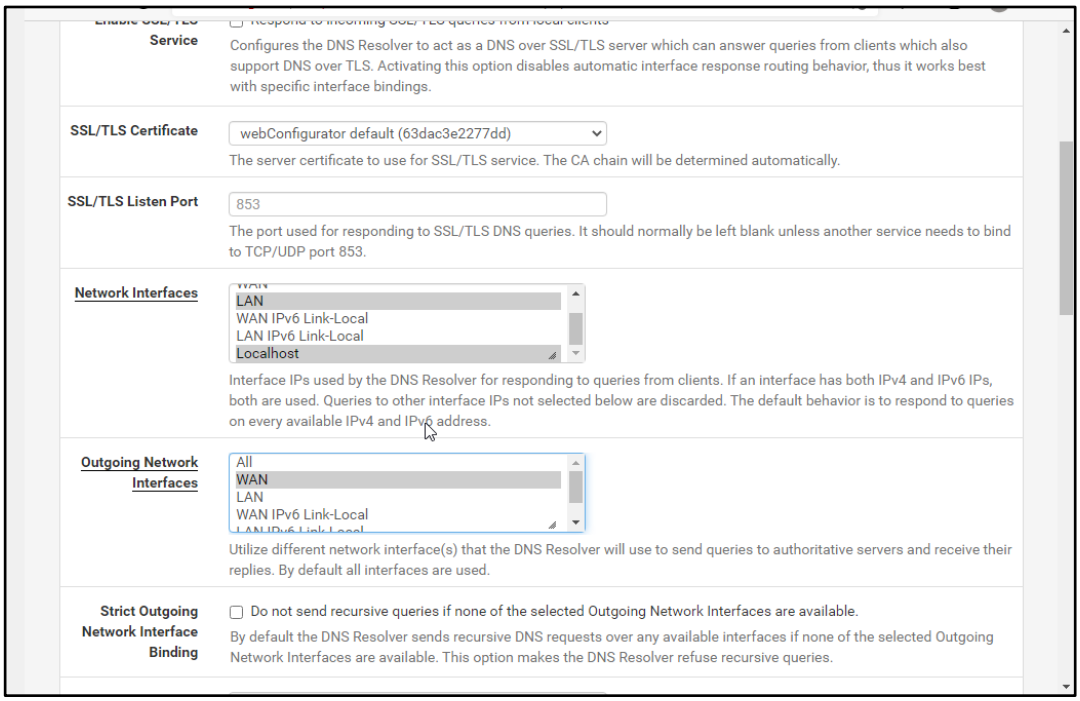


Figura 45. Configuración de Outgoing network interfaces de la pestaña de Services de Pfsense por: Autor

Nos dirigimos a la pestaña de System y dentro de ella seleccionamos la opción de “Packages Manager”. Esta opción nos permite acceder a los paquetes disponibles que podemos instalar en nuestro servidor Pfsense. Dentro de esta sección, podemos ver una lista de todos los paquetes disponibles, ordenados por categorías, para que podamos encontrar fácilmente aquellos que necesitemos.

Además, también podemos utilizar la barra de búsqueda situada en la parte superior de la página para buscar paquetes concretos. Al seleccionar un paquete de la lista, podemos ver más información acerca de él, incluyendo una descripción detallada, las

funcionalidades que ofrece y las versiones disponibles. De esta manera, podemos elegir con precisión los paquetes que necesitamos para mejorar la funcionalidad de nuestro servidor y adaptarlo a nuestras necesidades.

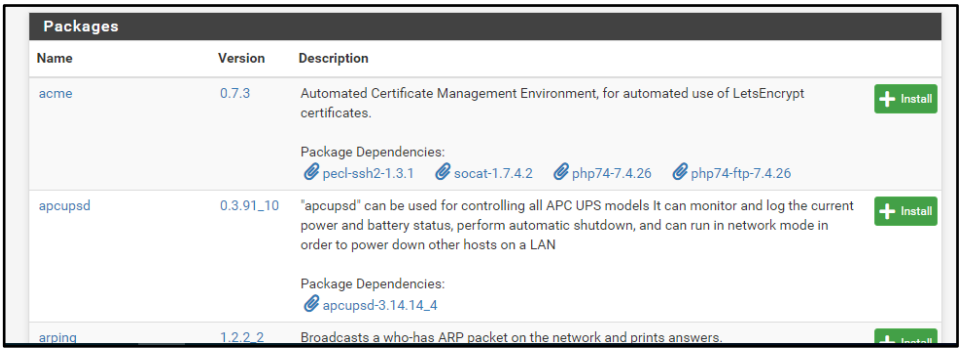


Figura 46. Vista general de la pestaña Packages de Pfsense por: Autor

Luego de seguir los pasos necesarios para instalar los paquetes Squid y SquidGuard, es importante comprobar que la instalación se haya realizado con éxito. Para hacer esto, debemos dirigirnos a la sección de System en el menú de Pfsense, y luego a la opción de Packages Manager. Una vez dentro de esta sección, debemos seleccionar la opción de Installed Packages. Si todo ha salido bien, en esta página deberíamos poder ver la lista de paquetes instalados. Esto nos asegurará de que todo este proceso ha sido un éxito y están funcionando de manera eficiente, permitiéndonos disfrutar de sus características y funcionalidades.

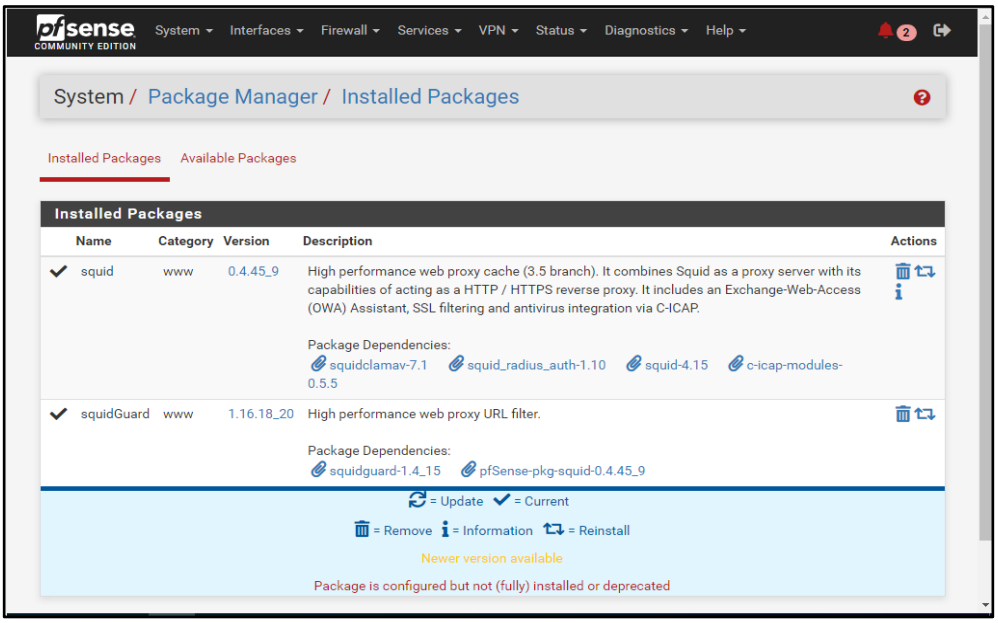


Figura 47. Squid & SquidGuard instalados en Pfsense por: Autor

Además, también es posible configurar otras opciones avanzadas en el Squid Proxy, como la autenticación de usuarios, restricciones de acceso basadas en direcciones IP y puertos, y reglas de filtrado basadas en URL. Para asegurarse de que todo esté funcionando correctamente, es importante hacer pruebas regulares y monitorear el registro de actividad para detectar cualquier problema o incidencia.

La habilitación de estas opciones en este apartado es crucial para la configuración de seguridad y accesibilidad en la red, y es fundamental para garantizar una conexión a Internet segura y estable para todos los usuarios en la red.

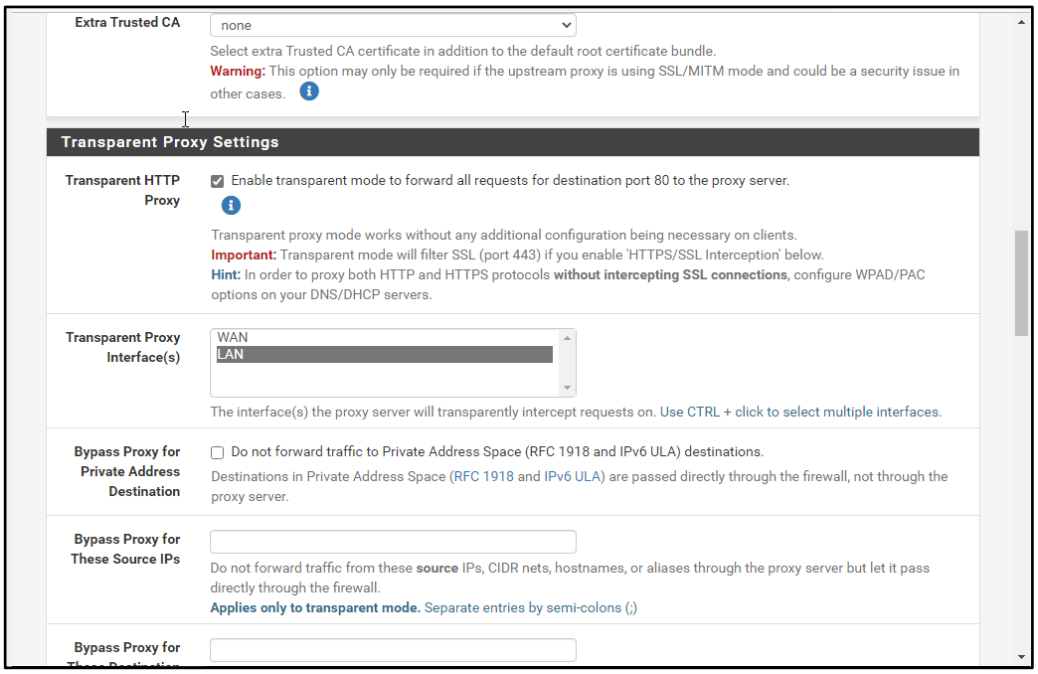


Figura 48. Configuración de Squid Proxy de Pfsense por: Autor

También, en la sección de diagnósticos, podemos verificar el estado del proxy Squid a través de la opción de sockets. Aquí podemos ver todos los detalles relevantes sobre la escucha de paquetes por parte de Squid, incluyendo el número de conexiones activas, la dirección IP y el puerto utilizado, y mucho más.

Esta información es muy útil para revisar si este apartado está funcionando de manera efectiva y para solucionar problemas en caso de ser necesario. Además, podemos verificar que los cambios realizados en la configuración de Squid se reflejan correctamente en la sección de sockets, lo que nos asegura de que estamos utilizando el proxy de manera adecuada.

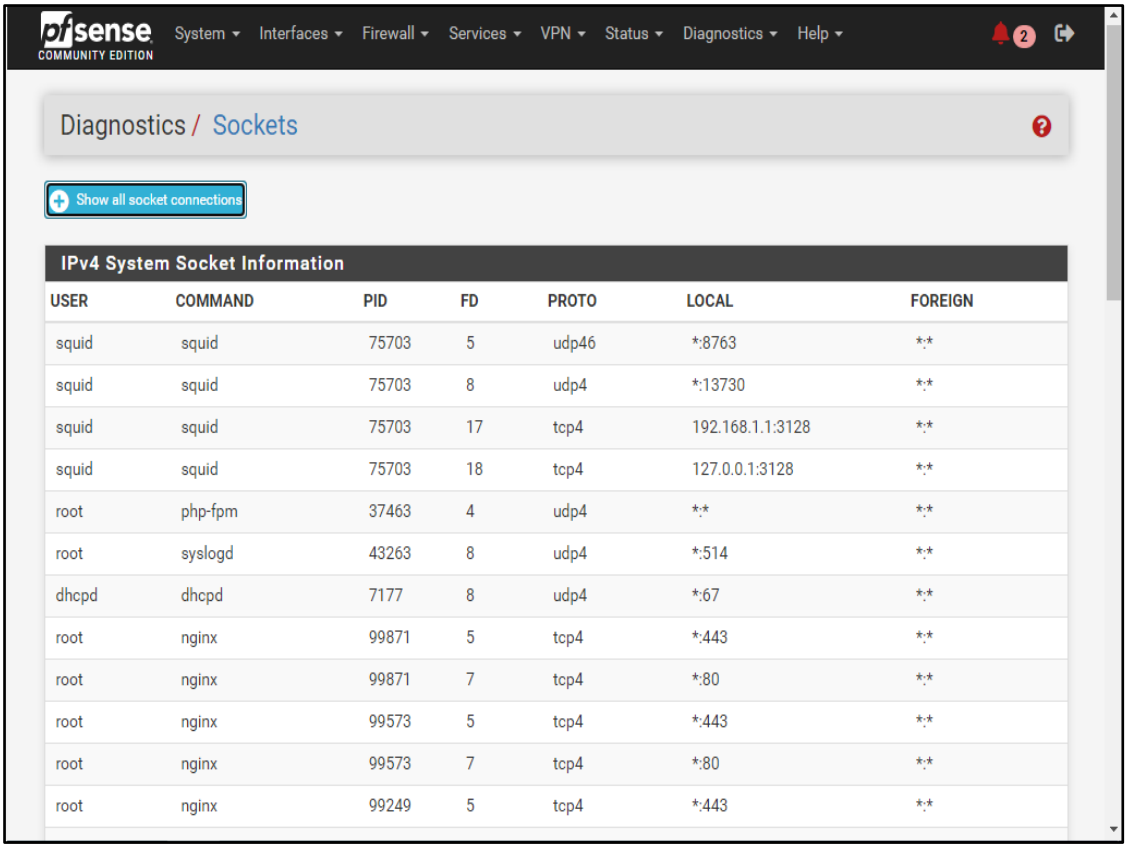


Figura 49. Vista general de pestaña Diagnostics de Pfsense por: Autor

Ahora vamos a desviar los paquetes HTTP hacia el proxy, esto lo hacemos creando una nueva regla en el firewall en la opción de NAT, Para hacer esto, debemos seguir un proceso detallado y específico. Primero, debemos seleccionar la opción de "New" para crear una nueva regla, y luego debemos elegir la opción de "Outbound" para indicar que estamos creando una regla de salida.

Una vez que hemos especificado estos detalles, debemos seleccionar la interfaz de red a la que se aplicará la regla, en este caso, sería la interfaz LAN. Además, debemos especificar la dirección IP del servidor proxy. Finalmente, debemos guardar los cambios y asegurarnos de que la nueva regla se encuentra activa.

Después de seguir estos pasos, los paquetes HTTP de nuestra red LAN serán desviados hacia el proxy Squid, permitiéndonos realizar un control detallado de los paquetes que entran y salen de nuestra red, así como también mejorar la seguridad y la eficiencia de nuestra conexión a Internet.

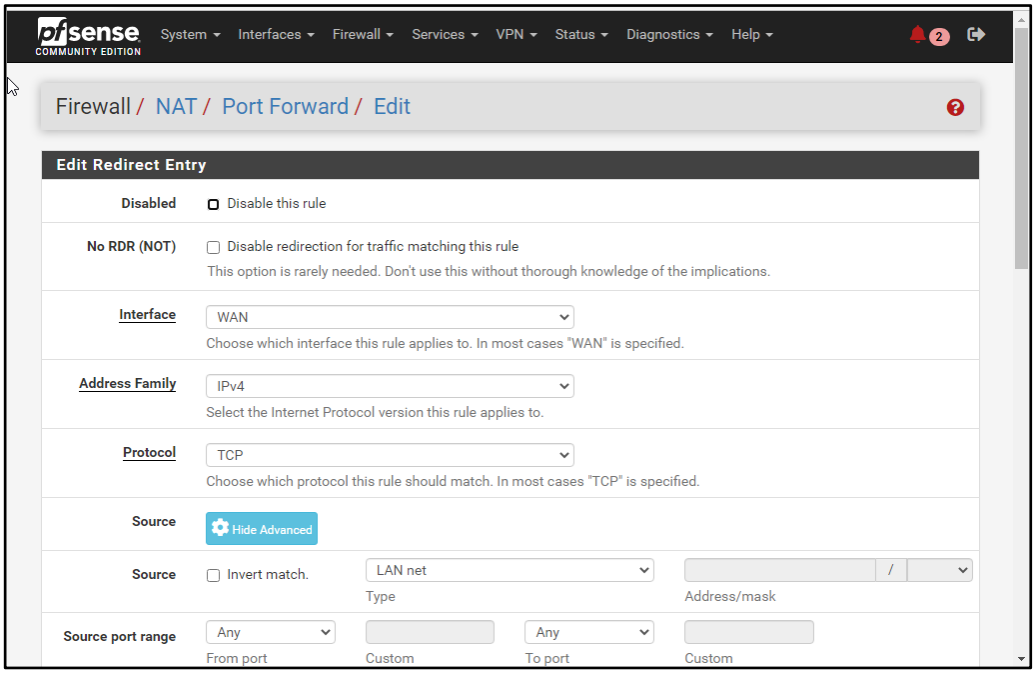


Figura 50. Creación de una regla en la NAT de Pfsense por: Autor

Ahora vamos a Firewall en la opción de rules y luego en LAN y crearemos una nueva regla, de esta manera, una vez configurado guardamos cambios. Una vez hecho esto ahora si vamos a configurar el SquidGuard, en donde ingresamos a Services en la opción de Proxy Filter SquidGuard general Setting. En esta sección, encontraremos la opción de General Setting, donde podremos activar el servicio de manera sencilla y efectiva.

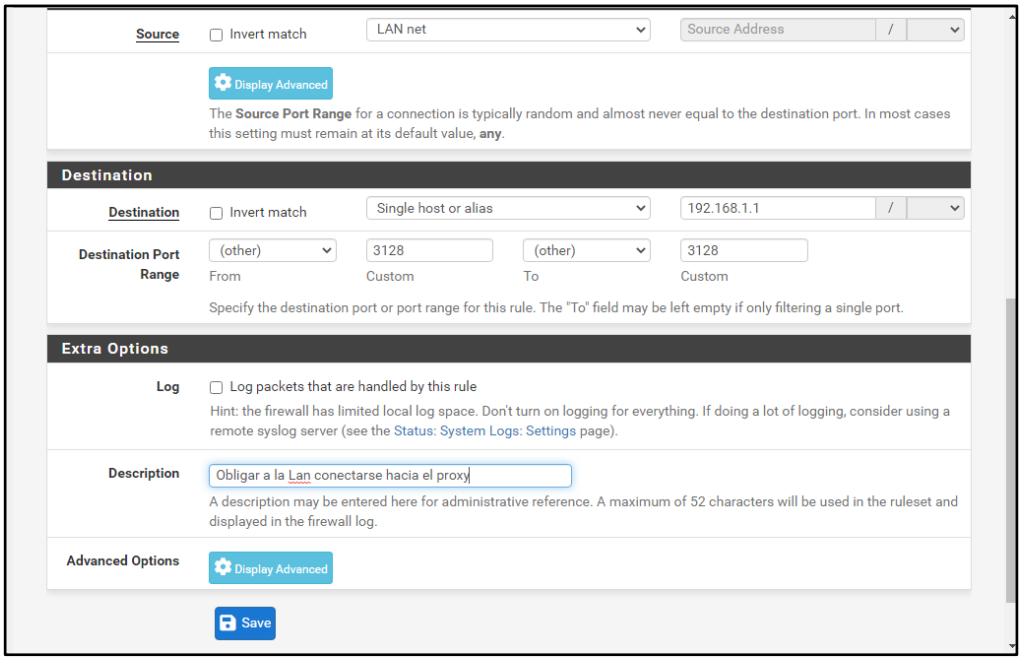


Figura 51. Creación de una regla en la LAN de Pfsense por: Autor

Una vez que hemos agregado la URL correspondiente, nos dirigimos a la opción de "Blacklist" dentro del servicio de SquidGuard. Al dar clic en "Download", el proceso de descarga comenzará y una vez finalizado, podremos verificar que se ha actualizado correctamente la lista negra.

Es importante tener en cuenta que esta lista es crucial para el filtrado de contenido inapropiado o malintencionado, por lo que es necesario asegurarse de que esté actualizada regularmente.

Además, al finalizar la descarga, se mostrará un mensaje indicando el estado de la misma, para que podamos estar seguros de que todo ha ido bien.

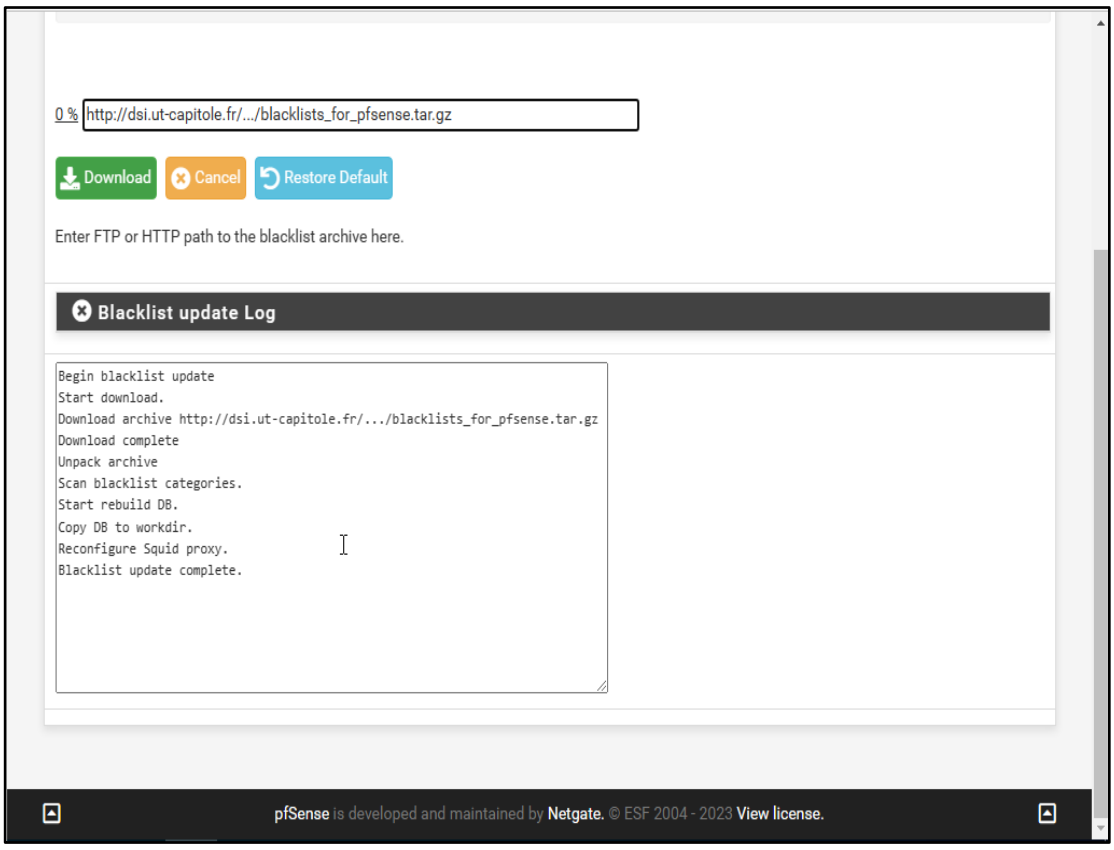


Figura 52. Configuración de Blacklist de Pfsense por: Autor

Ahora que hemos descargado la lista de direcciones web restringidas, podemos continuar con la configuración de SquidGuard. En la pestaña de “Grups ACL”, podemos crear un nuevo grupo para controlar el acceso a diferentes categorías de sitios web.

Es importante tener en cuenta que debemos ser específicos y selectivos con las categorías que permitimos o restringimos para mantener un equilibrio entre la seguridad y la funcionalidad. Al crear un nuevo grupo, es posible asignarle un nombre que refleje su objetivo, por ejemplo "Grupo para restringir sitios web inapropiados".

Una vez generado el grupo, podemos agregar las direcciones web que deseamos bloquear a través de la pestaña de “Blacklist” y asegurarnos de que el grupo esté asociado a las reglas adecuadas en la pestaña de Firewall en la opción de “Rules”. De esta manera, podemos asegurarnos de que el acceso a estas direcciones web esté restringido para los usuarios de nuestra red.

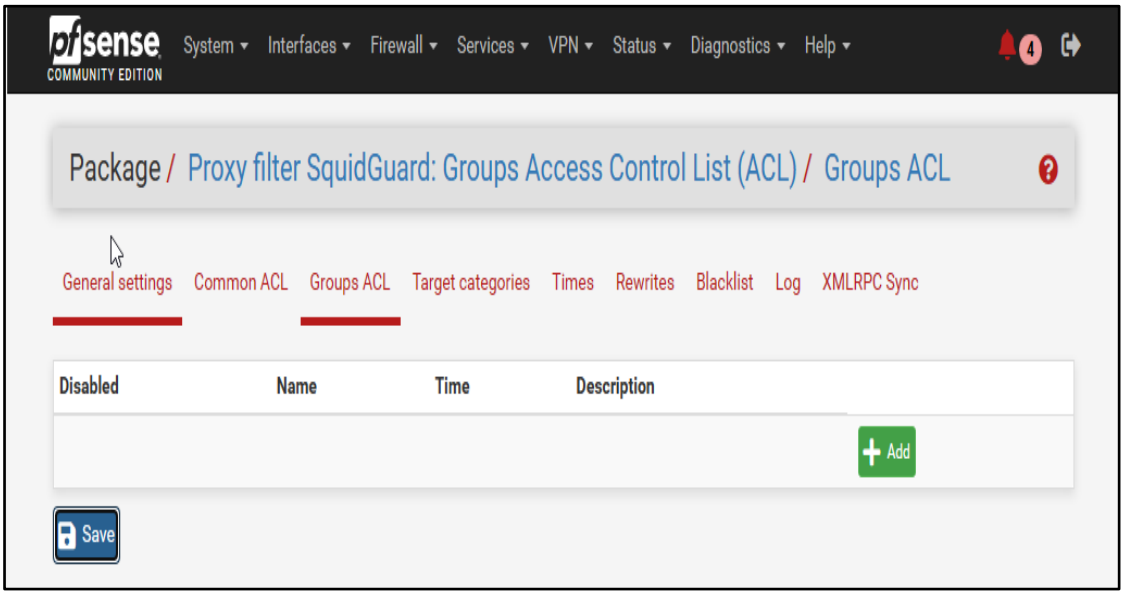


Figura 53. Creación de un nuevo grupo ACL en Pfsense por: Autor

Luego de completar todas las configuraciones y ajustes necesarios en Pfsense, podemos revisar el resultado final en el Dashboard. En este panel central podremos ver todas las opciones y estados actuales de los servicios y configuraciones que hemos realizado.

Además, en este apartado también nos brinda la capacidad de realizar cambios y ajustes adicionales, dependiendo de las necesidades de nuestra red y de las demandas de los usuarios.

Por lo tanto, es una herramienta esencial para mantener una red segura y eficiente, y para garantizar que todos los servicios y aplicaciones estén funcionando correctamente.

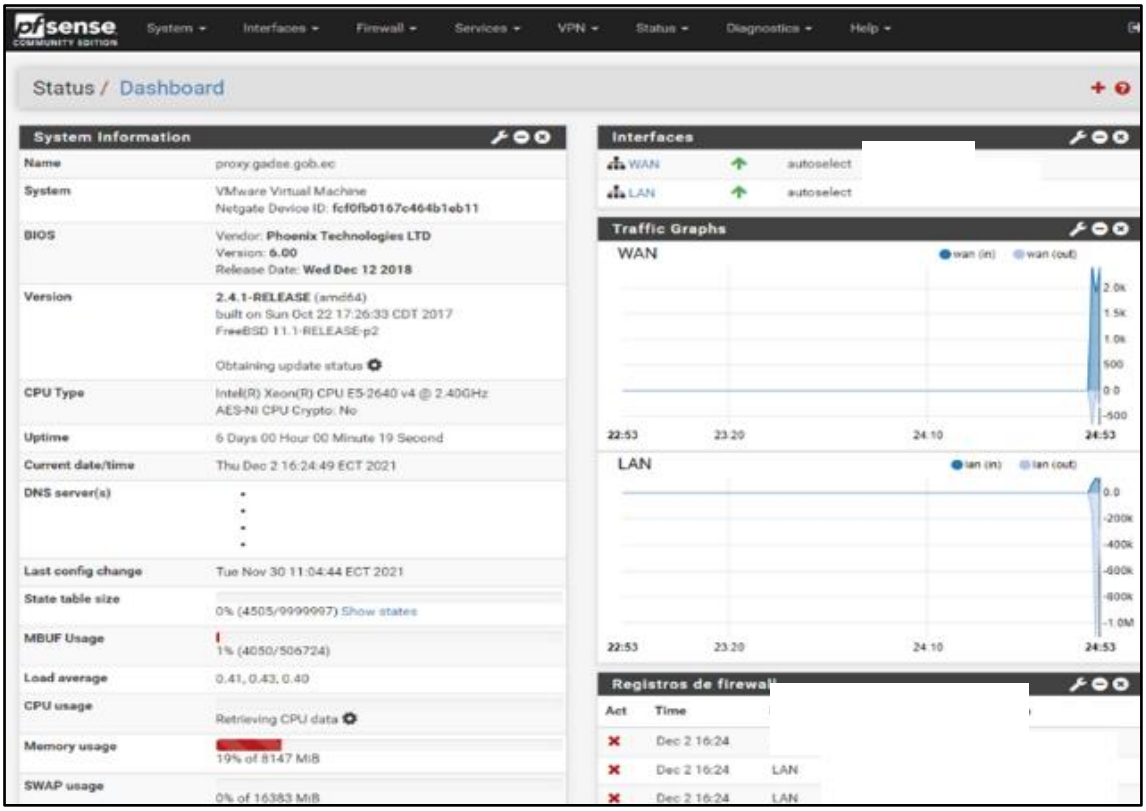


Figura 54. Vista general del Dashboard con todas las configuraciones realizadas en Pfsense por: Autor

En el firewall podemos bloquear diferentes categorías de sitios web, como, por ejemplo:

- Sitios web para adultos: para proteger a los usuarios más jóvenes o a los que no desean ver contenido explícito.
- Sitios de descarga de torrents y archivos: para evitar descargas ilegales y mejorar la velocidad de la red.
- Sitios de apuestas y juegos en línea: para prevenir adicción y mal uso del tiempo y recursos.
- Sitios de phishing y malware: para proteger la seguridad y privacidad de los usuarios.
- Sitios sociales: para reducir la distracción y mejorar la productividad en el trabajo o en el aula.

Estas son solo algunas de las categorías de sitios web que podemos bloquear en el firewall, dependiendo de las necesidades y preferencias de cada usuario o empresa. Con

un cortafuegos efectivo, podemos mejorar la seguridad y eficiencia de la red, así como proteger a los usuarios de contenido no deseado o perjudicial.

Estas categorías pueden incluir desde sitios web inapropiados, como contenido para adultos o violencia, hasta sitios que pueden contener software malicioso o phishing. Tener en cuenta que algunas de estas pueden ser subcategorías de otras, por lo que es importante revisarlos antes de bloquearlos.

Estas están diseñadas para proteger la seguridad y privacidad de los usuarios, por lo que es imprescindible ser cuidadoso al seleccionar las categorías que se van a bloquear en el firewall.

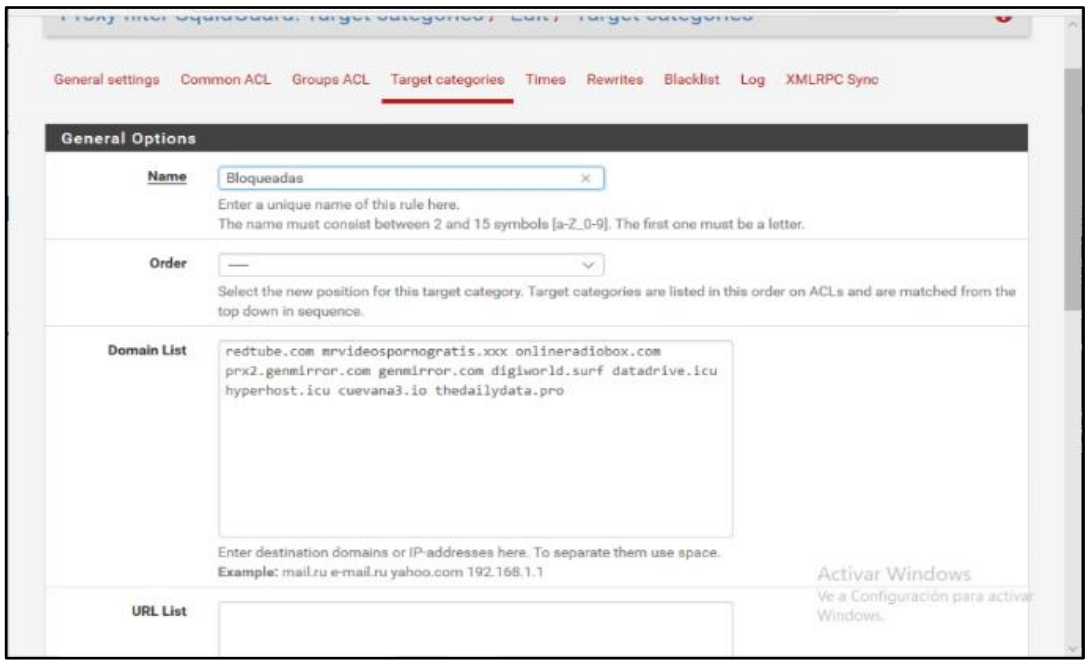


Figura 55. Categoría Bloqueadas de Pfsense por: Autor

A continuación, se presentan las distintas categorías que se han creado en el firewall para controlar y restringir el acceso a ciertos sitios web. Estas incluyen desde sitios inapropiados hasta sitios que pueden ser perjudiciales para la seguridad de la red, y son una forma efectiva de proteger a los usuarios y mantener una navegación segura en Internet.

Además, es posible agregar o quitar categorías según las necesidades y preferencias de cada usuario, lo que hace que sea una herramienta altamente personalizable y adaptable a las diferentes situaciones.

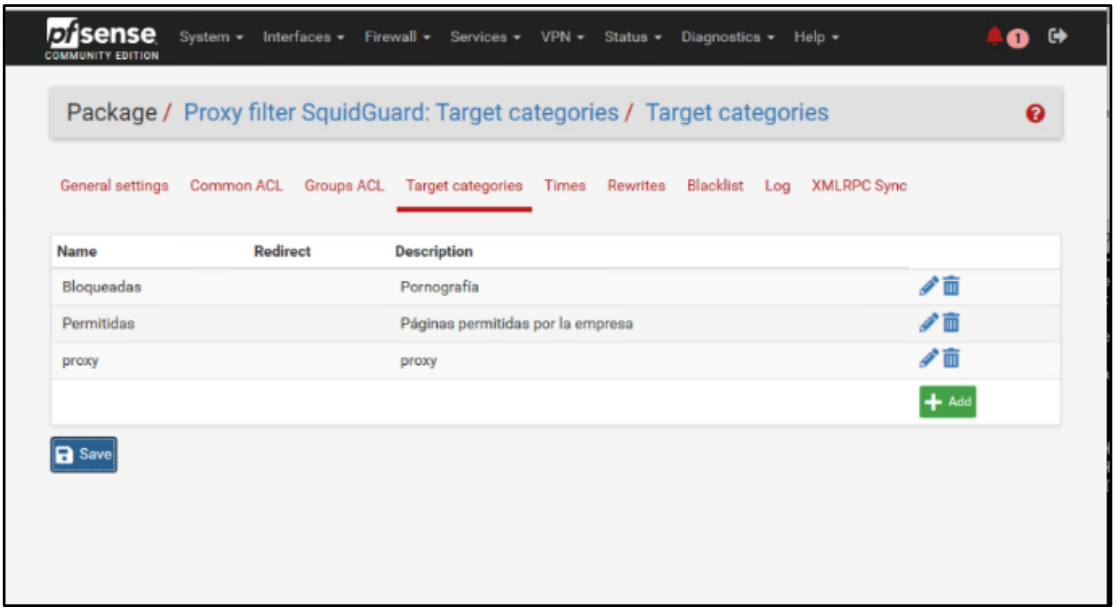


Figura 56. Categorías creadas en Pfsense por: Autor

Aquí se puede ver una lista detallada de todas las categorías de sitios que se han bloqueado en el firewall, incluyendo información sobre el nombre, el número de sitios bloqueados, y una descripción detallada de los sitios incluidos en cada grupo.

También se pueden realizar ajustes en las categorías bloqueadas, permitiendo la adición o eliminación de sitios específicos de la lista de bloqueo. De esta manera, se puede personalizar y controlar con precisión qué tipo de contenido se permite o no en la red.

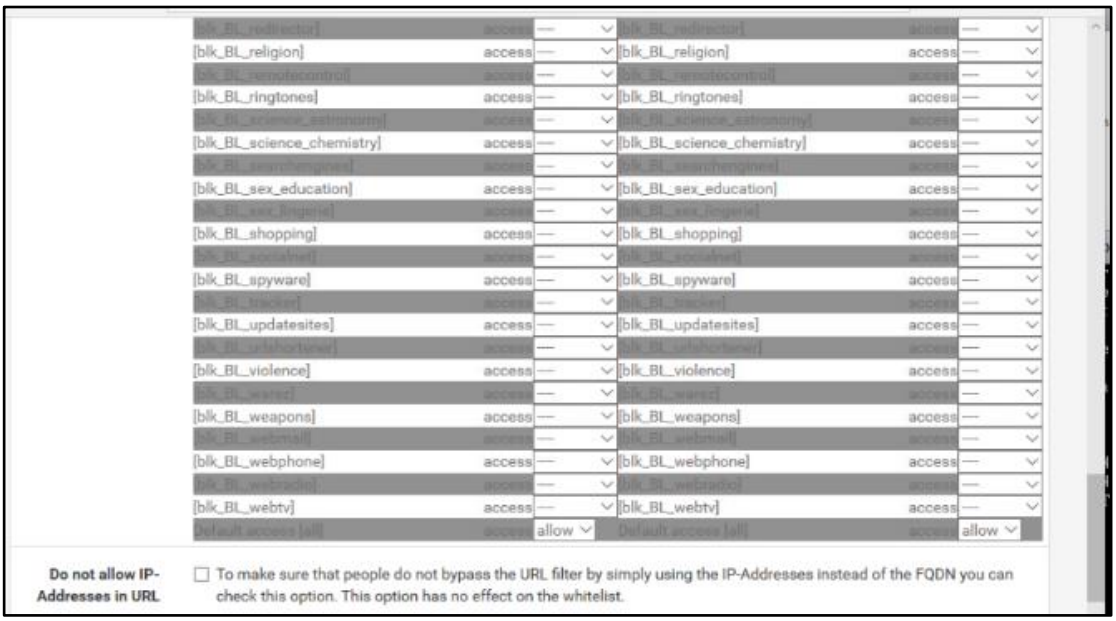


Figura 57. Lista de bloqueos implementados en el firewall de Pfsense por: Autor

Aquí se puede ver un registro detallado de los eventos y actividades que han ocurrido en el firewall. Esto incluye información sobre las conexiones permitidas y las conexiones bloqueadas, así como información sobre las reglas y configuraciones implementadas en el firewall. Además, los logs también pueden mostrar detalles sobre posibles intentos de ataques y otras amenazas a la seguridad de la red.

Esta información es muy valiosa para monitorear y detectar cualquier posible amenaza a la seguridad de la red, y para tomar medidas para corregir cualquier problema. Por lo tanto, es importante revisar los logs de registros del firewall con regularidad para mantener una seguridad óptima.

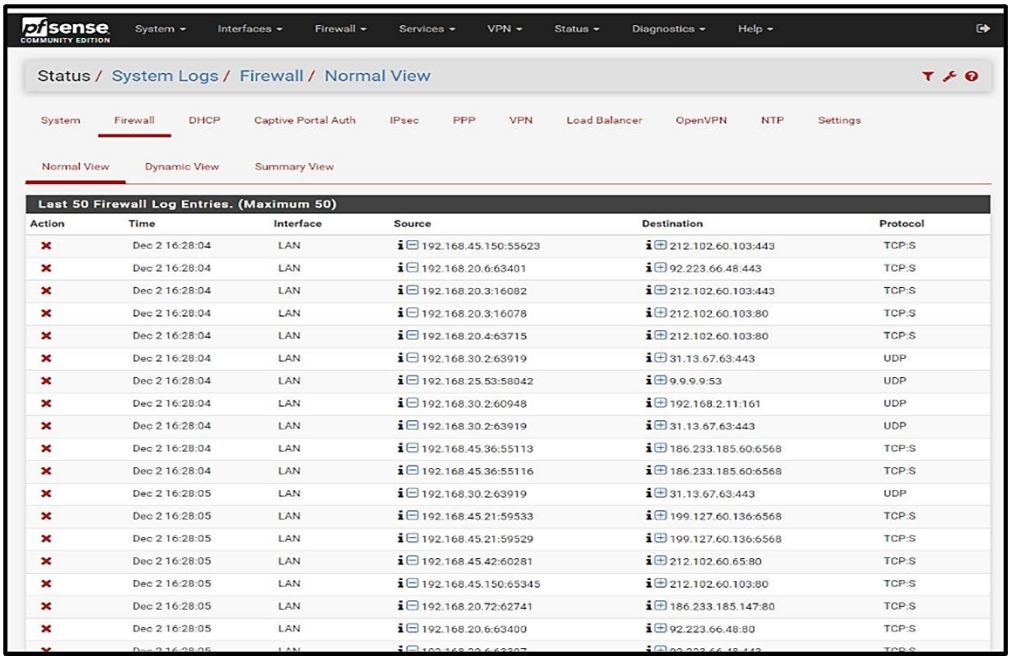


Figura 58. Logs de registros del firewall de Pfsense por: Autor

Aquí se pueden ver todas las ACL's generales que se han implementado en el firewall en el apartado específico de Common ACL. Esta sección permite verificar y modificar las reglas establecidas para el acceso a internet, permitiendo una gestión más eficiente y controlada de los recursos y la seguridad de la red. Al visualizar este apartado, se pueden ver detalladamente las configuraciones y reglas establecidas, y realizar cambios en caso de ser necesario para ajustarlas a las necesidades actuales de la red.

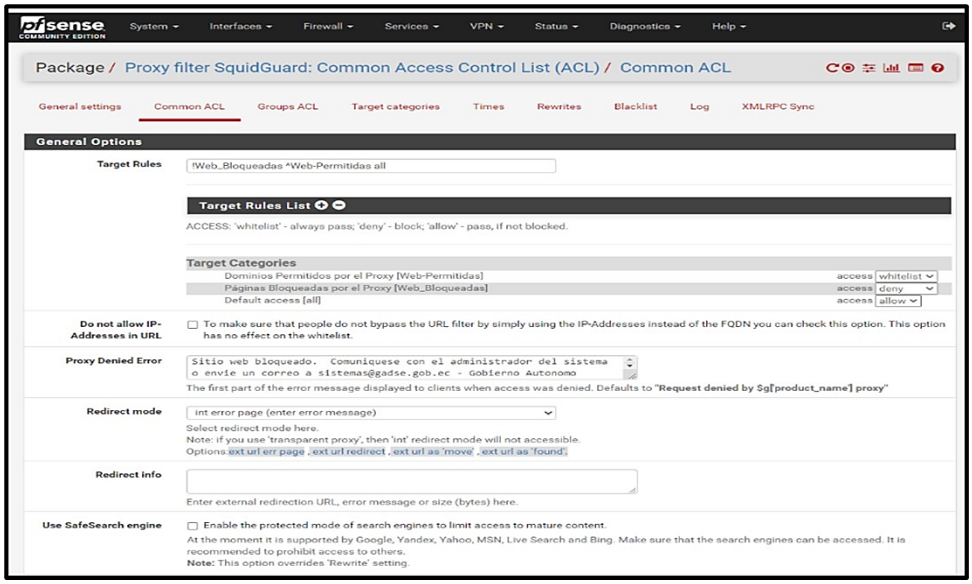


Figura 59. Configuración de Common ACL de Pfsense por: Autor

Aquí se muestran las categorías de destino específicas en las que se encuentran los dominios no permitidos. Estas incluyen, por ejemplo, contenido para adultos, juegos en línea, software malicioso, entre otros. De esta manera, se puede tener un control detallado de los sitios web que están restringidos y las razones por las que se han bloqueado. Además, esta información es útil para hacer ajustes y agregar o eliminar categorías según sea necesario.

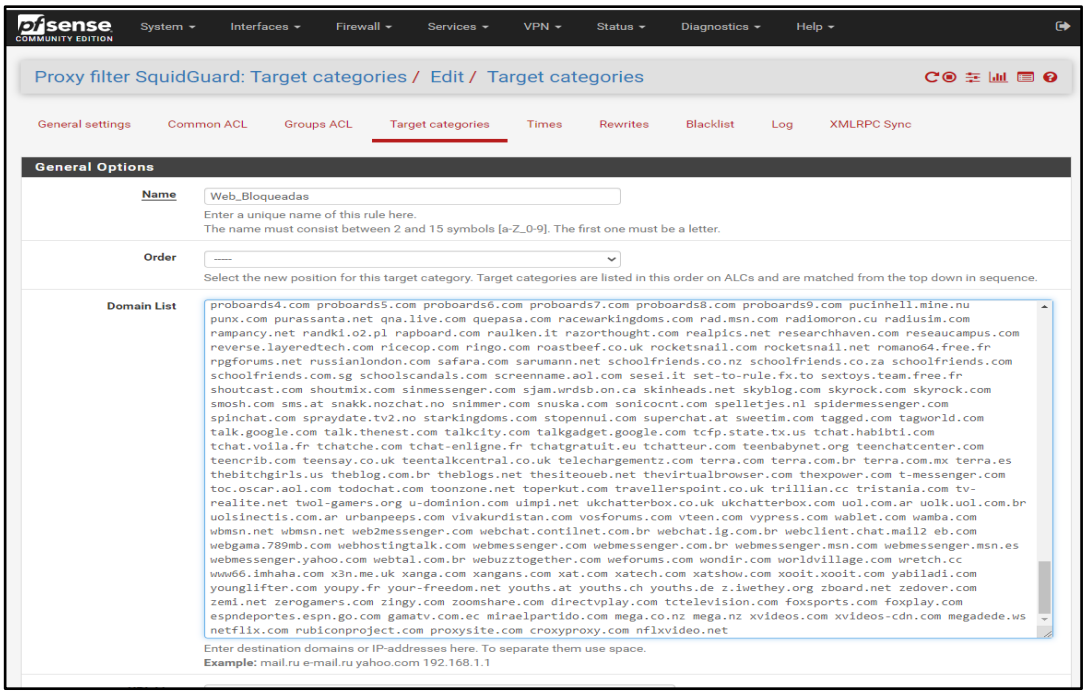


Figura 60. Listas de dominios no permitidos en Pfsense por: Autor

En esta sección, se presentan las listas de los dominios que han sido permitidos en el apartado de categorías objetivo. Estas son importantes ya que definen qué sitios web están autorizados para ser accedidos y utilizados por los usuarios en la red.

Por lo tanto, es importante revisar y mantener actualizadas estas listas para garantizar una experiencia segura y controlada para los usuarios de la red. Esta funcionalidad es crucial para mantener un control adecuado y evitar accesos no deseados o potencialmente peligrosos.

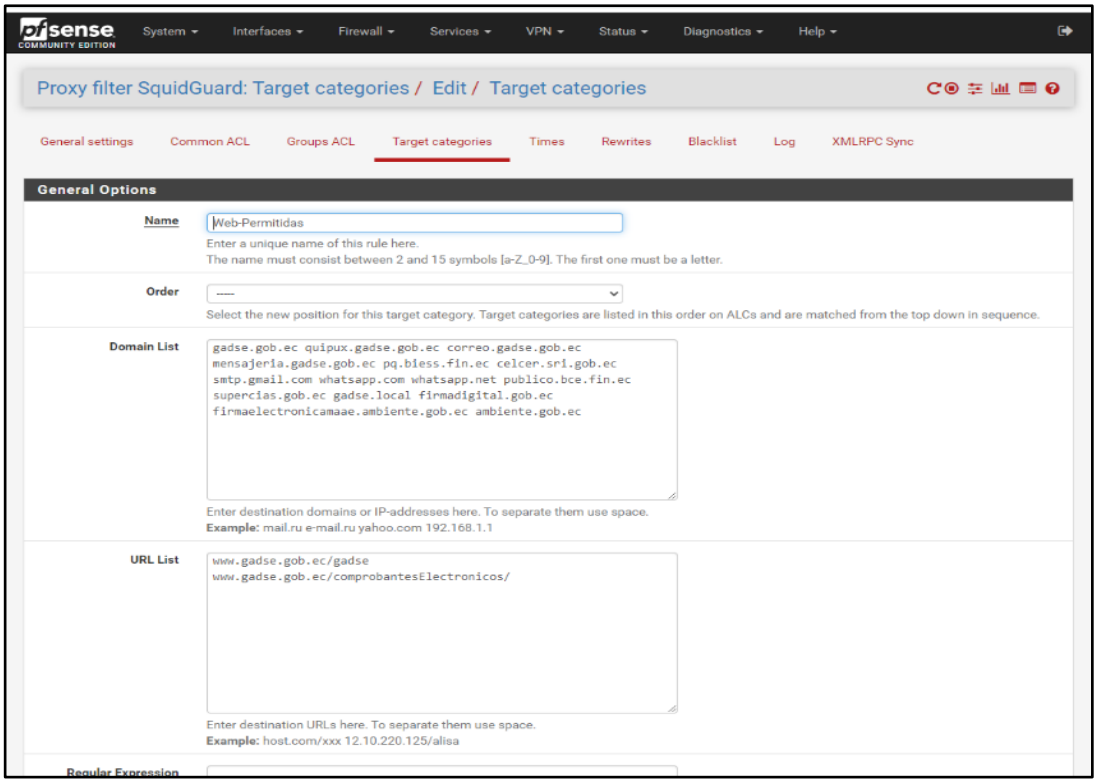


Figura 61. Listas de dominios permitidos en Pfsense por: Autor

Aquí se puede visualizar la lista de equipos que no tienen ninguna restricción en el apartado de Grupos ACL. Estos equipos tienen acceso ilimitado a todos los sitios web y aplicaciones en Internet, sin ningún tipo de filtro o bloqueo.

Es relevante destacar que este acceso sin restricciones solo debería ser otorgado a equipos de confianza, como aquellos utilizados por personal autorizado, debido a la posibilidad de exponer la red a posibles riesgos de seguridad. Es recomendable que se utilice el apartado para establecer políticas de acceso más estrictas y controlar los accesos a Internet en la red.

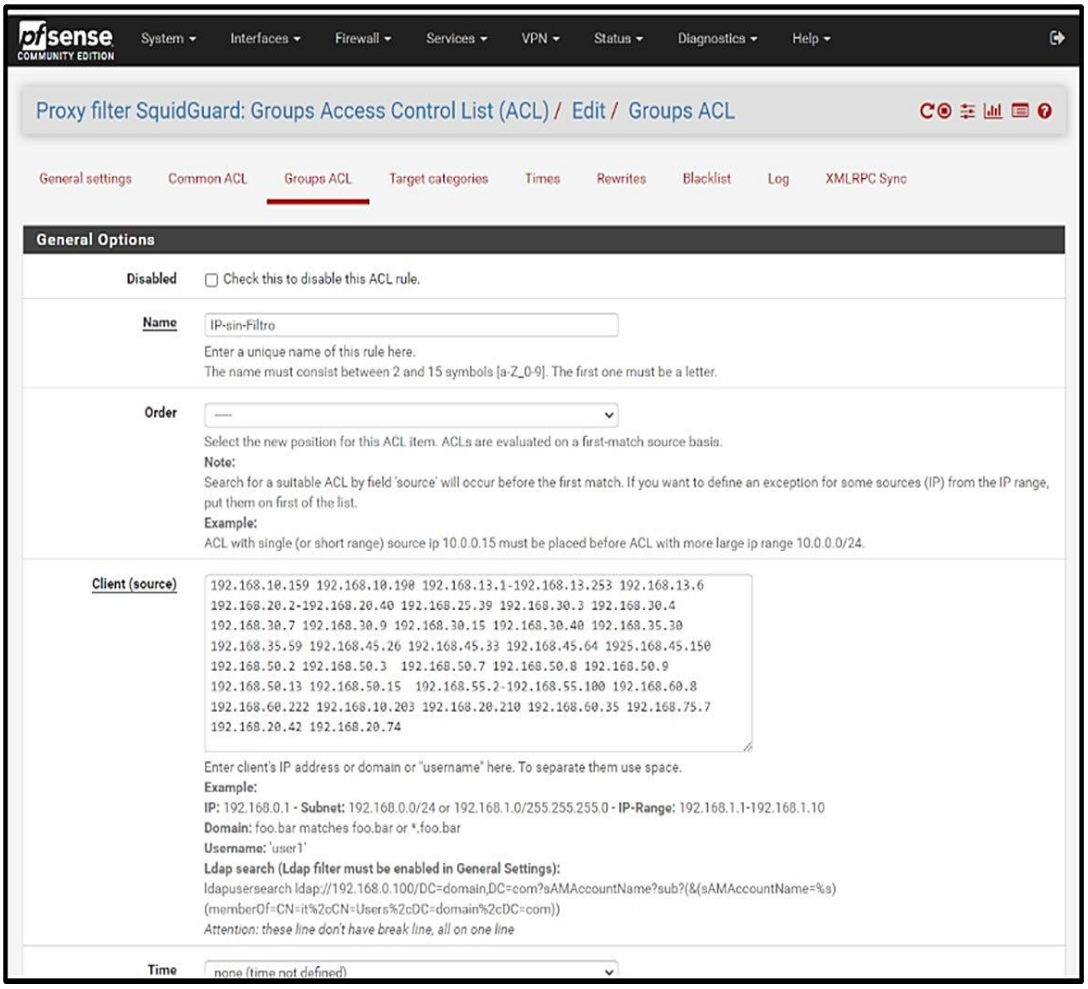


Figura 62. Lista de equipos sin restricciones en Pfsense por: Autor

Aquí se muestran las reglas de firewall configuradas en la sección LAN. Estas reglas establecen las políticas de seguridad de la red y determinan qué tráfico es permitido y cuál es bloqueado. Se puede ver una lista detallada de las reglas implementadas en la LAN y sus ajustes, incluyendo la dirección IP origen y destino, puertos y protocolos, y acción (permitir o bloquear).

Estas reglas se pueden ajustar y modificar según sea necesario para adaptarse a las necesidades de seguridad de la red y a los cambios en el tráfico de la misma. Es importante monitorear regularmente las reglas implementadas en este apartado para asegurarse de que estén funcionando correctamente y de que esta, esté protegida contra posibles amenazas.

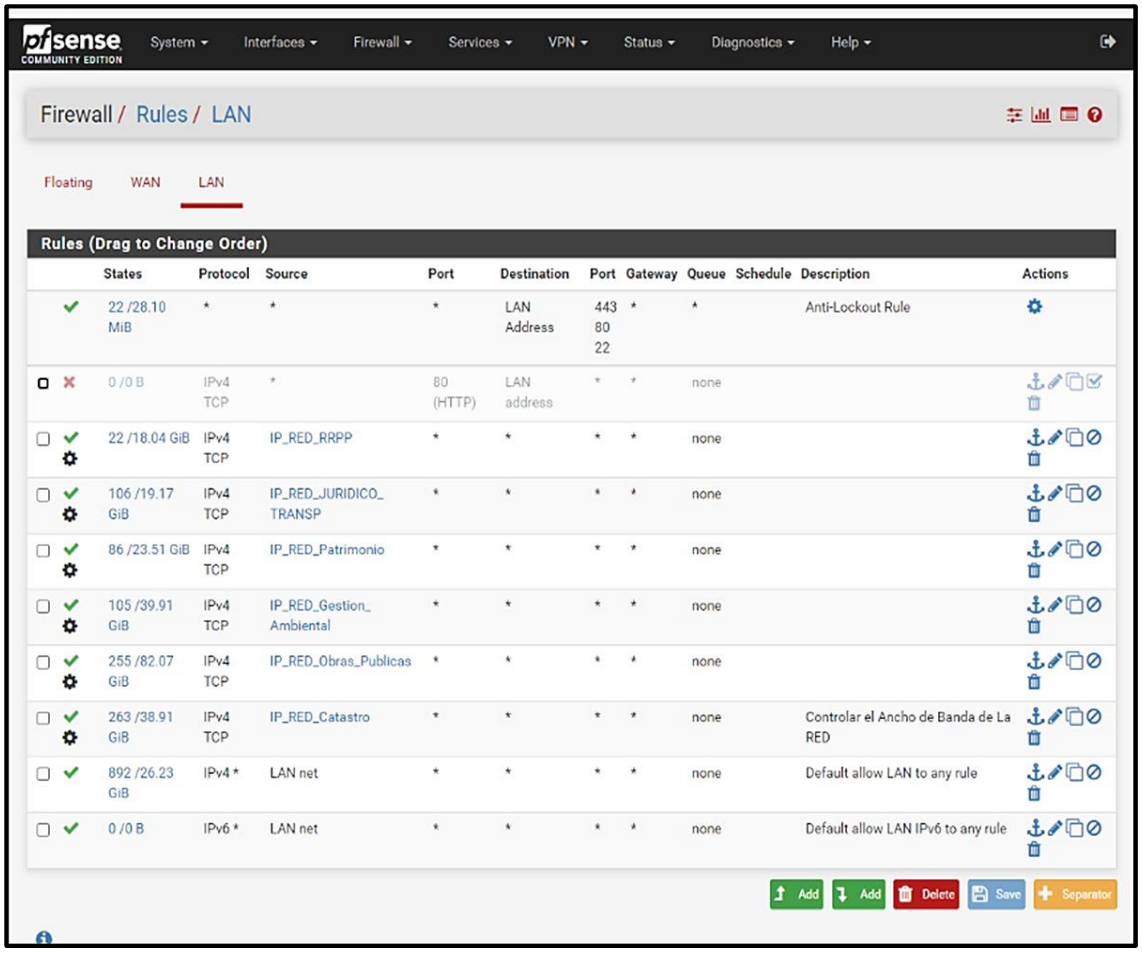


Figura 63. Reglas implementadas en la LAN de Pfsense por: Autor

En este apartado se pueden visualizar y administrar las reglas de firewall que se encuentran configuradas en la sección WAN de Pfsense. Estas reglas son de vital importancia para la seguridad de la red, ya que permiten o bloquean el tráfico de entrada y salida hacia y desde Internet.

Las reglas de firewall se crean para controlar el tráfico de red y proteger los dispositivos y los datos que se encuentran con posibles amenazas externas. En este sentido, es una herramienta fundamental para garantizar la seguridad de la red y evitar que los ciberdelincuentes puedan acceder a información confidencial o dañar los sistemas.

Entre las reglas más importantes que se pueden configurar en la sección WAN de Pfsense se encuentran la restricción de acceso a ciertos puertos, la limitación del tráfico de entrada y salida a direcciones IP específicas, la activación de la detección de intrusos, entre otras opciones.

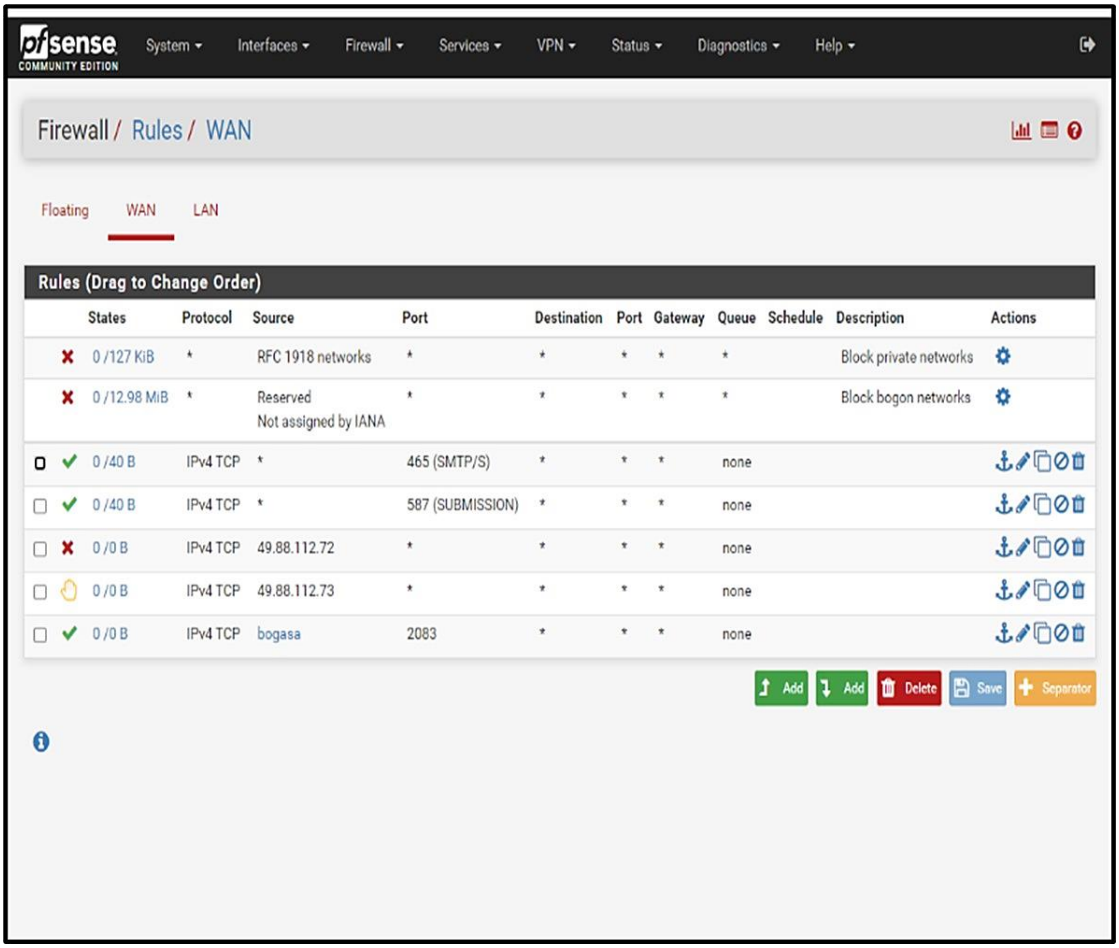


Figura 64. Reglas implementadas en la WAN de Pfsense por: Autor

2.4.7. PRUEBAS

Las páginas con contenido para adultos se encuentran restringidas para todos los departamentos, para esta prueba se está haciendo desde el departamento de sistemas y como se puede apreciar al intentar acceder a estos sitios, se produce una negación, lo que significa que el firewall está bloqueando el acceso a esta página web.

Este tipo de restricciones son importantes para asegurar un ambiente laboral apropiado y para cumplir con los estándares de seguridad de la empresa. Además, se puede personalizar la lista de sitios web restringidos para asegurarse de que no se acceda a contenido no deseado o inapropiado en la red.

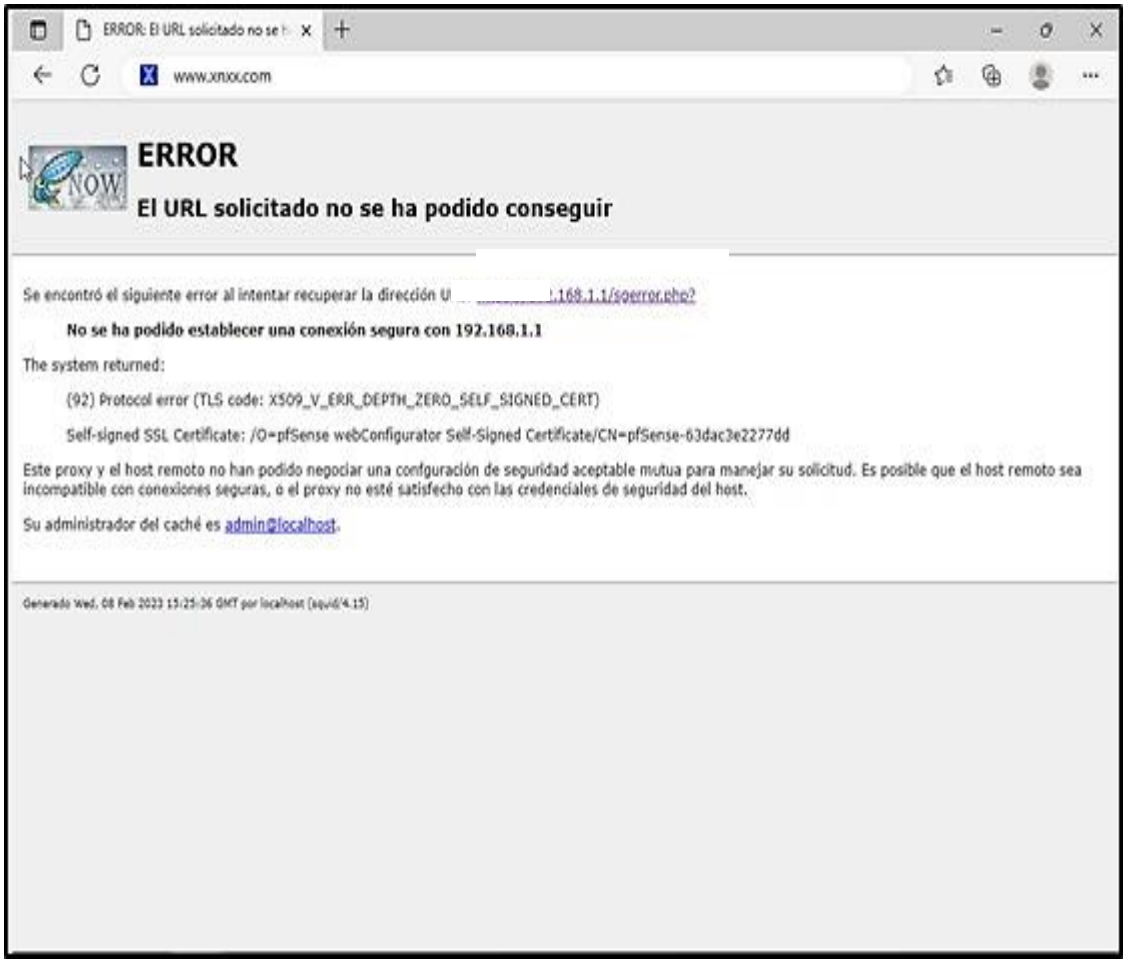


Figura 65. Primer prueba del Firewall Pfsense por: Autor

Ahora tenemos un departamento que no tiene acceso a contenido de multimedia, pero si tiene acceso a los sitios web oficiales de la institución. Para lograr esta restricción, se crearon reglas específicas en el firewall que bloquean el acceso a cualquier sitio web que contenga contenido multimedia como videos, audio, imágenes, etc. Esta medida se implementó para asegurar una navegación más segura y eficiente en el departamento.

Sin embargo, a pesar de esta restricción, los empleados de este departamento todavía tienen acceso a los sitios web oficiales de la institución, ya que estos son necesarios para el desempeño de sus tareas diarias. Por lo tanto, se permite el acceso a estos sitios web mientras se restringe el acceso a todas las demás páginas que contengan contenido multimedia no autorizado.

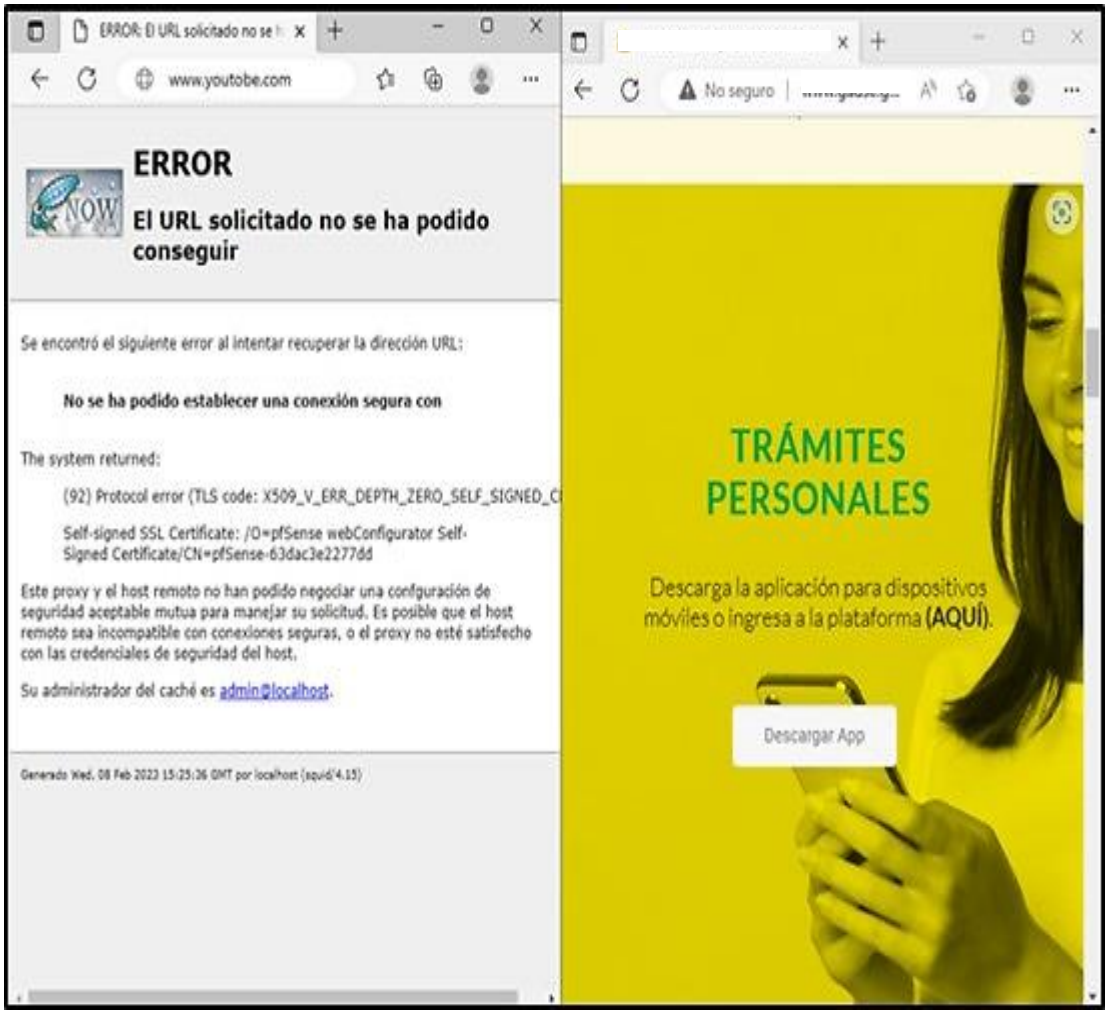


Figura 66. Segunda prueba del Firewall Pfsense por: Autor

También en los departamentos como Logística, desarrollo urbano, etc. Se encuentra restringidos el uso de redes sociales. Este departamento está restringido de acceder a cualquier tipo de red social, incluyendo Facebook, Twitter, Instagram y cualquier otra plataforma que se utilice para fines sociales. Sin embargo, tienen acceso total a los sitios web oficiales de la institución, lo que les permite realizar sus tareas de manera eficiente y sin interrupciones.

La razón detrás de esta restricción es preservar la productividad y evitar la distracción, ya que muchas veces las redes sociales pueden ser una fuente importante de distracción para los empleados. Además, esto también garantiza una mayor seguridad en cuanto a la información confidencial de la institución.

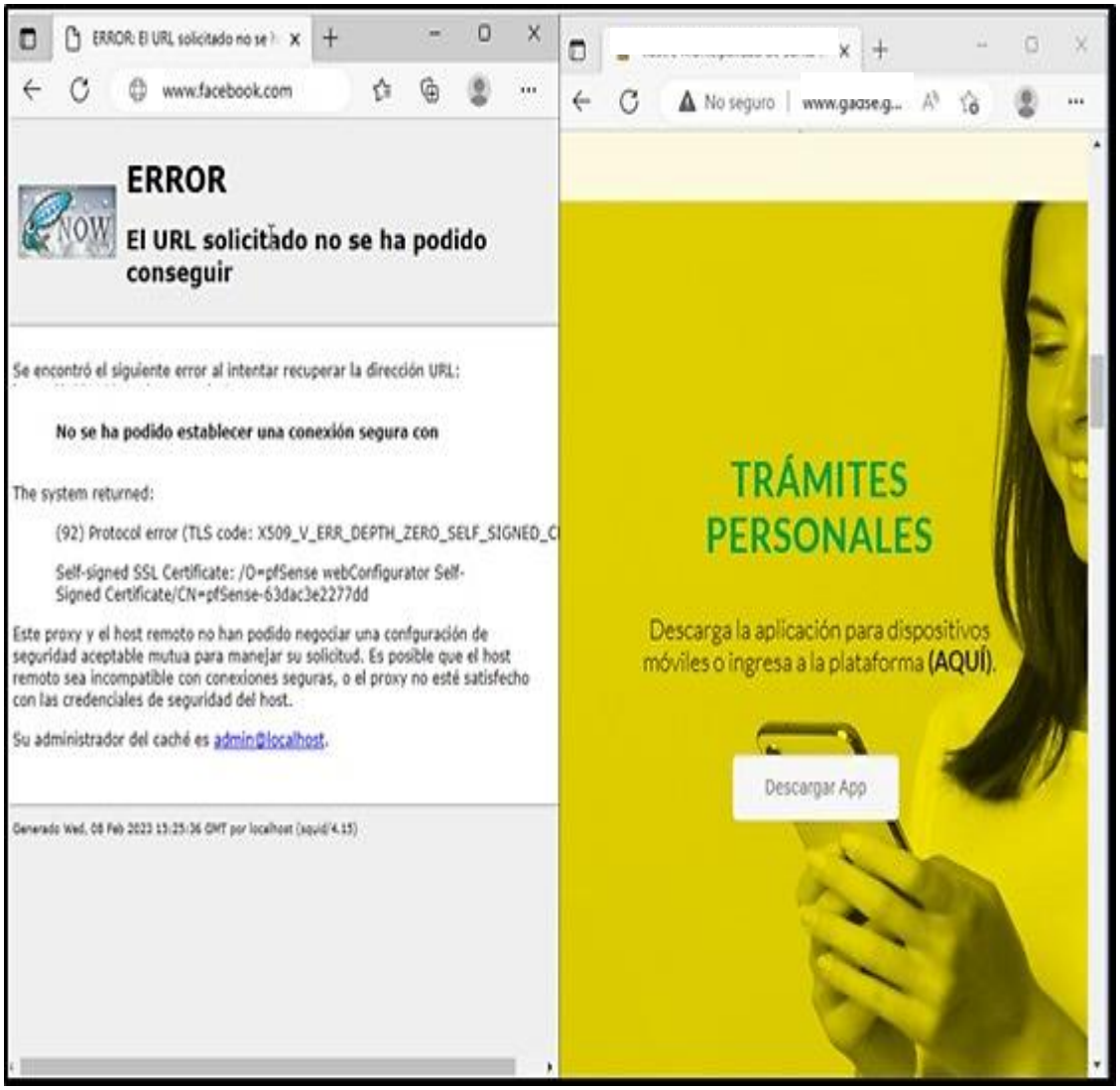


Figura 67. Tercer prueba del Firewall Pfsense por: Autor

Esta IP es una excepción y está destinada para uso exclusivo de la alta gerencia o departamentos críticos de la institución. Este tipo de acceso es necesario para que puedan realizar sus tareas de manera más eficiente y eficaz, sin tener que lidiar con las restricciones que se han implementado en el firewall.

Además, esta dirección IP en cuestión es monitoreada de manera constante para asegurarse de que se está utilizando de manera responsable y adecuada a sus necesidades. En definitiva, los usuarios que no cuentan con restricciones permiten a ciertos departamentos críticos efectuar sus tareas de manera eficiente y eficaz.

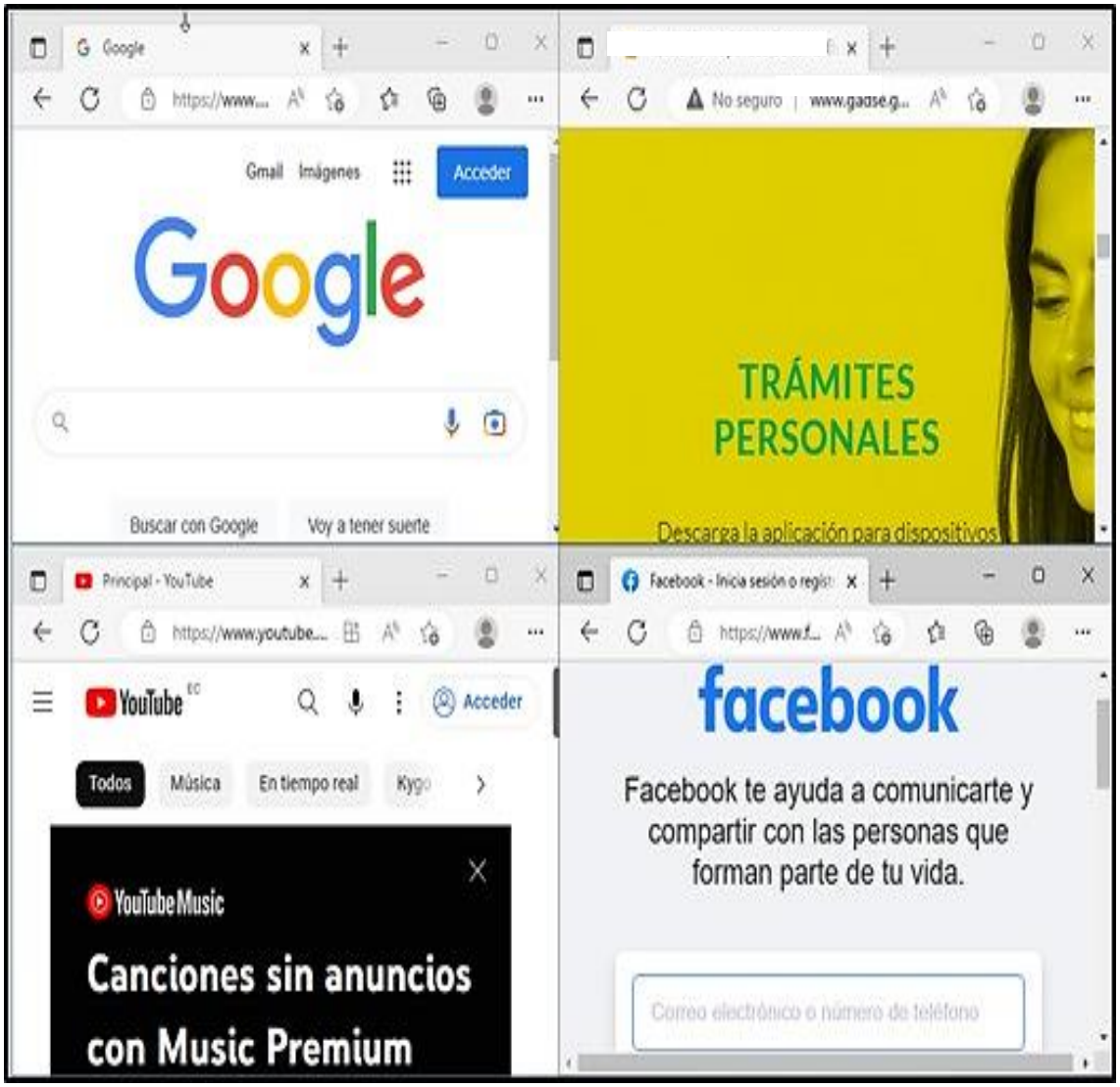


Figura 68. Cuarta prueba del Firewall Pfsense por: Autor

En esta sección se puede apreciar cómo se logra tener una buena conexión a Internet gracias a la configuración adecuada de Pfsense y el ancho de banda asignado. La combinación de estos factores permite optimizar el rendimiento de la red y garantizar una navegación fluida y sin interrupciones.

La configuración de Pfsense es clave para el correcto funcionamiento de la red, ya que permite establecer reglas de firewall, controlar el tráfico del sistema de comunicaciones y administrar los recursos de la misma de manera eficiente. Asimismo, la configuración del ancho de banda es fundamental para asegurar que dichos recursos se utilicen de manera adecuada, evitando que se saturen y se reduzca el rendimiento de la conexión a Internet.

Figura 69. Prueba de ancho de banca con Pfsense por: Autor

En este apartado se puede visualizar cómo, gracias a la configuración adecuada de Pfsense, se ha restringido el acceso a ciertos puertos de la red interna, como el puerto 465 y el puerto 587. Estos puertos son utilizados comúnmente para el envío de correos electrónicos, y su bloqueo puede resultar de gran utilidad para prevenir el envío de correos no autorizados y otros tipos de actividades maliciosas.

La configuración de Pfsense permite establecer reglas de firewall y controlar el tráfico de red de manera precisa, lo que resulta muy útil para restringir el acceso a ciertos puertos y proteger la red interna de posibles amenazas externas. En este sentido, se pueden establecer reglas que permitan el acceso únicamente a los puertos necesarios para el correcto funcionamiento de los servicios y aplicaciones utilizadas en la red.

Figura 70. Prueba de puertos 465 & 587 con Pfsense por: Autor

En esta sección se puede observar que con la configuración adecuada de Pfsense ha permitido restringir el acceso al puerto 22 de la red interna. Este puerto es comúnmente utilizado para la conexión remota mediante el protocolo SSH, lo que lo convierte en un posible punto de entrada para accesos no autorizados y ataques externos.

Es importante tener en cuenta que la configuración de Pfsense no solo permite restringir el acceso a ciertos puertos, sino también controlar el tráfico de red en general. Esto resulta de gran utilidad para garantizar una mayor estabilidad y seguridad en la red interna, especialmente en entornos donde el tráfico de datos es elevado.

Figura 71. Prueba de puerto 22 con Pfsense por: Autor

El filtrado de contenido HTTP y HTTPS es una herramienta muy útil en la configuración de Pfsense. Con esta funcionalidad, es posible restringir el acceso a ciertos sitios web y aplicaciones en línea, lo que puede resultar de gran utilidad en entornos empresariales y educativos, donde se necesita controlar el acceso a ciertos contenidos para garantizar un ambiente de trabajo adecuado y seguro.

En este sentido, este filtrado permite bloquear el acceso a páginas web que puedan contener contenido inapropiado o potencialmente peligroso, como sitios de phishing, malware, spam, contenido para adultos, entre otros. Además, esta herramienta también puede ser utilizada para bloquear el acceso a aplicaciones en línea, como juegos, redes sociales, servicios de streaming, entre otros.

Gracias al filtrado del firewall de Pfsense, el contenido no deseado puedo ser denegado de manera efectiva, lo que garantiza un ambiente de trabajo seguro y productivo. Esto es especialmente importante en entornos donde se requiere el acceso a internet para realizar tareas laborales o académicas, ya que se asegura que los usuarios no accedan a contenido inapropiado o potencialmente peligroso.

Es importante destacar este apartado debe ser configurado de manera cuidadosa, ya que es posible que algunos sitios web o aplicaciones legítimas sean bloqueados de manera accidental. Por esta razón, se recomienda realizar pruebas de validación de las reglas de filtrado antes de implementarlas en un entorno de producción.

Figura 72. Filtrado de contenido HTTP & HTTPS con Pfsense por: Autor

CONCLUSIONES

- Los objetivos establecidos al comienzo de este proyecto se cumplieron por completo, se ha comprobado que Pfsense es una solución adecuada, con gran flexibilidad y precio accesible para hardware especializado, que nos brinda la posibilidad de crear e implantar una infraestructura de red moderna y eficiente, que nos brinda las mismas características que muchos de estos dispositivos ofrecen por separado.

- La identificación y análisis de los problemas de la red de datos actual es un paso fundamental para la elaboración de un nuevo diseño de red mejorado. Al comprender los problemas y limitaciones de la red actual, se pueden identificar áreas de mejora y desarrollar un diseño que aborde de manera efectiva estos problemas.

- La generación del nuevo diseño de red utilizando la metodología Top-Down es esencial para garantizar que la infraestructura de red sea diseñada e implementada de manera efectiva y eficiente. Un diseño bien planificado permite la creación de una red sólida y segura, que cumpla con los requisitos de la organización y esté preparada para enfrentar los desafíos futuros.

- Después de analizar los requisitos informáticos para la mejora de la seguridad del centro de datos, se encontró que Pfsense es él más óptimo porque pertenece a la línea gratuita, el software está entre los tres mejores programas de seguridad del mundo y es compatible con el hardware que mantiene el GAD municipal de esta manera se tendrá niveles óptimos de protección.

- El realizar la configuración de las políticas de seguridad a través del Firewall Pfsense es fundamental para garantizar la protección de los sistemas y datos críticos de la organización. La implementación adecuada de estas políticas puede ayudar a prevenir posibles vulnerabilidades de seguridad y mantener la integridad y disponibilidad de la red de datos.

- Al instalar el firewall Pfsense en la plataforma de virtualización VMWARE, se tiene como resultado que son sistemas compatibles y realizan las mismas funciones que un firewall de nivel físico. Además, los servidores virtualizados tienen la ventaja de optimizar el uso de los recursos de hardware.

RECOMENDACIONES

- Los procesos de seguridad administrados en el Data Center deben contar con planes de respaldo que se actualicen constantemente para mejorar la confiabilidad de los datos ante el aumento repentino de ataques informáticos, aparición de nuevas vulnerabilidades y robo de datos, por lo que se recomienda revisiones constantes a los mismos.

- Mantener actualizado el sistema Pfsense periódicamente para mantener un alto nivel de protección y rendimiento. De igual manera, se recomienda realizar respaldos de las configuraciones del firewall cada vez que se agregue una nueva política

- Para obtener nuevos métodos de protección para la seguridad de la información, es necesario aplicar periódicamente prueba de seguridad hacia el firewall perimetral y los secundarios implementados

- Capacitar periódicamente a los responsables del centro de datos y a los usuarios en general, en temas de seguridad de la información para mantener un nivel óptimo de protección.

BIBLIOGRAFÍA

[1] A. d. C. E. M. Espinosa Otavalo, «Análisis de Vulnerabilidades de la Red,» 11 01 2012. [En línea]. Available: https://dspace.utpl.edu.ec/bitstream/123456789/1352/3/Espinosa_Otavalo_Ang%C3%A9lica%20del%20Cisne.pdf. [Último acceso: 12 06 2022].

[2] «Mision y Vision,» [En línea]. Available: http://www.cpccs.gob.ec/wp-t/uploads/GUIA-GAD.pdf [Último acceso: 12 06 2022].

[3] E. A. N. CEDILLOS JIMENEZ, VIERA QUIJANO, «biblioteca.utec.edu.sv,» 09 2016. [En línea]. Available: http://biblioteca.utec.edu.sv/siab/virtual/tesis/941000843.pdf. [Último acceso: 16 06 2022].

[4] A. L. Félix Bolaños, «repositorio.utn.edu.ec,» 23 10 2017. [En línea]. Available: http://repositorio.utn.edu.ec/handle/123456789/7189. [Último acceso: 16 06 2022].

[5] B. M. NURY, «repositorio.upse.edu.ec,» 2015. [En línea]. Available: https://repositorio.upse.edu.ec/bitstream/46000/2359/1/UPSE-TET-2015-0001.pdf. [Último acceso: 16 06 2022].

[6] Facsistel, «Facultad de Sistemas y Telecomunicaciones,» 16 06 2022. [En línea]. Available: http://facsistel.upse.edu.ec/index.php?option=com_content&view=article&id=58&Ite. [Último acceso: 22 11 2022].

[7] J. B. S. G. Centurión, «repositorio.ins.gob.pe,» 2020. [En línea]. Available: https://repositorio.ins.gob.pe/bitstream/handle/20.500.14196/1185/45-51.pdf?sequence=1&isAllowed=y. [Último acceso: 14 11 2022].

[8] E. 3, «newsinamerica,» 11 03 2021. [En línea]. Available: https://newsinamerica.com/pdcc/tecnologia/2021/por-que-es-importante-proteger-los-datos-personales/. [Último acceso: 14 11 2022].

[9] Á. M. Mendoza, «welivesecurity,» 16 10 2015. [En línea]. Available: https://www.welivesecurity.com/la-es/2015/10/16/importancia-datos-personales-proteccion/. [Último acceso: 20 06 2022].

[10] P. d. C. d. O. 2.-2. d. Ecuador, «observatorioplanificacion,» 2021. [En línea]. Available: https://observatorioplanificacion.cepal.org/es/planes/plan-de-creacion-de-oportunidades-2021-2025-de-ecuador. [Último acceso: 22 06 2022].

[11] A. O. Fidias G., «researchgate,» 07 2012. [En línea]. Available: https://www.researchgate.net/publication/301894369_EL_PROYECTO_DE_INVESTIGACION_6a_EDICION. [Último acceso: 26 06 2022].

[12] J. F. GUEVARA CAJAS, «ups,» 09 2017. [En línea]. Available: https://dspace.ups.edu.ec/bitstream/123456789/14613/1/UPS%20-%20ST003251.pdf. [Último acceso: 27 06 2022].

[13] E. Nathalia, «academia,» [En línea]. Available: https://www.academia.edu/31848671/Metodolog%C3%ADa_Top_Down_METODOLOGIA_DE_DISE%C3%91O_DE_RED_TOP_DOWN_Historia_de_la_Metodolog%C3%ADa_TOP_DOWN. [Último acceso: 27 06 2022].

[14] I. A. Cruz-Piza, M. O. Montoya-Tello y J. C. Quishpi-Rodríguez, «Gobiernos autónomos descentralizados del Ecuador,» 2020. [En línea]. Available: https://observatorioplanificacion.cepal.org/es/instituciones/gobiernos-autonomos-descentralizados-de-ecuador. [Último acceso: 20 01 2023].

[15] C. D. P. C. Y. C. SOCIAL, «amevirtual.gob.ec,» [En línea]. Available: http://conagopareazuay.gob.ec/w30/wp-content/uploads/2017/01/Guia-Rendici%C3%B3n-de-Cuentas-GADs.pdf. [Último acceso: 05 02 2023].

[16] E. Z. M. A. P. R. H. Luís Suarez Litardo, «http://scielo.sld.cu/,» 02 06 2019. [En línea]. Available: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202019000200193. [Último acceso: 20 01 2023].

[17] M. V. V. Christian ObandoI, «publicaciones.americana.edu.co,» 2022. [En línea]. Available: https://publicaciones.americana.edu.co/index.php/inam/article/view/405. [Último acceso: 20 01 2023].

[18] L. S. L. E. Z. M. A. P. R. H. Byron Oviedo, «http://scielo.sld.cu,» 02 06 2019. [En línea]. Available: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202019000200193. [Último acceso: 20 01 2023].

[19] vmware, «https://www.vmware.com/,» [En línea]. Available: https://www.vmware.com/content/dam/digitalmarketing/vmware/la/pdf/cloud/VMware-and-Cloud-Computing-Brochure.pdf. [Último acceso: 20 01 2023].

[20] J. P. C. OLAGO, «docplayer.es,» [En línea]. Available: https://docplayer.es/2771933-Diseno-e-implementacion-de-un-sistema-de-seguridad-perimetral-para-una-empresa-usando-la-herramienta-pfsense-presentador-por.html. [Último acceso: 20 01 2023].

[21] K. How, «ionos.es,» ionos.es/digitalguide, 18 07 2019. [En línea]. Available: https://www.ionos.es/digitalguide/servidores/know-how/los-tipos-de-redes-mas-conocidos/. [Último acceso: 20 01 2023].

[22] B. Díaz Chang y D. Ayala, «redalyc.org,» 2020. [En línea]. Available: https://www.redalyc.org/journal/5736/573667940029/573667940029.pdf. [Último acceso: 20 01 2023].

[23] A. Amavizca, «academia.edu,» 11 04 2020. [En línea]. Available: https://d1wqtxts1xzle7.cloudfront.net/62922066/INT.REDES.INFORMATICAS20200411-81235-1n2hnvl-libre.pdf?1586672153=&response-content-disposition=inline%3B+filename%3DINTRODUCCION_A_LAS_REDES_INFORMA

TICAS.pdf&Expires=1674661360&Signature=g3MJk-jIWesU75qL4ISR. [Último acceso: 20 01 2023].

[24] F. S. OFAIDER QUINTANA PEDRAZA, «repository.unad.edu.co,» 27 11 2022. [En línea]. Available: https://repository.unad.edu.co/handle/10596/52713. [Último acceso: 20 01 2023].

[25] C. C. O. Vera, «http://dspace.utb.edu.ec/,» 04 2022. [En línea]. Available: http://dspace.utb.edu.ec/bitstream/handle/49000/11625/E-UTB-FAFI-SIST-000306.pdf?sequence=1&isAllowed=y. [Último acceso: 20 01 2023].

[26] J. A. L. X. Bazurto Caiza Ronny Armando, «dspace.ups.edu.ec,» 2021. [En línea]. Available: https://dspace.ups.edu.ec/bitstream/123456789/20743/1/UPS-GT003338.pdf. [Último acceso: 20 01 2022].

[27] C. Y. A. Gómez, «bibliotecadigital.udea.edu.co,» 2020. [En línea]. Available: https://bibliotecadigital.udea.edu.co/bitstream/10495/18600/5/AmayaChristian_2020_AdministracionAvanzadaDireccionamento.pdf. [Último acceso: 20 01 2023].

[28] D. P. ANAYA, «repository.unad.edu.co,» 2021. [En línea]. Available: https://repository.unad.edu.co/bitstream/handle/10596/43760/dpoloa.pdf?sequence=1&isAllowed=y. [Último acceso: 20 01 2023].

[29] M. J. B. Herrera, «http://dspace.utb.edu.ec/,» 2020. [En línea]. Available: http://dspace.utb.edu.ec/bitstream/handle/49000/7631/BOHORQUEZ%20HERRERA.pdf?sequence=1&isAllowed=y. [Último acceso: 20 01 2023].

[30] S. L. V. C. Elias Fernando Mora Bandera, «revistas.uniguajira.edu.co/,» 20 10 2019. [En línea]. Available: http://revistas.uniguajira.edu.co/rev/index.php/cei/article/view/202/194. [Último acceso: 20 01 2023].

[31] D. Azizov, «ddd.uab.cat,» 2020. [En línea]. Available: https://ddd.uab.cat/pub/tfg/2020/tfg_286259/Arquitectura_DMZ_Perimetral_Una_Implementacin_Corporativa.pdf. [Último acceso: 20 01 2023].

[32] A. Galán, «revistasguatemala.usac.edu.g,» 2015. [En línea]. Available: http://www.revistasguatemala.usac.edu.gt/index.php/riyc/article/view/1028. [Último acceso: 20 01 2023].

[33] C. Martin, «techspring.mx,» techspring, 23 04 2020. [En línea]. Available: https://www.techspring.mx/organizador-de-cables/. [Último acceso: 14 11 2022].

[34] CISCO, «cisco.com,» cisco, 2021. [En línea]. Available: https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/network-switch-how.html. [Último acceso: 14 11 2022].

[35] J. A. Silva, «es.scribd.com,» scribd, [En línea]. Available: https://es.scribd.com/doc/235285825/Que-Es-Un-Patch-Panel. [Último acceso: 14 11 2022].

[36] J. Fock, «es.scribd.com,» scribd, [En línea]. Available: https://es.scribd.com/document/538079908/Construccion-de-un-patch-cord. [Último acceso: 14 11 2022].

[37] C. L. Jurado., «es.ccm.net,» ccm, 26 01 2021. [En línea]. Available: https://es.ccm.net/contents/187-conector-rj45. [Último acceso: 14 11 2022].

[38] CISCO, «CISCO,» [En línea]. Available: https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html#~how-to-choose-small-business-routers. [Último acceso: 14 11 2022].

[39] CISCO, «CISCO,» [En línea]. Available: https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html. [Último acceso: 14 11 2022]

ANEXOS

Anexo 1. Registro de técnica de observación aplicada en varios departamentos del GAD

	UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENAFACULTAD DE SISTEMAS Y TELECOMUNICACIONES CARRERA TECNOLOGIAS DE LA INFORMACIÓN Reingeniería de la infraestructura de red de datos lógica del Gobierno Autónomo Descentralizado (GAD)			
OBSERVACIÓN				
Observador:	Bastidas Orrala Ismael			
Tipo:	Directa			
Objetivo	Recopilar información de cómo se encuentra actualmente la infraestructura de la red física y lógica del GAD.			
Fecha:	12/04/2022			
Indicador	Siempre	Casi siempre	En ocasiones	Jamás
Hay problemas con la conectividad entre impresoras y la red.				
Existen inconvenientes con del servicio de internet debido IP duplicadas.				
Problemas con aplicaciones que funcionan con la red internet del GAD				
Perdida del servicio de internet.				
Usuarios usando otra VLAN que no corresponde a su área.				
Usuarios no pueden acceder a configuraciones del sistema para completar sus funciones.				
Existe el reparto el servicio de internet afectando la conectividad de uno o varios departamentos.				

Anexo 2. Formato de entrevista realizada los trabajadores del área de Sistema del GAD.

UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENAFACULTAD DE SISTEMAS Y TELECOMUNICACIONES CARRERA TECNOLOGIAS DE LA INFORMACIÓN

Reingeniería de la infraestructura de red de datos lógica del Gobierno Autónomo Descentralizado (GAD)

Entrevista realizada al director de informática y tecnologías.

Objetivo:	Recopilar información de cómo se encuentra actualmente la infraestructura de la red física y lógica del GAD

PREGUNTAS	**RESPUESTAS**
PREGUNTA 1 ¿Cuál es su cargo dentro del departamento de Sistemas?	Soy el director de informática y tecnologías.
PREGUNTA 2 ¿Cómo se encuentra estructurado el departamento de sistemas?	Está conformado por el área de desarrollo de sistemas y el área de soporte técnica.
PREGUNTA 3 ¿Cómo está estructurada la red de datos?	En cada piso está distribuido por VLANS, estos están habilitados por router cisco, físicamente no cuentan con un firewall.
PREGUNTA 4 ¿Cuentan con Firewall en la red y si es así, cuantos tienen y de qué forma está estructurado cada Firewall?	Si se cuenta con Firewall, más específico con un Proxy.
PREGUNTA 5 ¿Cuántos proxys manejan?	Se cuenta con dos proxys ya que tienen dos proveedores de internet y tienen un proxy para cada uno, esto con el fin de aumentar los filtros de seguridad.
PREGUNTA 6 ¿Qué políticas de seguridad se tienen implementadas actualmente?	Como políticas de seguridad se tiene el controlador de dominios por Windows Server el cual es usado para el control de usuario, acceso a las computadoras, carpetas compartidas. Todo se maneja por una LAN de forma cableada no hay Acces Point, todo se

	maneja por IP fijas esto es controlado por switch cisco administrables
PREGUNTA 7 ¿Cuentan con los planos de la estructuración de la red de datos?	Si se tiene los planos de la red de datos de cada piso, pero solo se tiene de manera física y por el uso del mismo ya se está desgastando porque solo se tiene en ese formato físico y no hay en formato digital.

Anexo 3. Visita a las instalaciones del GAD Municipal.