Gestión de seguridad informática en PYMES de San Juan de Pasto mediante la implementación de un dispositivo de seguridad perimetral usando software y hardware libre.

Jose Fernando Imbajoa Sacanambuy, ✉ josfer805@gmail.com

Proyecto presentado para optar al título de Ingeniero de Sistemas

Asesor: Martha Lisbeth Buritica Leon

Esp. Telemática.

Universidad CESMAG

Facultad de Ingeniería

Ingeniería de Sistemas

San Juan de Pasto

2025

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

NOMBRE JURADO 1

_____

NOMBRE JURADO 2

San Juan de Pasto, 2024

NOTA DE EXCLUSIÓN

El autor de esta obra es el único responsable de las ideas expresadas en ella, y esta no refleja o no compromete la ideología de la Universidad CESMAG.

Dedicatoria

Con profundo amor y gratitud, dedico este trabajo de grado a mi madre, Luz Mery, quien con su incondicional apoyo, esfuerzo y amor me ha guiado en cada paso de mi vida. Este logro es tan mío como suyo, pues sus sacrificios y enseñanzas han sido la base de mi crecimiento personal y profesional.

A mis profesores, por su paciencia, conocimientos y orientación a lo largo de este camino académico, quienes no solo fueron guías, sino también inspiración para alcanzar mis metas.

Y finalmente, a la Universidad Cesmag, por brindarme las herramientas, el espacio y el acompañamiento necesario para formarme como profesional, inculcándome valores y conocimientos que llevaré conmigo a lo largo de mi vida.

A todos ustedes, mi más sincero agradecimiento por ser parte fundamental de este importante capítulo en mi vida.

Agradecimiento

Primero que todo, agradezco a Dios, fuente de fortaleza y guía en cada paso de mi vida. Su presencia ha sido mi refugio y motivación en los momentos de desafío, permitiéndome llegar a este importante logro.

A mis padres, quienes con amor, dedicación y sacrificio han sido el pilar fundamental de mi formación personal y profesional. Su apoyo incondicional y confianza en mí han sido mi mayor inspiración para seguir adelante.

A la asesora del proyecto, Martha Lisbeth Buriticá León, por su paciencia, orientación y compromiso en cada etapa de este proceso. Su experiencia y sabiduría han sido clave para culminar este proyecto con éxito.

Finalmente, a la Universidad Cesmag, por brindarme una educación integral y por ser el escenario donde construí los conocimientos y valores que hoy me acompañan. Este trabajo es un reflejo de los aprendizajes obtenidos y del esfuerzo conjunto de todos quienes han sido parte de mi formación.

A todos, mi más sincero agradecimiento.

Glosario

Antivirus:

Software diseñado para detectar, prevenir y eliminar programas maliciosos, como virus, spyware o ransomware, que pueden comprometer sistemas informáticos.

Ciber amenaza:

Cualquier acción o evento que pueda poner en riesgo la seguridad de los sistemas informáticos, como ataques de malware, accesos no autorizados o suplantaciones de identidad.

Ciberdelincuencia:

Conjunto de actividades ilegales realizadas mediante tecnologías de la información, como el robo de datos, hackeos o ataques de denegación de servicio (DoS).

Debian:

Sistema operativo basado en el núcleo Linux, conocido por su estabilidad y versatilidad. Es utilizado como base de muchas distribuciones populares y es ideal para servidores y sistemas embebidos como Raspberry Pi.

Django:

Framework web de alto nivel y código abierto basado en Python, diseñado para facilitar el desarrollo rápido y limpio de aplicaciones web.

Firewall:

Sistema de seguridad, físico o lógico, que controla el tráfico de red entrante y saliente, permitiendo o bloqueando datos según reglas predefinidas.

Linux:

Familia de sistemas operativos de código abierto basados en el núcleo Linux. Es ampliamente utilizado en servidores, dispositivos embebidos, sistemas de red y computadoras personales.

PYMES (Pequeñas y Medianas Empresas):

Empresas clasificadas según su número de empleados y nivel de ingresos, que representan una parte fundamental de la economía.

Raspberry Pi:

Microcomputadora de bajo costo y tamaño compacto diseñada para promover la enseñanza de

informática y el desarrollo de proyectos tecnológicos. Es ampliamente utilizada en sistemas embebidos, domótica y análisis de tráfico de red.

Red perimetral:
Zona de la red que actúa como límite entre una red interna segura y redes externas menos seguras, como Internet.

Riesgo informático:
Probabilidad de que un sistema sea afectado por vulnerabilidades o amenazas que comprometan su funcionamiento o datos.

Seguridad perimetral:
Conjunto de métodos y tecnologías diseñados para proteger la infraestructura de una red, incluidas medidas como firewalls y sistemas de detección de intrusos.

Sistema de gestión de seguridad de la información (SGSI):
Modelo basado en estándares internacionales como ISO/IEC 27001 que ayuda a gestionar y proteger la información crítica de una organización.

SQLite3:
Sistema de gestión de bases de datos relacional ligero y sin servidor. Es ampliamente utilizado en proyectos pequeños y medianos debido a su simplicidad y bajo requerimiento de recursos.

Vulnerabilidad:
Falla o debilidad en un sistema que puede ser explotada por amenazas para acceder a datos o comprometer la seguridad.

Código abierto (Open Source):
Modelo de desarrollo de software donde el código fuente está disponible para su libre uso, modificación y distribución.

Norma ISO/IEC 27001:
Estándar internacional que proporciona requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información.

Panel de administración (Admin Panel):
Interfaz gráfica en sistemas como Django que permite a los usuarios administrar datos, usuarios y configuraciones del sistema.

Servidor:
Computadora o programa que proporciona servicios a otros programas o dispositivos dentro de una red. Por ejemplo, un servidor web o de bases de datos.

Python:
Lenguaje de programación interpretado y de alto nivel utilizado en aplicaciones web, análisis de datos, inteligencia artificial y más.

SSH (Secure Shell):
Protocolo que permite la conexión remota segura entre computadoras para ejecutar comandos y transferir datos.

Tabla de contenido

INTRODUCCIÓN 16

I. PROBLEMA DE INVESTIGACIÓN 18

A. Objeto o Tema De Investigación 18

B. Línea de investigación 18

C. Sublinea de investigación 18

D. Planteamiento del problema 18

E. Formulación del problema 20

F. Objetivos 20

1) Objetivo General 20

2) Objetivos específicos 20

G. Justificación 20

H. Delimitaciones 21

II. MARCO TEÓRICO 22

A. Antecedentes 22

1) Internacionales 22

2) Nacionales 23

3) Regionales 25

B. Norma ISO 26

C. Metodología Scrum 26

D. Supuestos Teóricos de la Investigación. 27

Confidencialidad 27

Información 28

Sistema tecnológico 29

Integridad 29

Disponibilidad 29

Manejo de Riesgos 30

Red 31

Firewall o Cortafuegos. 31

Amenazas y Ataques 32

Amenaza 33

Servicio 33

Restricción al uso del sistema 33

PYME 33

Ransomware 34

Raspbian 35

Raspberry PI 35

GNU/Linux 35

Software libre 36

Hardware libre 37

Modelo TCP/IP 37

E. Variables de estudio 38

- Variable independiente 38

- Variable dependiente 38

F. Definición nominal de variables 38

- Variable dependiente 38

- Variable independiente 39

- Definición operativa de variables 39

G. Formulación de hipótesis 41

1) Hipótesis de investigación 41

2) Hipótesis nula 41

3) Hipótesis alterna 41

III. METODOLOGÍA 42

A. Paradigma 42

B. Enfoque 42

C. Método científico 42

D. Tipo de investigación 42

F. Población 43

G. Muestra 43

H. Técnicas de recolección de la información 44

1) Validez de las técnicas 44

2) Confiabilidad de la técnica 45

I. Instrumentó de recolección de datos 45

IV. RESULTADOS DE LA INVESTIGACION 46

A. Documentación de pruebas. 46

B. Desarrollo de producto tecnológico 51

C. Validar el comportamiento de la información en el dispositivo de seguridad. 71

V. ANÁLISIS DE LOS RESULTADOS 87

CONCLUSIONES 92

RECOMENDACIONES 93

Anexos 94

Anexo1 – firma de aval de la carta 94

Anexo3. Encuesta 96

BIBLIOGRAFIA 101

CONTENIDO

LISTA DE TABLAS

TABLA I. TIEMPO DE LATENCIA 34

TABLA II. USABILIDAD 34

TABLA III. EFICIENCIA DE LAS REGLAS 34

TABLA IV. ANALISIS DE ENCUESTA 40

TABLA V. REVISIÓN DE EXPERTOS 44

TABLA VI. APLICACIÓN DE ENCUESTA 45

TABLA VII. REQUERIMIENTOS FUNCIONALES Y NO FUNCIONALES 45

TABLA VIII. PRODUCT BACKLOG 47

TABLA IX. HISTORIA DE USUARIO: CREACIÓN DE ROLES 48

TABLA X. HISTORIA DE USUARIO: PANEL DE INICIO DE SESIÓN 49

TABLA XI. HISTORIA DE USUARIO: ADMINISTRADOR DE USUARIOS 49

TABLA XII. HISTORIA DE USUARIO: ADMINISTRADOR DE REGLAS 50

TABLA XIII. HISTORIA DE USUARIO: PANEL DE ALERTAS 51

TABLA XIV. HISTORIA DE USUARIO: PANEL DE DNS 52

RESUMEN ANALÍTICO DE ESTUDIO RAE

Facultad: Ingeniería.

Programa: Ingeniería de Sistemas.

Fecha de elaboración: 30 de octubre del 2024.

Autores de la investigación:

José Fernando Imbajoa Sacanambuy

Asesor: Esp. Martha Lisbeth Buriticá León

Título de la investigación:Gestión de seguridad informática en PYMES de San Juan de Pasto mediante la implementación de un dispositivo de seguridad perimetral usando software y hardware libre.

PALABRAS CLAVE: Raspberry, seguridad informática, nftables, firewall, Linux

DESCRIPCIÓN: Este proyecto implementa un sistema de seguridad perimetral en Raspberry Pi para proteger la red y la información de PYMES en San Juan de Pasto. El sistema permite monitorear y controlar el tráfico de red, detectando posibles amenazas y brindando una solución accesible, escalable y de bajo costo, adecuada a las necesidades de las empresas locales.

CONTENIDO

El informe final está estructurado de la siguiente forma:

Este proyecto implementó un sistema de seguridad perimetral en PYMES de San Juan de Pasto, utilizando una Raspberry Pi para mejorar la protección de la información frente a ciber amenazas comunes. La investigación reveló que estas empresas tienen limitadas políticas de seguridad y conocimiento sobre ciberataques. Con el nuevo sistema, se logró un monitoreo efectivo del tráfico de red y una mayor percepción de seguridad, aunque persisten áreas de mejora en capacitación y recursos. Se concluye que esta solución es viable y se recomienda continuar fortaleciendo la formación y la infraestructura de seguridad en las PYMES locales.

Conclusiones: La implementación del sistema de seguridad perimetral basado en Raspberry Pi ha demostrado ser una solución efectiva y accesible para las PYMES en San Juan de Pasto. Este sistema ha incrementado la seguridad de la red y permitido el monitoreo constante del tráfico, facilitando la detección de anomalías. La solución es escalable y adaptable a las necesidades específicas de cada empresa, ofreciendo un enfoque innovador y económico para la protección de la información.

Recomendación: Las PYMES deben mejorar su infraestructura de seguridad mediante actualizaciones periódicas y la incorporación de nuevas tecnologías en su sistema perimetral, optimizando la detección y respuesta a incidentes de seguridad.

METODOLOGÍA

Se usó la metodología Scrum, permitiendo desarrollar el sistema de seguridad perimetral en Raspberry Pi en ciclos iterativos. Cada sprint permitió planificar, desarrollar y ajustar el sistema, integrando retroalimentación y adaptándose a las necesidades de las PYMES, con entregas incrementales y valor agregado en cada fase.

LÍNEA DE INVESTIGACIÓN: Seguridad de la información.

SUB LÍNEA DE INVESTIGACIÓN: La seguridad informática

INTRODUCCIÓN

Según la Ley 905 de 2004, las micro, pequeñas y medianas empresas (PYMES) en Colombia se clasifican con base en el valor de sus activos y el número de empleados. Aunque la Ley 1450 de 2011 contempla incluir las ventas como un criterio adicional, esto aún no ha sido reglamentado. Así, una microempresa cuenta con hasta 10 empleados y activos inferiores a 500 salarios mínimos legales mensuales vigentes (SMLMV); una pequeña empresa, entre 11 y 50 empleados y activos entre 501 y 5.000 SMLMV; y una mediana empresa, entre 51 y 200 empleados, con activos de 5.001 a 30.000 SMLMV (Ley 905 de 2004, Ley 1450 de 2011) [1].

Aunque la normativa podría incorporar las ventas como criterio en el futuro, actualmente las PYMES se clasifican por empleados y activos. Estas empresas enfrentan diversos desafíos de seguridad informática. Según Citrix, un estudio de OnePoll revela que en Colombia las principales preocupaciones incluyen phishing (56%), ataques de denegación de servicio (DoS) (56%) y ransomware (34%). Estas amenazas comprometen la integridad de los sistemas y ponen en riesgo la información empresarial [2].

Por su parte, la Universidad Autónoma de Ciudad Juárez (UACJ) destaca la importancia de implementar medidas de seguridad para garantizar el buen uso de los recursos tecnológicos y proteger los datos empresariales. En este contexto, resulta esencial desarrollar soluciones económicas y efectivas, como un dispositivo de seguridad perimetral basado en una Raspberry Pi 4, que permita monitorear y gestionar el tráfico de red, controlando posibles anomalías mediante tecnologías de software y hardware libre [3].

En Colombia, el panorama de seguridad informática en las PYMES sigue siendo preocupante. Muchas de estas empresas no valoran adecuadamente la información que manejan, adoptando actitudes confiadas frente a posibles incidentes. Según ESET, en 2016 el 40.6% de las empresas colombianas fueron afectadas por malware [4]. Entre las razones más comunes para no invertir en

seguridad destacan la falta de personal calificado, limitaciones de espacio físico y altos costos, según lo reporta la revista Semana [5].

Este proyecto propone configurar un dispositivo Raspberry Pi 4 como una herramienta accesible para implementar controles de seguridad perimetral en PYMES de San Juan de Pasto. Al integrar funcionalidades de firewall y monitoreo del tráfico de red, esta solución busca mitigar riesgos y proteger la información empresarial de forma eficiente y económica. Su implementación permitirá a las empresas locales fortalecer su seguridad, adaptarse a las demandas tecnológicas actuales y mejorar su desempeño frente a amenazas cibernéticas.

I. PROBLEMA DE INVESTIGACIÓN

A. Objeto o Tema De Investigación

Protección de datos a partir de una Raspberry PI4

B. Línea de investigación

La línea de investigación de este Proyecto se basa en Seguridad de la información: “Mantener la Integridad, Disponibilidad y Confiabilidad de la información, se propone por el desarrollo de proyectos investigativos en torno a la seguridad en la informática, la cual abarca los conceptos de seguridad física (Hardware) y seguridad lógica (Software).” [6]

C. Sublinea de investigación

Como sublínea de investigación se toma: “La seguridad informática consiste en prácticas y tecnologías diseñadas para proteger sistemas de información y datos. Su objetivo es mantener la información a salvo de accesos no autorizados y garantizar la disponibilidad de los sistemas. Incluye la protección de redes, aplicaciones y datos, siendo esencial para asegurar la confidencialidad, integridad y disponibilidad en un entorno digital en constante cambios.” [7]

D. Planteamiento del problema

Las PYMES enfrentan riesgos significativos de pérdida de información, lo que puede interrumpir sus operaciones y generar consecuencias graves, como pérdidas económicas y daños reputacionales. Este problema se agrava por el desconocimiento generalizado sobre la seguridad tecnológica y la falta de implementación de medidas adecuadas de ciberseguridad. La exposición diaria de datos empresariales ocurre debido a prácticas inseguras, desinformación y ausencia de dispositivos de protección específicos.

Kaspersky Lab resalta que solo el 10% de los empleados conoce las políticas de seguridad de Tecnologías de la Información (TI) de sus empresas, mientras que el resto considera que la

protección contra ciberamenazas es una responsabilidad compartida. Esto dificulta establecer un marco sólido de ciberseguridad dentro de las organizaciones [8].

De acuerdo con un informe de PROTEK, entre los virus informáticos más peligrosos están los TROYANOS, que permiten a los hackers controlar dispositivos para robar datos; los GUSANOS, que se propagan a través de transferencias de archivos y generan daños significativos; y el RANSOMWARE, que cifra los datos y exige un rescate para restaurar el sistema. Estas amenazas representan un riesgo creciente para las empresas que no adoptan medidas preventivas [9].

En el caso de Colombia, según Fortinet, el país ocupa el cuarto lugar en intentos de ciberataques en Latinoamérica, con un promedio de 289.000 millones de intentos diarios. Además, el National Cyber Security Index (NCSI) posiciona al país en el puesto 72 entre 160 evaluados, lo que evidencia la necesidad urgente de mejorar la seguridad informática en las empresas [10].

Aunque los sistemas operativos más utilizados, como Windows, Linux, Unix y Mac OS, ofrecen herramientas para la protección de datos, muchas PYMES no las implementan debido al costo elevado de dispositivos especializados. Esta falta de inversión deja sus redes vulnerables a ciberataques y posibles pérdidas económicas. Asimismo, las malas prácticas y el desconocimiento entre empleados agravan la situación, afectando tanto la infraestructura tecnológica como la integridad de la información empresarial [11].

Sin embargo, existen soluciones de bajo costo que podrían mitigar estos problemas. Un ejemplo es la Raspberry Pi, una microcomputadora económica, versátil y eficiente, recomendada por Dynamo Electronics como una alternativa accesible para mejorar la seguridad en las PYMES. En Colombia, su precio oscila entre 200.000 y 300.000 pesos, lo que la convierte en una herramienta viable para las empresas que desean implementar sistemas de seguridad perimetral sin incurrir en altos costos [12].

E. Formulación del problema

¿Cómo fortalecer los procesos en la red mediante la implantación de una Rasberry Pi4 como dispositivo de seguridad perimetral en las PYMES de San Juan de Pasto?

F. Objetivos

1) Objetivo General

Desarrollo de un aplicativo de seguridad perimetral para PYMES implementado en una Raspberry Pi4

2) Objetivos específicos

- Caracterizar los procesos de información en PYMES según el tipo de muestra dada en esta investigación para la ciudad de San Juan de Pasto.
- Implementar un sistema de seguridad perimetral en Raspberry que contribuya a la protección de la información.
- Validar el comportamiento de la información en el dispositivo de seguridad.

G. Justificación

La ciberseguridad es un desafío creciente para las empresas, especialmente para aquellas con recursos limitados, como las PYMES. A pesar de los avances tecnológicos, muchas organizaciones siguen siendo vulnerables a ciberataques debido a la falta de conocimiento y a la implementación insuficiente de medidas de protección. Según datos de la Southern New Hampshire University, el 62% de los encargados de seguridad informática en las empresas se siente medianamente seguro o nada seguro respecto a los sistemas informáticos de sus organizaciones, mientras que solo un 7% se siente extremadamente seguro al respecto. Este nivel de inseguridad refleja la necesidad urgente de soluciones efectivas y accesibles para mejorar la ciberseguridad en el entorno empresarial. [13]

Para abordar esta problemática, se propone un sistema de seguridad perimetral basado en la Raspberry Pi 4. Este dispositivo realizará análisis continuos y activos para detectar vulnerabilidades en la red, ayudando a las empresas a proteger sus datos y a reducir el riesgo de

ataques cibernéticos. La Raspberry Pi, conocida por su reducido costo y tamaño, ofrece una alta capacidad de procesamiento y es ideal para su implementación en entornos donde los recursos son limitados. El uso de Nftables para el filtrado de paquetes añade una capa adicional de seguridad, permitiendo un control más granular y eficiente del tráfico de red.

Lo innovador de este proyecto radica en la combinación de la Raspberry Pi con Nftables, una tecnología que, a pesar de su bajo costo, ofrece una protección robusta contra una amplia gama de amenazas cibernéticas. Esto no solo reduce los riesgos asociados con la seguridad de los equipos, sino que también permite a las empresas implementar medidas de protección avanzadas sin incurrir en gastos significativos.

Con la correcta implementación de este sistema, se espera no solo mejorar la seguridad de los datos empresariales, sino también fomentar una mayor conciencia sobre la ciberseguridad. Como menciona Nuria Estruga, "la ciberseguridad es un ámbito complejo y cambiante, debido a que está estrechamente ligada a los avances tecnológicos y a los nuevos riesgos que aparecen" [14]. Por tanto, es fundamental que las empresas se mantengan al día en la protección de su información para evitar pérdidas significativas, tanto de datos como financieras. En línea con esta necesidad, Chema Alonso subraya que "diariamente, en todo el mundo, se producen millones de ciberataques y nadie está exento de ser una víctima más. Pero al igual que la ciberdelincuencia es cada vez más grave y sofisticada, también lo es la manera de subsanar estos conflictos". [15]

H. Delimitaciones

La investigación se desarrollará en la Ciudad de San Juan de Pasto, en un ambiente controlado simulando el estado actual de las PYMES, donde se implementará un dispositivo de seguridad perimetral conocido como Raspberry Pi4. La duración del proyecto tiene un tiempo estimado de 8 meses.

II. MARCO TEÓRICO

A. Antecedentes

1) Internacionales

La investigación titulada "Seguridad informática: una problemática de las organizaciones en el sur de Sonora", realizada por Edgar Alberto Espinoza y Zallas Rodolfo Rodríguez Pérez en la Ciudad de México en 2017, destaca la importancia de la seguridad informática en las empresas para garantizar un buen funcionamiento de los sistemas y el uso adecuado de los equipos tecnológicos. El objetivo principal del estudio es analizar los procedimientos adecuados para mantener la integridad de los datos en los equipos informáticos. Su metodología se basa en la reducción de riesgos mediante la implementación de medidas de protección, sustentadas en el análisis y la clasificación de amenazas.

Como conclusión, se señala que la seguridad informática implica minimizar riesgos y generar confianza, aunque no garantiza la eliminación total de las amenazas. Se enfatiza la importancia de un uso adecuado de los equipos y la implementación de restricciones necesarias para proteger la información. Entre las recomendaciones destacan la realización de respaldos periódicos de los datos para prevenir su pérdida ante cualquier amenaza y la conservación de la información en un servidor espejo, garantizando su disponibilidad en caso de vulnerabilidad.

Esta investigación resulta relevante para el proyecto actual, ya que subraya la necesidad de analizar constantemente los equipos y promover su manejo adecuado por parte del personal de las empresas. Además, aborda la falta de conocimiento respecto a medidas de protección y clasificación de riesgos, proporcionando un enfoque integral basado en un informe concreto [16].

Como segundo referente internacional, se tiene la investigación titulada "Seguridad informática en las PYMES de la ciudad de Quevedo", realizada por Andrea Raquel Zúñiga Paredes, Italo Mecías Serrano Quevedo y Luis Javier Molina Chalacán en Quevedo, Ecuador, en 2020. Este estudio resalta la importancia de implementar controles de seguridad en las TIC para impulsar la competitividad y el desarrollo empresarial. El objetivo principal es identificar el estado actual de

la seguridad informática en las empresas, utilizando una metodología cualitativa que examina diversas situaciones relacionadas con la seguridad en las PYMES de Quevedo.

Como conclusión, se destaca que muchas de estas empresas interactúan mediante el marketing digital, exponiendo su información y, por lo tanto, requieren medidas de seguridad informática. Este referente es relevante para el proyecto actual, ya que promueve la competitividad y la integridad empresarial mediante mecanismos de control en redes, especialmente en la parte administrativa, enfatizando la protección de datos en las PYMES [17].

Por otra parte, la investigación titulada "Evaluación del sistema de seguridad de la información para empresas de proyectos", de los autores Lázaro Tundidor, Alberto Medina y Dianelys Nogueira, realizada en Holguín, Cuba, en 2019, aborda la necesidad de evaluar los sistemas informáticos para mejorar el control de gestión en la seguridad de la información. El objetivo principal es aplicar un índice integral que contribuya a la gestión de la seguridad informática. Este estudio utiliza el método científico para analizar datos y diagnosticar los sistemas informáticos.

El aporte de este referente al proyecto radica en la relevancia de optimizar procesos y gestionar los datos en los equipos empresariales mediante controles efectivos y análisis previos, garantizando una mayor seguridad informática [18].

2) Nacionales

La investigación llevada a cabo en la Universidad Cooperativa de Colombia, Facultad de Ingeniería de Sistemas en Neiva, el 25 de febrero del año 2019, se tituló "Análisis de seguridad perimetral en la empresa Servitienda de Colombia y Dsurtiendo", y fue realizada por Alexander Avendaño Meneses, David Díaz Perdomo y Miguel Ángel Tafur. Este estudio destaca la importancia de la seguridad perimetral en la red, con el objetivo de proteger el bien más valioso de la empresa: la información. El análisis tiene como objetivo general la evaluación de un sistema de seguridad perimetral que garantice la protección de los datos. La metodología empleada fue cualitativa, basada en observaciones de los comportamientos de los usuarios al manipular la red.

Como conclusión, se estableció que el sistema propuesto sigue el modelo OSI para el flujo de datos y que, aunque un dispositivo UTM (Unified Threat Management) puede ser costoso, es capaz de detectar vulnerabilidades y amenazas, mejorando así la seguridad de la red. Esta investigación es de relevancia para el proyecto actual, ya que se enfoca en la gestión de perfiles de usuarios con restricciones, asegurando la confidencialidad y el acceso adecuado a la información [19].

En la investigación "Diseño de un sistema de seguridad perimetral en las instalaciones del consorcio de la expansión PTAR SALITRE SEDE BOGOTÁ D.C", realizada en el año 2017 en la Universidad Católica de Colombia por los autores Marcel Andrés Bohórquez y Luis Angelo Páez Cuadros, se subraya la importancia de implementar un diseño de seguridad perimetral tanto físico como lógico. El estudio tiene como objetivo caracterizar la protección de la infraestructura física y lógica dentro de las instalaciones del consorcio, buscando educar a los usuarios finales sobre un adecuado manejo de la información.

La metodología empleada incluye fases de trabajo, instrumentos utilizados y una muestra poblacional. Como conclusión, se destaca la necesidad de implementar seguridad perimetral mediante "anillos de seguridad", asegurando así la capa de red utilizando el modelo OSI. Se resalta la importancia de gestionar la información basada en roles y perfiles de acceso, garantizando la seguridad de la periferia y facilitando la gestión del personal encargado de la seguridad [20].

Finalmente, la investigación titulada "Diseño de sistemas de seguridad de la información para los procesos de soporte y desarrollo de software en la empresa Alkom S.A, basado en la norma ISO/IEC 27001:2017", realizada por Juan Pablo Ramírez Benavides en la Universidad Piloto de Colombia, en Bogotá, en 2020, aborda la importancia de utilizar una metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT). Este enfoque permite identificar los factores de riesgo y establecer los niveles de protección para cada activo de la empresa.

El objetivo principal del estudio es diseñar un sistema de gestión de seguridad para los procesos de soporte y desarrollo del software en la empresa Alkom S.A, identificando el estado actual, realizando un inventario con análisis de riesgos y proponiendo una implementación de un sistema

de gestión de seguridad. Como conclusión, se destaca que un Sistema de Gestión de Seguridad de la Información (SGSI) es una herramienta clave para la gerencia, ya que facilita la toma de decisiones y el control dentro de la empresa, permitiendo una visión más clara del estado actual de los riesgos y sus posibles soluciones en el ámbito empresarial [21].

3) Regionales

La investigación titulada "Casos de estudios de cibercrimen en Colombia", realizada por Nancy Adriana Gonzales en la Universidad Nacional Abierta y a Distancia (UNAD) en Pasto, Nariño, en el año 2020, aborda la importancia de implementar los canales necesarios para enfrentar los ataques de ciberdelincuentes, que actualmente se han vuelto cada vez más sofisticados y son utilizados principalmente para la suplantación de identidad. El objetivo principal de la investigación es analizar la problemática que enfrentan las empresas con la ciberdelincuencia y evaluar su impacto negativo. Además, presenta estadísticas que permiten ofrecer recomendaciones clave, como la necesidad de organizar la seguridad de la información dentro de las empresas, asignando roles y responsabilidades claras a los miembros de la organización. Es esencial, según la investigación, definir políticas de seguridad de la información, orientadas a los integrantes de la empresa, y fomentar la comunicación sobre el uso adecuado de los recursos de información, con el fin de prevenir y controlar vulnerabilidades. Este estudio destaca las vulnerabilidades más comunes que los ciberdelincuentes aprovechan, proporcionando un panorama global sobre el tema de la ciberseguridad [22].

En la investigación "Auditoría a la seguridad de la red de datos del Instituto Departamental de Salud de Nariño", realizada por Javier Orlando Mesías Narváez y Diego Fernando Rosero Almeida en la Universidad Nacional Abierta y a Distancia (UNAD) en Pasto, Colombia, en el año 2016, se subraya la importancia de implementar una auditoría de seguridad informática para evaluar la vulnerabilidad de la red de datos de la institución. El objetivo principal del proyecto fue establecer sistemas de control para prevenir posibles ataques. La metodología aplicada se estructuró en fases: conocimiento, planeación y ejecución de la auditoría, con el fin de elaborar un informe final que permitiera identificar los niveles de madurez de la red y proponer recomendaciones precisas. La conclusión principal del estudio fue que es fundamental realizar auditorías periódicas para identificar y corregir vulnerabilidades, y se destacó la importancia de

proteger la integridad de los datos personales, especialmente cuando estos están almacenados en redes inseguras [23].

Finalmente, el proyecto "Rediseño de políticas y procedimientos de seguridad informática para la Gobernación de Nariño", realizado por Jorge Daniel Álvarez García en la Universidad Nacional Abierta y a Distancia (UNAD) en San Juan de Pasto, en el año 2018, tiene como objetivo mejorar la seguridad informática dentro de la Gobernación de Nariño mediante el rediseño de sus políticas y procedimientos, a partir de un análisis diagnóstico del estado actual de la seguridad. Este proyecto se enfoca en identificar los riesgos y amenazas que enfrenta la institución, con el fin de establecer medidas correctivas. La metodología empleada fue el ciclo PVHA (Planificar, Verificar, Hacer y Actuar), y el estudio subraya la importancia de un análisis exhaustivo de todos los sistemas de información, con el fin de garantizar que las políticas implementadas sean efectivas en la protección de los datos y la infraestructura tecnológica de la entidad [24].

B. Norma ISO

Es una norma que permite administrar la información de las empresas, sin importar su estructura ni sus campos laborales; un sistema de seguridad para la protección de datos se debe ejecutar de manera continua y mitigar los riesgos de los datos de una empresa u organización. [25]

C. Metodología Scrum

El proceso Scrum es un marco de trabajo ágil diseñado para facilitar la colaboración efectiva en proyectos complejos, especialmente aquellos relacionados con el desarrollo de software. Consiste en una serie de interacciones en grupo, donde las entregas se realizan de manera parcial y regular, enfocándose en la calidad del producto final que se ofrece a los clientes. Este enfoque incremental permite no solo una organización eficiente del trabajo, sino también una rápida adaptación y aprendizaje sobre los problemas que surgen durante el desarrollo. Gracias a las herramientas y recursos específicos que Scrum proporciona, los equipos pueden integrarse y colaborar con mayor facilidad, asegurando un flujo de trabajo continuo y efectivo.

Un proceso Scrum típico se divide en varias partes clave:

El quién y el qué: Esta fase identifica los roles de cada uno de los miembros del equipo, definiendo claramente sus responsabilidades dentro del proyecto. Los roles principales en Scrum incluyen el Product Owner, el Scrum Master y el equipo de desarrollo. El Product Owner se encarga de gestionar el backlog del producto y priorizar las tareas según el valor que aportan al cliente. El Scrum Master facilita el proceso y asegura que el equipo siga los principios ágiles, mientras que el equipo de desarrollo se enfoca en construir el producto según los requisitos establecidos.

El dónde y el cuándo: Estos aspectos se representan principalmente a través del Sprint, que es un ciclo de trabajo fijo, generalmente de 2 a 4 semanas, en el que el equipo trabaja en un conjunto específico de tareas del backlog. Al final de cada Sprint, se realiza una revisión del progreso, lo que permite al equipo ajustar sus métodos y estrategias para mejorar en el siguiente ciclo. Este enfoque iterativo asegura que el proyecto avance de manera constante, con oportunidades regulares para ajustes y mejoras.

El por qué y el cómo: Estos elementos representan las herramientas y métodos que los miembros del equipo de Scrum utilizan para cumplir con sus tareas. Incluyen prácticas como las reuniones diarias de pie (Daily Standups), donde se discuten los progresos y obstáculos del día, y el uso de tableros visuales como el Kanban para rastrear el estado de las tareas. Estas herramientas permiten una mayor transparencia y colaboración dentro del equipo, facilitando la identificación y resolución rápida de problemas. [26]

En resumen, Scrum es un marco de trabajo estructurado pero flexible, que optimiza la colaboración en equipo, la entrega de productos de alta calidad y la capacidad de adaptación a cambios y desafíos durante el desarrollo del proyecto.

D. Supuestos Teóricos de la Investigación.

Confidencialidad

La Seguridad y la Confidencialidad de la Información y la LORTAD “La LORTAD se refiere a la confidencialidad de los datos de carácter personal, pero puede ser una excelente oportunidad para mentalizar a los "propietarios" de la información y directivos en general, ya que muchas de las

medidas y controles pueden servir tanto para garantizar la confidencialidad como la seguridad en general, y lógicamente no sólo de los datos de carácter personal sino de todos ellos. Los objetivos de la seguridad abarcan: las personas (y funciones que desempeñan, con la debida segregación), las propias instalaciones, los equipos y comunicaciones, los programas y, muy especialmente, los datos". [27]

Según el blog de la firma -e consultorio y desarrollo TI Pilares de la Seguridad de la Información: confidencialidad, integridad y disponibilidad por firma de los datos no pueden ser expuestos a las demás personas o sistemas no autorizados para denigrar que se puede ver afectada de alguna manera. [28]

La confidencialidad ha sido definida por la Organización Internacional de Estandarización (ISO) en la norma ISO/IEC 27002 cómo "garantizar que la información es accesible sólo para aquellos autorizados a tener acceso" y es una de las piedras angulares de la seguridad de la información. La confidencialidad es uno de los objetivos de diseño de muchos criptosistemas, hecha posible en la práctica gracias a las técnicas de criptografía moderna. [29]

Información

Según Idalberto Chiavenato, la información "es un conjunto significativo de datos, es decir, reduce la incertidumbre o aumenta el conocimiento sobre algo. En efecto, la información es un mensaje que cobra sentido en un contexto dado, está disponible para su uso inmediato y orienta las acciones al reducir el nivel de incertidumbre asociado a sus decisiones." [30]

Para Ferrell y Hirt, la información "es comprender los datos y los conocimientos utilizados en la toma de decisiones". [31]

Para Weller la información "está vinculada a muchos aspectos de la sociedad que han sido, a lo largo de la historia, invisibles y permanentes, y su expresión por generación dice mucho sobre las actitudes de la sociedad hacia el control, la cultura, la política, el conocimiento y la educación." [32]

Sistema tecnológico

En el artículo de Werner Rammert explica que “La tecnología generalmente se define como un conjunto de herramientas hechas por el hombre, ya sea como un medio efectivo para un fin o como una colección de artefactos físicos. Pero la tecnología también incluye prácticas instrumentales, como la creación, fabricación y uso de vehículos y máquinas; incluir toda la información técnica tangible e intangible” [33]

La tecnología ha contribuido a mejorar la calidad de vida de las personas y de la sociedad en general, mediante la generación de máquinas, equipos, procesos, métodos, productos y servicios para facilitar el desarrollo y realización de las actividades cotidianas de las personas. [34]

Integridad

Como afirma Vyncke” la integridad trata de evitar la alteración de los datos sin que sea detectado, en otras palabras, no se puede modificar la información excepto con las credenciales apropiadas, en este caso a la legitimidad de modificar la información, por lo que se debe hacer un registro de o log que permita auditar tales cambios”, en otras palabras, la importancia de la información requerida por todo el tipo de datos para así tener una buena protección solicitada. [35]

Según Jean-François Carpentier “detectar cualquier cambio intencional o no vinculado a los datos transmitidos y almacenados”, así mismo, de acuerdo a la afirmación de Aguilera López, mediante el control de seguridad de un sistema se debe mantener de una forma discreta la confidencialidad de los datos sin ser expuestos a demás personas sin ninguna autorización. [36]

De igual manera en el artículo de Dunia Duque” un sistema integrado de gestión. Para ello se requiere partir de modelos previos, comprender las interacciones que subyacen entre los componentes y elementos que configuran el modelo, identificar posibles elementos”. [37]

Disponibilidad

En el libro de introducción a la seguridad informática afirma Aguilera López “permite que la información esté disponible cuando se requieran por entidades autorizadas el sistema debe ser capaz de verificar que el usuario acceda al sistema” según ello es necesario que las personas que

tengan acceso a ello sean personas que les permitan la manipulación de datos en el sistema con una verificación previa al uso de datos. [38]

La disponibilidad, afirma Jesús Costas Santos “la información se encuentra accesible en todo momento a los distintos usuarios autorizados hay que tener en cuenta que tanto las amenazas como mecanismos para así contrarrestarlas”. [39]

En su artículo de investigación Ciro Antonio Dussan Clavijo afirma que “Una política de seguridad para que sea efectiva, necesita contar con elementos indispensables que apoyen este proceso: La cultura organizacional, las herramientas y el monitoreo. Esto involucra la participación directa y comprometida de las personas, el diseño de planes de capacitación constante a los usuarios. La disponibilidad de recursos financieros, técnicos y tecnológicos es fundamental y sobre todo actividades de control y retroalimentación que diagnostiquen e identifiquen puntos débiles para fortalecerlos siguiendo las mejores prácticas”. [40]

Manejo de Riesgos

Según el Reporte Norton de Symantec (SYMANTEC, 2014), los ataques a la información llegaron en el año 2013 a la alarmante cifra de 378 millones de víctimas, o sea, más de un millón de personas diarias, ocasionando pérdidas cercanas a los 113 millones de dólares. [41]

Afirman Michel Miranda Cairo1*, Osmany Valdés Puga , Iván Pérez Mallea , Renier Portelles Cobas, Raúl Sánchez Zequeira “ la gestión de riesgos con un enfoque de automatización durante las etapas de operación, monitorización y revisión de un Sistema de Gestión de Seguridad de la Información” en lo dicho anteriormente es claro que si existen riesgos en la seguridad de los diferentes sistemas llevando a cabo una suma pérdida monetaria para ello es necesario seguir en diferentes etapas haciendo clara la visualización de ello. [42]

En la revista de ciencia Une mí el autor Rocha Haro, Cristhian Alexander refiere a el manejo de riesgos “la importancia en la administración de riesgos de La Seguridad Informática Tecnología la información, como estrategia del negocio a través de programas que, aunque rudimentarios de cierta forma, están evolucionando y tomando madurez.” [43]

Afirma el artículo de guía de gestión de riesgos de seguridad y privacidad de la información del Ministerio de las T.I.C “A través de esta guía se busca orientar a las Entidades a gestionar los riesgos de Seguridad de la información basado en los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad) buscando la integración con la Metodología de riesgos del DAFP. Ayudar a que las Entidades logren vincular la identificación y análisis de Riesgos de la Entidad hacia los temas de la Seguridad de la Información”. [44]

Red

El autor Areitio Bertolin, Javier “la red es una conexión atravesando un cortafuego la amenaza específica en este caso es un sujeto de red externa intenta suplantar a un sujeto de red interna” de igual manera en el libro de Javier Areitio afirma que las redes como función especial la definen como “un tipo de red posee una política de seguridad en redes, una arquitectura y un diseño del sistema coherente”. [45]

William Stallingsa comenta que un sistema de gestión de red se compone de “software y hardware adicionalmente implementados entre los componentes de redes ya existentes” en este punto de vista todo tipo de red tienen sus componentes necesarios para la revisión de componentes y su uso al momento de ser ya utilizados. [46]

En el artículo de Amelia C, Colina Rafael Belloso Chacín. Núñez Steve Universidad Rafael se analiza los que “Finalmente, todo mecanismo de protección de información en una red debe estar enmarcado dentro de una política de seguridad adecuada y consistente; el seguimiento de esta política de seguridad evitaría que las medidas de protección se vuelvan un obstáculo para el trabajo habitual con los sistemas de información, garantizando la calidad y confidencialidad de la información presente en los sistemas de la empresa”. [47]

Firewall o Cortafuegos.

En el artículo escrito por los autores Kelly Johanna Martínez Molina Javys Pacheco Meneses Isaac Zúñiga Silgado “Para la implementación de un Firewall existen algunas arquitecturas para determinar la ubicación del firewall más adecuada Arquitectura de Host de protección: posee un firewall compuesto por un Router para el filtrado de paquetes y un host bastión para el filtrado de

conexiones a nivel de circuito y aplicación" de la misma manera se puede corroborar "la implementación de un Firewall bajo plataforma Linux para dar respuesta a los problemas de seguridad informática para las PYMES. Se propone una solución para conectar un pequeño negocio a Internet, con defensa integrada, protección automática contra amenazas y necesidad de inversión y administración casi nulas" esto debido a que la implementación de los cortafuegos tiene diferentes arquitecturas y se debe utilizar la más adecuada para ello. [48]

Un Cortafuegos o Firewall "es un dispositivo de red capaz de clasificar o filtrar el tráfico que pasa, además de moverlo entre redes de forma análoga a un router" como comenta Eloy Seoane este protege de un tráfico no deseado llegue a los servidores o a los lugares principales de trabajo este es dispositivo de hardware dedicado al tráfico de toda la red. [49]

La revista Ospina, Myrian Marin, Martin, Bedoya, Guerra Gómez, " Un firewall o cortafuego es una barrera defensiva entre redes que filtra el tráfico controlando todas las comunicaciones. Para su funcionamiento se establecen reglas de filtrado las cuales definen qué paquete es recibido y cual es rechazado". [50]

Amenazas y Ataques

Un ataque informático es un intento por parte de una persona o un grupo organizado de causar daño o alterar un sistema o red por diversas razones. Dependiendo de la forma de ataque que se lleve a cabo, puede realizarlos con buenas intenciones para descubrir cuál es el agujero de seguridad o con malas intenciones para obtener información importante. [51]

Para un negocio una de las características de realizar un ataque es que los atacantes se aprovechan de una vulnerabilidad en un sistema operativo, e incluso personas que utilizan este sistema para afectar negativamente a la seguridad informática. [52]

Un ataque informático lo lleva a cabo un delincuente informático que se aprovecha de una debilidad en el sistema, el hardware y las personas que forman parte del entorno informático y de trabajo de la organización. [53]

La amenaza se puede definir como cualquier factor o acción que tiene el potencial de amenazar la seguridad de la información. Las amenazas surgen de la existencia de vulnerabilidades, es decir,

una amenaza solo puede existir si existe una vulnerabilidad explotable e incluso si la seguridad de un sistema de información está comprometida. ¿Delito o no? [54]

Amenaza

Esta situación o circunstancias no son favorables y cuando lo son pueden tener efectos negativos, tales como indisponibilidad, pérdida total o parcial de información y mal funcionamiento. [55]

Servicio

Stanton, Etzel y Walker, definen los servicios "como actividades identificables e intangibles que son el objeto principal de una transacción ideada para brindar a los clientes satisfacción de deseos o necesidades"[56]

Kotler, Bloom y Hayes, definen un servicio de la siguiente manera: "Un servicio es una obra, una realización o un acto que es esencialmente intangible y no resulta necesariamente en la propiedad de algo. Su creación puede o no estar relacionada con un producto físico". [57]

Restricción al uso del sistema

Puede establecer límites de uso para diferentes usuarios donde solo tienen acceso a ciertos procesos contenidos en un módulo o aplicación y qué acciones están permitidas en él enfatizada la necesidad de regular el software desconocido o poco confiable. Con el uso cada vez mayor de redes informáticas como Internet y el correo electrónico como herramientas comerciales y de investigación, los usuarios están expuestos a nuevas instalaciones de software de muchas maneras diferentes, generalmente un virus o un troyano, lo que dificulta que los usuarios tomen las decisiones correctas. Mediante el uso de políticas, puede proteger su computadora de software que no es de confianza y especificar qué software puede ejecutarse en la computadora. [58]

PYME

Sobre el concepto de "PYME". Por lo general, se utilizan otros criterios para determinar el tamaño de una empresa, número de empleados, volumen de ventas y valor agregado, definido como costos totales de personal, depreciación, gastos financieros, utilidad neta e impuestos. [59]

PYME definida en la ley colombiana como aquellas empresas con una fuerza laboral de menos de 200 empleados y activos totales de hasta 30.000 salarios mínimos legales mensuales vigentes. [60]

Las PYMES surgen en la década de 1950, destacándose en la producción de tejidos, madera y alimentos, al tiempo que generaban fuentes de empleo y contribuyen a reducir el índice de pobreza. Sin embargo, este sector se vio afectado por condiciones limitantes para su desarrollo, como: escasos planes de apoyo, falta de normas legales que impedían la conformación de estas empresas. [61]

Por otra parte, según la definición adoptada por la Unión Europea (UE) Cuarta Directiva de Sociedades, se considera pequeña a una empresa cuando tiene menos de 50. empleados, su patrimonio neto no supera los 1,2 millones de euros y sus ventas no superan los 1,2 millones de euros. No dejará de llegar a los 5 millones. medianas empresas son aquellas con una plantilla de 50 a 250 empleados, con activos netos entre 1,2 y 2,7 millones de euros y ventas entre 5 y 10,7 millones. Las principales empresas, según esta misma directiva, son con una plantilla de al menos 250 trabajadores, activos netos superiores a 2,7 millones de euros, y con ventas superiores a 10,7 millones. [62]

Ransomware

El Ransomware es un programa malicioso diseñado para bloquear el acceso a documentos o en algunos casos al sistema operativo, el atacante logra tomar una imagen que afecta uno de los tres pilares de la seguridad informática, la disponibilidad, este tipo de ataque bloquea el acceso mediante el cifrado de archivos, donde el atacante conoce la clave de cifrado, luego le pide a la víctima una cierta cantidad (en criptomoneda) para que vuelva a emitir la contraseña de acceso al archivo (cifrado de clave). [63]

Un Ransomware (del inglés ransom, rescate y ware, software) es un tipo de malware que restringe o bloquea el acceso a ciertos componentes o archivos del sistema infectados y exige "rescate" para liberarlos. [64]

El Ransomware usa las debilidades del sistema operativo, a menudo con la ayuda involuntaria del usuario, para tomar el control del sistema y darle al desarrollador del sistema la capacidad de bloquearlo, lo que generalmente ocurre automáticamente. [65]

Raspbian

En Raspberry pi se pueden instalar varios sistemas operativos adaptadas como Ubuntu, Windows 10, servidores multimedia, entre otros. Raspbian es el sistema operativo basado en la distribución de GNU/Linux Debian. Raspbian cuenta en su web oficial de Raspberry Pi de dos versiones diferenciadas principalmente el entorno gráfico o modo consola.[66]

Raspberry PI

La tarjeta Raspberry PI es un dispositivo que cuenta con todas las características de un mini ordenador personal que proporciona un procesador ARM, memoria RAM DDR, una GPU, puertos USB/UART y puertos de entradas y salidas digitales GPIO, audio, salida de video HDMI y composite y slot para tarjeta SD, y tiene un entorno de propósito general de programación de alto nivel, denominado Python, el cual cuenta con varias características generales que lo hacen especial, por ser fácil de leer y simple de implementar, además de ser un código abierto (de libre uso). [67]

Raspberry Pi es una placa reducida, de bajo costo desarrollada en el Reino Unido por la fundación “Raspberry Pi”, con el objetivo de estimular la enseñanza de ciencias de la computadora en las escuelas y universidades. [68]

GNU/Linux

GNU es un sistema operativo de software libre, es decir, respeta la libertad de los usuarios. El sistema operativo GNU consiste en paquetes de GNU (programas publicados específicamente por el proyecto GNU) además de software libre publicado por terceras partes. El desarrollo de GNU ha permitido que se pueda utilizar un ordenador sin software que atropelle nuestra libertad.[69]

Software libre

El software respeta las libertades de los usuarios y de la comunidad. En general, esto significa que los usuarios son libres de ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software. Es decir, el "software libre" tiene que ver con la libertad, no con el precio. Para entender el concepto. [70]

Según Argudo (2004), el término software libre se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software. Específicamente, aborda cuatro libertades para los usuarios del software:

ejecutar el programa para cualquier propósito, operaciones de programas de estudio para adaptarse a cualquier necesidad, copias redistribuidas; y mejorar el programa y poner las mejoras a disposición del público.

Por libertad de uso de un programa se entiende la libertad de cualquier persona u organización para usarlo en cualquier tipo de sistema informático y para realizar cualquier tipo de trabajo, sin obligación, debiendo notificar dicho uso y disposición al desarrollador o a un propietario particular.

Libre para hacer cambios y usarlos privadamente en un contexto de trabajo o de ocio, sin obligación de notificar cambios o requerir autorización especial.

El usuario tiene la libertad de distribuir copias, sea con o sin modificaciones. Esto incluye tanto las formas binarias o ejecutables del programa, como su código fuente, sean versiones modificadas o sin modificar (distribuir programas de modo ejecutable es necesario para que los sistemas operativos libres sean fáciles de instalar).

Para que el ejercicio de las libertades de realizar modificaciones y publicar versiones mejoradas del programa tengan sentido, se tendrá acceso al código fuente del programa. Por lo tanto, el acceso al código fuente es una condición necesaria para que se hable de software libre. [71]

Hardware libre

Open Source Hardware (OSHW) es hardware cuyo diseño se hace público para que cualquier persona pueda estudiarlo, modificarlo, distribuirlo, realizarlo y venderlo, tanto original como otros objetos basados en el dispositivo siguiente. Las fuentes documentales (entendidas como archivos fuente) deben estar disponibles en un formato adecuado para que puedan ser modificadas. [72]

El hardware abierto es un enfoque de desarrollo en el que los dispositivos se fabrican "con el código fuente, la especificación del proceso de fabricación y el diseño conceptual disponible de forma que proporcionen: libertad de uso, investigación y modificación, mejora de la distribución y redistribución" (Desarrollo de hardware libre Plataforma, 2012a). Esto significa que un desarrollo de este tipo permite que cualquier persona tenga libre acceso a los recursos de diseño y programación para replicar o mejorar la fabricación de un dispositivo. [73]

Modelo TCP/IP

El diseño del modelo TCP/IP es la idea de que dos dispositivos en una red pueden comunicarse entre sí independientemente de la ubicación geográfica donde residen, y para ello no son necesarios los dispositivos involucrados, se debe entender cómo funciona el sistema subyacente. Ni tecnología de red u operaciones requeridas para completar el proceso. Para ello, el sistema se apoya en la interconexión de redes independientes.

Para lograr los objetivos de diseño necesarios, el modelo TCP/IP se define en cuatro capas y cada capa corresponde a uno o más modelos OSI.

Capas:

1) Capa de aplicación

2. Capa de transporte

3. Capa de red

4. Capa de enlace [74]

E. Variables de estudio

- Variable independiente

Prototipo de seguridad perimetral

- Variable dependiente

Tiempo de latencia.

Usabilidad del software.

Eficiencia de las reglas

F. Definición nominal de variables

- Variable dependiente

Tiempo de latencia

La latencia, en términos informáticos, se define como el tiempo transcurrido entre un comando y la respuesta que se produce a este en particular. Continuando con ello la latencia se mide en unidades de tiempo, más precisamente milisegundos o microsegundos, ya que el segundo sería una medida demasiado alta para aplicarla a sistemas de microinformática.

Con la latencia se mide el tiempo esperado desde que se da el comando hasta que se obtiene la respuesta, ya sea en forma de información en la computadora o en movimiento. [75]

Usabilidad del software

Es un atributo cualitativo generalmente definido como la facilidad de uso, ya sea un sitio web, una aplicación informática o cualquier otro sistema que interactúe con el usuario. El concepto

suele hacer referencia a una aplicación o dispositivo informático, de igual modo también se puede aplicar a cualquier sistema diseñado para un fin específico, este cubre los métodos de mejora de la usabilidad durante el proceso de diseño. [76]

Eficiencia de las reglas

Las reglas (rules) son acciones que se configuran en cadena o serie. Proteger la integridad y privacidad almacenada en el dispositivo de seguridad perimetral. [77]

- Variable independiente

Prototipo de seguridad perimetral

La importancia de la seguridad perimetral para las empresas como lo resalta Luis Puente dentro de ellas es llevar a cabo una seguridad preventiva permitiendo aislar diferentes zonas, para evitar entradas extrañas, esto permite contar como una barrera virtual que para detectar y prevenir la presencia de todas las series de amenazas que se presentan. La importancia de la seguridad perimetral para las empresas - SI-MAD por otra parte La seguridad perimetral es el establecimiento de controles para garantizar que la información y los sistemas dentro de la infraestructura tecnológica de una organización no sean pirateados o accedidos desde redes no confiables. Por ejemplo, el acceso a los recursos corporativos, la seguridad e integridad de la información intercambiada o la disponibilidad de los sistemas controlados. Por tanto, es un elemento importante de la ciberseguridad en las empresas. [78]

- Definición operativa de variables

Tiempo de latencia: se define como el tiempo transcurrido entre él envió de paquetes hasta que se da la respuesta, en la simulación se establece valores de tiempo de un ping inferior a 20 ms, desde el envío de paquetes y un tiempo de respuesta del dispositivo de seguridad

TABLA I. TIEMPO DE LATENCIA

Inestable	Estable

Autoría Movistar [79] url: https://ww2.movistar.cl/blog/post/que-es-la-latencia

Nota: Usabilidad: se establecen parámetros para medir interacción del usuario con la Raspberry Pi y la facilidad de detección de intrusos en el dispositivo.

TABLA II. USABILIDAD

Usabilidad del dispositivo		
Difícil	Entendible	Fácil

Nota: Eficiencia de las reglas: Teniendo en cuenta las configuraciones de la Raspberry Pi, para proteger la integridad de las empresas, se establecen mediciones para observar el cumplimiento de las reglas en el dispositivo.

TABLA III. EFICIENCIA DE LAS REGLAS

Cantidad	Cumplen	No cumplen

G. Formulación de hipótesis

1) Hipótesis de investigación

El dispositivo de seguridad perimetral basado en software y hardware libre permite agilizar los procesos de seguridad en la información del área TI en PYMES de San Juan Pasto.

2) Hipótesis nula

El dispositivo de seguridad perimetral basado en software y hardware libre para PYME de San Juan Pasto no agiliza los procesos de seguridad en la información del área TI (Tecnología de Información).

3) Hipótesis alterna

El sistema de seguridad perimetral de software y hardware libre logra reducir en parte el costo en la compra de dispositivos requeridos en las PYME de la ciudad de San Juan Pasto.

III. METODOLOGÍA

A. Paradigma

El paradigma propuesto para esta investigación es el denominado paradigma positivista, ya que se basa en observación directa verificando teorías para poder identificar causas reales, como afirma Quijano una investigación cuantitativa, que se entiende como conocimiento científico para esta investigación se aplica dicho método ya que se realiza el conocimiento a través de la observación directa explicando los fenómenos observados [80]

B. Enfoque

El enfoque de esta investigación es cuantitativo, según Sampieri se basa en la forma deductiva y lógica, buscando preguntas o hipótesis que comprueban dicha investigación, dado el caso un análisis de datos puede servir a la recolección de información en dicho proceso y contestar lo planteado previamente para ayudar a resolver dudas concretas.[81]

C. Método científico

El método científico conforme a Westreicher, es una técnica que ayuda a acercarse a la realidad, con un conocimiento que siempre es válido desde el punto de la ciencia, la observación es prioritaria puesto a que se adquiere una información real para encontrar alguna relevancia que merece dicha investigación.[82]

D. Tipo de investigación

Esta investigación es de tipo longitudinal porque se centra en observar la evolución de una serie de variables a lo largo del tiempo y cuantitativa porque los datos son medibles y cuantificables. Permitiendo realizar un análisis descriptivos e inferenciales. Utilizando herramientas de estudio, permitiendo conocer de forma real las falencias para ello conocer su efectividad y analizar el tráfico que existe en la red. [83]

E. Diseño de investigación

El diseño de esta investigación es cuasiexperimental ya que permite la manipulación de una o más variables independientes, según la implementación del instrumento de recolección de datos,

se medirá las vulneraciones o falencias que tienen las empresas y lograr un ambiente controlado de laboratorio donde se explote las vulnerabilidades encontradas, facilitando así las diferentes pruebas en el software tanto con lo experimental como sin él, además de ello permite una preprueba y una posprueba, lo cual otorga una comparativa de resultados que van a permitir evaluar la herramienta software en el proceso de identificar habilidades como también un nivel de aprendizaje, de igual manera una causa y efecto en las PYMES es decir evaluar cómo están las empresas en el torno a la seguridad informática antes de implementar el dispositivo y el efecto de ellas después. [84]

F. Población

Para esta investigación se cuenta con pequeñas, microempresas (PYMES) en San Juan de Pasto con un total de 1.046 que se encuentran registradas en la cámara de comercio. [85]

G. Muestra

La muestra respectiva de la cámara de comercio de Pasto en el año (2021) se observa que el 95.92% corresponde a Micro empresa, la pequeña empresa corresponde a 3.1%, la mediana empresa es un 0.78% y la gran empresa es de apenas un 0.14%. Esto indica que la micro empresa es la base empresarial y por ende la generadora de empleo del departamento.

Para esta investigación se cuenta con las pequeñas y medianas empresas correspondiente a 1046, se aplica la fórmula de la muestra finita y para el cálculo se utiliza la macro en Excel, tomando un tamaño de universo de 1046, una probabilidad del 0,9, dando los resultados: nivel de confianza del 90% y un error de 5.0%, para ello una muestra del 89. [86]

Matriz de Tamaños Muestrales para diversos margenes de error y niveles de confianza, al estimar una proporción en poblaciones Finitas

N [tamaño del universo]	1.046
p [probabilidad de ocurrencia]	0,9

Escriba aquí el tamaño del

Escriba aquí el valor de p

Nivel de Confianza (alfa)	1-alfa/2	z (1-alfa/2)
90%	0,05	1,64
95%	0,025	1,96
97%	0,015	2,17
99%	0,005	2,58

Fórmula empleada

$$n = \frac{n_o}{1 + \frac{n_o}{N}} \quad \text{donde:} \quad n_o = p^*(1-p)^* \left(\frac{Z\left(1-\frac{\alpha}{2}\right)}{d} \right)^2$$

Matriz de Tamaños muestrales para un universo de 1046 con una p de 0,9

Nivel de Confianza	d [error máximo de estimación]									
	10,0%	9,0%	8,0%	7,0%	6,0%	5,0%	4,0%	3,0%	2,0%	1,0%
90%	24	29	37	47	63	89	132	214	383	730
95%	33	41	51	66	88	122	179	281	473	803
97%	41	50	62	80	106	146	211	325	526	839
99%	57	69	86	109	144	195	276	407	616	891

Fórmula tamaño de la muestra [fig. 1]

Con lo anterior se puede obtener una caracterización de las PYMES, para realizar un ambiente simulado de laboratorio, teniendo en cuenta la encuesta que se aplicará.

H. Técnicas de recolección de la información

La técnica de recolección para esta investigación como referente Sanchez, Revilla,Alayza, Sime, Mendivil y Tafur en 2020 afirma que “las encuestas en línea tienen mayor rentabilidad debido a que no es necesario el monitoreo durante el periodo de recolección de datos y se puede obtener los datos en un tiempo real ” de igual manera Westreicher, recolecta información tanto cualitativa como cuantitativa a diferente tipo de personas de igual manera se puede medir estadísticamente logrando lo requerido en la encuesta.

Por lo cual en esta investigación a su importancia en vista de que se hará en un entorno controlado de PYME se verificará sus debilidades y se podan sacar datos estadísticos de gran ayuda para obtener lo requerido actualmente se realizan las encuestas en línea con la facilidad e ser diligenciada por el tipo de personal que se necesite.[87]

1) Validez de las técnicas

Los instrumentos para la recolección serán validados por expertos precedentes de la Universidad CESMAG, teniendo en cuenta los siguientes perfiles: Germán Augusto Mora Ruiz ingeniero de sistemas de igual manera Alex Urbina profesor de seguridad informática.

2) Confiabilidad de la técnica

La confiabilidad de las técnicas de recolección es fiable ya que se ha dado a partir del juicio previo de un experto, para que garantice a los usuarios (PYMES) una mejora de la seguridad informática en el área TI, la realidad del proceso de la investigación es su confiabilidad. Para ello se realizan las encuestas en línea anteriormente mencionadas por los autores Revilla,Alayza, Sime ,Mendivil y Tafur en 2020 “ya que es necesario un monitoreo constante real y verificado con técnicas de recolección de información”. [88]

I. Instrumentó de recolección de datos

El instrumento de recolección de datos es el cuestionario, que se usa para recolectar información medible, necesaria para la investigación, obteniendo datos reales del problema a investigar.

“Un cuestionario consiste en un conjunto de preguntas, en donde se obtiene información acerca de las variables a estudiar, puede ser aplicado personalmente o por correo y en forma individual o colectiva. Debe ser congruente con el planteamiento del problema e hipótesis”. [89]

Según Schwaber y Sutherland (2013), “el equipo de Scrum elige la mejor forma de llevar a cabo su trabajo, y no es dirigido por personas externas al equipo” [100]. El Scrum Team, está conformado por un Dueño del producto, el Equipo de desarrollo y un Scrum Master; a los cuales definen de la siguiente manera:

- Scrum Team
  José Fernando Imbajoa S.
- Product Owner
  Martha Lisbeth Buritica L.
- Scrum Master

Luis Arnoby Escobar H.

Jose Fernando imbajoa S.

IV. RESULTADOS DE LA INVESTIGACION

A. Documentación de pruebas.

Con el presente informe, se da inicio a la fase de Documentación de Pruebas. Durante esta etapa, se caracteriza los procesos de información en PYMES según el tipo de muestra dada en la investigación para la ciudad de San Juan de Pasto.

TABLA IV. ANALISIS DE ENCUESTA

No	Descripción	Duración	Necesidad desarrollo (1-10)	Prioridad (1-100)	Complejidad
1. Desarrollo del formulario	Crear encuesta para obtener datos sobre las PYMES de San Juan de Pasto	1 semana	10	100	Baja
2. Petición para aplicar la prueba	Redacción de una carta al Decano de Ingeniería de Sistemas para desarrollar el primer objetivo: caracterizar los procesos de información en PYMES según la muestra establecida en San Juan de Pasto.	1 Dia	10	100	Media
3. Petición para realizar encuesta a las empresas	Con el permiso del director y el decano, se realizó un acercamiento a la Cámara de Comercio de Pasto y ACOPI, quienes respondieron con una espera para la realización de la encuesta. Ambas cartas tienen acuse de recibo con fecha del 1 de septiembre de 2022.	1 Dia	10	100	Media

4. Aplicación de una Encuesta.	Se aplicó una encuesta a seis personas, internas y externas a la Universidad CESMAG, algunas con conocimiento en informática y otras sin experiencia en el tema. Esto permitió obtener correcciones generales sobre términos técnicos y aspectos de privacidad empresarial.	1 semana	10	100	Media

Una vez aplicado los instrumentos de recolección de la información, se procedió a realizar el tratamiento correspondiente para el análisis de los mismos, al proyecto de grado titulado Gestión de Seguridad Informática en Entorno Controlado de Pymes de San Juan de Pasto mediante un Dispositivo de Seguridad Perimetral usando Software y Hardware Libre.

1. ¿Existe un área informática?

La mayoría de empresa si cuenta con un área de informática con un 80%, esto a que se logró una gran acogida a esta área en la parte laboral por diferentes procedimientos que pueden venir surgiendo dentro de la empresa con el efecto de realizar procesos o actividades a mano. esto ya que poco a poco se ha ido implementado de manera importante de esta área informática comenzaran hacer bien valoradas por la sencilla razón de un mejoramiento general de control y el 20 % no cuenta con esta área.

2. ¿El área de informática tiene dependencia encargada de la seguridad informática?

Es muy importante destacar en esta pregunta ya que esto fue un 50% que sí cuentan con esta dependencia y el otro 50% no cuentan con ella , La información es uno de los recursos más relevantes de una empresa, esta se encarga de conectar cada una de las áreas del negocio, De ahí surge la importancia de la seguridad informática de las empresas: la información es valiosa y debe ser protegida de forma adecuada caso contrario se perdería la información de ellas ya que no conocen el riesgo que puede esto estar causando.

3. ¿Tienen políticas de navegación en internet?

El 70% de ella cuenta con las políticas de navegación entre ellas el 30% no cuenta con ellos con lo que se miraría factible dar a conocer acerca de los diferentes riesgos que corren al no tener ciertas políticas.

4. La empresa bloquea contenido relacionado con:

YouTube, Spotify, Video juegos, Páginas para adultos esto a que un 30% restringen dichas páginas en el entorno laboral, Videojuegos, Paginas para adultos el 20% junto a ella el que la empresa No bloquea contenidos en ello se mira de una manera mucho más investigativa lo que es el 10% al Spotify, Video juegos, Páginas para adultos y de misma manera el 10% no bloquean las páginas para los adultos.

5. ¿Tiene conocimiento sobre ataques informáticos?

El porcentaje de las empresas que conocen de ciertos ataques informáticos con un 90% los que poseen el conocimiento y así poder tener algunas directrices para proteger dicha información, el 10% no tiene conocimiento alguno.

6. ¿Actualmente su empresa cuenta con un antivirus en sus equipos?

En las opciones que se requiere con negación de No un 10% si cuentan con ello No lo sé con un 20% y el sí con un El 70% de las personas cuentan con ello y asegura que si tiene conocimiento.

7. ¿Qué software antivirus utilizas?

Los que se dieron a conocer en el resultado de las encuestas con 360 security un 10% a ello Avast 10%, Cybereason 10% con un mayor uso de antivirus está McAfee con un 20% del personal que habitualmente lo utiliza McAfee, Avast, Microsoft Defender 10%, McAfee, Microsoft Defender 10% las personas que no tienen conocimiento de ello No lo sé es un 20% , SOPHOS 10%

8. ¿Con qué frecuencia actualizas un software antivirus?

De vez en cuando con un 10%, De vez en cuando, cuando recuerdo 10%, la frecuencia automática de la actualización de los antivirus es un 80%.

9. ¿Generalmente realizan copias de seguridad a la información?

La importancia de ello con las opciones de Frecuente es un 10%, Muy frecuente y Poco frecuente es entre los mayores porcentajes con un 40% y 40% y de la manera en que no realizan las copias de seguridad se cuenta con un 10%

10. ¿Cada cuánto tiempo realizan copias de seguridad de su Empresa?

Entre los menores porcentajes de las opciones que se pudieron verificar Anual lo hace un 10% de las opciones Diario Mensual y Semanal se establece un 30% para cada una de ellas.

11. ¿Usted es consciente de la importancia de los datos generales de la empresa?

Las opciones que se presentaron en ellas fueron positivas con un Importante la cual cuenta con un 20% y la Muy Importante con un 80% esto a que las empresas son algo conscientes de la información que tienen ellas del riesgo de perder la información

12. ¿Permitiría que personas enfocadas a la parte de seguridad de acceso hacer cierto tipo de pruebas para verificar que tan íntegra es la seguridad de su información dentro de Empresa?

Esta pregunta fue muy importante para laborar nuestro proyecto la cual se pudo verificar que No acepto un 80% no acepta que personas diferentes a ellas manipulen cierto tipo de información, Acepto 30% esto a que restringen cierto tipo de información fue muy difícil que las empresas nos permitan la práctica del proyecto para ello se realizará un entorno controlado de PYMES para llevar a cabo el proyecto.

En la siguiente etapa se tiene en cuenta la revisión de expertos para tener claridad de las preguntas que se va a realizar a las PYMES de san juan de pasto.

TABLA V. REVISIÓN DE EXPERTOS

No	Descripción	Duración	Necesidad desarrollo (1-10)	Prioridad (1-100)	Complejidad
1. Revisión de expertos.	La revisión de expertos se realizó con el asesor del proyecto de grado, Germán Mora, quien nos brindó pautas clave para ajustar la encuesta final. Se corrigieron seis puntos de forma verbal para mejorar la claridad de la encuesta, considerando observaciones de personas no familiarizadas con la seguridad informática.	1 semana	10	100	Media

Se llevó a cabo un estudio con enfoque en las pequeñas y medianas empresas (PYMES) de la ciudad de San Juan de Pasto, para el cual se diseñó una encuesta utilizando la fórmula de población. Esta herramienta fue aplicada con el objetivo de recopilar información relevante para el análisis del comportamiento empresarial en la región. Posteriormente, el contenido y metodología de la encuesta fueron revisados por un experto, quien en este caso fue el asesor del proyecto. Como resultado de esta revisión, se validó la pertinencia de los datos recolectados. En el anexo del presente informe, se adjunta la firma del asesor que certifica haber realizado la revisión, así como una copia de la encuesta aplicada a las PYMES.

Se anexa la firma del cuestionario validado por el Asesor del proyecto de grado – fig. 2

TABLA VI. APLICACIÓN DE ENCUESTA

No	Descripción	Duración	Necesidad de desarrollo (1-10)	Prioridad (1-100)	Complejidad
1. Aplicación de Encuesta. Anexo3*	Se realiza la encuesta a las PYMES de San Juan de Pasto	2 semanas	10	100	Alta

*En Anexos se encuentra Anexo. 3 - Encuesta

B. Desarrollo de producto tecnológico

En el desarrollo del producto tecnológico se tomó como metodología SCRUM por su agilidad en la gestión de proyectos cortos, iniciando con los requerimientos.

TABLA VII. REQUERIMIENTOS FUNCIONALES Y NO FUNCIONALES

No	Descripción	Duración	Necesidad de desarrollo (1-10)	Prioridad (1-100)	Complejidad
1	Se especifica el tipo de requerimientos que especifica el cliente para la funcionalidad del producto	1 semana	10	100	Media

Debido a la importancia de la seguridad informática en las PYMES se optó por analizar las encuestas realizadas a las empresas y sugerir los siguientes requerimientos para el dispositivo de seguridad perimetral.

1) Requerimientos funcionales

- Identificación de los posibles puntos de acceso de la red y monitorización de tráfico en estos puntos.
- Detección de intrusiones en la red y generación de alertas en tiempo real para notificar al equipo de seguridad.
- Capacidades de firewall, incluyendo permitir o denegar el acceso de ciertas direcciones IP, puertos, y protocolos de red.
- Filtrado de contenido para prevenir ataques por medio de malware y virus.
- Prevención de ataques de denegación de servicio (DoS).
- Monitoreo de la red y análisis de tráfico para detectar posibles anomalías.
- Implementación de autenticación, autorización y control de acceso (AAA) para gestionar la seguridad en la red.

2) Requerimientos no funcionales

- Escalabilidad, el software debe ser capaz de manejar y procesar grandes cantidades de tráfico de red.
- Rendimiento, el software debe ser capaz de analizar el tráfico de red en tiempo real y sin retrasos significativos.
- Disponibilidad, el software debe estar disponible en todo momento para asegurar la seguridad de la red.
- Seguridad, el software debe cumplir con los estándares y regulaciones de seguridad relevantes, y asegurar la confidencialidad, integridad y disponibilidad de los datos.
- Usabilidad, el software debe ser fácil de usar para el equipo de seguridad y administradores de red que lo utilizan.
- Mantenimiento y soporte, el software debe ser fácil de actualizar y mantener, y el proveedor debe ofrecer soporte técnico y actualizaciones de seguridad periódicas.

Teniendo en cuenta los requerimientos del producto tecnológico se desarrolla lo siguiente:

TABLA VIII. PRODUCT BACKLOG

No	Descripción de la H. U	Duración	Necesidad de desarrollo (1-10)	Prioridad (1-100)	Complejidad
1	Preparación del entorno del sistema operativo Linux	5 horas	10	100	ALTA
2	Creación de roles para el ingreso a la aplicación web	4 horas	10	100	ALTA
3	Panel de inicio de sesión de la aplicación	3 horas	10	100	ALTA
4	Menú para administrar los usuarios	1 hora	6	60	MEDIA
5	Menú de administración de reglas nftables	1 semana	10	100	ALTA
6	Menú de alertas de suricata	2 semanas	10	100	ALTA
7	Menú para el Dns	2 semanas	10	100	ALTA

En este proceso se desarrolla las historias de usuario para el proyecto de seguridad perimetral con reglas de *nftables*. Este proyecto, implementado en Django, permite el procesamiento y la visualización de logs de Suricata, así como consultas DNS y monitoreo de tráfico en tiempo real. Las historias de usuario que se creó tienen como objetivo especificar, desde la perspectiva del usuario final, las funcionalidades y los requisitos clave de la aplicación.

TABLA IX. HISTORIA DE USUARIO: CREACIÓN DE ROLES

Historia de usuario					
Código			HU002		
Nombre			Inicio de sesión		
Actor			Usuario (Administrador)		
Descripción			Inicio de sesión para el administrador		
HU Relacionada(s):	HU003	Código:	HU003	Nombre	Inicio de sesión
Módulo			Módulo inicio de sesión		
Criterios de aceptación	Condición		Resultados		
	Se administra usuario y contraseña para el ingreso		Entrada a la página principal		
Excepción	No guardar usuario en la base de datos				

TABLA IX. HISTORIA DE USUARIO: USUARIO(OPERADOR)

Historia de usuario					
Código			HU003		
Nombre			Inicio de sesión		
Actor			Usuario (Operador)		
Descripción			Inicio de sesión para el operador		
HU Relacionada(s):	HU004	Código:	HU004	Nombre	Inicio de sesión
Módulo			Módulo inicio de sesión		
Criterios de aceptación	Condición		Resultados		
	Se administra usuario y contraseña para el ingreso		Entrada a la página principal		
Excepción	No guardar usuario en la base de datos				

TABLA X. HISTORIA DE USUARIO: PANEL DE INICIO DE SESIÓN

Historia de usuario					
Código			HU004		
Nombre			Inicio de sesión		
Actor			Usuario (Operador) – Usuario (Administrador)		
Descripción			Inicio de sesión		
HU Relacionada(s):	HU002 HU003	Código:	HU002 HU003	Nombre	Inicio de sesión
Módulo			Módulo inicio de sesión		
Criterios de aceptación		Condición		Resultados	
		Se administra usuario y contraseña para el ingreso		Entrada a la página de administración	
Excepción		HU002: Usuario y contraseña no coinciden para ingresar HU003: Usuario y contraseña no coinciden para ingresar			

TABLA XI. HISTORIA DE USUARIO: ADMINISTRADOR DE USUARIOS

Historia de usuario					
Código			HU005		
Nombre			Página de administración		
Actor			Usuario (Administrador)		
Descripción			Página donde se puede administrar los usuarios		
HU Relacionada(s):	HU002	Código:	HU002	Nombre	Inicio de sesión
Módulo			Módulo página de administración de usuarios		
Criterios de aceptación		Condición		Resultados	
		Debe agregar usuarios		Inicio de sesión con credenciales	
Excepción		Error al crear usuarios y permisos			

TABLA XII. HISTORIA DE USUARIO: ADMINISTRADOR DE REGLAS

Historia de usuario					
Código			HU006		
Nombre			Página de administración		
Actor			Usuario (Administrador)		
Descripción			Página donde se puede administrar las reglas para el firewall (Agregar, eliminar y visualizar las reglas).		
HU Relacionada(s):	HU002	Código:	HU002	Nombre	Inicio de sesión
Módulo			Módulo página de administración		
Criterios de aceptación		Condición		Resultados	
		Debe agregar reglas para que el firewall funcione y acceso para agregar usuarios con restricciones		Aplicación de las reglas en la Raspberry	
Excepción		URL o Puertos no válidos y no se pueda crear las reglas, error con el sistema de alertas			

Historia de usuario					
Código			HU007		
Nombre			Página de administración		
Actor			Usuario (Operador)		
Descripción			Inicio de sesión		
HU Relacionada(s):	HU003	Código:	HU003	Nombre	Inicio de sesión
Módulo			Módulo página de administración		
Criterios de aceptación		Condición		Resultados	
		Debe agregar reglas para que el firewall funcione		Aplicación de las reglas en la Raspberry	
Excepción		URL o Puertos no válidos y no se pueda crear las reglas, error con el sistema de alertas			

TABLA XIII. HISTORIA DE USUARIO: PANEL DE ALERTAS

<table>
<tr><td colspan="6">Historia de usuario</td></tr>
<tr><td colspan="3">Código</td><td colspan="3">HU008</td></tr>
<tr><td colspan="3">Nombre</td><td colspan="3">Página de administración</td></tr>
<tr><td colspan="3">Actor</td><td colspan="3">Usuario (Operador) – Usuario (Administrador)</td></tr>
<tr><td colspan="3">Descripción</td><td colspan="3">Monitorear el tráfico de red</td></tr>
<tr><td>HU Relacionada(s):</td><td>HU002
HU003</td><td>Código:</td><td>HU002
HU003</td><td>Nombre</td><td>Inicio de sesión</td></tr>
<tr><td colspan="3">Módulo</td><td colspan="3">Módulo para monitorear el tráfico de la red en el servidor</td></tr>
<tr><td colspan="2" rowspan="2">Criterios de aceptación</td><td colspan="2">Condición</td><td colspan="2">Resultados</td></tr>
<tr><td colspan="2">Debe ingresar al administrador para verificar las alertas de ataques</td><td colspan="2">Visualizar todas las alertas</td></tr>
<tr><td colspan="2">Excepción</td><td colspan="4">Error de código o internet demasiado lento para visualizar las alertas</td></tr>
</table>

TABLA XIV. HISTORIA DE USUARIO: PANEL DE DNS

Historia de usuario					
Código			HU009		
Nombre			Página de administración		
Actor			Usuario (Operador) – Usuario (Administrador)		
Descripción			traduce los nombres de dominios		
HU Relacionada(s):	HU002 HU003	Código:	HU002 HU003	Nombre	Inicio de sesión
Módulo			Módulo para monitorear el tráfico de la red en el servidor		
Criterios de aceptación		Condición		Resultados	
		Debe ingresar al administrador para traducir los dominios		Visualizar todas las listas de los dominios	
Excepción		Error de código o internet demasiado			

Sprint 1: Preparación del entorno

En este primer sprint 1, el objetivo es configurar el entorno de desarrollo para garantizar una base sólida que permita avanzar con fluidez en los siguientes sprints. Esto incluye la instalación de las herramientas necesarias, la configuración del entorno de programación y la integración de control de versiones.

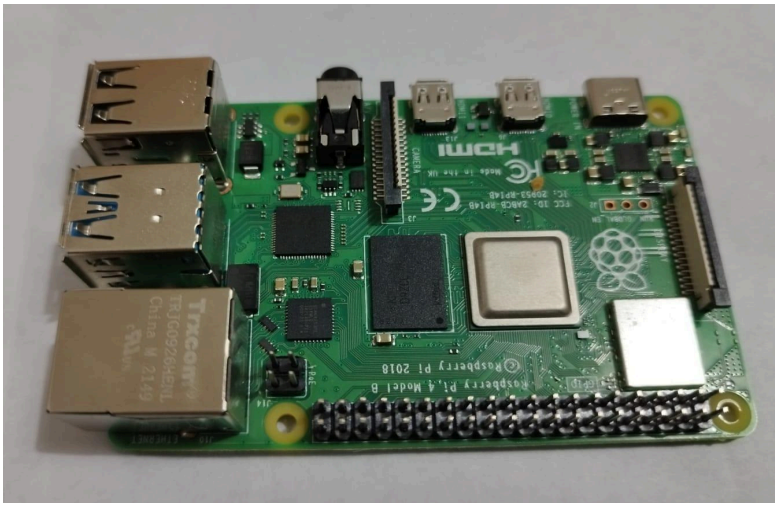


fig. 4 Raspberry Pi 4

El sistema operativo denominado Raspbian, es un sistema operativo basado en Debian, una distribución de GNU/Linux, desarrollado específicamente para funcionar bajo el computador de placa reducida Raspberry Pi, este es Open Source y gratuito, lo que implica una reducción de costos y brinda una orientación adecuada en la consecución del objetivo general del presente proyecto. Este sistema operativo cuenta con 2 versiones que pueden ser descargables fácilmente desde la página oficial del proyecto Raspberry Pi, www.raspberrypi.org, Raspbian stretch con entorno de escritorio y la versión Lite sin entorno de escritorio, para este proyecto se optó por la versión Lite debido a que la Raspberry Pi al ser un computador de placa reducida tiene limitaciones en cuanto a capacidad de procesamiento y un entorno de escritorio demandaría muchos recursos del sistema, al optar por la versión Lite se reserva todo el poder de cómputo

destinado al entorno gráfico para el análisis y filtrado del tráfico de red, brindando así un mejor desempeño y evitando la saturación del ancho de banda de la red debido a este proceso.

Para la instalación del sistema operativo Raspbian stretch Lite, fue necesario una memoria clase 10, en este proyecto se utilizó una de estas memorias con 32 gigabytes de capacidad. En esta memoria a través del programa Etcher se transfirió la imagen del sistema operativo ya previamente descargado, una vez terminado este proceso se realizaron las pruebas del correcto funcionamiento del sistema operativo, al cual se le habilito el protocolo SSH para poder ingresar a la Raspberry Pi de forma remota en el proceso de instalación y configuración tanto del sistema operativo como de los servicios de seguridad a implementar. ver figura 2

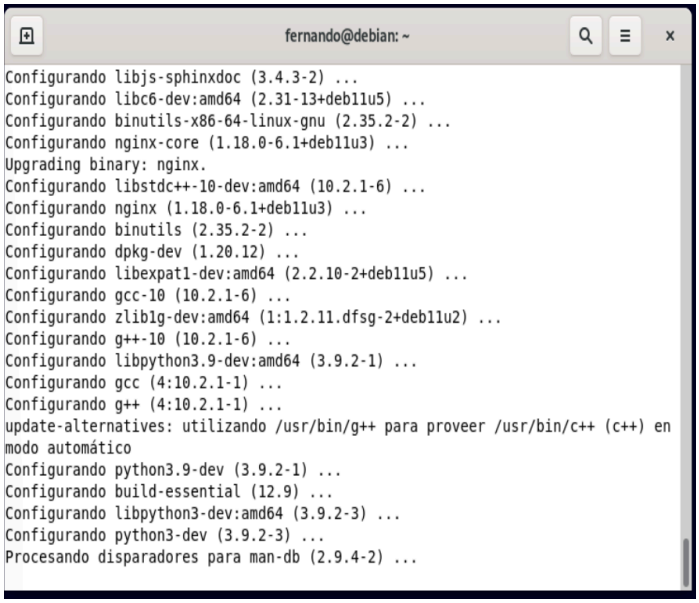


Fig. 5 - Debian en la raspberry pi

Para configurar el sitio web en Django fue necesario instalar el sistema operativo Django en su nueva versión, python3 y sqlite3 con los siguientes comandos:

- Instalar Python3, Django y SQLite:

sudo apt-get install python3 python3-pip sqlite3

sudo pip3 install django

- Verifica si Django y SQLite están instalados correctamente:

python3 -m django --version

sqlite3 –versión

Sprint 2: Creación de roles

Siguiendo las configuraciones se debe tener en cuenta la creación de los roles para el ingreso al administrador de Django; Para crear un usuario administrador (superusuario) en un proyecto Django desde la consola en Linux, sigue estos pasos:

1. Abre una terminal en tu sistema Linux.

2. Navega al directorio raíz de tu proyecto Django. Puedes hacerlo utilizando el comando `cd` y especificando la ubicación de tu proyecto.

3. Activa tu entorno virtual si estás utilizando uno. Puedes hacerlo con el siguiente comando:

source ven/bin/activate

Reemplaza "source ven/bin/activate″ con la ruta real a tu entorno virtual.

4. Una vez que estés dentro del entorno virtual (si es necesario), ejecuta el siguiente comando para crear un usuario administrador:

Python3 manage.py createsuperuser

5. A continuación, se te pedirá que ingreses un nombre de usuario, una dirección de correo electrónico y una contraseña para el usuario administrador. Debes proporcionar esta información cuando se te solicite.

6. Después de ingresar la información requerida, el comando creará el usuario administrador y te mostrará un mensaje de confirmación de que se ha creado correctamente.

Ahora has creado un usuario administrador en tu proyecto Django que puede acceder al panel de administración y realizar tareas de administración. Puedes iniciar el servidor de desarrollo de Django utilizando **`python3 manage.py runserver 0.0.0.0:8000/admin`** y acceder al panel de

administración en tu navegador ingresando la URL ***"http://localhost:8000/admin/"*** (reemplaza "localhost:8000" con la dirección y puerto del servidor si son diferentes). Luego, inicia sesión con las credenciales del usuario administrador que acabas de crear.

Se aprecia un panel de inicio en la figura 3 de sesión donde se registra el usuario creado anteriormente para ingresar al administrador donde se puede configurar nuevos usuarios con permisos de administrado u operadores.

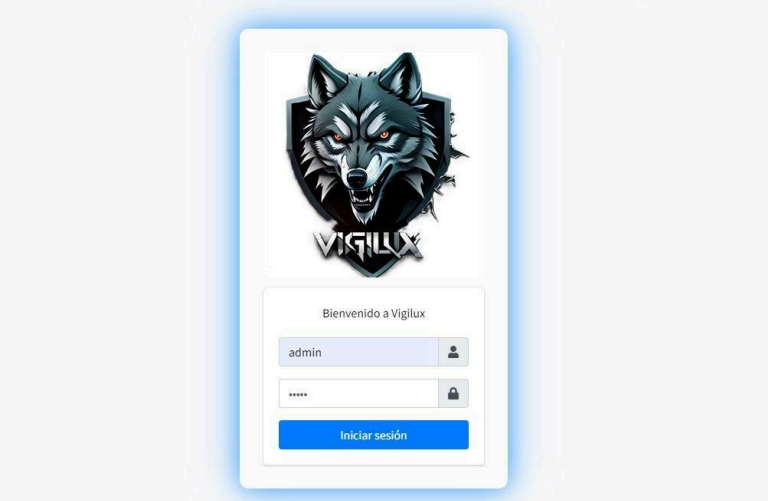


Fig. 6 – Panel de inicio de sesión

En la figura 7 se visualiza el panel de administración de roles dentro de la aplicación de Django, tener en cuenta los tipos de usuarios que desea crear y otorgar permisos.

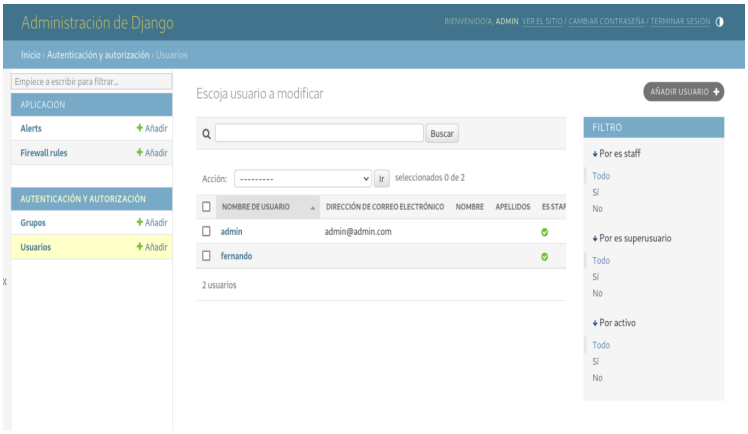


Fig. 7 – Administrador de Django

Sprint 3 – Sprint 4: Inicio de sesión y Administrador de reglas

El siguiente paso fue crear el entorno donde se va a trabajar el firewall y el script para que se ejecuten en la Raspberry Pi de manera automatizada.

Para facilitar la administración de los servicios instalados y configurados en este proyecto se creó un programa en Django a ejecutar en un entorno visual que ofrece dos funcionalidades, este programa se lo denominó “Secure Django”.

Como se aprecia en la figura 5 y 6 ofrece funcionalidades de configuración para firewall y un inicio de sesión para el administrador donde puede bloquear puertos y Dominios, basta con tan solo dar clic en cada opción correspondiente para ingresar a las funcionalidades que ofrece la aplicación.

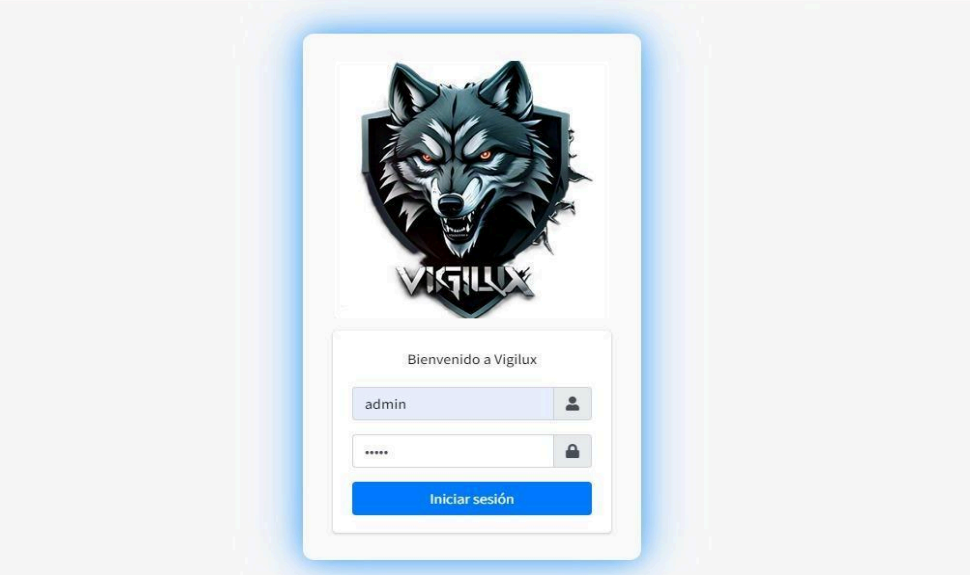


Fig. 8 – Inicio de sesión

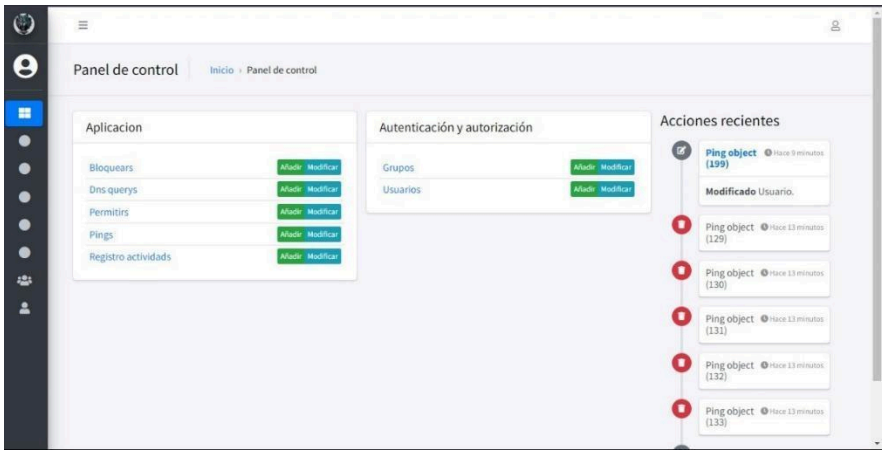


Fig. 9 – Panel de administrador

El administrador de Django es una interfaz de usuario que permite gestionar los datos del sitio web de manera fácil y rápida. Con él, se crea, lee, actualiza y elimina los puertos y Dominios en la base de datos sin necesidad de escribir código. Es una herramienta completa y útil para el desarrollador web que trabajó con Django, ya que permite realizar tareas de administración sin tener que crear una interfaz desde cero.

Dentro del sistema operativo utilizamos el siguiente script para obtener lo que se encuentra en la base de datos como se observa en las siguientes figuras 10 y 11

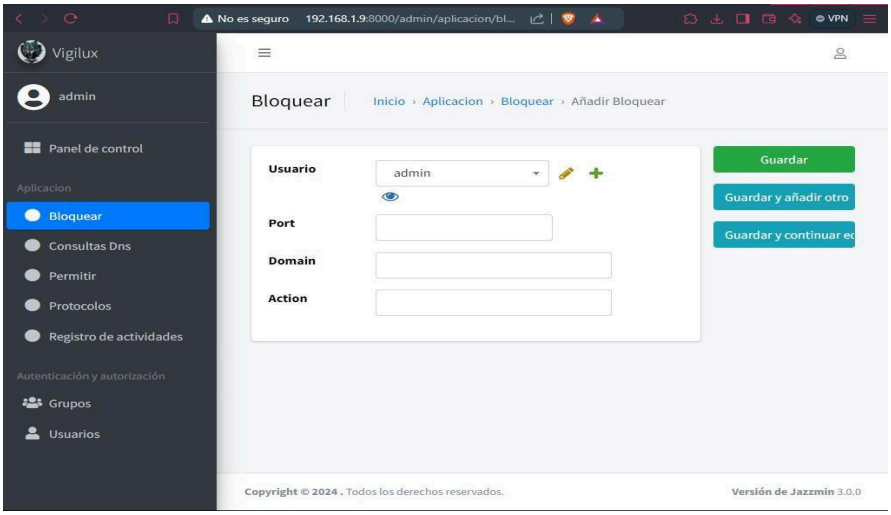


Fig. 10 – Panel para añadir la regla

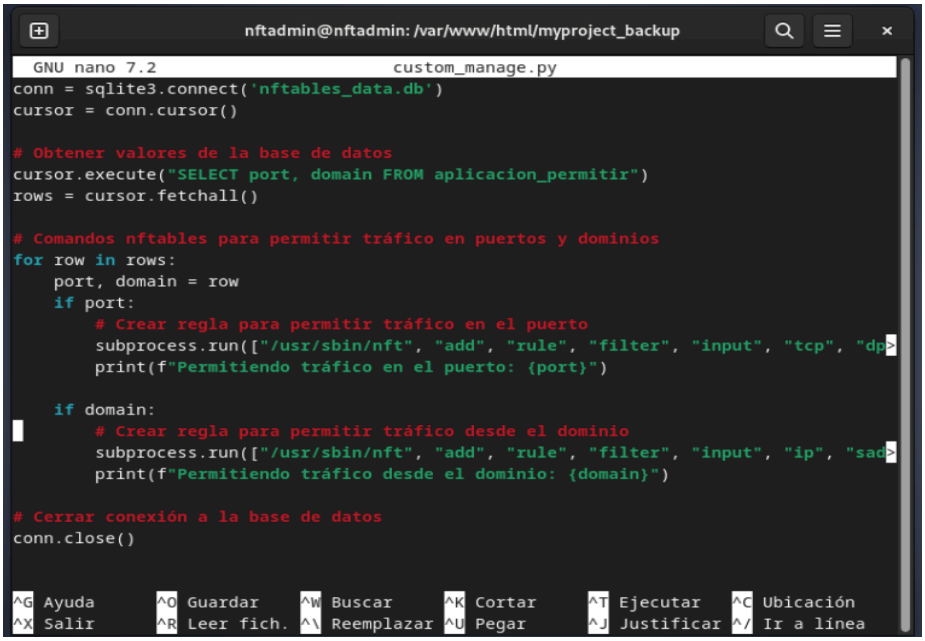


Fig. 11 – Script para bloquear dominios

El siguiente paso en el desarrollo es crear una vista dentro del administrador de Django que gestione las reglas de tráfico de red. Esta vista permitirá monitorear y configurar los permisos de acceso para proteger el perímetro de la red de manera eficiente.

Pasos:

A. Definir la Vista en Django: Se crea una vista personalizada dentro de Views.py para controlar las reglas de tráfico de red, utilizando el framework de Django y su integración con los modelos ya existentes.

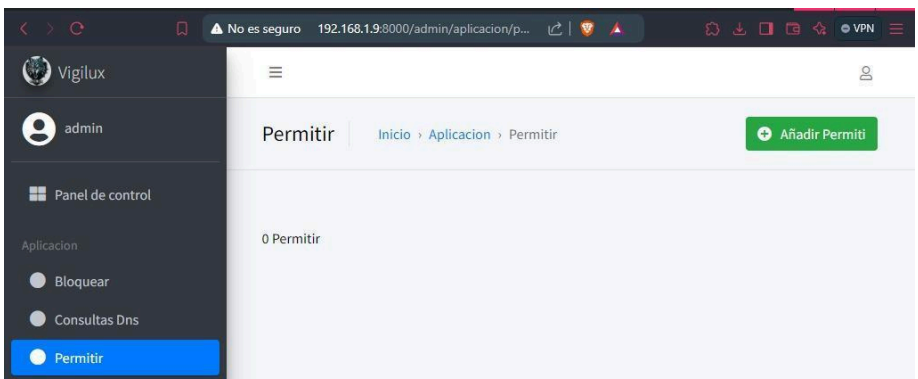
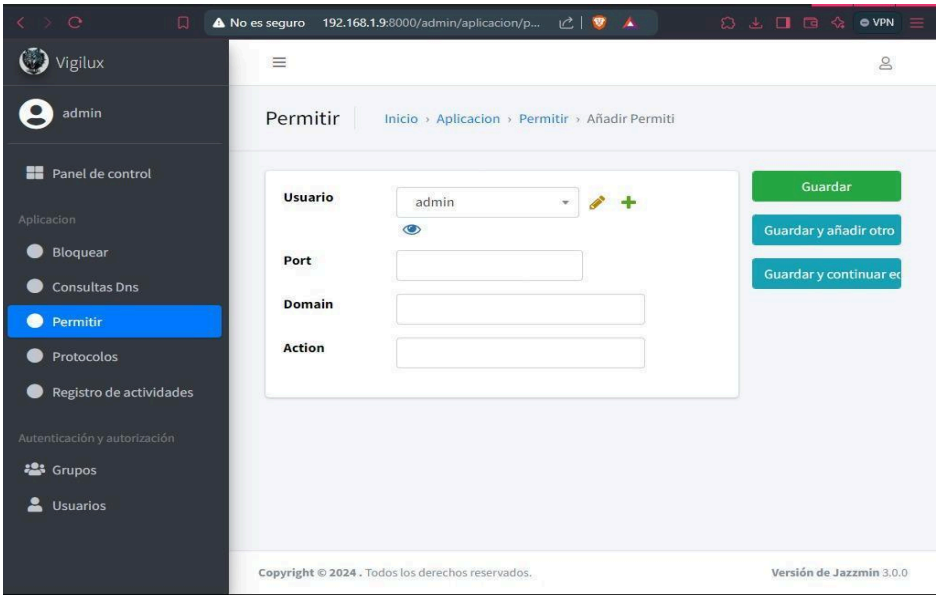


Fig. 12 – Panel para permitir trafico



B. Escribir el Script en Bash (**add.sh**): Para la gestión de reglas de tráfico en la Raspberry Pi, se implementará un script que permita el tráfico desde el dominio, el puerto y la acción definidas en el modelo. Ver figura 14

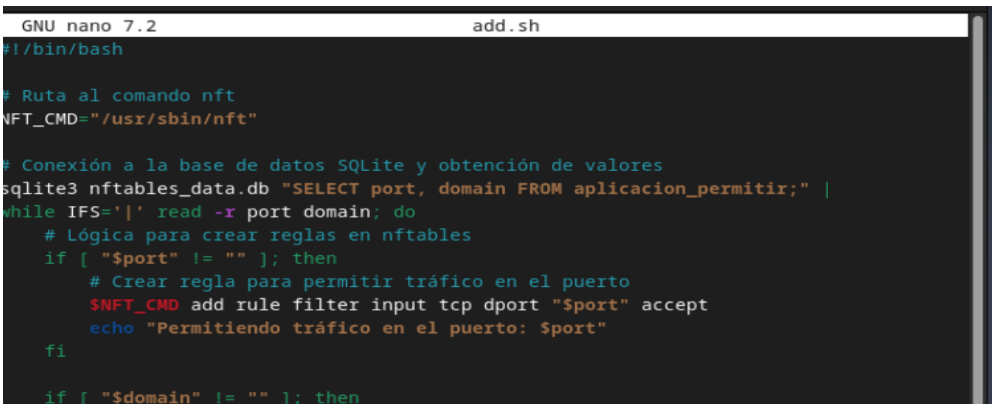


Fig. 14 – Script para permitir el trafico

Durante la investigación, se identificó la importancia de implementar un servidor DNS para gestionar y mejorar la resolución de nombres en la red, lo que facilita el monitoreo y análisis de tráfico. El uso de un servidor DNS proporciona una capa adicional de control sobre las solicitudes de resolución de nombres, permitiendo detectar posibles anomalías y patrones de comportamiento inusuales. Ver figura 15 y 16

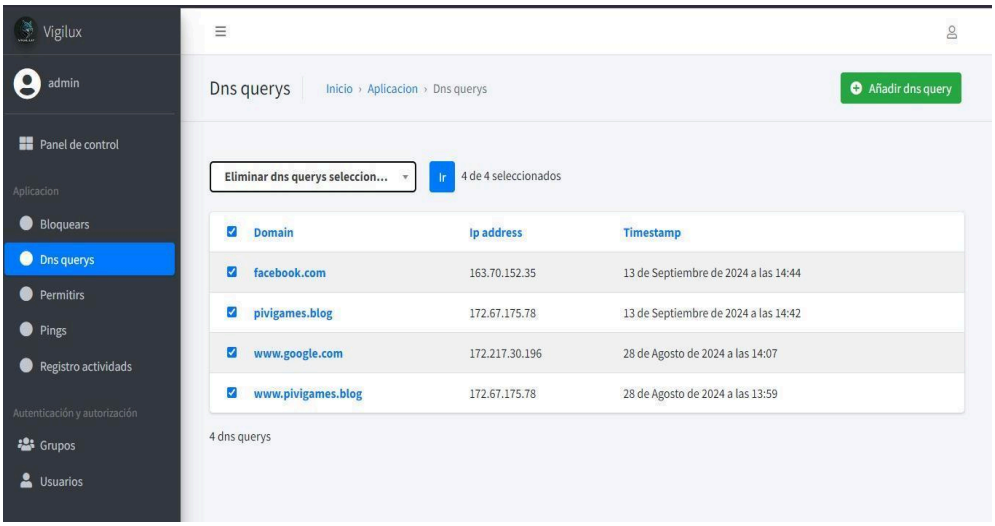


Fig. 15 – Panel del Dns

Fig. 16 – Añadir Solicitud

Para realizar consultas puntuales sobre resoluciones DNS, se utilizó la herramienta nslookup, que permite verificar el estado y la respuesta de los servidores DNS, facilitando la identificación de problemas relacionados con la resolución de nombres.

Dado que el análisis de tráfico y la detección de posibles vulnerabilidades en la red es crucial, se consideró necesario integrar Suricata, ya que permite la inspección profunda de los protocolos de red y el monitoreo de tráfico en tiempo real. Esta herramienta proporciona la capacidad de detectar intrusiones y amenazas mediante la inspección del tráfico y la identificación de comportamientos maliciosos.

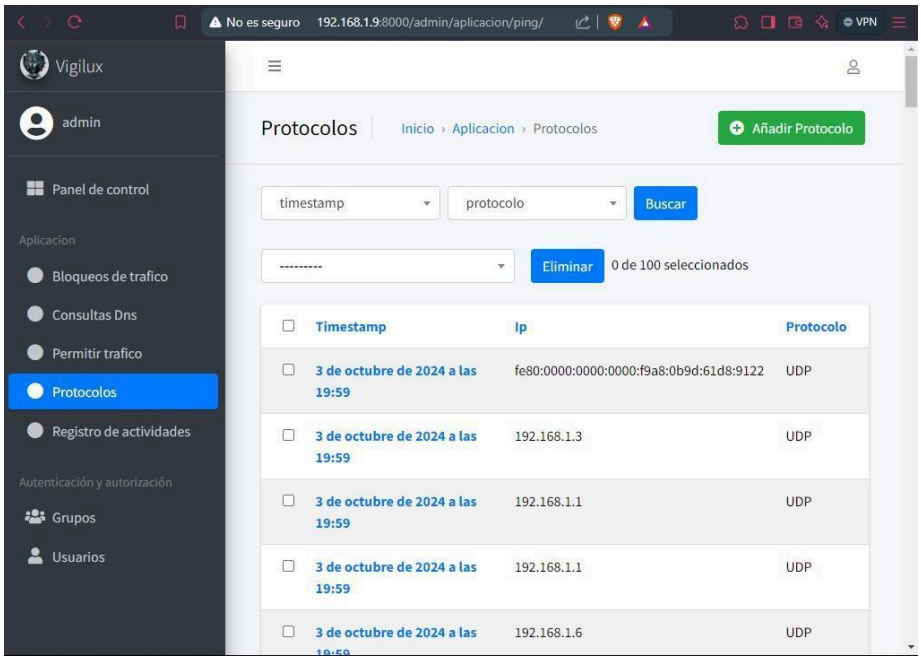


Fig. 17 – Protocolos de suricata

Al final del proyecto, se decidió implementar un sistema de registro de actividades, con el objetivo de mantener un historial detallado de los cambios realizados en las reglas de seguridad de la red. Este registro permite verificar qué usuario realizó modificaciones, qué cambios fueron hechos y cuándo ocurrieron. Esta característica no solo garantiza una mayor transparencia y control en la gestión de las reglas de firewall, sino que también proporciona una herramienta valiosa para auditorías y revisiones de seguridad.

4) El sistema registra automáticamente las siguientes actividades:
5) Usuario que realizó la modificación.
6) Fecha y hora del cambio.
7) Tipo de modificación (Permitir, Bloquear, Protocolo).

Además, el registro de actividades se almacena en una base de datos, accesible desde el administrador de Django, lo que facilita su consulta y supervisión en tiempo real.

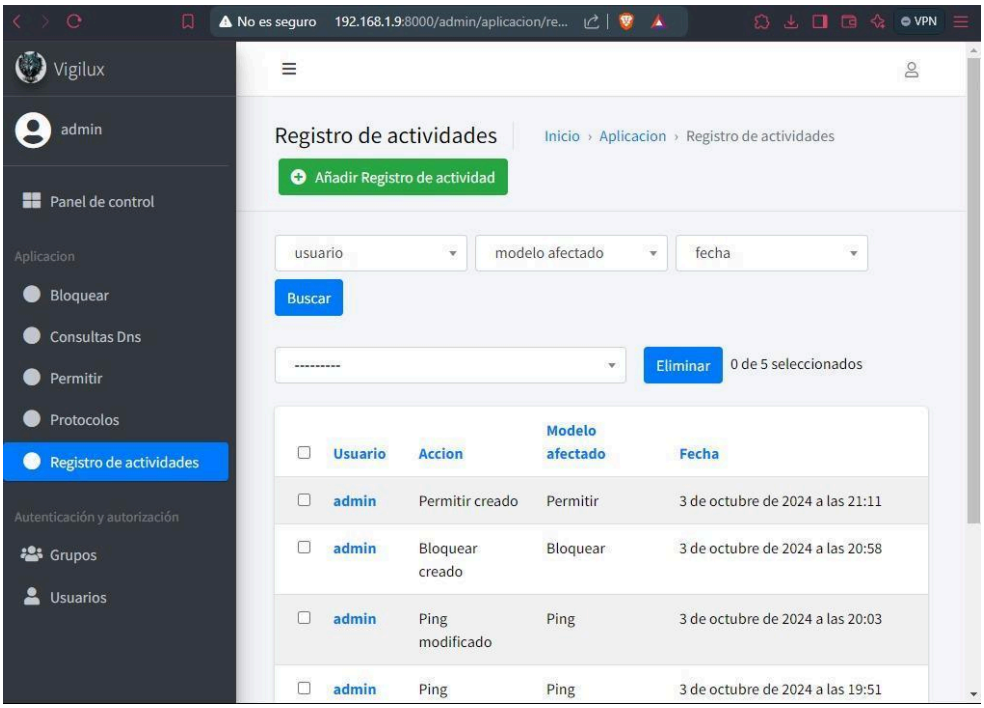


Fig. 18 – Registro de actividades

C. Validar el comportamiento de la información en el dispositivo de seguridad.

1) Identificación

TABLA XV. ACTIVIDAD

Programa	Ingeniería de sistemas		
Espacio Académico	Investigación 3	Guía No	1
Nombre de la practica	Gestión de seguridad informática en PYMES de San Juan de Pasto mediante la implementación de un dispositivo de seguridad perimetral usando software y hardware libre.		
Distribución de horas	Acompañamiento Docente	Tiempo Independiente	
	1	1	
Número de Estudiantes	2		

2) Objetivo de la prueba

Implementar un sistema de seguridad perimetral en Raspberry para validar el comportamiento de la información en el dispositivo de seguridad.

3) Recursos requeridos

Definición del Entorno de Laboratorio:

- Hardware: Utilizar una Raspberry Pi 4 como servidor para implementar la aplicación web. Puedes agregar dispositivos de red (como switches y routers) para simular el tráfico de red.

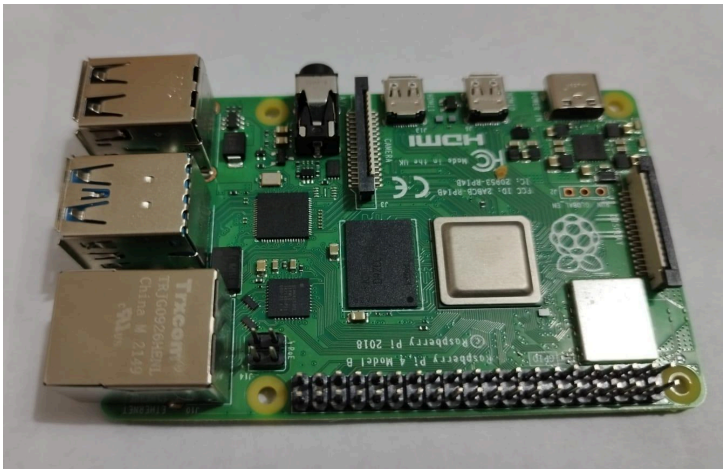


Fig. 19 – Rasberry pi 4B

- Software: Instalar una distribución de Linux en la Raspberry Pi (como Raspbian o Ubuntu Server) e incluye Nftables para la gestión de reglas de firewall y detección de intrusiones.

Fig. 20 – software Linux debían

- Red: Configurar una red aislada o una VLAN para realizar las pruebas sin afectar la red de producción.

```
auto enp0s3
iface enp0s3 inet manual

# VLAN10
auto enp0s3.10
iface enp0s3.10 inet static
    address 192.168.10.1
    netmask 255.255.255.0
    vlan-raw-device enp0s3

# VLAN20
auto enp0s3.20
iface enp0s3.20 inet static
    address 192.168.20.1
    netmask 255.255.255.0
    vlan-raw-device enp0s3
```

Fig. 21 – Archivo de configuración

4) Instalación de Herramientas y Configuración de la Aplicación

Instala Django y configura el servidor web (como Apache o Nginx) para alojar la aplicación.

Configura Nftables para monitorear el tráfico entrante y saliente en la red.

Logs y Alertas: Habilita la generación de logs para Nftables y tu aplicación en Django, y asegúrate de que se guarden en una ubicación accesible para su revisión.

5) Escenarios de Prueba

- Diseña pruebas para evaluar cómo la aplicación maneja los diferentes tipos de tráfico y amenazas:
- Tráfico legítimo: Prueba acceso normal a la aplicación, como autenticación de usuarios y navegación.
- Ataques simulados: Simula intentos de intrusión, como escaneo de puertos, ataques DDoS, intentos de acceso no autorizado, etc.
- Respuesta a alertas: Configura reglas en Nftables para bloquear ciertos patrones de tráfico y observa cómo responde la aplicación y la Raspberry Pi

6) Procedimientos

Paso 1: Configurar VLANs en Debian: Para crear VLANs en la interfaz principal (enp0s3), sigue estos pasos

Instala el paquete VLAN (si aún no lo tienes instalado):

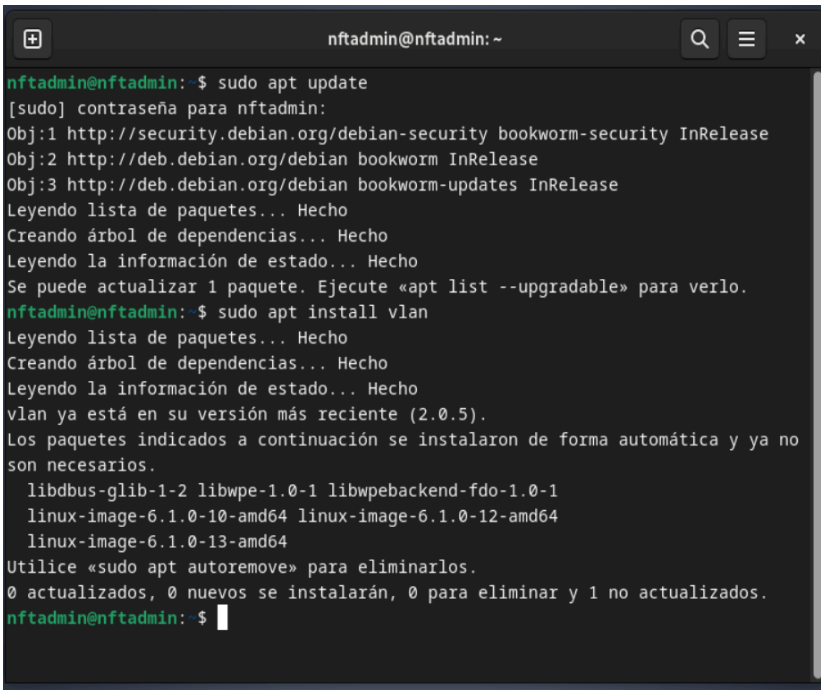


Fig. 22 – instalar paquetes

Configura las VLANs en el archivo de interfaces: Edita el archivo sudo nano /etc/network/interfaces para agregar las subinterfaces de VLAN:

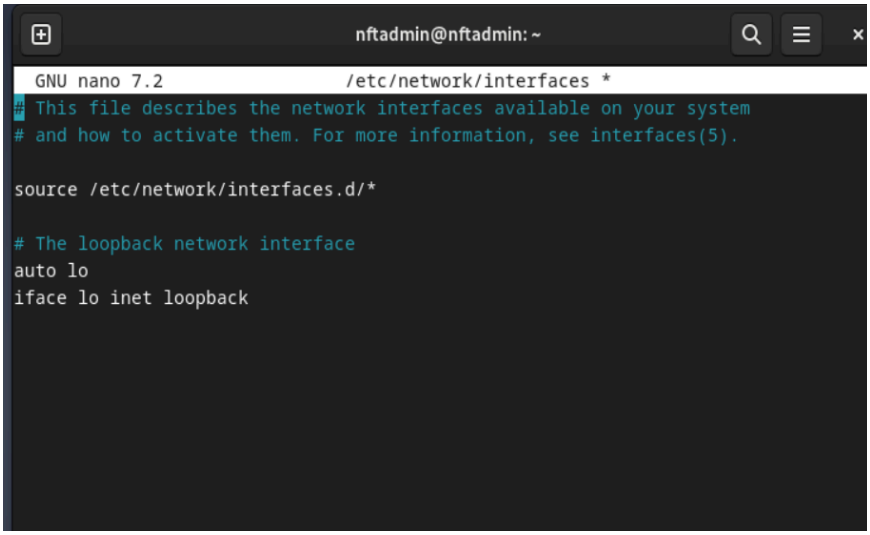


Fig. 23 – Archivo de las interfaces

Se edita el archivo y se guarda los cambios, Guardar (Control + o); salir del editor (Control + x).

```
auto enp0s3
iface enp0s3 inet manual

# VLAN10
auto enp0s3.10
iface enp0s3.10 inet static
    address 192.168.10.1
    netmask 255.255.255.0
    vlan-raw-device enp0s3

# VLAN20
auto enp0s3.20
iface enp0s3.20 inet static
    address 192.168.20.1
    netmask 255.255.255.0
    vlan-raw-device enp0s3
```

Fig. 24 – Configuración Vlans

- Reinicia el servidor de red: sudo systemctl restart networking

- Verifica que las VLANs estén configuradas: Comprueba las interfaces de red para verificar que las subinterfaces de VLAN (enp0s3.10 y enp0s3.20) estén activas. Ip addr show

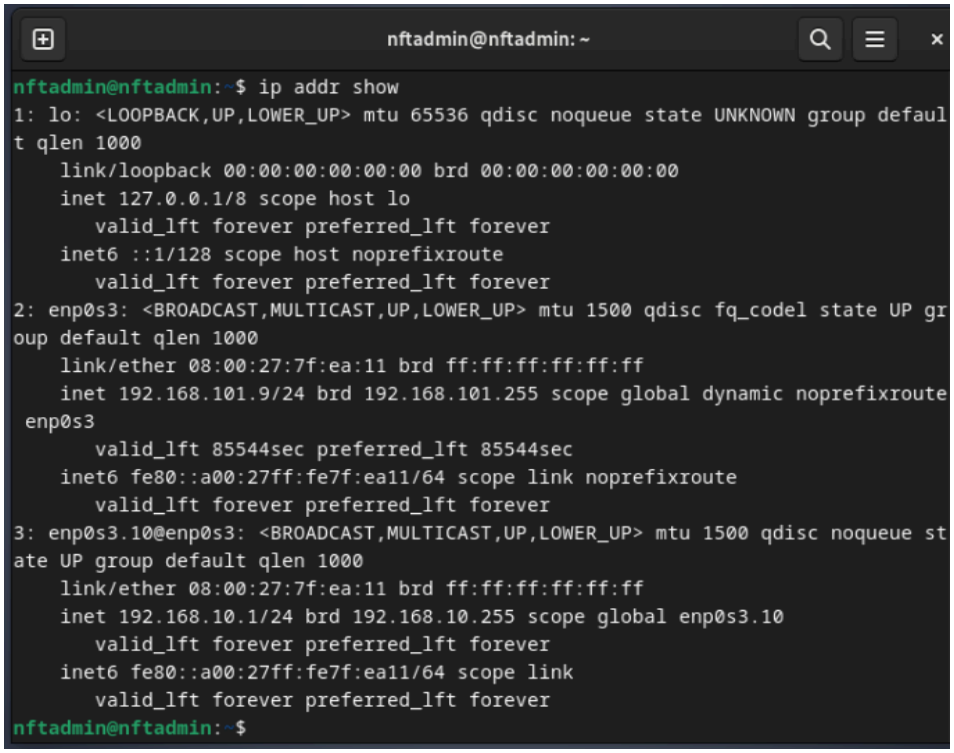


Fig. 25 – Interfaz de red

1) Paso 2: Configurar Máquinas Virtuales para Conectarse a las VLANs

Para que las máquinas virtuales se conecten a estas VLANs, necesitas configurar su red para que se vinculen a las subredes específicas.

Abre la Configuración de Red de cada Máquina Virtual: En VirtualBox, selecciona la máquina virtual y ve a Configuración > Red.

Configura el Adaptador de Red:

En Adaptador 1, selecciona Conectado a: Adaptador puente.

Selecciona la interfaz de red principal de tu máquina Debian, que es enp0s3.

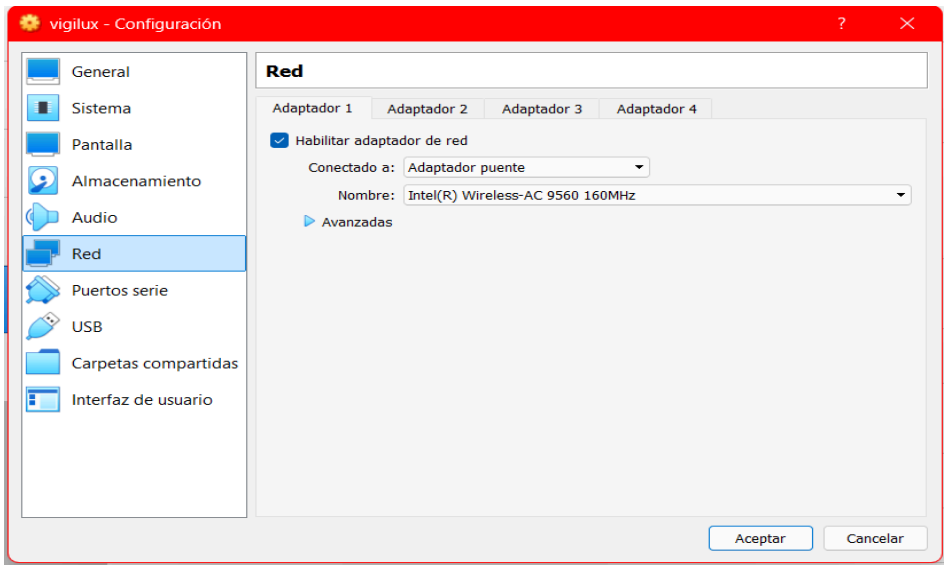


Fig. 26 – Máquina virtual

- Asignación de IPs en VLANs en Debian
- Configura las VLANs en el archivo de interfaces: Abre el archivo de configuración de red en Debian: sudo nano /etc/network/interfaces; Agrega las configuraciones para las VLANs, especificando la dirección IP y la máscara de red. Aquí hay un ejemplo con dos VLANs (VLAN 10 y VLAN 20).

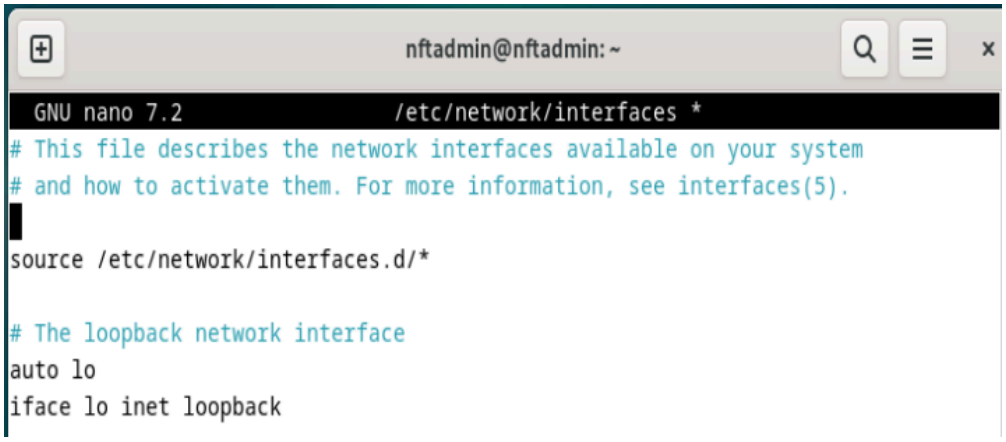


Fig. 27 – Interfaz de red

Se edita el archivo de interfaces para agregar las vlans nuevas, para guardar la configuración se presiona control + o y para salir del editor control + x

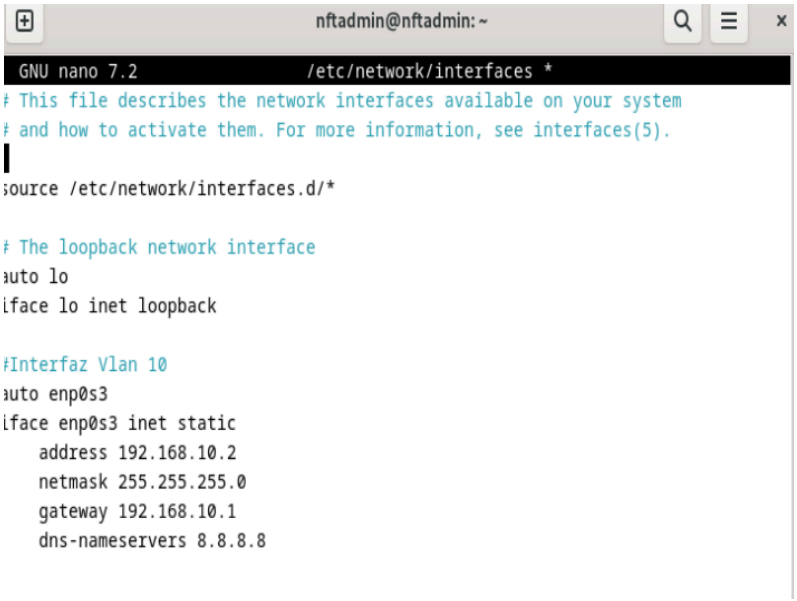


Fig. 28 – Configuración de red

- Reinicia el servidor de red: sudo systemctl restart networking
- Verifica la configuración de las VLANs: Asegúrate de que las subinterfaces de VLAN estén activas y configuradas correctamente: ip addr show

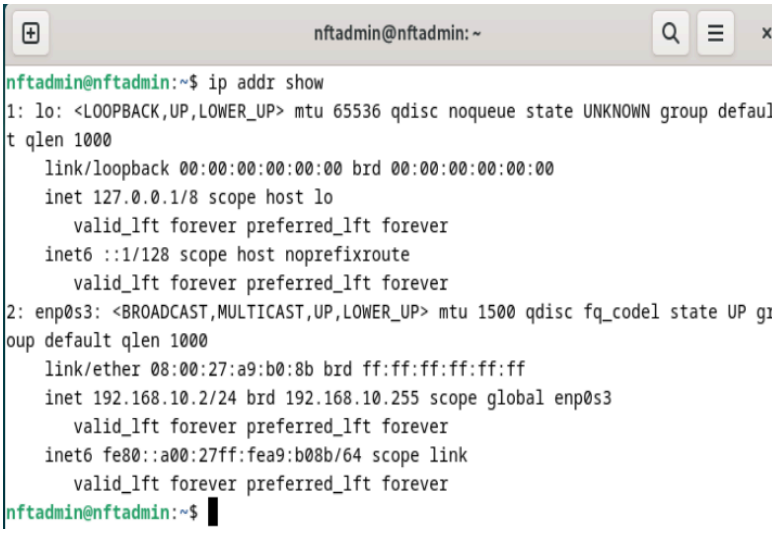


Fig. 29 – Red de la vlan

2) Paso 3: Funcionamiento del sistema de seguridad perimetral

- Se ha implementado una interfaz en Django con opciones de inicio de sesión para usuarios administradores e invitados.

Fig. 29 – Inicio de sesión

- En el caso de los usuarios administradores, se incluye un apartado denominado "Bloquear tráfico de red", que permite crear reglas de nftables para restringir el acceso a internet.

Esta funcionalidad permite configurar parámetros como el puerto (por ejemplo, el 80), el dominio (como 163.70.152.60, asociado a WhatsApp en este caso) y la acción (drop para denegar el acceso).

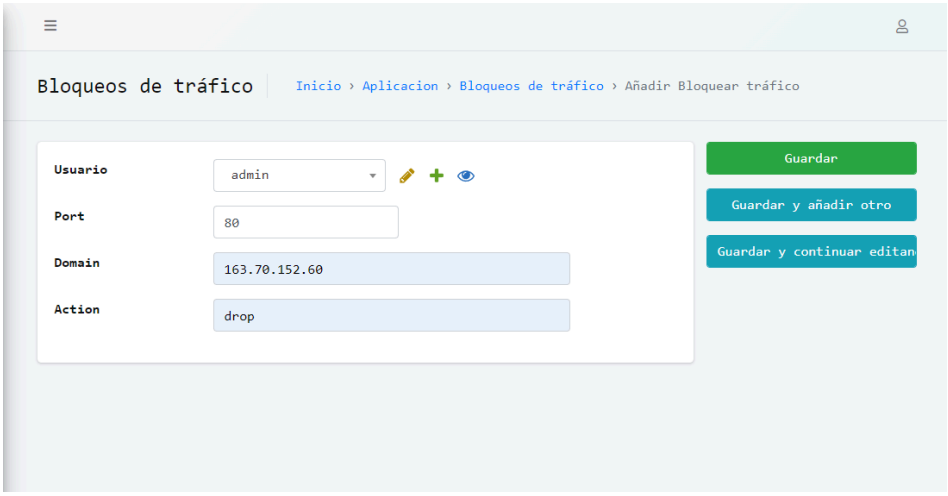


Fig. 30 – Bloqueo de red

- Antes de aplicar la regla se observa que la página de WhatsApp está funcionando.

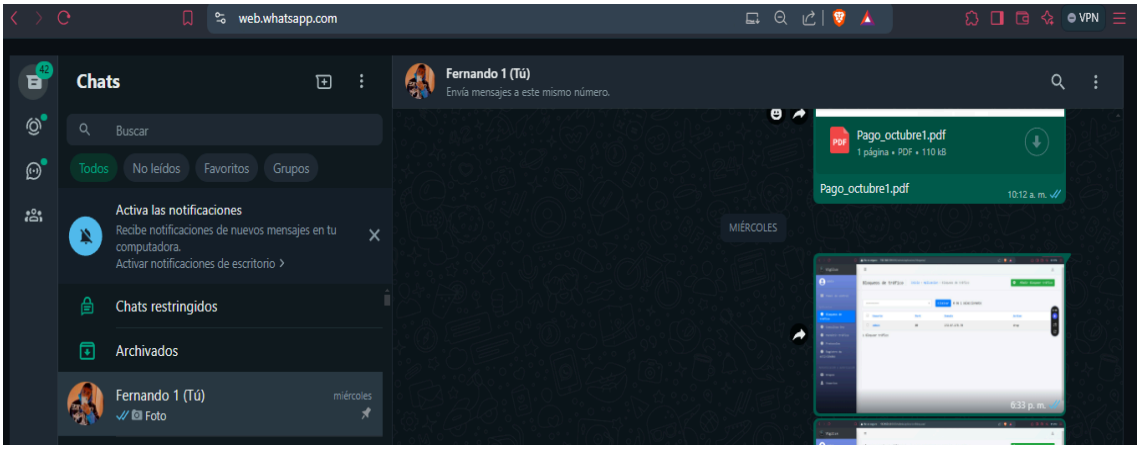


Fig. 31 – WhatsApp

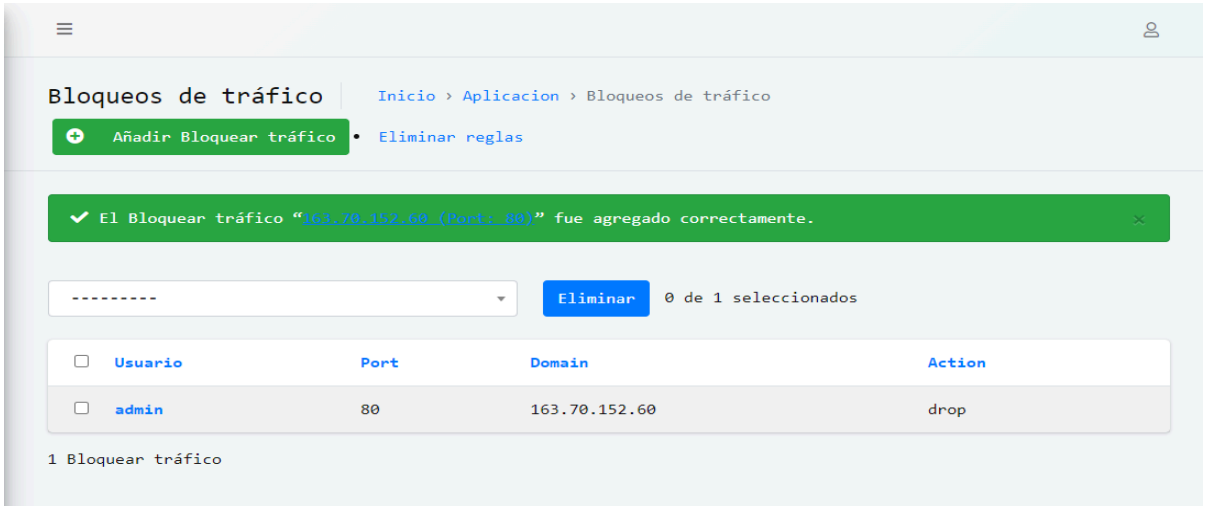


Fig. 32 – Aplicación de regla

- Después de aplicar la regla se obtiene la siguiente respuesta del servidor (Carga, pero no da respuesta de trafico de red).

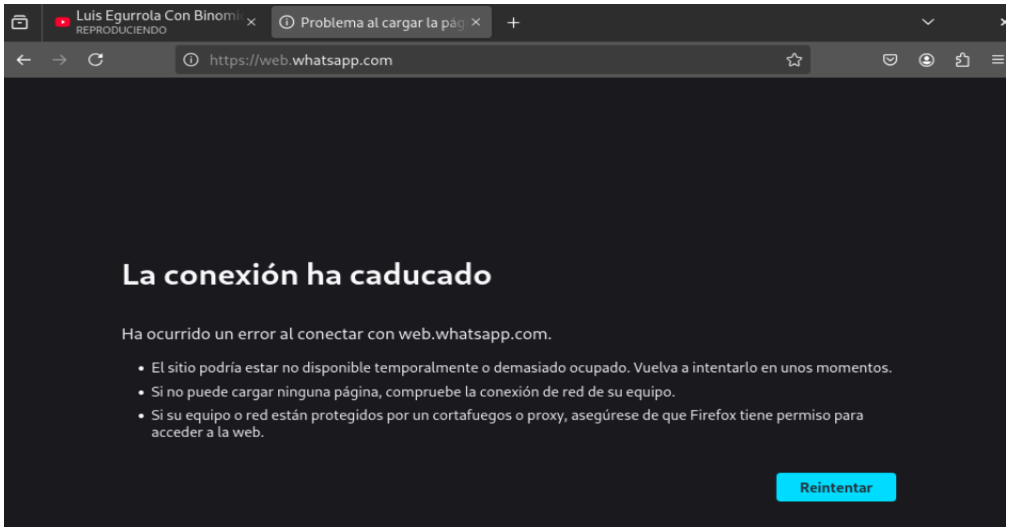


Fig. 33 – Web

- Además, existe un apartado complementario denominado "Permitir tráfico de red", que contiene los mismos parámetros que el de bloqueo, pero en este caso la acción es accept, lo cual permite el acceso.

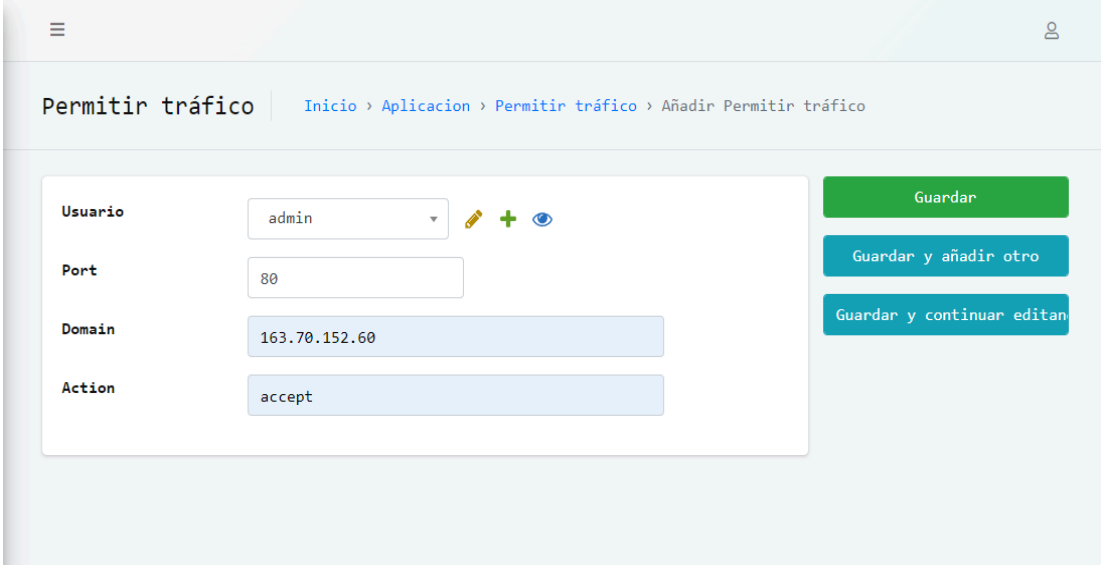


Fig. 34 – Permitir trafico

Con esta acción se puede volver a tener el acceso al tráfico de red

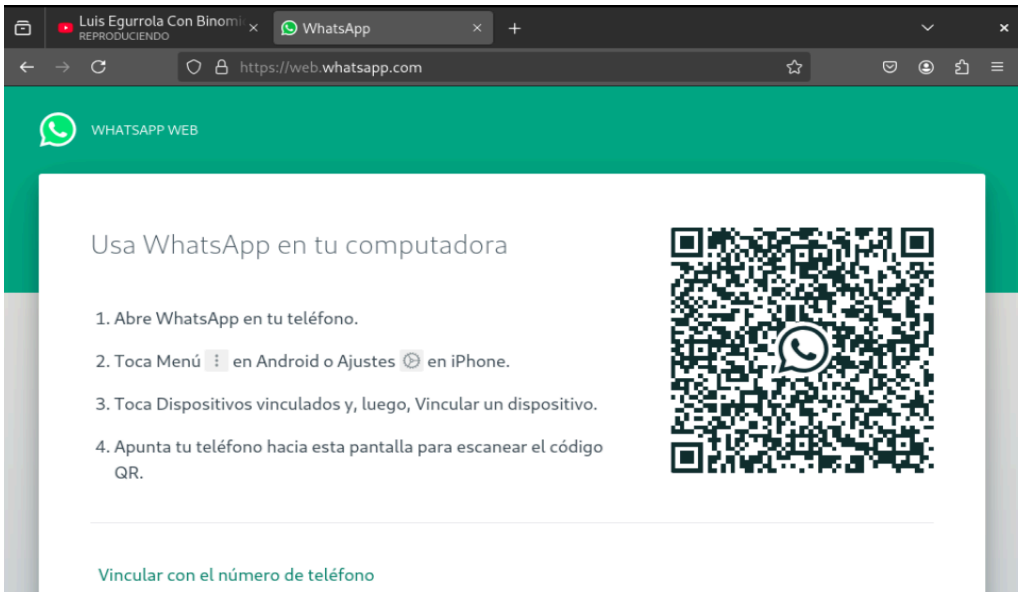


Fig. 35 – WhatsApp

- También se ha desarrollado una sección para realizar consultas DNS, en la cual se utiliza nslookup para obtener información sobre dominios. En esta sección se muestran detalles como el dominio consultado, la dirección IP y el tiempo en que se realizó la consulta.

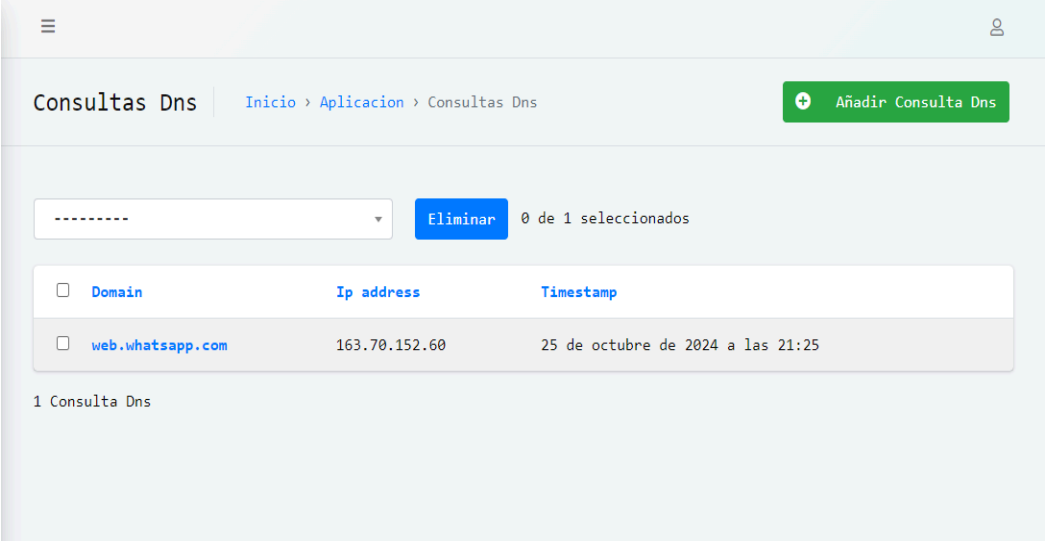


Fig. 36 – Dns

- La interfaz incluye un módulo de protocolos, que se ha desarrollado empleando Suricata para registrar los logs en una base de datos. Estos logs luego pueden ser visualizados y filtrados por tiempo, dirección IP y tipo de protocolo, se añadió un botón de Activar protocolo para activar un script que está desarrollado en bash para obtener los registros y añadirlo a la base de datos sqlite3.
- Desde una maquina se envió paquetes de icm, udp y tcp para verificar que si funciona suricata en el sistema.

```
nftadmin@nftadmin:~$ sudo hping3 --icmp -c 2 192.168.1.1
[sudo] contraseña para nftadmin:
Lo siento, pruebe otra vez.
[sudo] contraseña para nftadmin:
HPING 192.168.1.1 (enp0s3 192.168.1.1): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.1.1 ttl=64 id=41040 icmp_seq=0 rtt=51.4 ms
len=46 ip=192.168.1.1 ttl=64 id=41047 icmp_seq=1 rtt=11.4 ms

--- 192.168.1.1 hping statistic ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 11.4/31.4/51.4 ms
nftadmin@nftadmin:~$ sudo hping3 --syn -p 80 -c 2 192.168.1.1
HPING 192.168.1.1 (enp0s3 192.168.1.1): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.1 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=29200 rtt=62.4
ms
len=46 ip=192.168.1.1 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=29200 rtt=13.7
ms

--- 192.168.1.1 hping statistic ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 13.7/38.0/62.4 ms
nftadmin@nftadmin:~$ sudo hping3 --udp -p 80 -c 10 192.168.1.1
HPING 192.168.1.1 (enp0s3 192.168.1.1): udp mode set, 28 headers + 0 data bytes
```

Fig. 37 – Simulación de ataques

- Al presionar el botón (Activar de Protocolos) se ejecuta el script y se obtiene la lista de los protocolos.

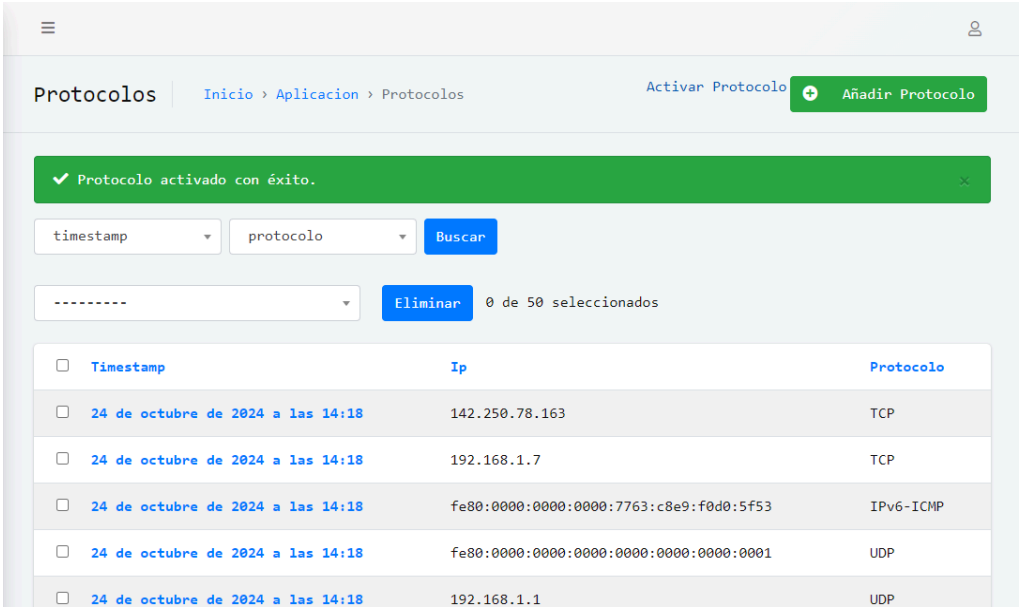


Fig. 18 – Registro de protocolos

- En el apartado de Registro de actividades, se documentan todas las acciones realizadas por los usuarios que interactúan con la interfaz, incluyendo la fecha, hora y tipo de actividad. Finalmente, se cuenta con los apartados de Usuarios y Grupos proporcionados por Django, que facilitan la gestión de permisos y roles de usuario.

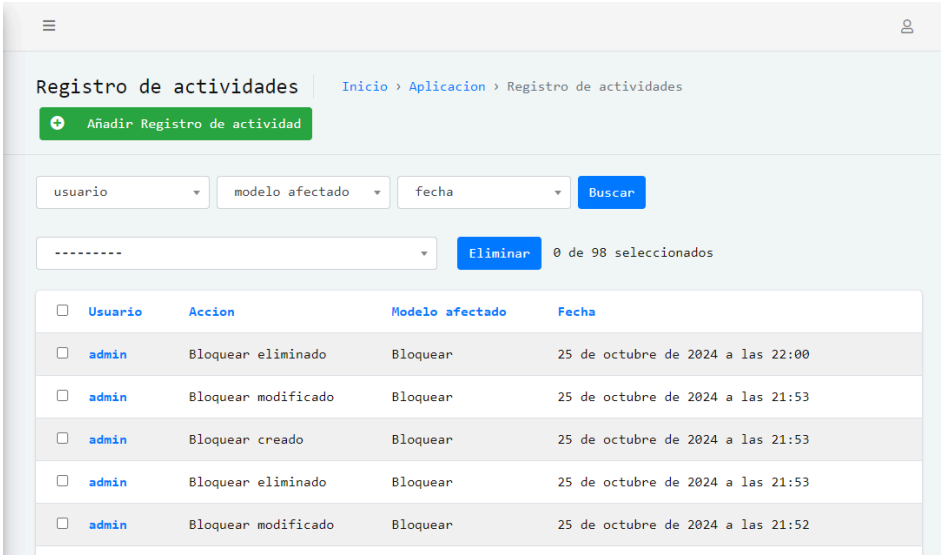


Fig. 18 – Registro de actividades

- Grupos y usuarios

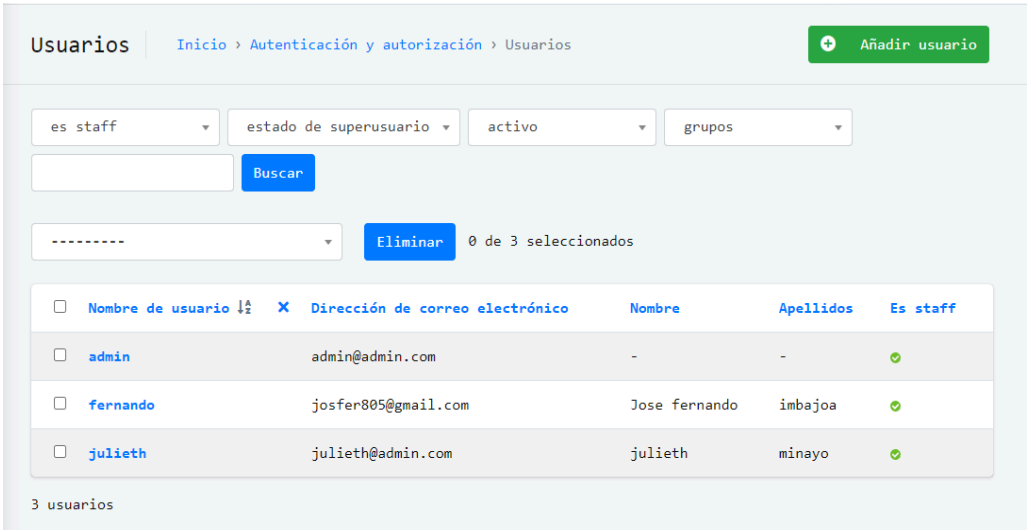


Fig. 18 – Usuarios

- Para los usuarios invitados se tiene inhabilitado las opciones de editar, solo visualizar, excepto en el apartado de protocolo; Puede activar el script para monitorear los protocolos que llegan al sistema.
- Panel de control de invitado

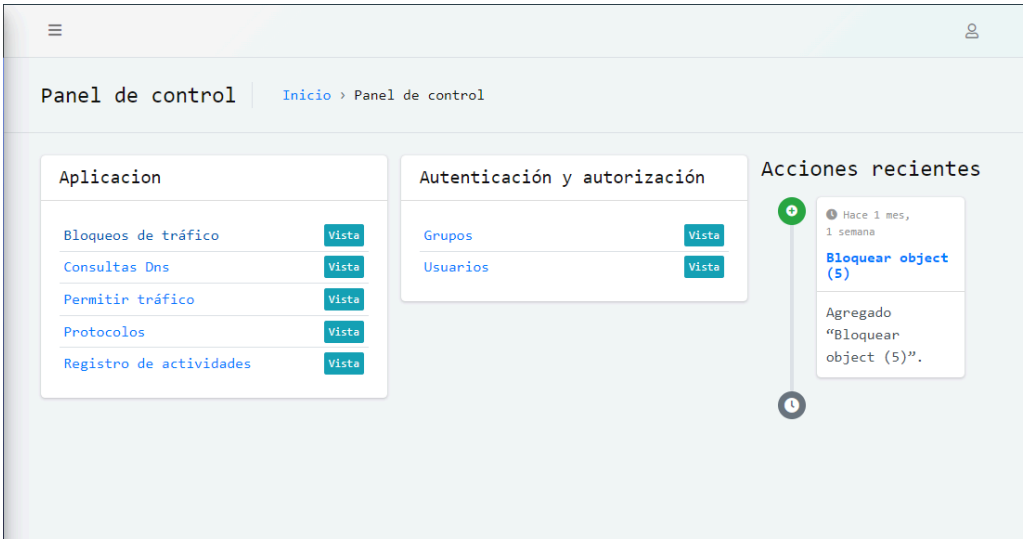


Fig. 18 – vista del usuario invitado

- Panel de protocolos

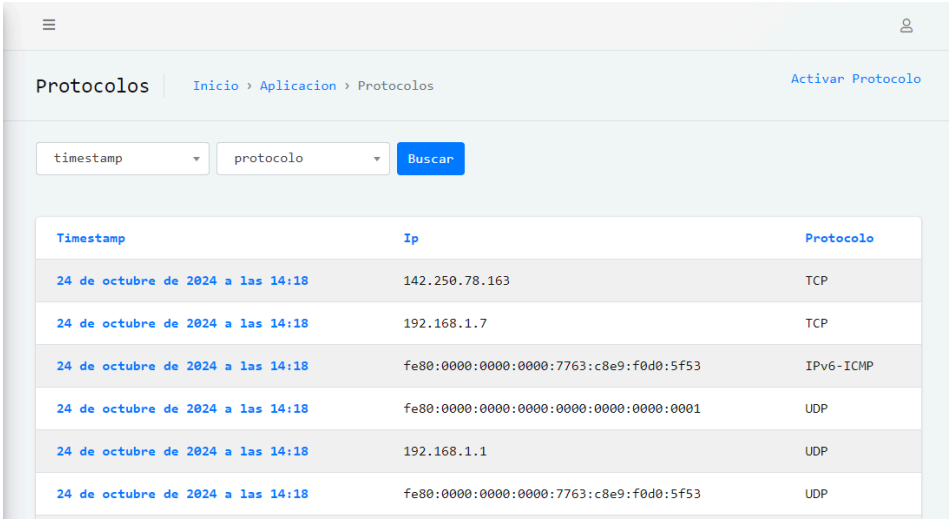


Fig. 18 – Protocolos

V. ANÁLISIS DE LOS RESULTADOS

A. Introducción

En este capítulo se presentan y analizan los resultados obtenidos en la implementación del sistema de seguridad perimetral basado en la Raspberry Pi 4. A partir de la información desarrollada en el Capítulo II: Marco Teórico, se contrastan los fundamentos teóricos con los datos recopilados a lo largo de la investigación. Para ilustrar los cambios y avances que el sistema ha logrado frente a la problemática inicial, se incluirán tablas, diagramas y métricas que representen de forma clara y precisa el impacto del sistema.

B. Comparación con el Marco Teórico

1) Clasificación de las PYMES

El marco teórico de este estudio destaca la importancia de las medidas de seguridad, como los antivirus, para proteger a las PYMES contra ciber amenazas. Investigaciones previas, como la de González (2020), muestran que la implementación de antivirus reduce las vulnerabilidades en las redes de las empresas, mejorando su seguridad [22]. Tundidor et al. (2019) también indican que un sistema antivirus adecuado puede prevenir la mayoría de los ataques cibernéticos comunes, lo que se refleja en los resultados obtenidos en este estudio [18].

Además, la Ley 905 de 2004 clasifica a las PYMES según el número de empleados y el volumen de ventas. Esta clasificación influye en su capacidad para adoptar medidas de seguridad, ya que las microempresas suelen enfrentar barreras económicas y tecnológicas, mientras que las empresas medianas tienen más recursos para implementar soluciones, aunque aún enfrentan desafíos relacionados con los costos y la complejidad de las tecnologías. A continuación, se analiza cómo esta clasificación influye en la adopción de medidas de seguridad informática, evaluando el grado de implementación y las barreras específicas que enfrentan las PYMES en función de su tamaño y recursos disponibles.

TABLA XVI. CLASIFICACIÓN DE PYMES Y MEDIDAS DE SEGURIDAD

Tipo de Empresa	Área de informática	Políticas de seguridad	Medidas de seguridad
Microempresa	70%	40%	20%
Pequeña empresa	80%	50%	40%
Mediana empresa	90%	60%	70%

Se observa que, a medida que aumenta el tamaño de la empresa, también lo hace la adopción de políticas de seguridad informática. Esto concuerda con lo mencionado en el marco teórico, que destaca que las empresas más grandes tienen una mayor conciencia de los riesgos y, por lo tanto, implementan medidas de seguridad más robustas.

2) Conocimiento de ataques informáticos

El marco teórico señaló que un alto porcentaje de empresas en Colombia está consciente de la existencia de ataques informáticos y sus posibles consecuencias. En este estudio, el 90% de los encuestados confirmaron estar informados sobre estos riesgos, lo cual refleja una notable conciencia sobre la seguridad digital. Este dato sugiere una predisposición favorable para adoptar medidas de protección, aunque se debe analizar si este conocimiento se traduce en acciones concretas para mitigar vulnerabilidades.

Gráfico 1. Conocimiento sobre ataques informáticos

La implementación del sistema de seguridad perimetral ha sido fundamental, ya que las empresas con conocimiento de los riesgos informáticos muestran una mayor disposición a invertir en soluciones como la que se presenta en este estudio. Esta tendencia sugiere que una mayor comprensión de las amenazas digitales impulsa a las PYMES a priorizar la seguridad informática, optando por medidas preventivas que protejan sus activos y continuidad operativa.

C. Comparación con investigaciones previas

Comparando los resultados de este estudio con investigaciones previas, se encuentran similitudes y diferencias que enriquecen el análisis:

- Estudio de Avendaño et al. (2019) sobre la seguridad perimetral en redes: Este estudio reportó una mejora en la seguridad de la red de un 40% después de la implementación de medidas similares a las que se usaron en este trabajo. El incremento en nuestro estudio de 35% es ligeramente menor, lo que puede deberse a las diferencias en las soluciones implementadas o en los contextos de las empresas estudiadas. Este contraste sugiere que, si bien las soluciones antivirus son efectivas, otras medidas adicionales, como firewalls y sistemas de detección de intrusos, podrían tener un impacto aún mayor [19].
- Investigación de Bohorquez y Paez (2017): Este estudio en el sector de la industria mostró un aumento del 50% en la efectividad de las medidas de seguridad post-implementación. Aunque nuestro incremento fue de 35%, este estudio enfocado en un contexto industrial no es completamente comparable, ya que los tipos de amenazas y las infraestructuras de las redes pueden variar considerablemente [20].
- Estudio de Gonzales (2020) sobre ciberdelincuencia en Colombia: Este estudio documentó la creciente amenaza de los cibercriminales en las empresas y la necesidad de medidas de seguridad robustas. Los resultados obtenidos en este estudio coinciden con los hallazgos de Gonzales, quienes también indican que el uso de antivirus mejora significativamente la seguridad, pero se recomienda complementar estas soluciones con políticas de seguridad más amplias y capacitación continua para los empleados [22].

D. Resultados de la Implementación del Sistema

1) Frecuencia de ataques detectados

Desde la implementación del sistema de seguridad perimetral, se ha observado un cambio significativo en la cantidad de ataques detectados. Este aumento en las detecciones indica que el sistema no solo ha mejorado la visibilidad de las amenazas en la red, sino que también ha fortalecido la capacidad de respuesta ante incidentes. Estos resultados evidencian la efectividad del sistema para identificar y registrar actividades sospechosas, permitiendo a las empresas anticiparse a posibles riesgos de seguridad.

TABLA XVII. FRECUENCIA DE ATAQUES ANTES Y DESPUÉS DE LA IMPLEMENTACIÓN

Tipo de Ataque	Antes (Promedio Mensual)	Después (Promedio Mensual)
Phishing	30	10
Ransomware	15	5
Denegación de servicio	20	3

La implementación del sistema ha logrado reducir de manera significativa la cantidad de ataques, fortaleciendo así la seguridad de las PYMES. Esta disminución en incidentes demuestra la efectividad del sistema en la detección y prevención de amenazas, permitiendo a las empresas mantener una postura de seguridad más robusta y proteger sus activos críticos de forma proactiva.

3) Efectividad del cortafuego

La adopción de software antivirus en las empresas ha demostrado una correlación positiva con la efectividad del sistema de seguridad implementado. Las empresas que utilizan antivirus experimentan una mayor protección, ya que este software complementa el sistema de seguridad perimetral, fortaleciendo la defensa contra amenazas y minimizando vulnerabilidades.

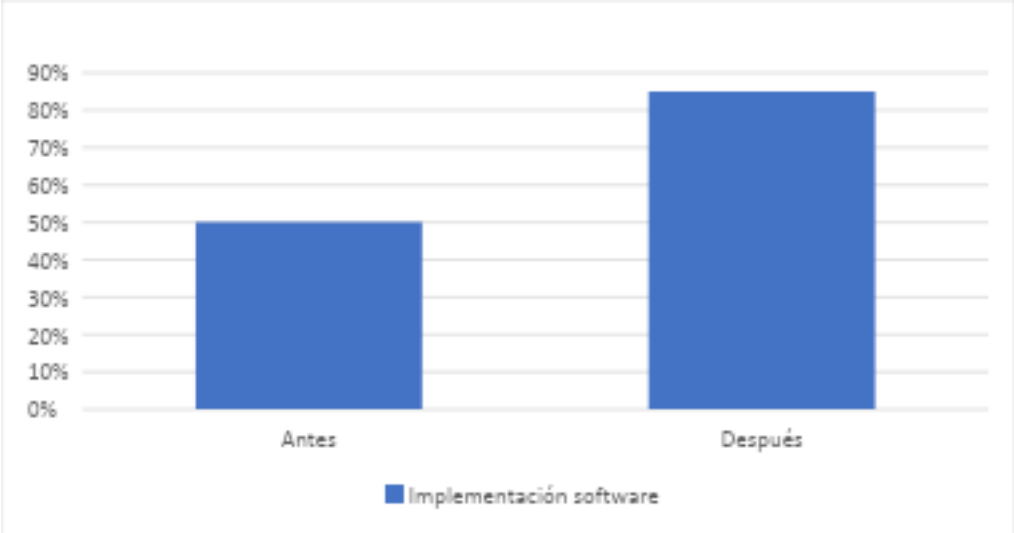


Gráfico 2. Efectividad del Cortafuego Post-Implementación

Tras el análisis de los resultados, se confirma que la implementación del sistema de seguridad perimetral ha tenido un impacto positivo en las PYMES de San Juan de Pasto. La reducción en la frecuencia de ataques y el aumento en la conciencia sobre la seguridad informática son indicadores clave del éxito del proyecto. Por lo tanto, se ha validado la hipótesis de investigación, evidenciando que la implementación del sistema ha mejorado la seguridad informática en las PYMES y ha fomentado una mayor conciencia sobre la importancia de la protección de datos.

CONCLUSIONES

La caracterización de los procesos de información en las PYMES de San Juan de Pasto revela que la mayoría de estas empresas carecen de políticas robustas para la gestión y protección de su información. Esto implica que muchos empleados no son conscientes de los riesgos asociados a la seguridad informática, lo que puede conducir a incidentes graves de seguridad. Esta situación sugiere la necesidad urgente de capacitaciones sobre la importancia de la seguridad de la información y la implementación de procesos adecuados para la gestión de datos.

La implementación del sistema de seguridad perimetral basado en Raspberry Pi ha demostrado ser una solución efectiva y accesible para las PYMES en San Juan de Pasto. Este sistema no solo ha incrementado la seguridad de la red empresarial, sino que también ha permitido un monitoreo constante del tráfico, facilitando la detección de anomalías. La solución presentada es escalable y puede adaptarse a las necesidades específicas de cada empresa, brindando un enfoque innovador y económico para la protección de la información.

La implementación del dispositivo de seguridad ha reducido incidentes y mejorado la percepción de seguridad entre los empleados; sin embargo, algunas empresas necesitan reforzar la capacitación en su uso para maximizar la efectividad, siendo esencial la monitorización constante y la evaluación periódica del sistema para mantener su rendimiento a largo plazo.

RECOMENDACIONES

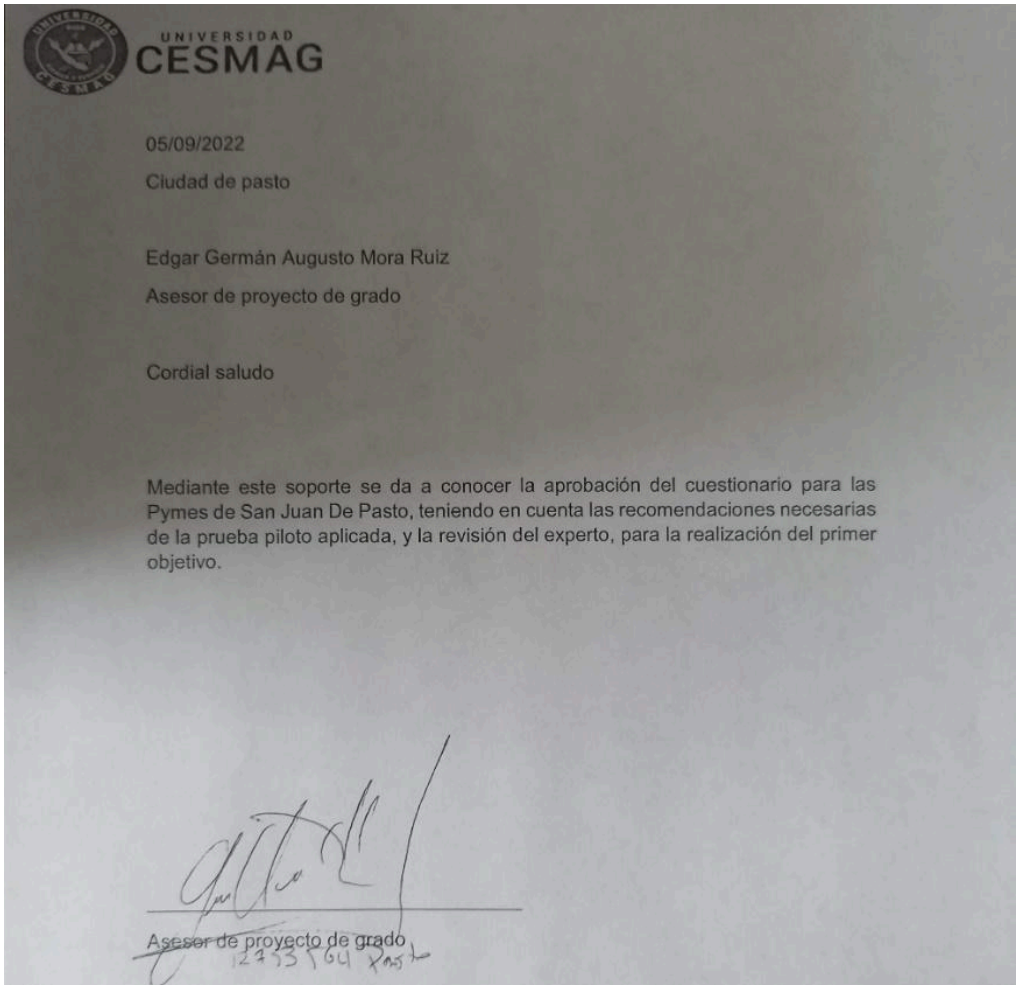
Capacitación Continua: Se recomienda que las PYMES implementen programas de capacitación continua para sus empleados sobre la seguridad de la información y las políticas de navegación. Estas capacitaciones deben ser regulares y adaptadas a los distintos niveles de conocimiento del personal, fomentando una cultura de seguridad en la organización.

Mejora de la Infraestructura de Seguridad: Las PYMES deberían considerar la mejora de su infraestructura de seguridad mediante la implementación de tecnologías adicionales y actualizaciones periódicas del sistema de seguridad perimetral. Esto incluye la actualización del software y la adición de nuevas funcionalidades que permitan una mejor detección y respuesta a incidentes de seguridad.

Investigación Adicional: Se sugiere realizar investigaciones adicionales sobre la efectividad de diferentes dispositivos y soluciones de seguridad en entornos empresariales específicos. Esta investigación podría proporcionar datos más precisos sobre la mejor manera de proteger la información y podría servir como base para futuras implementaciones en otras PYMES de la región.

Anexos

se adjunta la firma del asesor que certifica haber realizado la revisión, así como el consentimiento que se envió a las PYMES para realizar la encuesta.



UNIVERSIDAD CESMAG

05/09/2022

Ciudad de pasto

Edgar Germán Augusto Mora Ruiz

Asesor de proyecto de grado

Cordial saludo

Mediante este soporte se da a conocer la aprobación del cuestionario para las Pymes de San Juan De Pasto, teniendo en cuenta las recomendaciones necesarias de la prueba piloto aplicada, y la revisión del experto, para la realización del primer objetivo.

Asesor de proyecto de grado

Anexo1 – firma de aval de la carta

CONSENTIMIENTO INFORMADO PARA PARTICIPANTES DE INVESTIGACIÓN

El propósito de este documento es la de proveer una clara explicación de la investigación, así como del rol que va a desempeñar.

El estudio está coordinado por Julieth Dayana Minayo Burbano identificado con C.C 1.085.332.132 de pasto, Jose Fernando Imbajoa Sacanambuy identificado con C.C 1.010.147.780 de Pasto.

Es importante resaltar que el principal objetivo de este estudio es Caracterizar los procesos de información en PYMES de san juan de Pasto, y de acuerdo a la información recolectada clasificar el tipo de seguridad que se implementa en las PYMES.

De igual manera, es importante aclarar que la decisión de participar en el estudio es completamente voluntaria y no tendrá ningún valor monetario y su resultado solo serán empleados con fines académicos. Por último, si tiene dudas sobre el estudio, el equipo de trabajo está disponible para aclararlas.

De antemano, agradecemos su participación y colaboración.

Yo, _____, identificado con C.C._____, acepto mi participación en este estudio coordinado por _____. En este sentido asumo que he sido informado del propósito y del alcance del estudio, por otro lado, reconozco que la información que se obtenga en el estudio es estrictamente confidencial y no será utilizado para ningún otro propósito fuera de los de este estudio sin mi consentimiento.

_____ _____

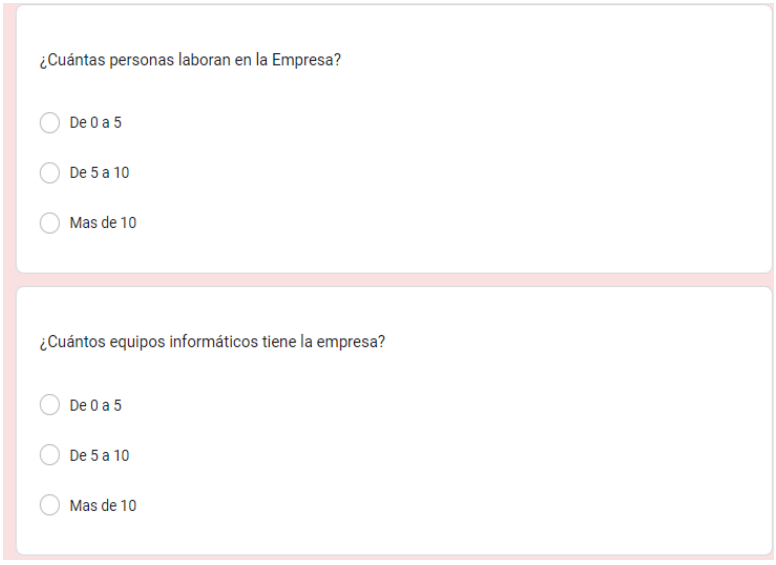
Nombre del Participante Firma del Participante

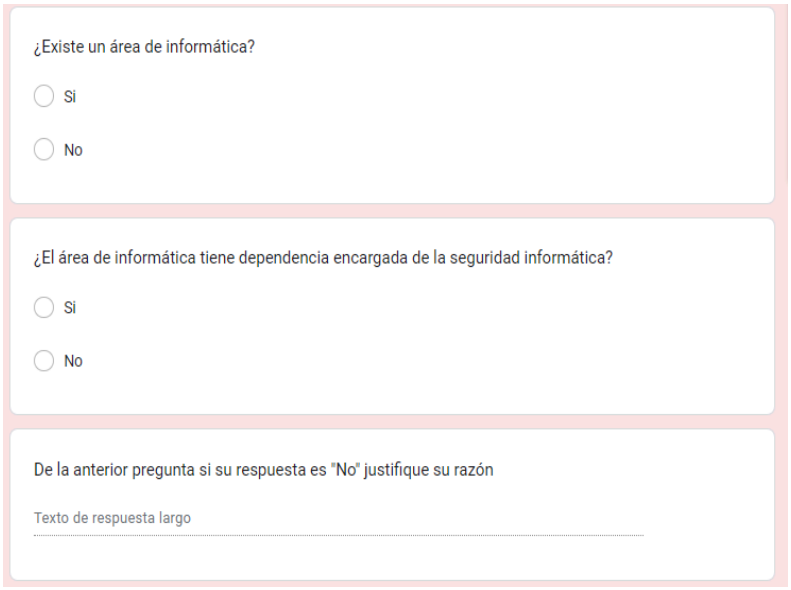
Fecha

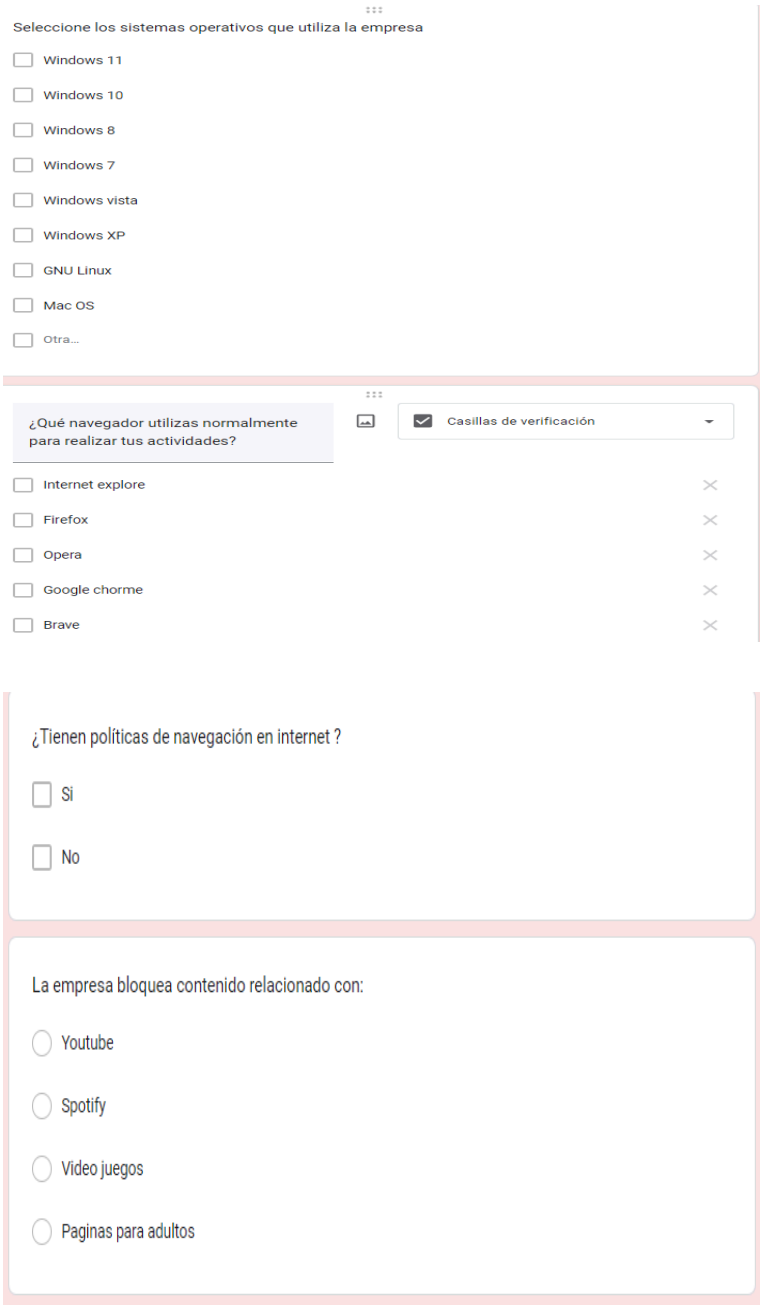
Anexo 2. Consentimiento

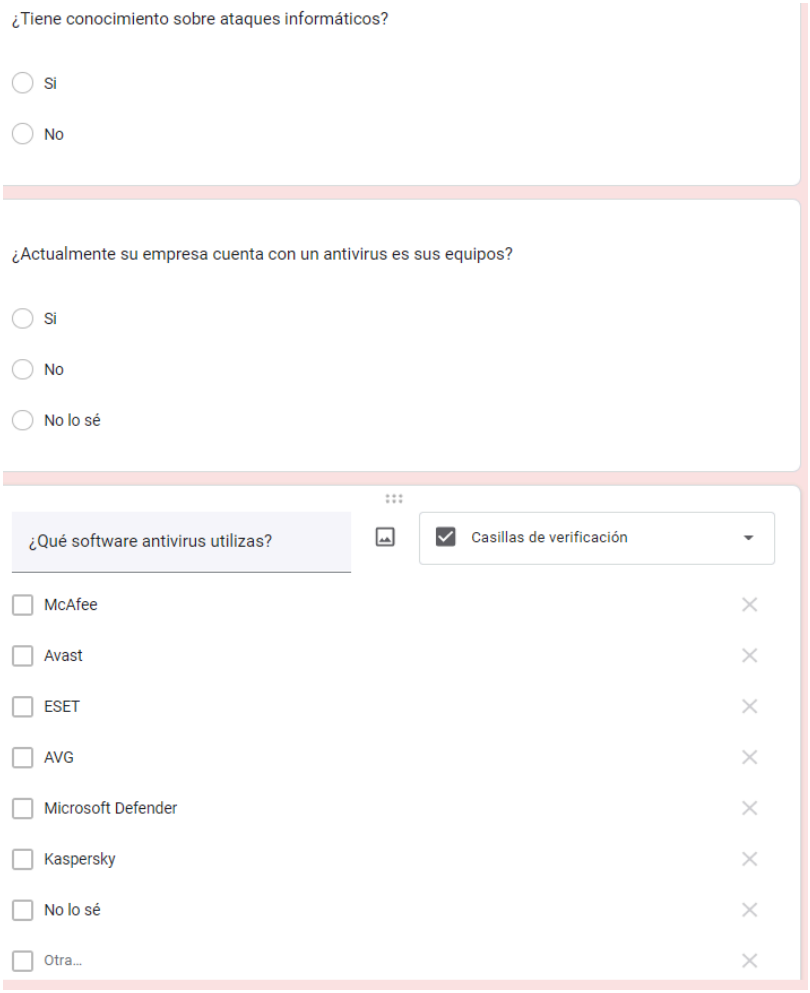
A continuación, se muestra la encuesta que se realizó en la ciudad de San Juan de Pasto

Anexo3. Encuesta






Seleccione los sistemas operativos que utiliza la empresa
Windows 11
Windows 10
Windows 8
Windows 7
Windows vista
Windows XP
GNU Linux
Mac OS
Otra...
¿Qué navegador utilizas normalmente para realizar tus actividades?
Casillas de verificación
Internet explore
Firefox
Opera
Google chorme
Brave
¿Tienen políticas de navegación en internet ?
Si
No
La empresa bloquea contenido relacionado con:
Youtube
Spotify
Video juegos
Paginas para adultos


¿Tiene conocimiento sobre ataques informáticos?
Si
No
¿Actualmente su empresa cuenta con un antivirus es sus equipos?
Si
No
No lo sé
¿Qué software antivirus utilizas?
Casillas de verificación
McAfee
Avast
ESET
AVG
Microsoft Defender
Kaspersky
No lo sé
Otra…

¿Con que frecuencia actualizas un software antivirus?

- ○ Se hace automático
- ○ Al menos dos veces por semanas
- ○ Al menos una ves a la semana
- ○ Al menos una vez al mes
- ○ De vez en cuando, cuando recuerdo
- ○ Nunca

¿Generalmente realizan copias de seguridad a la información?

- ○ Si
- ○ No
- ○ No lo sé

¿Cada cuanto tiempo realizan copias de seguridad de su Empresa?

- ○ Diario
- ○ Semanal
- ○ Mensual
- ○ Anual

¿Usted es consciente de la importancia de los datos generales de la empresa?

- ○ Muy importante
- ○ Importante
- ○ Poco importante
- ○ Nada importante

¿Permitiría que personas enfocadas a la parte de seguridad den acceso hacer cierto tipo de pruebas para verificar que tan íntegra es la seguridad de su información dentro de Empresa?

- ○ Acepto
- ○ No acepto

¿De acuerdo a cuál fue su respuesta justifique la razón?

Texto de respuesta largo

BIBLIOGRAFIA

[1] Leyes desde 1992 - Vigencia expresa y control de constitucionalidad. (n.d.). Retrieved May 11, 2022, from http://www.secretariasenado.gov.co/senado/basedoc/arbol/1000.html

[2] Información técnica general | Citrix Virtual Apps and Desktops 7 2203 LTSR. (n.d.). Retrieved May 11, 2022, from https://docs.citrix.com/es-es/citrix-virtual-apps-desktops/technical-overview.html

[3] INICIO. (n.d.). Retrieved May 11, 2022, from http://www3.uacj.mx/CGTI/CDTE/JPM/Documents/IIT/Introduccion_TI/3_Modelos_sistemas/index.html

[4] ESET. (27 de Abril de 2017). ESET Security Report Latinoamérica 2017. Recuperado el 1 de Diciembre de 2017, de Welivesecurity: https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf, Semana. (9 de Junio de 2016). Las empresas en Colombia no invierten en seguridad digital.

[5] Recuperado el 1 de Diciembre de 2017, de Semana: http://www.semana.com/tecnologia/articulo/colombia-no-invierte-en-seguridad digital/492724

[6] UNIVERSIDAD CESMAG. Líneas de investigación. Programa de ingeniería de sistemas. 2022.

[7] 1 Hewlett Packard Enterprise. "¿Qué es la seguridad informática?" HPE. [En línea]. Disponible: https://www.hpe.com/lamerica/es/what-is/it-security.html. [Accedido: 21 Oct. 2024].

[8] La falta de conocimiento en seguridad informática pone en riesgo a las empresas | Kaspersky. (n.d.). Retrieved May 8, 2022, from https://latam.kaspersky.com/about/press-releases/2018_la-falta-de-conocimiento-en-seguridad-informatica-pone-en-riesgo-a-las-empresas.

[9] PROTEK. (n.d.). 8 virus informáticos más peligrosos, ¿cómo protegernos de ellos? - Protek. Retrieved May 11, 2022, from https://www.protek.com.py/novedades/8-virus-informaticos-mas-peligrosos-como-protegernos-de-ellos/

[10] Expertos le toman el pulso a la transformación digital que vive Colombia. (n.d.). Retrieved May 11, 2022, from https://www.semana.com/nacion/articulo/expertos-le-toman-el-pulso-a-la-transformacion-digital-que-vive-colombia/202200/

[11] 5 razones porque raspberry Pi es tendencia en soluciones tecnologicas. (n.d.). Retrieved May 11, 2022, from https://dynamoelectronics.com/5-razones-porque-raspberry-pi-es-tendencia-en-soluciones-tecnologicas/

[12] Qué tipos de sistemas operativos existen | Blog | Hosting Plus Colombia. (n.d.). Retrieved May 11, 2022, from https://www.hostingplus.com.co/blog/que-tipos-de-sistemas-operativos-existen/

[13] Tutor, P. (2012). COSTOS POR ÓRDENES DE PRODUCCIÓN: SU APLICACIÓN A LA INDUSTRIA PAULA GISELLA IAVARONE.

[14] FREDY YESID AVILA NIÑO. (n.d.). EVOLUCIÓN E IMPACTO DEL RANSOMWARE EN AMÉRICA LATINA DESDE EL AÑO 2015. Retrieved April 26, 2022, from https://repository.unad.edu.co/bitstream/handle/10596/42667/fyavilan.pdf?sequence=3&isAllowed=y.

[15] Entrevista a Chema Alonso. (n.d.). Retrieved May 8, 2022, from https://www.campusciberseguridad.com/blog/item/145-entrevista-a-chema-alonso-hacker.

[16] E. A. Espinoza Zallas, R. Rodríguez Pérez, y U. Estatal de Sonora, «Seguridad informática una problemática de las organizaciones en el Sur de Sonora», SINFRONTERA, n.º 25, may 2018.

[17] Seguridad informática en las PyMES de la ciudad de Quevedo - Dialnet. (n.d.). Retrieved May 8, 2022, from https://dialnet.unirioja.es/servlet/articulo?codigo=7888305

[18] Holguín, C. (2019). PDF generado a partir de XML-JATS4R por Redalyc Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto. https://www.redalyc.org/articulo.oa?

[19] Análisis de seguridad perimetral en la Empresa Servitiendas de Colombia y Dsurtiendo. (n.d.). Retrieved May 8, 2022, from https://1library.co/document/z3d86lmy-analisis-seguridad-perimetral-empresa-servitiendas-colombia-dsurtiendo.html

[20] Diseño de un sistema de seguridad perimetral en las instalaciones del consorcio expansión PTAR Salitre, Sede Bogotá D C. (n.d.). Retrieved May 8, 2022, from https://1library.co/document/zgw64x6y-diseno-seguridad-perimetral-instalaciones-consorcio-expansion-salitre-bogota.html

[21] JUAN PABLO RAMIREZ BENAVIDES. (n.d.). DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LOS PROCESOS DE SOPORTE Y DESARROLLO DE SOFTWARE EN LA EMPRESA ALFCOM S.A BASADO EN LA NORMA ISO/IEC 27001:2013. Retrieved May 8, 2022, from http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/11101/TRABAJO%20DE%20GRADO%20ESI43.pdf?sequence=1&isAllowed=y

[22] NANCY ADRIANA GONZÁLEZ. (2020). CASOS DE ESTUDIO DE CIBERCRIMEN EN COLOMBIA. UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA PROYECTO EN SEGURIDAD INFORMÁTICA II. https://repository.unad.edu.co/bitstream/handle/10596/36606/nagonzalezso.pdf?sequence=1&isAllowed=y

[23] Auditoría a la seguridad de la red de datos del Instituto Departamental de Salud de Nariño. (n.d.). Retrieved May 8, 2022, from https://1library.co/document/qo356kkq-auditoria-seguridad-red-datos-instituto-departamental-salud-narino.html

[24] REDISEÑO DE POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD INFORMÁTICA PARA LA GOBERNACIÓN DE NARIÑO. (n.d.). Retrieved May 8, 2022, from https://1library.co/document/y4gw3nry-rediseno-politicas-procedimientos-seguridad-informatica-gobernacion-narino.html

[25] ISO 27001 - Certificado ISO 27001 punto por punto - Presupuesto Online. (n.d.). Retrieved August 12, 2022, from https://normaiso27001.es/

[26] Hurtado, J. S. (2021). Cómo funciona la Metodología Scrum: Qué es y cómo utilizarla. Thinking for Innovation. https://www.iebschool.com/blog/metodologia-scrum-agile-scrum/

[27] FIRMA-E. (2014). Pilares de la Seguridad de la Información: confidencialidad, integridad y disponibilidad | Firma-e. Ciberseguridad/GRC. https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/

[28] ¿QUÉ ES CONFIDENCIALIDAD? - Seguridad y Redes de Datos. (n.d.). Retrieved May 8, 2022, from https://sites.google.com/site/seguridadyredesdedatos/confidencialidad

[29] Confidencialidad de los datos - Seguridad Informática. (n.d.). Retrieved May 8, 2022, from https://sites.google.com/site/seguridadinformaticaeeso213/conceptos-utiles/confidencialidad-de-los-datos

[30] Del libro: «Introducción a la Teoría General de la Administración», Séptima Edición, de Chiavenato Idalberto, McGraw-Hill Interamericana, 2006, Pág. 110.

[31] Del libro: «Introducción a los Negocios en un Mundo Cambiante», Cuarta Edición, de Ferrell O. C. y Hirt Geoffrey, McGraw-Hill Interamericana, 2004, Pág. 121.

[32] De la revista: «E-Ciencias de la Información», de la Universidad de Costa Rica, de Celso Martínez Musiño, 2012, Pág. 2.

[33] La tecnología: sus formas y las diferencias de los medios. Hacia una teoría social pragmática de la tecnificación. (n.d.). Retrieved May 8, 2022, from http://www.ub.edu/geocrit/sn-80.htm

[34] (PDF) La tecnología: Sus formas y las diferencias de los medios. Hacia una teoría social pragmática de la tecnificación. (n.d.). Retrieved May 8, 2022, from https://www.researchgate.net/publication/28054841_La_tecnologia_Sus_formas_y_las_diferencias_de_los_medios_Hacia_una_teoria_social_pragmatica_de_la_tecnificacion

[35] CAPITULO II MARCO TEORICO. (n.d.). Retrieved May 8, 2022, from http://virtual.urbe.edu/tesispub/0104997/cap02.pdf

[36] La seguridad informática en la PYME: Situación actual y mejores prácticas - Jean-François CARPENTIER - Google Libros. (n.d.). Retrieved May 8, 2022, from https://books.google.com.co/books?id=LKE5_6gzBmgC&pg=PA175&lpg=PA175&dq=Se

g%C3%BAn+Jean-Fran%C3%A7ois+Carpentier+detectar+cualquier+cambio+intencional&source=bl&ots=52s2d8Za7N&sig=ACfU3U0T95pA4W5Dd8CW9l9lefDm5gfdAg&hl=es&sa=X&ved=2ahUKEwjVirS5yNP3AhVskGoFHdUOAoEQ6AF6BAgCEAM#v=onepage&q=Seg%C3%BAn%20Jean-Fran%C3%A7ois%20Carpentier%20detectar%20cualquier%20cambio%20intencional&f=false

[37] Dunia Duque. (n.d.). Modelo teórico para un sistema integrado de gestión (seguridad, calidad y ambiente). Retrieved May 8, 2022, from https://www.redalyc.org/pdf/2150/215052403009.pdf

[38] Martha Irene Romero Castro, Grace Liliana Figueroa Moràn, Denisse Soraya Vera Navarrete, José Efraín Álava Cruzatty, Galo Roberto Parrales Anzúles, Christian José Álava Mero, Ángel Leonardo Murillo Quimiz, & Miriam Adriana Castillo Merino. (n.d.). INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES. Octubre 2018. Retrieved May 9, 2022, from https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

[39] Seguridad Informática (GRADO MEDIO) - Jesús Costas Santos - Google Libros. (n.d.). Pag 22. Retrieved May 11, 2022, from https://books.google.com.co/books?id=7I6fDwAAQBAJ&printsec=frontcover&dq=disponibilidad+seguridad+informatica&hl=es&sa=X&redir_esc=y#v=onepage&q=disponibilidad&f=false

[40] Políticas de seguridad informática. (n.d.). Pag 91. Retrieved May 11, 2022, from https://www.redalyc.org/articulo.oa?id=265420388008

[41] Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática. (2016). Pag 15. https://www.redalyc.org/articulo.oa?id=378345292002

[42] Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática. (n.d.). Retrieved May 11, 2022, from http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992016000200002

[43] Cristhian Alexander, R. H. (n.d.). La seguridad informática. Pag 28. Retrieved May 11, 2022, from http://repositorio.unemi.edu.ec/bitstream/123456789/2976/1/LA%20SEGURIDAD%20INFORM%c3%81TICA.pdf

[44] SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. (n.d.). Guía de gestión de riesgos. Pag 6. Retrieved May 11, 2022, from https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

[45] Seguridad de la información. Redes, informática y sistemas de información - AREITIO BERTOLIN, JAVIER - Google Libros. (n.d.). Retrieved May 11, 2022, from https://books.google.com.co/books?id=_z2GcBD3deYC&printsec=frontcover&dq=red+en+seguridad+informatica&hl=es&sa=X&redir_esc=y#v=onepage&q=red%20en%20seguridad%20informatica&f=false

[46] William Stallings. (n.d.). Comunicaciones y Redes de Computadores. Retrieved May 11, 2022, from http://www.uenicmlk.edu.ni/img/biblioteca/ing%20%20en%20sistema%20%20Comunicaciones%20y%20Redes%20de%20Computadores%20-%20William%20Stallings%20-%207ed.pdf

[47] Amelia C, C. S. (n.d.). ANÁLISIS DEL ALGORITMO DE SEGURIDAD EN REDES WIMAX. Pag 19. Retrieved May 11, 2022, from https://www.redalyc.org/pdf/784/78460113.pdf

[48] Firewall – Linux: Una Solución De Seguridad Informática Para Pymes (Pequeñas Y Medianas Empresas). Pag 157. (n.d.). Retrieved May 11, 2022, from https://www.redalyc.org/articulo.oa?id=553756879003

[49] Estrategia para la implantación de nuevas tecnologías en PYMEs - Eloy Seoane - Google Libros. (n.d.). Retrieved May 11, 2022, from https://books.google.com.co/books?id=e9JZeFKjJzwC&pg=PA154&dq=cortafuegos&hl=es&sa=X&ved=2ahUKEwidsIjcjKH3AhUERzABHS-6CGoQ6AF6BAgDEAI#v=onepage&q=cortafuegos&f=false

[50] MYRIAN MARIN OSPINA, R. A. M., BEDOYA, J. A. G., & GOMEZ. (n.d.). MODELO DE SOLUCIÓN DE ENRUTAMIENTO DE DATOS A BAJO COSTO BASADO EN SOFTWARE LIBRE. Pag 209. Retrieved May 11, 2022, from https://www.redalyc.org/pdf/849/84911639036.pdf

[51] Tesis: «ANÁLISIS Y DISEÑO DE UNA PROPUESTA PARA MITIGAR ATAQUES CIBERNÉTICOS A CORREOS ELECTRÓNICOS UTILIZANDO TÉCNICAS DE HACKING ÉTICO», Quito, de FRANCISCO XAVIER ALVEAR REINOSO, 2019, Pág. 15.

[52] Tesis: «Las Vulnerabilidades Humanas En Relación A La Seguridad Informática Para Evitar La Fuga De Información Confidencial En El Departamento De Recursos Humanos De La Universidad Técnica De Ambato», Ambato-Ecuador, de María Gabriela Cortez Pinto, 2013, Pág. 19

[53] Tesis: «DIAGNOSTICO DE LAS VULNERABILIDADES INFORMATICAS EN LOS SISTEMAS DE INFORMACION PARA PROPONER SOLUCIONES DE SEGURIDAD A LA RECTIFICADORA GABRIEL MOSQUERA S.A.», Guayaquil-Ecuador, de Karen Andrea Pintado Cují, Cesar Luis Hurtado Valero, 2015, Pág. 45.

[54] FREDY YESID AVILA NIÑO. (2021). EVOLUCIÓN E IMPACTO DEL RANSOMWARE EN AMÉRICA LATINA DESDE EL AÑO 2015. 10 de Abril 2021. https://repository.unad.edu.co/bitstream/handle/10596/42667/fyavilan.pdf?sequence=3&isAllowed=y

[55] Del libro: «Fundamentos de Marketing», 13va. Edición, de Stanton William, Etzel Michael y Walker Bruce, Mc Graw Hill, 2004, Págs. 333 y 334.

[56] Del libro: «El marketing de Servicios Profesionales», de Kotler Philip, Bloom Paul y Hayes Thomas, Editorial Paidós SAICF, 2004, Págs. 9 y 10.

[57] Zafiro Business Software. (n.d.). Seguridad del ERP y restricciones dentro del sistema - Evaluando ERP. Adaptado Por La División Consultoría de EvaluandoERP.Com. Retrieved May 9, 2022, from https://www.evaluandoerp.com/software-erp/seguridad-erp/

[58] Departamento de Computo COLMICH - Políticas de Seguridad. Retrieved May 9, 2022, from https://www.colmich.edu.mx/computo/index.php?option=com_content&task=view&id=24&Itemid=66

[59] PAULA GISELLA IAVARONE. (n.d.). COSTOS POR ÓRDENES DE PRODUCCIÓN: SU APLICACIÓN A LA INDUSTRIA PANIFICADORA. MENDOZA, 2012. Retrieved May 9, 2022, from https://bdigital.uncu.edu.ar/objetos_digitales/5230/iavaronitrabajodeinvestigacion.pdf

[60] Mónica Franco-Ánge, D. U. (n.d.). Caracterización de las pymes colombianas y de sus fundadores: un análisis desde dos regiones del país. Estudios Gerenciales Vol. 35, N° 150, 2019, 81-91. Retrieved May 9, 2022, from http://www.scielo.org.co/pdf/eg/v35n150/0123-5923-eg-35-150-81.pdf

[61] Rommel Carranco Gudiño MBA. (n.d.). LA APORTACIÓN DE LAS PEQUEÑAS Y MEDIANAS EMPRESAS (PYMES) EN LA ECONOMÍA ECUATORIANA. ACEPTADO: 21/11/2017. Retrieved May 9, 2022, from https://www.uv.mx/iiesca/files/2018/03/14CA201702.pdf

[62] Definición de PYME en la UE. (n.d.). Retrieved May 22, 2022, from http://www.ipyme.org/es-ES/UnionEuropea/UnionEuropea/PoliticaEuropea/Marco/Paginas/NuevaDefinicionPYME.aspx

[63] FREDY YESID AVILA NIÑO. (2021). EVOLUCIÓN E IMPACTO DEL RANSOMWARE EN AMÉRICA LATINA DESDE EL AÑO 2015. Pag 25. https://repository.unad.edu.co/bitstream/handle/10596/42667/fyavilan.pdf?sequence=3&isAllowed=y

[64] Este trabajo está licenciado bajo, & Licencia Reconocimiento-Compartir Igual 4.0 España (CC BY-SA 4.0 ES). (2018). Guía para evitar infecciones de. Septiembre 2018. https://owasp.org/www-pdf-archive/Owasp-guia-evitar-ransomware_es.pdf

[65] El ransomware en móviles también existe: qué es, cómo evitarlo y cómo librarte de él. (n.d.). 13 Mayo 2017 Actualizado 28 Mayo 2018. Retrieved May 9, 2022, from https://www.xatakamovil.com/seguridad/el-ransomware-en-moviles-tambien-existe-que-es-como-evitarlo-y-como-librarte-de-el

[66] Instalar Raspbian en Raspberry Pi - Arrancando raspberry por primera vez. (n.d.). Retrieved May 22, 2022, from https://www.domocasainteligente.com/instalar-raspbian-en-raspberry-pi/

[67] José Daniel Ramírez-Corzo, & Luis Enrique Mendoza. (2016). Desarrollo de un sistema de comunicación silenciosa dual basado en habla subvocal y Raspberry Pi. 18 de Abril de 2016. http://www.scielo.org.co/pdf/rfing/v25n43/v25n43a09.pdf

[68] Ricador Cajo Diaz (2015). Diseño e implementacion de sistema interactivo de informacion de docentes,raspberry pi. https://dspace.ups.edu.ec/handle/123456789/10408

[69] El sistema operativo GNU y el movimiento del software libre. (n.d.). Retrieved May 22, 2022, from https://www.gnu.org/home.es.html

[70] Patrocinado por la Free Software Foundation. (n.d.). ¿Qué es el Software Libre? - Proyecto GNU - Free Software Foundation. 2021/09/02. Retrieved May 9, 2022, from https://www.gnu.org/philosophy/free-sw.es.html

[71] Gladys Stella Rodríguez*. (n.d.). EL SOFTWARE LIBRE Y SUS IMPLICACIONES JURÍDICAS. No 30, Barranquilla, 2008. Retrieved May 9, 2022, from http://www.scielo.org.co/pdf/dere/n30/n30a07.pdf

[72] Vista de Hardware libre en el aula: Una experiencia de capacitación en el uso de recursos educativos abiertos en escuelas técnicas en Tucumán, Argentina. (n.d.). Retrieved May 9, 2022, from https://revistas.unc.edu.ar/index.php/vesc/article/view/27457/29025

[73] (PDF) Desarrollo de hardware libre para la apropiación de tecnología de procesos agrícolas en casas de cultivo. (n.d.). Retrieved May 9, 2022, from https://www.researchgate.net/publication/325576987_Desarrollo_de_hardware_libre_para_la_apropiacion_de_tecnologia_de_procesos_agricolas_en_casas_de_cultivo

[74] Diseño de un sistema de desarrollo con pila TCP/IP basado en un microcontrolador de 16 bits. (n.d.). Pag 82-83. Retrieved May 11, 2022, from http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/806/A6.pdf?sequence=6

[75] Qué es la latencia en informática y cómo medirla. (n.d.). Retrieved May 11, 2022, from https://www.profesionalreview.com/2019/01/03/latencia-en-informatica/

[76] Walter Sanchez. (2011). La usabilidad en Ingeniería de Software: definición y características. Pag 8. https://core.ac.uk/download/pdf/47264961.pdf

[77] Introducción a Nftables - Eduardo Collado. (n.d.). Retrieved May 11, 2022, from https://www.eduardocollado.com/2019/07/12/introduccion-a-nftables/

[78] EALDE. (n.d.). Qué es la seguridad perimetral y cuál es su aplicación. 4 Febrero, 2021. Retrieved May 11, 2022, from https://www.ealde.es/seguridad-perimetral-y-su-aplicacion/

[79] ¿Qué es la latencia y cómo se puede medir? - Movistar. (n.d.). Retrieved May 11, 2022, from https://ww2.movistar.cl/blog/post/que-es-la-latencia/

[80] QUIJANO, Armando, Guía de investigación parte 1 cuantitativa, 1 ed. San Juan de Pasto: INSUCA, 2009. ISBN: 978-958-8439-12-9.

[81] PLAN DE NEGOCIOS COMO ESTRATEGIA COMPETITIVA DEL CAMPAMENTO TOMACOCO. (n.d.). Pag 44. Retrieved May 11, 2022, from http://catarina.udlap.mx/u_dl_a/tales/documentos/lad/armida_r_a/capitulo3.pdf

[82] Método científico - Qué es, definición y concepto | 2022 | Economipedia. (n.d.). Retrieved May 11, 2022, from https://economipedia.com/definiciones/metodo-cientifico.html

[83] Tipos de investigación - Qué es, definición y concepto | 2022 | Economipedia. (n.d.). Retrieved May 22, 2022, from https://economipedia.com/definiciones/tipos-de-investigacion.html

[84] Encuesta - Qué es, definición y concepto | 2022 | Economipedia. (n.d.). Retrieved May 11, 2022, from https://economipedia.com/definiciones/encuesta.html

Sánchez Huarcaya Diana M Revilla Figueroa Mariana Alayza Degola Luis Sime Poma, A. O., & Tafur Puente, R. (2020). Escuela de Posgrado. Pag 51, http://blog.pucp.edu.pe/blog/maestriaeducacion/2020/07/23/los-metodos-de-

[85] Diseño de la Estratégica Metodológica. (2009). https://sites.google.com/a/udo.edu.ve/adsi/diseno-de-la-estrategica-metodologica?tmpl=%2Fsystem%2Fapp%2Ftemplates%2Fprint%2F&showPrintDialog=1

[86] Cámara de Comercio de Pasto. (n.d.). Retrieved May 11, 2022, from https://www.ccpasto.org.co/

[87] en Educación, M., Sánchez Huarcaya Diana M Revilla Figueroa Mariana Alayza Degola Luis Sime Poma, A. O., & Tafur Puente, R. (n.d.). Escuela de Posgrado. Pag 54. Retrieved May 11, 2022, from http://blog.pucp.edu.pe/blog/maestriaeducacion/2020/07/23/los-metodos-de-

[88] Casas Anguita, J., Repullo Labrador, J. R., & Donado Campos, J. (2003). La encuesta como técnica de investigación. Elaboración de cuestionarios y tratamiento estadístico de los datos (I). Atención Primaria, 31(8), Pag 143–144. https://doi.org/10.1016/S0212-6567(03)70728-8

[89] La estructura del cuestionario - Trabajos - JAD8524. (n.d.). Retrieved May 22, 2022, from https://www.clubensayos.com/Temas-Variados/La-estructura-del cuestionario/441493.html

UNIVERSIDAD CESMAG NIT: 800.109.387-7 VIGILADA MINEDUCACIÓN	**CARTA DE ENTREGA TRABAJO DE GRADO O TRABAJO DE APLICACIÓN – ASESOR(A)**	**CÓDIGO:** AAC-BL-FR-032
		VERSIÓN: 1
		FECHA: 09/JUN/2025

San Juan de Pasto, 09 de junio del 2025

Biblioteca
REMIGIO FIORE FORTEZZA OFM. CAP.
Universidad CESMAG
Pasto

Saludo de paz y bien.

Por medio de la presente se hace entrega del Trabajo de Grado / Trabajo de Aplicación denominado Gestión de seguridad informática en PYMES de San Juan de Pasto mediante la implementación de un dispositivo de seguridad perimetral usando software y hardware libre. presentado por el (los) autor(es) José Fernando Imbajoa Sacanambuy del Programa Académico ingeniería de sistemas al correo electrónico biblioteca.trabajosdegrado@unicesmag.edu.co. Manifiesto como asesor(a), que su contenido, resumen, anexos y formato PDF cumple con las especificaciones de calidad, guía de presentación de Trabajos de Grado o de Aplicación, establecidos por la Universidad CESMAG, por lo tanto, se solicita el paz y salvo respectivo.

Atentamente,

Martha Lisbeth León Buritica
Cc. 1087205515
Ingeniería de sistemas
Tel: 3187730426
Correo: mlburitica@unicesmag

INFORMACIÓN DEL (LOS) AUTOR(ES)	
Nombres y apellidos del autor: José Fernando imbajoa sacanambuy	**Documento de identidad:** 1010147780
Correo electrónico: Josfer805@gmail.com	**Número de contacto:** 3112242413
Nombres y apellidos del autor:	**Documento de identidad:**
Correo electrónico:	**Número de contacto:**
Nombres y apellidos del autor:	**Documento de identidad:**
Correo electrónico:	**Número de contacto:**
Nombres y apellidos del autor:	**Documento de identidad:**
Correo electrónico:	**Número de contacto:**
Nombres y apellidos del asesor: Martha Lisbeth león buritica	**Documento de identidad:** 1087205515
Correo electrónico: mlburitica@unicesmag	**Número de contacto:** 3187730426
Título del trabajo de grado: Gestión de seguridad informática en PYMES de San Juan de Pasto mediante la implementación de un dispositivo de seguridad perimetral usando software y hardware libre.	
Facultad y Programa Académico: Facultad de ingeniería - ingeniería de sistemas	

En mi (nuestra) calidad de autor(es) y/o titular (es) del derecho de autor del Trabajo de Grado o de Aplicación señalado en el encabezado, confiero (conferimos) a la Universidad CESMAG una licencia no exclusiva, limitada y gratuita, para la inclusión del trabajo de grado en el repositorio institucional. Por consiguiente, el alcance de la licencia que se otorga a través del presente documento, abarca las siguientes características:

a) La autorización se otorga desde la fecha de suscripción del presente documento y durante todo el término en el que el (los) firmante(s) del presente documento conserve (mos) la titularidad de los derechos patrimoniales de autor. En el evento en el que deje (mos) de tener la titularidad de los derechos patrimoniales sobre el Trabajo de Grado o de Aplicación, me (nos) comprometo (comprometemos) a informar de manera inmediata sobre dicha situación a la Universidad CESMAG. Por consiguiente, hasta que no exista comunicación escrita de mi(nuestra) parte informando sobre dicha situación, la Universidad CESMAG se encontrará debidamente habilitada para continuar con la publicación del Trabajo de Grado o de Aplicación dentro del repositorio institucional. Conozco(conocemos) que esta autorización podrá revocarse en cualquier momento, siempre y cuando se eleve la solicitud por escrito para dicho fin ante la Universidad CESMAG. En estos eventos, la Universidad CESMAG cuenta con el plazo de un mes después de recibida la

petición, para desmarcar la visualización del Trabajo de Grado o de Aplicación del repositorio institucional.

b) Se autoriza a la Universidad CESMAG para publicar el Trabajo de Grado o de Aplicación en formato digital y teniendo en cuenta que uno de los medios de publicación del repositorio institucional es el internet, acepto(amos) que el Trabajo de Grado o de Aplicación circulará con un alcance mundial.
c) Acepto (aceptamos) que la autorización que se otorga a través del presente documento se realiza a título gratuito, por lo tanto, renuncio(amos) a recibir emolumento alguno por la publicación, distribución, comunicación pública y/o cualquier otro uso que se haga en los términos de la presente autorización y de la licencia o programa a través del cual sea publicado el Trabajo de grado o de Aplicación.
d) Manifiesto (manifestamos) que el Trabajo de Grado o de Aplicación es original realizado sin violar o usurpar derechos de autor de terceros y que ostento(amos) los derechos patrimoniales de autor sobre la misma. Por consiguiente, asumo(asumimos) toda la responsabilidad sobre su contenido ante la Universidad CESMAG y frente a terceros, manteniéndose indemne de cualquier reclamación que surja en virtud de la misma. En todo caso, la Universidad CESMAG se compromete a indicar siempre la autoría del escrito incluyendo nombre de(los) autor(es) y la fecha de publicación.
e) Autorizo(autorizamos) a la Universidad CESMAG para incluir el Trabajo de Grado o de Aplicación en los índices y buscadores que se estimen necesarios para promover su difusión. Así mismo autorizo (autorizamos) a la Universidad CESMAG para que pueda convertir el documento a cualquier medio o formato para propósitos de preservación digital.

NOTA: En los eventos en los que el trabajo de grado o de aplicación haya sido trabajado con el apoyo o patrocinio de una agencia, organización o cualquier otra entidad diferente a la Universidad CESMAG. Como autor(es) garantizo(amos) que he(hemos) cumplido con los derechos y obligaciones asumidos con dicha entidad y como consecuencia de ello dejo(dejamos) constancia que la autorización que se concede a través del presente escrito no interfiere ni transgrede derechos de terceros.

Como consecuencia de lo anterior, autorizo(autorizamos) la publicación, difusión, consulta y uso del Trabajo de Grado o de Aplicación por parte de la Universidad CESMAG y sus usuarios así:

- Permito(permitimos) que mi(nuestro) Trabajo de Grado o de Aplicación haga parte del catálogo de colección del repositorio digital de la Universidad CESMAG por lo tanto, su contenido será de acceso abierto donde podrá ser consultado, descargado y compartido con otras personas, siempre que se reconozca su autoría o reconocimiento con fines no comerciales.

En señal de conformidad, se suscribe este documento en San Juan de Pasto a los 9 días del mes de junio del año 2025

 rma del autor Firma del autor	Firma del autor
Nombre del autor: José Fernando imbajoa	Nombre del autor:
Firma del autor	Firma del autor
Nombre del autor:	Nombre del autor:

_____

Nombre del asesor: Martha Lisbeth León Buritica