UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES E COMUNICACIÓN

IMPLEMENTACIÓN DE UN FIREWALL DE SIGUIENTE GENERACIÓN QUE MINIMICE EL RIESGO QUE CORREN LOS NIÑOS AL NAVEGAR POR INTERNET EN UNA RED DOMÉSTICA

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

AUTOR: GUANOTOA CHUMA ALEXANDER MAURICIO

DIRECTOR: MSC. VÁSQUEZ AYALA CARLOS ALBERTO

IBARRA - ECUADOR

2024

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley Orgánica de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte de manera digital para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1004979991		
APELLIDOS Y NOMBRES:	Guanotoa Chuma Alexander Mauricio		
DIRECCIÓN:	Ibarra – La Florida, El Rosal 6-129		
EMAIL:	alexander_guanotoa@hotmail.com		
TELÉFONO FIJO:	-	**TELÉFONO MÓVIL:**	0999116449

DATOS DE LA OBRA		
TÍTULO:	Implementación de un Firewall de Siguiente Generación que minimice el riesgo que corren los niños al navegar por internet en una red doméstica.	
AUTOR:	Guanotoa Chuma Alexander Mauricio	
FECHA DE APROBACIÓN:	01 de febrero 2024	
PROGRAMA:	☑ PREGRADO	☐ POSGRADO
TÍTULO POR EL QUE OPTA:	Ingeniería en Electrónica y Redes de Comunicación	
ASESOR / DIRECTOR:	MsC. Carlos Alberto Vásquez Ayala	

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 1 días del mes de FEBRERO de 2024

EL AUTOR:

(Firma).....

Nombre: Alexander Mauricio Guanotoa Chuma

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

MAGISTER CARLOS VÁSQUEZ, DIRECTOR DEL PRESENTE TRABAJO DE TITULACIÓN CERTIFICA:

QUE, EL PRESENTE TRABAJO DE TITULACIÓN "IMPLEMENTACIÓN DE UN FIREWALL DE SIGUIENTE GENERACIÓN QUE MINIMICE EL RIESGO QUE CORREN LOS NIÑOS AL NAVEGAR POR INTERNET EN UNA RED DOMÉSTICA". Ha sido desarrollado por el señor Guanotoa Chuma Alexander Mauricio bajo mi supervisión.

Es todo en cuanto puedo certificar en honor a la verdad.

MsC. Carlos Alberto Vásquez Ayala

CC: 1002424982

DIRECTOR

DEDICATORIA

Este trabajo se lo dedico:

A mis padres Rosa y Mauricio, quienes me han brindado su apoyo incondicional durante todo este tiempo de formación académica, a mi hijo Nicolas quien ha sido la motivación más grande para seguir adelante a pesar de las adversidades.

Alexander Guanotoa

AGRADECIMIENTO

Agradezco a mis padres quienes siempre se han preocupado por mí, brindándome su apoyo y sus consejos siempre, especialmente en los momentos más difíciles, alentándome a seguir siempre adelante.

A mi esposa Dayana quien es mi compañera de vida y mi hijo Nicolas quien siempre me motiva a ser mejor.

A mi profesor y director MSc. Calos Vásquez quien supo guiarme con su conocimiento y consejo para el desarrollo y culminación de este trabajo de titulación.

A mis amigos de la Universidad Israel, Andrés, Jonathan con quienes compartí gratos momentos durante el inicio de mi formación en la carrera, a Mónica, Fredy, Will, Max, Chandi, Santiago y Jampy, quienes nunca se negaron a compartir su conocimiento y brindarme su apoyo cuando los necesitaba.

Alexander Guanotoa

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente proyecto desarrolla un sistema de seguridad para las redes domésticas, basado en un Firewall de Siguiente Generación (NGFW) con un enfoque a la protección de los niños mientras navegan en internet. El objetivo del sistema es que, mediante la implementación de una capa adicional de seguridad, que consta de la aplicación de políticas de control acceso a contenidos y aplicaciones, permisos basados en usuarios y monitoreo de las actividades se impida que los menores sean vulnerados por los riesgos que conllevan la navegación libre en internet.

Para el diseño del sistema se implementó la metodología del modelo iterativo, que permite la evaluación constante del sistema y la aplicación de cambios en cualquier etapa hasta cumplir con los objetivos planteados. El sistema se encuentra conformado principalmente por 2 dispositivos electrónicos, para el acceso se utilizó un Access Point con capacidades de implementación de VLANs y para el procesamiento se utilizó un MiniPC basado en arquitectura x86_64.

Este sistema tiene la capacidad de filtrado de paquetes avanzado, identificación de aplicaciones y usuarios, control de acceso avanzado, prevención de intrusiones, detección de malware, control de contenido web y generación de informes detallados. Esta solución mejorará significativamente la seguridad de red y brindará visibilidad y control mejorado sobre el tráfico y las aplicaciones.

El sistema cuenta además con una WebUI que facilita la implementación de las políticas, la gestión de los usuarios y el monitoreo de la actividad de la red interna, logrando de esta forma elevar la capacidad de control que se tiene sobre la red.

ABSTRACT

The present project develops a security system for home networks, based on a Next-Generation Firewall (NGFW) with a focus on protecting children while they browse the internet. The system's objective is to provide an additional layer of security by implementing access control policies for content and applications, user-based permissions, and activity monitoring, aiming to prevent minors from being exposed to the risks associated with unrestricted internet browsing.

For the system design, an iterative model methodology was implemented, allowing for continuous evaluation and the application of changes at any stage to meet the set objectives. The system primarily consists of two electronic devices: an Access Point with VLAN implementation capabilities for access and a MiniPC based on x86_64 architecture for processing.

This system has advanced packet filtering capabilities, application and user identification, advanced access control, intrusion prevention, malware detection, web content control, and detailed reporting. This solution will significantly enhance network security and provide improved visibility and control over traffic and applications.

Furthermore, the system features a WebUI that simplifies policy implementation, user management, and monitoring of internal network activity, thereby increasing control over the network.

Capítulo I: Antecedentes

1.1 Tema

Implementación de un Firewall de Siguiente Generación que minimice el riesgo que corren los niños al navegar por Internet en una red doméstica.

1.2 Problema

De acuerdo con (Puerta et al., 2008) jóvenes y adultos consideran a las computadoras como una fuente de información confiable y exacta. En los últimos años el despliegue de las redes de internet ha ido en aumento, llegando cada vez a más lugares y siendo más accesible, lo que ha desplegado el uso de nuevos productos y servicios en donde las personas gozan de acceso a la información de forma ilimitada y que además brinda nuevas oportunidades para la interacción y comunicación. Sin embargo, esto conlleva a tener una nueva puerta abierta ante los peligros y vulnerabilidades que conlleva el tener a los niños sin supervisión.

El (Consejo Nacional para la Igualdad Intergeneracional, 2020) expresa que a raíz de la emergencia sanitaria a causa del COVID-19 se experimentó una digitalización acelerada para los niños, niñas y adolescentes del Ecuador, esto como mecanismo de acceso para la implementación y uso en la educación, la interacción social y la recreación. De acuerdo con la Encuesta Nacional Multipropósito de Hogares 2020 desarrollada por el (Instituto Nacional de Estadística y Censos, 2020), en el año 2019 el 49,45% de las personas entre los 5 y 15 años utilizaban internet, mientras que para el año 2020 esta cifra aumentó hasta el 79,27%. En el 2019 el 68,12% de las personas encuestadas accedía a internet desde su hogar, mientras que en 2020 esta cifra aumentó hasta llegar al 86,12%, lo que significa un crecimiento importante en cuando al uso de internet en los hogares en el Ecuador, especialmente en el grupo que contiene al sector objetivo el cual son los niños, que por su inexperiencia resultan ser los más vulnerables y susceptibles ante los peligros de la web.

Los tutores de los menores deben tener la capacidad de identificar y tomar acciones para evitar que estos sean víctimas del contenido sensible que es de libre acceso en Internet, para que esto sea realizable se vuelve necesario la implementación de mecanismos de filtrado y control de contenidos como Firewalls avanzados basados en nuevas tecnologías de análisis como lo son los Next-Generation Firewall.

Cada vez más personas gozan de un acceso libre a internet, sin embargo, esto genera la necesidad de controlar el acceso a los más vulnerables de la sociedad, que son los niños, niñas y adolescentes para salvaguardar su integridad y seguridad, debido a que la red puede resultar ser un lugar peligroso para navegar si no se cuenta con la vigilancia continua de un adulto responsable que sea capaz de discernir entre el tipo de contenido consumido.

1.3 Objetivos

1.3.1 Objetivo General

Implementar un Firewall de Siguiente Generación (NGFW) desarrollado en Linux que minimice el riesgo que corren los niños mientras navegan por Internet mediante el control y filtrado avanzado de contenidos en una red doméstica.

1.3.2 Objetivos Específicos

Describir los fundamentos teóricos de los diferentes tipos de Firewalls, funciones de los Firewalls de Siguiente Generación y afecciones del uso de internet en edades tempranas mediante la recopilación y análisis de información para la selección de la mejor solución.

Determinar la combinación adecuada de componentes de software y hardware a implementar en el Firewall de Nueva Generación, mediante la aplicación de la metodología del modelo iterativo.

Definir las políticas del Firewall de Nueva Generación, mediante en una simulación del sistema de seguridad con el software GNS3, para verificar sus características y funciones como el filtrado de tráfico, control de aplicaciones y gestión de niveles de acceso de los usuarios en un entorno controlado.

Comprobar la efectividad del sistema, mediante la implementación en una red doméstica, para verificar la funcionalidad del Firewall de Nueva Generación en un entorno real.

1.4 Alcance

Para el desarrollo de este proyecto se aplicará la metodología del modelo iterativo, en el cual de acuerdo con (Eby, 2019), se desarrollarán las siguientes etapas:

Durante la etapa de planificación y requisitos se realizará la fundamentación teórica de los tipos de Firewalls existentes y sus diversas características de acuerdo con el tipo de aplicación, los sistemas de Detección y Prevención de Intrusos (IDS e IPS), Sandbox como solución de seguridad, Gestión unificada de amenazas (UTM), Segmentación de redes mediante VLANS, además de la revisión del estado del arte sobre las soluciones de seguridad basadas en Software Libre, para que de esta manera se pueda elegir el tipo de Sistema operativo y Hardware que se adecuen a las necesidades del proyecto, además se analizará la situación actual de las redes domésticas, determinando los tipos de dispositivos finales más comúnmente presentes en este tipo de redes mediante encuestas, la revisión y análisis de estadísticas locales.

En la etapa de análisis y diseño se definirán las políticas a aplicar en el Firewall de acuerdo con las necesidades y requerimientos de la red, además se realizará la segmentación de la red mediante la difusión de 3 SSID asociadas a distintas VLANs de acuerdo al tipo de usuarios, tanto para la seguridad de la red, como para la segregación de las redes, se aplicará el manual de buenas prácticas propuestas en el estándar ISO/IEC 27002, se realizará la selección de hardware y software mediante la técnica de benchmarking para elegir la opción más idónea de acuerdo con las funciones y la escalabilidad del sistema, se establecerá la topología de red a desarrollar en la cual se establecerán las configuraciones del firewall de siguiente generación tales como; enrutamiento, visualización de estadísticas de tráfico, aplicación reglas de tráfico, monitor de contenidos para la validación de firmas y certificados digitales, implementación de un Directorio Activo para la gestión y monitoreo de los usuarios así como la asignación de sus niveles de acceso.

Para la etapa de implementación se levantará la topología de red en el Software de simulación de redes GNS3, lo que permitirá establecer las configuraciones del Firewall tales como: las reglas de control de tráfico basado en aplicaciones, la configuración de los diferentes tipos de Usuarios en el Directorio Activo, la segmentación de la red mediante la aplicación de VLANs para cada SSID permitiendo una mejor gestión y aislamiento de las subredes (Herbst, 2017), la intercomunicación de los dispositivos en las distintas subredes mediante el protocolo 802.1Q, se realizará la integración de los sistemas de detección y prevención de intrusos (IDS e IPS) los que se encargaran de la inspección profunda del tráfico mediante la comparación de firmas y certificados digitales.

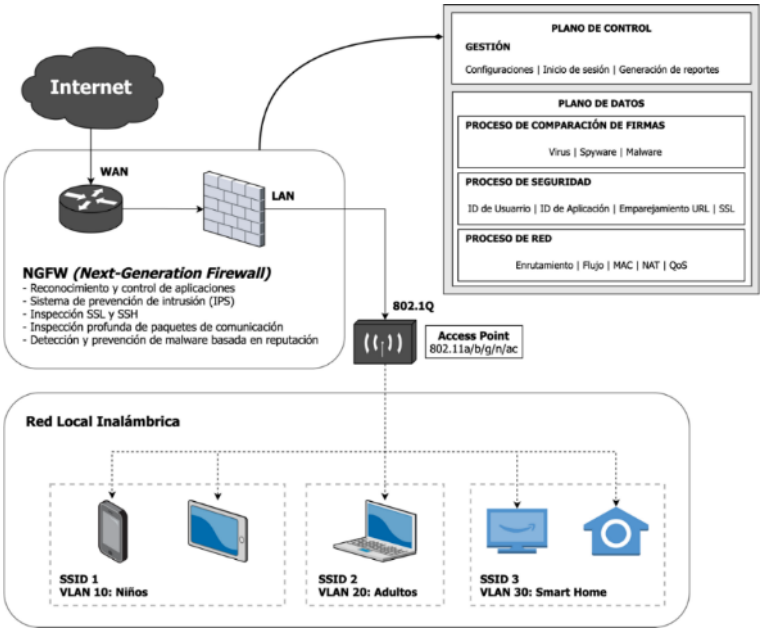
Durante la etapa de pruebas se instalará el Firewall en una red doméstica en donde se comprobarán las capacidades y funcionalidades del Sistema de Seguridad propuesto, verificando el correcto filtrado, control y análisis del tráfico de red de acuerdo con las políticas establecidas e implementadas en el Firewall, se comprobará además el proceso de

autenticación de los usuarios de la red con el Directorio Activo.

En la etapa de Evaluación y Revisión se compararán los resultados obtenidos en la etapa de pruebas con los requisitos iniciales, se verificará el nivel de cumplimiento de las políticas y funciones establecidas, mediante la aplicación del proceso iterativo se realizarán las modificaciones y adición de funcionalidades hasta cubrir completamente los requisitos del Sistema de Seguridad, finalmente se aplicará el Modelo de calidad establecido por el estándar ISO/IEC 9126 para verificar los parámetros de cumplimiento en cuanto a: funcionalidad, confiabilidad, usabilidad, eficiencia, mantenibilidad, y portabilidad.

Figura 1

Arquitectura de red



1.5 Justificación

Debido a la emergencia sanitaria causada por la Covid-19, se dio paso a una digitalización más acelerada, lo que a su vez llevó al incremento de los riesgos al usar internet, nuevos tipos de amenazas y transgresión de derechos, especialmente para los niños, niñas y adolescentes en el Ecuador (Agencia de Regulación y Control de las Telecomunicaciones, 2020).

En ocasiones resulta incontrolable el contacto que los niños pueden llegar a tener con extraños en la web, además de la navegación sin control que estos experimentan en sus tiempos libres. La falta de “control” durante el uso de internet, genera que sean vulnerables a los peligros de la red, como el ciberacoso, pornografía infantil, sexting, entre otros, consecuente a ello, la vulneración de sus derechos como la vida, la integridad, la dignidad y la libertad, entonces, se deben crear estrategias para proteger a este grupo vulnerable en donde es necesaria la integración los diferentes entes de la sociedad (Ministerio de Inclusión Económica y Social et al., 2020).

En la actualidad los equipos terminales de red que se instalan en los hogares son equipos básicos sin capacidades de control de tráfico, debido a que los proveedores de internet usan estos equipos por su bajo coste y porque cumplen con la principal funcionalidad que es la de brindar el servicio, pero esto conlleva a un sacrificio en temas de seguridad en el cual se vuelve responsabilidad del usuario final la gestión y protección de su red interna (El Universo, 2021).

Un firewall tradicional se limita a funciones como filtrado de paquetes, traducción de direcciones de red y puerto (NAT) y VPN, toma sus decisiones basándose en puertos, protocolos y direcciones IP (Cortés Aldana, 2016). Hoy en día ya no es práctico ni confiable implementar políticas de seguridad de una manera tan inflexible y poco transparente. Los NGFW brindan un nuevo enfoque al agregar más robustez a las políticas de seguridad. Estos sistemas están diseñados para utilizar información como ubicación, identidad u hora, de forma inteligente con el propósito de tomar decisiones de seguridad más efectivas (Orange Cyberdefense, 2017).

Los cortafuegos de próxima generación protegen a las redes mediante funciones de seguridad avanzadas. Los NGFW brindan funciones como inspección profunda de

paquetes, prevención de intrusiones (IPS), detección avanzada de malware, control de aplicaciones y mayor visibilidad general de la red a través de la inspección del tráfico cifrado (Shah, 2021).

Con la implementación del presente proyecto se busca proteger a los usuarios más vulnerables del hogar que son los niños, este Firewall de Siguiente Generación tendrá la capacidad de gestionar de forma inteligente los horarios y los contenidos a los que estos usuarios acceden desde sus dispositivos, que se encontrarán correctamente identificados y autenticados en la red.

Capítulo II: Marco Teórico

2.1 Redes de Datos

Las redes de datos son sistemas diseñados para transferir datos entre dos o más puntos de acceso mediante el uso de controles de sistema, líneas de transmisión y conmutación de datos.

En general, las redes de datos se definen por su capacidad para transmitir señales a través de la conmutación de paquetes. El mensaje de datos se divide en bits discretos llamados paquetes, y estos paquetes luego se envían a través de una red digital que utiliza una ruta óptima para minimizar el retraso en la velocidad de la red de datos. Una vez transmitidos, los paquetes de datos se vuelven a ensamblar al llegar al destino (World Wide Technology, 2021).

2.1.1 Usos de las redes de datos

Las redes informáticas tienen una variedad de usos, entre los principales se encuentran los siguientes (Gillis, 2021):

- **Uso compartido de archivos:** permite a los usuarios compartir archivos de datos a través de una red.
- **Uso compartido de aplicaciones:** permite a los usuarios compartir aplicaciones a través de una red.
- **Uso compartido de Hardware:** permite a los usuarios de una red compartir dispositivos de hardware, como impresoras y discos duros.
- **Modelo Cliente-Servidor:** permite que los datos se almacenen en servidores, donde los dispositivos de los usuarios finales (o clientes) pueden acceder a esos datos.
- **Voz sobre IP (VoIP):** permite a los usuarios enviar datos de voz a través de protocolos de internet.

- **Comunicación:** puede incluir video, texto y voz;
- **Comercio electrónico:** permite a los usuarios vender y comprar productos a través de internet.
- **Juegos:** permite que varios usuarios jueguen juntos desde varios lugares.

2.1.2 Ventajas

Hay varias ventajas para configurar una arquitectura de red de datos (Mostak, 2021):

- **Recursos compartidos:** una red de datos permite compartir información sin necesidad de una conexión física. Se pueden compartir recursos como impresoras, almacenamiento e Internet.
- **Comunicación:** vincular computadoras a través de una red de datos permite una comunicación fácil y rápida, como correos electrónicos y transferencias de archivos, sin necesidad de un medio de transferencia físico, como una unidad flash USB.
- **Colaboración:** varios usuarios en diferentes ubicaciones pueden trabajar de forma colaborativa y simultánea en el mismo documento o proyecto de forma remota.
- **Software almacenado centralmente:** un usuario determinado con credenciales de acceso puede acceder de forma remota a una sola copia del software almacenado en un recurso central.
- **Base de datos central:** cualquier miembro relevante de una organización puede acceder a una base de datos central a través de redes de datos con credenciales de acceso

El avance de las tecnologías de redes de datos ha cambiado la forma en que los sistemas de redes informáticas comparten datos. Donde antes bastaba con una sola conexión, ahora es necesario el uso de tecnologías de redes informáticas, como

concentradores de red, conmutadores y enrutadores, para enrutar datos a través de una gran variedad de rutas y entre una gran cantidad de nodos diferentes.

2.1.3 Topologías

La topología de red corresponde a una disposición física a través de la cual varios dispositivos de red se comunican entre sí. Los administradores de red utilizan la topología para definir cómo se vinculan los nodos entre sí. Existen dos categorías principales de topología los cuales son física y lógica. La topología de red física se refiere a la estructura del medio físico para la transmisión de datos. Por otro lado, la topología de red lógica se refiere a cómo la red transmite datos entre dispositivos, independientemente de cómo estos dispositivos estén conectados físicamente (Ashtari, 2022).

La estructura de una red puede afectar directamente a su funcionamiento. Por lo tanto, el administrador de red debe seleccionar la topología más adecuada para su red para reforzar el rendimiento y mejorar la eficiencia de los datos. La topología correcta también optimiza la asignación de recursos y minimiza los costos operativos.

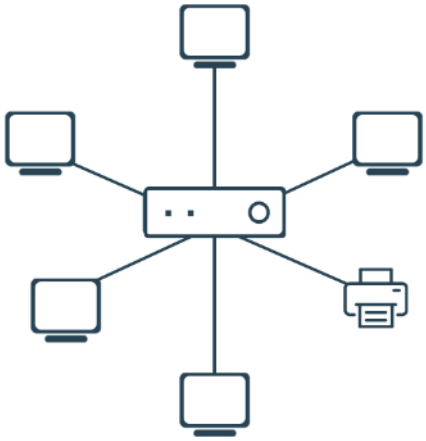
Existen diferentes tipos de topologías de red y el administrador puede elegir la que mejor se adapte a sus requisitos teniendo en cuenta el tamaño, el presupuesto y los objetivos de su organización.

2.1.3.1 Topología en estrella

En una topología en estrella, todos los nodos están conectados a un concentrador central mediante un enlace de comunicación. Como se muestra en la Figura 2 cada nodo necesita un cable separado para establecer una conexión punto a punto con el concentrador, que funciona como un servidor para controlar y administrar toda la red (Ashtari, 2022).

Figura 2

Topología en estrella



Nota. Tomado de What Is Network Topology?, por Ashtari, 2022, spiceworks (https://www.spiceworks.com/tech/networking/articles/what-is-network-topology/)

2.1.4 Dispositivos de la Red de Datos

Al referirse a dispositivos de red, son todos aquellos que forman parte de una red informática, se habla de aquellas piezas físicas que hacen posible la comunicación, como por ejemplo las tarjetas de red, los enrutadores o los switches que sustentan la transmisión de los datos. Los equipos de red impulsan, combinan o transfieren paquetes de información usando protocolos específicos en una red.

De acuerdo con (SolarWinds, 2021) la interconexión entre varios dispositivos de comunicación a través de diferentes enlaces de comunicación se puede definir como una red. La red se utiliza para intercambiar, almacenar, enviar y recuperar datos entre dispositivos de red, también conocidos como nodos de red. Cada nodo de la red actúa como un punto de conexión para la transmisión de datos, el reconocimiento de procesos, la conmutación de paquetes y la distribución de la red. Generalmente, los nodos están programados para identificar, procesar y transmitir datos de un nodo a otro. Pueden realizar varias funciones según la aplicación y la red.

En una red, se utilizan múltiples nodos. Un nodo puede ser una computadora, una impresora, un conmutador o un enrutador. Los nodos dependen en gran medida de la red de referencia y de la capa de protocolo para formar una conexión de red. Además, cada nodo de una red incluye una dirección IP única.

2.1.4.1 Access Point

Un punto de acceso (AP) es un dispositivo que envía y recibe datos de forma inalámbrica a través de frecuencias de radio, utilizando las bandas de 2,4 GHz o 5 GHz. Los clientes como: computadoras portátiles o teléfonos móviles, se conectan a un AP mediante una señal inalámbrica, lo que les permite unirse a la LAN inalámbrica creada por el AP. Un cable Ethernet conecta físicamente el AP a un enrutador o conmutador en una LAN cableada, lo que proporciona al AP acceso a Internet y al resto de la red (English, 2022).

2.1.4.2 Router

Es el que se encarga de dirigir las solicitudes de datos de una red a otra. Los enrutadores examinan los paquetes entrantes para determinar la dirección IP de destino adecuada y luego reenvían el paquete a ese destino. Un enrutador también puede permitir el acceso a Internet a través de su conexión con un módem, esto es lo más común en las redes domésticas en donde se implementan Router de tipo doméstico, que combina las capacidades de un Switch, un Access Point y Router y un Modem (English, 2022).

Los enrutadores mantienen y usan tablas de enrutamiento que contienen información de ruta, como direcciones IP e interfaces. Una vez que un enrutador inspecciona un paquete, se basa en la información de la tabla de enrutamiento para encontrar la mejor ruta hacia el destino. Los enrutadores utilizan protocolos de enrutamiento para comunicarse e intercambiar datos.

2.1.4.3 Switch

El Switch o conmutador de red reenvía datos a su destino examinando la dirección MAC de una trama entrante y enviándola al dispositivo con la dirección correspondiente.

Los dispositivos se conectan a los puertos de un conmutador generalmente a través de un cable Ethernet. El conmutador almacena las direcciones MAC de esos dispositivos en una tabla de direcciones que utiliza como referencia al transferir tramas. Mientras que un enrutador envía datos a una dirección IP o red, un conmutador envía la información directamente al puerto de destino específico.

2.1.4.4 ONU

En una red de fibra, la ONT/ONU se encuentra en tu domicilio. El propósito de este dispositivo es usar fibra óptica para conectarse a la red óptica pasiva (PON) y comunicarse con su proveedor de servicios de Internet para obtener una conexión a Internet.

Una ONU está ubicada fuera del hogar. Una ONU convierte señales ópticas en señales eléctricas a través de un cable de fibra. Una ONU organiza y optimiza diferentes tipos de datos provenientes de los clientes para enviarlos de manera eficiente al OLT. (Hitron Technologies Americas, 2020).

2.1.4.5 Firewall

Un Firewall es un dispositivo de hardware o software entre una computadora y el resto de la red abierto a atacantes o piratas informáticos. Por lo tanto, una LAN puede protegerse de los atacantes informáticos colocando un firewall entre la LAN y la conexión a Internet. Un firewall permite el paso de conexiones autorizadas y correos electrónicos o páginas web similares a datos, pero bloquea las conexiones no autorizadas realizadas a una computadora o LAN (Kanade, 2022).

2.2 Redes Inalámbricas

Una red inalámbrica se refiere a una red informática que utiliza conexiones de radiofrecuencia (RF) entre los nodos de la red. Las redes inalámbricas representan una solución popular para hogares, empresas y redes de telecomunicaciones.

Las redes inalámbricas están presentes casi en cualquier sitio en donde la gente resida o trabaje, a pesar de ello la mayoría desconoce su funcionamiento. De la misma manera las personas comúnmente asumen que todas las conexiones inalámbricas se refieren al denominado Wi-Fi, lo cual no es cierto ya que esta es una de las varias tecnologías existentes (Bluetooth, ZigBee, LTE, 5G), mientras que Wi-Fi es específico para el protocolo inalámbrico definido por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) en la especificación 802.11 (Fortinet, 2021).

2.2.1 Estándar IEEE 802.11

De acuerdo con (Juniper Networks, 2018), el estándar de red utilizado por la arquitectura inalámbrica es IEEE 802.11. Sin embargo, esta norma está en continuo desarrollo y periódicamente se publican nuevas modificaciones. A los distintos protocolos de la norma se les asignan letras y aunque se han publicado varios, los más conocidos son:

2.2.1.1 802.11a

En este estándar se agregó soporte para la banda de 5 GHz, lo que permite la transmisión de hasta 54 megabits de datos por segundo. El estándar 802.11a utiliza multiplexación por división de frecuencia ortogonal (OFDM). Divide la señal de radio en subseñales antes de que lleguen a un receptor. 802.11a es el estándar más antiguo y ha sido reemplazado en gran medida por tecnologías más nuevas.

2.2.1.2 802.11b

802.11b agregó velocidades más rápidas en la banda de 2,4 GHz al estándar original. Puede pasar hasta 11 megabits de datos en un segundo. Utiliza modulación de codificación de código complementario (CCK) para lograr mejores velocidades.

2.2.1.3 802.11g

802.11g estandarizó el uso de la tecnología OFDM utilizada en 802.11a en la banda de 2,4 GHz. Era compatible con versiones anteriores de 802.11 y 802.11b.

2.2.1.4 802.11n

Durante este periodo fue la primera vez que la norma era unificada y cubría las bandas de 2.4GHz y 5GHz. Este protocolo ofrece una mejor velocidad en comparación con los que le precedieron al aprovechar la idea de transmitir utilizando múltiples antenas simultáneamente, tecnología generalmente llamada Multiple In Multiple Out (MIMO).

2.2.1.5 802.11ac

En 802.11ac solo se especificó para la banda de 5 GHz. Se basó en los mecanismos introducidos en 802.11n. Si bien no fue tan revolucionario como lo fue 802.11n, amplió las velocidades y las capacidades en la banda de 5 GHz. La mayoría de los dispositivos en la actualidad disponibles son probablemente dispositivos 802.11ac.

La tecnología 802.11ac se lanzó en dos grupos principales, generalmente llamados "ondas". La principal diferencia es que los dispositivos Wave 2 tienen algunas capacidades técnicas más en comparación con Wave 1, pero todos son interoperables.

2.2.1.6 802.11ax (Wi-Fi 6)

802.11ax (al igual que 802.11n) unificó la especificación en todas las bandas de frecuencia aplicables. En nombre de la simplicidad, la industria comenzó a referirse a él

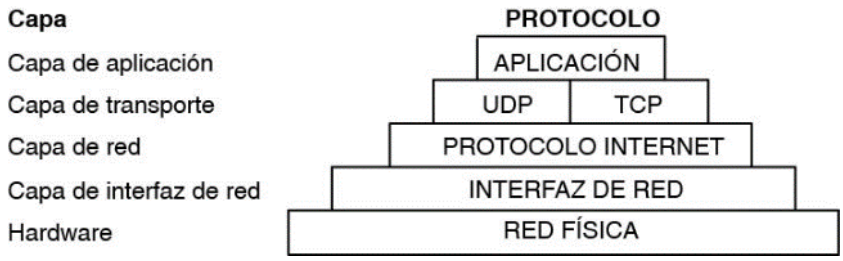
como Wi-Fi 6. Wi-Fi 6 ha ampliado las tecnologías utilizadas para la modulación para incluir OFDMA, que permite un uso más eficiente del espectro disponible y mejora el rendimiento general de la red. Wi-Fi 6 es la última tecnología y es con lo que disponen la mayoría de los dispositivos nuevos.

2.3 TCP/IP

El flujo de información entre las computadoras se hace posible a través de los protocolos, que son reglas que establecen los formatos de mensajes y operaciones. Para que el host receptor pueda comprender el mensaje, cada computadora involucrada en la transmisión debe cumplir con estas reglas. Las capas, como se muestran en la Figura 3 son una forma útil de conceptualizar el conjunto de protocolos (o niveles) de TCP/IP.

Figura 3

Conjunto de protocolos TCP/IP



Nota. Adaptado de TCP/IP Protocols, por IBM, 2022, IBM Documentation (https://www.ibm.com/docs/en/aix/7.3?topic=protocol-tcpip-protocols).

El flujo de información del remitente hacia el receptor está definido con precisión por el modelo TCP/IP. Los programas de aplicación primero transmiten flujos de datos o mensajes a uno de los Protocolos de capa de transporte de Internet, como el Protocolo de datagramas de usuario (UDP) o el Protocolo de control de transmisión (TCP). Estos protocolos toman los datos de la aplicación, los dividen en unidades más pequeñas conocidas como paquetes, agregan una dirección de destino y luego transmiten los paquetes a la siguiente capa de protocolo, la capa de red de Internet.

La capa de red de Internet convierte el paquete en un datagrama IP, inserta el encabezado y el final, elige si enviar el datagrama directamente al destino o a través de una puerta de enlace y luego transfiere el datagrama a la capa de interfaz de red (IBM, 2022).

2.3.1 Dirección MAC

Al igual que cada persona tiene una Cédula de Identidad, cada dispositivo conectado a una red tiene una Dirección de Control de Acceso a Medios (MAC) que lo identifica de manera única.

La dirección MAC está vinculada al controlador de interfaz de red (NIC), La NIC es donde se realiza la conexión física a la red, conectando un cable Ethernet o mediante una señal WiFi (Link, 2021).

2.3.2 Dirección IP

La dirección IP es la dirección única que permite identificar a un dispositivo en una red local o en internet. IP o "Internet Protocol", es el conjunto de reglas que determinan el formato de los datos que se envían a través de la red.

Esencialmente, las direcciones IP son el identificador que permite la comunicación entre dispositivos que conforman una red. Dentro de Internet es necesaria una forma de diferenciar entre los diferentes enrutadores, ordenadores y sitios web. Las direcciones IP proporcionan una forma de hacerlo siendo una parte esencial del funcionamiento de Internet (AO Kaspersky Lab, 2022).

La forma en que funciona el Protocolo de Internet es que la información se transmite a través de la red en fragmentos discretos llamados paquetes; cada paquete se compone

principalmente de los datos que el remitente intenta comunicar, pero también incluye un encabezado que consta de metadatos sobre ese paquete.

Entre otros datos almacenados en el encabezado del paquete se encuentran la dirección IP del dispositivo que envió el paquete y la dirección IP del dispositivo al que se dirige el paquete. Los enrutadores y otra infraestructura de red usan esta información para asegurarse de que los paquetes lleguen a donde se supone que deben ir (Fruhlinger, 2022).

2.3.3 Puertos Lógicos de Red

Un puerto lógico es un número que se asigna a una conexión "lógica" en informática. En TCP/IP y UDP, es el punto final de una conexión lógica que especifica un servicio. Hay 65.536 puertos TCP y 65.536 puertos UDP. A un servicio se le asigna un número de puerto, lo que ayuda a TCP/IP a determinar a qué puertos necesita enviar tráfico. El puerto TCP 80, por ejemplo, maneja el tráfico http, que es tráfico web sin cifrar. Como resultado, siempre que TCP/IP maneje la comunicación entre un cliente y un servidor web, utilizará el puerto TCP 80 (o el puerto TCP 443 para https). La Autoridad de Números Asignados en Internet (IANA) realiza un seguimiento de las asignaciones de puertos oficiales y las clasifica en tres grupos (Haber, 2021):

2.3.3.1 Puertos conocidos

Los números de puerto del 0 al 1023 están designados para aplicaciones típicas de TCP/IP y se conocen como puertos conocidos. Los programas cliente pueden encontrar rápidamente los procesos de aplicación de servidor apropiados en otros hosts gracias al uso de puertos conocidos. Por ejemplo, un proceso cliente que desee comunicarse con un proceso DNS que se ejecuta en un servidor debe transmitir un datagrama a un puerto determinado. El número de puerto DNS conocido es 53, y el proceso del servidor debería estar escuchando las consultas de los clientes en ese puerto.

Los puertos del servidor son persistentes en el sentido de que duran un período prolongado de tiempo, o al menos mientras la aplicación esté funcionando. Los puertos de cliente son efímeros debido a que duran poco tiempo, esto en el sentido de que "van y vienen" a medida que el usuario ejecuta las aplicaciones cliente (Goralski, 2017).

2.3.3.2 Puertos registrados

Los puertos en el rango 1024 a 49151 no se asignan ni se administran, sin embargo, se pueden registrar para evitar la duplicación. Los números de puerto registrados son puertos no conocidos que los proveedores utilizan para sus propias aplicaciones de servidor

Los puertos registrados se encuentran asignados por la IANA, estos puertos pueden ser utilizados por procesos de usuarios ordinarios o aplicaciones ejecutadas por usuarios ordinarios en la mayoría de los sistemas. La diferencia entre un puerto conocido y un puerto registrado es que en el primer caso los puertos se asignan y controlan y en el segundo no lo hacen, pero se pueden registrar para evitar la duplicación (Oracle, 2018).

2.3.3.3 Puertos dinámicos

Los puertos en el rango 49152 a 65535 son dinámicos, lo que significa que no están asignados, regulados ni registrados. Están destinados para su uso como puertos temporales o privados. También se conocen como puertos privados o no reservados. Muchos sistemas no permiten que los clientes seleccionen números de puerto efímeros de este rango (Goralski, 2017).

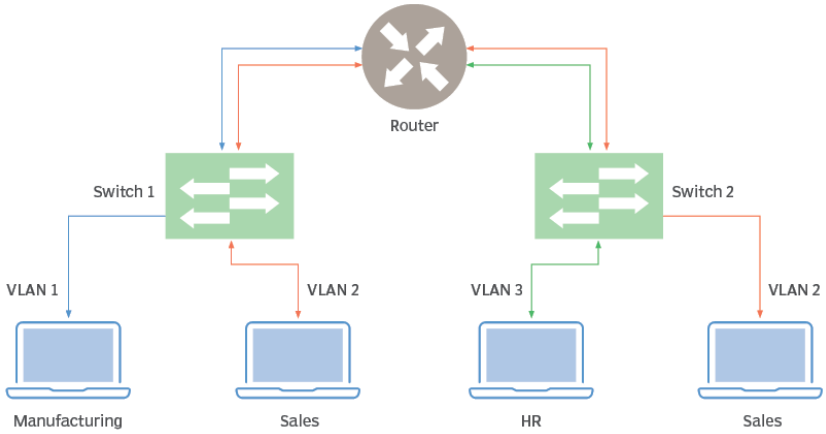
2.3.4 Redes Virtuales (VLAN)

Una red de área local virtual (VLAN) es una red local que agrupa un conjunto de máquinas de forma lógica y no física, aislando el tráfico para cada grupo (Slattery & Burke, 2020). Como se observa en la Figura 4 el uso de VLAN para agrupar puntos finales también

permite a los administradores agrupar dispositivos con fines puramente administrativos y no técnicos.

Figura 4

Red segmentada en VLANs



Nota. Una LAN virtual, o VLAN, segmenta los dispositivos y el tráfico dentro de una red. Las VLANs encapsulan paquetes para que el tráfico se transmita entre puertos y dispositivos etiquetados con VLAN. Tomado de, *What is a VLAN (virtual LAN)?,* por Slattery, 2020, Techtarget, (https://www.techtarget.com/searchnetworking/definition/virtual-LAN).

Al limitar la cantidad de tráfico que ve y procesa un punto final específico, las VLAN son capaces de mejorar el rendimiento de los dispositivos mientras operan en ellas. Al dividir los dominios de transmisión, las VLAN limitan la cantidad de otros hosts desde los que un dispositivo determinado puede ver transmisiones. Por ejemplo, los teléfonos IP no son capaces de observar ningún tráfico de difusión generado por las estaciones de trabajo si todas están en una VLAN aislada de las demás estaciones. Cada dispositivo puede limitar u optimizar el tráfico en sus respectivas redes virtuales según sea necesario (Slattery & Burke, 2020).

Las VLAN se basan en conmutadores especialmente diseñados con capacidades para reconocerlas. Para configurar una red basada en VLAN, el administrador de la red decide cuántas de ellas habrá, qué computadoras estarán en qué VLAN y cuál será el nombre de cada una. (Tanenbaum, 2003)

2.4 Seguridad Cibernética

La ciberseguridad es la protección de los sistemas conectados a Internet mediante la aplicación de tecnologías, procesos y controles, como hardware, software y datos, contra las ciber amenazas. Esta práctica es utilizada por personas y empresas para protegerse contra el acceso no autorizado a, redes, centros de datos, programas, dispositivos y otros sistemas informáticos (IT Governance, 2019).

Una estrategia sólida de ciberseguridad puede proporcionar una buena postura de seguridad contra ataques maliciosos diseñados para acceder, alterar, eliminar, destruir o extorsionar los sistemas y datos confidenciales de una organización o usuario. La ciberseguridad también es fundamental para prevenir ataques que tienen como objetivo deshabilitar o interrumpir las operaciones de un sistema o dispositivo (Shea et al., 2021).

2.4.1 Importancia de la ciberseguridad

Con un número cada vez mayor de usuarios, dispositivos y programas tanto en la empresa moderna como en el hogar, combinado con el aumento de los datos a los que se tiene acceso, muchos de los cuales son sensibles o confidenciales, la importancia de la ciberseguridad sigue creciendo. El creciente volumen y la sofisticación de los atacantes cibernéticos y las técnicas de ataque agravan aún más el problema (Shea et al., 2021).

2.4.2 Riesgos y amenazas a la ciberseguridad

Debido a la necesidad de las personas de estar conectadas a una red de internet, la mayoría de las ocasiones se pasa por alto los inminentes peligros que conllevan el navegar en entornos no seguros como las redes públicas. Cualquier persona que cuente con un dispositivo inteligente conectado a una red o a un servicio de telecomunicaciones se encuentra expuesto a sufrir un riesgo de ciberseguridad.

2.4.3 Tipos de ciberamenazas

De acuerdo con (Cordón, 2021), una ciberamenaza es toda aquella actividad maligna que ocurre dentro de un entorno digital, ya sea esta en computadores, tablets, smartphones y demás dispositivos con la capacidad de conexión a la red. Entre las principales ciberamenazas se encuentran:

2.4.3.1 Malware

Es una forma de software malicioso en el que cualquier archivo o programa puede usarse para dañar a un usuario de computadora. Esto incluye gusanos, virus, troyanos y spyware.

El software malicioso (malware) está aumentando a un ritmo alarmante, y algunos malware pueden ocultarse en el sistema mediante el uso de diferentes técnicas de ofuscación. Para proteger los sistemas informáticos e Internet del malware, es necesario detectar el malware antes de que afecte a una gran cantidad de sistemas.

De acuerdo con (Aslan & Samet, 2020), se han realizado varios estudios sobre enfoques de detección de malware. Sin embargo, la detección de malware sigue siendo problemática. Los enfoques de detección basados en firmas y basados en heurística son rápidos y eficientes para detectar malware conocido. Por otro lado, los enfoques basados en el comportamiento, en la verificación de modelos y en la nube funcionan bien para el malware desconocido y complicado.

2.4.3.2 Ransomware

Es otro tipo de malware. Se trata de que un atacante bloquee los archivos del sistema informático de la víctima, generalmente mediante el cifrado, y exija un pago para descifrarlos y desbloquearlos.

El ransomware se ha convertido en un negocio lucrativo que ha ganado una creciente popularidad entre los atacantes. A diferencia del malware tradicional, inclusive después de eliminarlo, el efecto del ransomware es irreversible sin la ayuda de su creador. Además de los costos del tiempo de inactividad y el dinero que las personas y las entidades comerciales podrían pagar como rescate, esas víctimas podrían sufrir otros daños, como la pérdida de datos o mala reputación (Al-rimy et al., 2018).

2.4.3.3 Ingeniería Social

Es un ataque que se basa en la interacción humana para engañar a los usuarios para que rompan los procedimientos de seguridad en donde su objetivo es manipular a personas y empresas para divulgar datos valiosos y confidenciales de interés para los ciberdelincuentes (Salahdine & Kaabouch, n.d.).

La ingeniería social está desafiando la seguridad de todas las redes, independientemente de la solidez de sus firewalls, métodos criptográficos, sistemas de detección de intrusos y sistemas de software antivirus. Es más probable que los humanos confíen en otros humanos en comparación con las computadoras o las tecnologías. Por lo tanto, son el eslabón más débil de la cadena de seguridad. Las actividades maliciosas realizadas a través de interacciones humanas influyen psicológicamente en una persona para divulgar información confidencial o para romper los procedimientos de seguridad (Pokrovskaia & Snisarenko, n.d.).

De acuerdo con (Aroyo et al., 2018), determinan que, debido a estas interacciones humanas, los ataques de ingeniería social son los ataques más poderosos porque amenazan todos los sistemas y redes. No se pueden prevenir usando soluciones de software o hardware mientras las personas no estén capacitadas para prevenir estos ataques. Los ciberdelincuentes eligen estos ataques cuando no hay forma de piratear un sistema sin vulnerabilidades técnicas.

2.4.3.4 Phishing

El phishing es una técnica de ingeniería social que, mediante el uso de diversas metodologías, tiene como objetivo influir en el objetivo del ataque para revelar información personal, como una dirección de correo electrónico, un nombre de usuario, una contraseña o información financiera. Esta información es luego utilizada por el atacante en detrimento de la víctima. El término phishing se deriva de la palabra pescar en inglés (fishing). La lógica de esta terminología es que un atacante usa un "cebo" para atraer a la víctima y luego "pesca" la información personal que quiere robar (Alabdan, n.d.).

2.4.3.5 Los ataques de denegación de servicio distribuido (DDoS)

Los ataques DoS y DDoS se han convertido en las principales amenazas para las redes informáticas. En dichos ataques, al agotar los recursos, se desactivan varios servicios y se degrada el rendimiento de la red. Estos ataques se consideran exitosos cuando el atacante consume intencionalmente recursos que impiden que los hosts utilicen el servicio de destino. Se pueden usar diferentes enfoques para realizar ataques DoS/DDoS, incluidos enfoques basados en la red, como la inundación a través de paquetes TCP SYN, ICMP o UDP, y enfoques basados en host, donde uno o varios hosts se dirigen a aplicaciones específicas para explotar su estructura de memoria, su protocolo de autenticación o un algoritmo particular (Eliyan & Di Pietro, 2021).

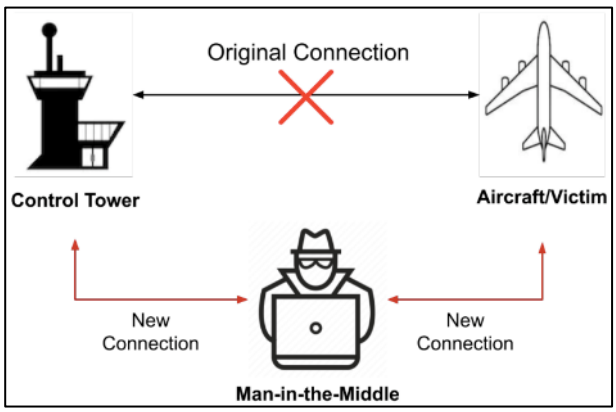
2.4.3.6 Man-in-the-Middle (MitM)

Los ataques MitM, también conocidos como ataques de secuestro, son un ataque cibernético en el que un atacante intercepta una conexión de red para alterar los datos que se transfieren entre los dos extremos. Por ejemplo, en la Figura 5, un atacante secuestra la conexión inalámbrica entre una aeronave y una torre de control, de tal manera que la aeronave considera al atacante como la torre de control y la torre de control considera al

atacante como la aeronave; por lo tanto, el atacante actúa como un repetidor malicioso que puede espiar y alterar las comunicaciones sin ser notado (Wong & Luo, 2020).

Figura 5

Ataque Man in the Middle



Nota. Tomado de Man-in-the-Middle Attacks on MQTT-based IoT Using BERT Based Adversarial Message Generation, por Wong & Luo, 2020.

2.4.3.7 Publicidad Maliciosa

En la publicidad maliciosa, el atacante, denominado Malvertiser, desempeña el papel de anunciante y entrega anuncios que tienen como objetivo comprometer la seguridad de los dispositivos donde se muestra el anuncio (por ejemplo, tratando de persuadir al usuario para que instale un malware) (Jyotiyana & Maheshwari, 2016).

Existen dos tipos principales de ataques de publicidad maliciosa. En el primer tipo, el atacante inyecta algún código en el anuncio que busca vulnerabilidades en el dispositivo del usuario a infectar. Este ataque no requiere una acción proactiva del usuario. En el segundo tipo de ataque, los anunciantes maliciosos entregan anuncios (atractivos) para persuadir al usuario de que haga clic y lo redirija a un sitio web de destino administrado por el anunciante malicioso. (Arrate et al., 2020).

2.5 Seguridad Perimetral

La seguridad perimetral es la capacidad de establecer técnicas o aparatos que funcionen en el perímetro de la red para proteger los datos y los recursos. Es una de las piezas fundamentales en el campo de la ciberseguridad (UNIR, 2020).

La seguridad perimetral en ciberseguridad se refiere al proceso de defender los límites de la red de una empresa de piratas informáticos, intrusos y otras personas no deseadas. Esto implica detección de vigilancia, análisis de patrones, reconocimiento de amenazas y respuesta efectiva.

Cada red privada está rodeada por un perímetro que sirve como un muro seguro entre las redes, como la intranet privada de una empresa y la Internet pública (Foss & Grant, 2020). El proveedor de servicios administrados (MSP) o, a veces, el departamento de TI interno son los encargados de proporcionar medidas que protegen a la red de ataques externos a través de la web pública. Estos riesgos incluyen intentos de piratería, malware, ransomware y otros métodos de infiltración en la red (Macy, 2022).

La seguridad perimetral se compone de sistemas como firewalls y sistemas de aislamiento del navegador. Las mejores prácticas en seguridad perimetral incluyen reconocimiento de amenazas, detección de vigilancia y análisis de patrones (UNIR, 2020).

2.5.1 Elementos de seguridad perimetral

Un perímetro de red es la barrera protectora entre el lado privado y administrado localmente de una red, generalmente la intranet de una empresa, y su lado público, que con frecuencia es la Internet (Shea, 2021). Una red perimetral contiene:

2.5.1.1 Router de Borde

Los enrutadores funcionan como semáforos en una red. Enrutan datos desde, hacia y a través de las redes. El enrutador de borde es el último enrutador bajo el control de una organización antes de que el tráfico ingrese a una red no confiable como Internet (Barracuda Networks, 2021).

2.5.1.2 Firewall

Un firewall es un equipo con un conjunto de reglas que definen los tipos de comunicación que permitirá o rechazará. Por lo general, un firewall es el dispositivo que continúa el trabajo en donde lo dejó el enrutador de borde y se encarga de filtrar el tráfico mucho más a fondo (Barracuda Networks, 2021).

2.5.1.3 Sistemas de detección de Intrusos (IDS)

Un sistema de detección de intrusos (IDS) observa el tráfico de la red en busca de comportamientos inusuales y emite notificaciones cuando las detecta.

En su publicación (Lutkevich, 2021) explica que, si bien las funciones principales de un IDS son la detección y el informe de anomalías, ciertos sistemas de detección de intrusos también están equipados para responder a comportamientos sospechosos o tráfico anormal al bloquear el tráfico proveniente de direcciones de Protocolo de Internet (IP) sospechosas.

Los sistemas para detectar intrusiones se emplean en un esfuerzo por atrapar a los piratas informáticos en el acto antes de que dañen gravemente una red. Existen IDS que pueden estar basados en el host o en la red. Mientras que un sistema de detección de intrusos basado en la red se encuentra en la infraestructura de red, un sistema de detección de intrusos basado en host está instalado en la computadora cliente.

La forma en que funcionan los sistemas de detección de intrusos es buscando firmas de ataque conocidos o desviaciones de la actividad rutinaria. Estas desviaciones o anomalías se empujan hacia la capa superior y se examinan en la capa de protocolo y aplicación. Son capaces de detectar de manera efectiva eventos como envenenamiento de Nombres de Dominio (DNS).

2.5.1.4 Sistemas de prevención de intrusiones (IPS)

Un sistema de prevención de intrusos (IPS), a diferencia de un IDS, monitorea los paquetes de red en busca de actividad de red potencialmente dañina, tal como lo hace un IDS, con el objetivo principal de prevenir las amenazas una vez que han sido identificadas (Lutkevich, 2021).

Se utiliza un IPS para detectar comportamientos maliciosos, registrar amenazas encontradas y tomar medidas preventivas para evitar que las amenazas causen daños. Una red puede ser vigilada continuamente en tiempo real utilizando una herramienta IPS.

Un sistema de prevención intrusiones opera escaneando toda la comunicación de la red. Una herramienta IPS a menudo es ubicada directamente detrás de un firewall, sirviendo como una capa adicional para observar eventos en busca de tráfico dañino. Al ubicarse en estos canales de comunicación directos entre un sistema y una red, las tecnologías IPS pueden examinar el tráfico de la red.

Si se encuentran amenazas, el software IPS es capaz de proporcionar notificaciones al administrador, descartar cualquier paquete de red malicioso y restablecer las conexiones mediante la reconfiguración de los firewalls, realizar el reempaquetado de las cargas útiles y eliminando archivos infectados adjuntos en los servidores (Gillis, 2020).

2.5.1.5 Zona Desmilitarizada (DMZ)

El propósito de DMZ es permitir el acceso a los recursos de la red que no es de confianza mientras se mantiene seguro el sistema o el host en una red privada interna. Los recursos que comúnmente se colocan dentro de la DMZ son servidores de correo, servidores FTP, servidores web y servidores VoIP (UNISERVE, 2020).

2.6 Firewall de Siguiente Generación (NGFW)

Un Firewall de Siguiente generación (NGFW) es una solución de seguridad de red que va más allá de las capacidades de un Firewall convencional. En la mayoría de las circunstancias, un cortafuegos clásico permite un examen detallado de los paquetes de red entrantes y salientes. Habilita o rechaza la comunicación de red en función de la dirección IP de origen/destino, el número de puerto y el protocolo. También filtra el tráfico según las reglas establecidas en las políticas de funcionamiento o tiene capacidad para proveer una red privada virtual.

Por otro lado, un firewall de próxima generación tiene capacidades como la inspección profunda de paquetes, el control de aplicaciones, la detección de contenido en línea, la prevención de intrusiones y la información sobre amenazas en la nube.

Los NGFW tienen un gran control y visibilidad sobre las aplicaciones que pueden identificar a través del análisis y la coincidencia de firmas. Pueden usar listas blancas o un sistema de prevención de intrusiones basado en firmas para diferenciar entre programas seguros y peligrosos detectados a través del descifrado SSL. Además, a diferencia de la mayoría de los firewalls tradicionales, los NGFW tienen un camino para futuras actualizaciones.

2.6.1 Capacidades de un Firewall de Siguiente Generación

(Shah, 2021) define a los NGFW como, sistemas que brindan capacidades de seguridad sofisticadas para proteger a la red interna de una organización de ataques y vulnerabilidades externas.

Un sistema de seguridad para ser determinado como un Firewall de Siguiente Generación debe contar con al menos las siguientes funcionalidades (Sunney Valley Networks, 2020):

- Traducción de direcciones de red (NAT)
- Inspección de protocolo con estado (SPI)
- Redes privadas virtuales (VPN)
- Descifrado SSL para la detección de aplicaciones cifradas sospechosas
- IPS basado en firmas
- La capacidad de incorporar datos desde fuera del firewall, como listas blancas, listas negras, políticas basadas en directorios
- Ruta de actualización para incluir futuras amenazas de seguridad y fuentes de información
- Descifrado SSL para permitir la identificación de aplicaciones cifradas no deseadas

2.6.2 Beneficios de los NGFW

Los NGFW brindan numerosas ventajas para todo tipo de redes de organizaciones, incluidas empresas, pequeñas empresas e incluso redes domésticas (Sunney Valley Networks, 2020). Los beneficios de un firewall de próxima generación se detallan a continuación.

2.6.2.1 Mayor productividad

La principal ventaja de usar un NGFW es habilitar de forma segura el uso de aplicaciones de Internet. Los cortafuegos de próxima generación logran esto mediante el uso de una inspección profunda de paquetes para identificar y controlar las aplicaciones, independientemente de su puerto IP.

2.6.2.2 Multifuncionalidad

los NGFW son soluciones de seguridad multifuncionales en una única plataforma. Los cortafuegos de última generación incluyen sistemas integrados de detección de intrusos (IDS) y sistemas de protección contra intrusos (IPS) que detectan ataques basados en análisis de comportamiento de red (NBA), firmas de amenazas o actividad anómala, además de todas las funcionalidades de los cortafuegos tradicionales. Esta funcionalidad ayuda a realizar una inspección de tráfico de red más profunda y a mejorar el filtrado de contenido de paquetes hasta la capa de aplicación.

2.6.2.3 Visibilidad y Manejabilidad

Los NGFW proporcionan una mayor visibilidad de las aplicaciones y la red. Este ayuda a los administradores a ver lo que sucede desde la red interna a la red externa o viceversa. Además, pueden identificar a los clientes que visitan los sitios web maliciosos o descargan código malicioso, cuál es el nombre del código y de qué país. Esto se soluciona mediante la integración de NGFW con directorios de usuarios de terceros, como Microsoft Active Directory.

La política dinámica basada en la identidad proporciona una visibilidad y un control más detallados sobre los usuarios y grupos que la política estática basada en IP y es más fácil de administrar. Los administradores definen los objetos solo una vez en una sola consola unificada. Cuando los cortafuegos de la red detectan una nueva conexión, la

dirección IP se asigna al usuario y al grupo consultando un directorio de usuarios de terceros.

2.6.2.4 Filtrado de contenido

Otra ventaja de NGFW es el filtrado de contenido, que es muy útil para evitar la fuga de datos y detener las amenazas cibernéticas con una inspección de paquetes detallada y en tiempo real. Las capacidades de filtrado de contenido incluyen filtrado de URL, prevención de amenazas y filtrado de datos.

2.6.2.5 Prevención y mitigación de amenazas

Los firewalls de próxima generación (NGFW) incluyen protección antivirus y contra malware que se actualiza automáticamente cada vez que se detectan nuevas amenazas. El dispositivo NGFW también reduce las vías de ataque al restringir las aplicaciones que se ejecutan en él. También inspecciona todas las aplicaciones aceptadas en busca de fallas de seguridad ocultas o violaciones de datos confidenciales, así como los riesgos que plantean las aplicaciones desconocidas. Esto tiene como objetivo minimizar el uso de ancho de banda del tráfico innecesario.

2.6.2.6 Control avanzado de políticas

Una aplicación que puede ser dañina para una organización puede ser beneficiosa para otra. Los NGFW permiten niveles granulares de control, lo que permite que los empleados apropiados accedan a los aspectos positivos de una aplicación mientras bloquea todo acceso a los aspectos negativos.

2.6.2.7 Bajo costo

Debido a que pueden combinar las capacidades de los firewalls, los antivirus, los filtros web y otras aplicaciones de seguridad en una sola solución, los NGFW también

pueden ser una opción de bajo costo para las empresas que intentan mejorar la seguridad de su infraestructura.

2.7 Seguridad de la Información

Dado que la información es uno de los recursos más valiosos de una organización, debe salvaguardarse mediante un conjunto de actividades, controles y políticas de seguridad que deben implementarse utilizando recursos humanos, de hardware y de software.

La seguridad de la información depende de la gestión y los procesos efectivos, los empleados, proveedores, clientes y accionistas de la empresa, y el nivel de seguridad de los medios técnicos (Vega Velasco, n.d.).

2.7.1 Políticas y Seguridad de la Información

Cuando se realiza la instalación de un sistema de seguridad, este siempre debe estar acompañado con la implementación de políticas de seguridad.

Para desarrollar una política de seguridad es necesario conocer los peligros a los que son vulnerables los datos, los recursos con los que cuenta una organización y determinar el origen de estos, sean internos o externos a la organización.

Es importante la implementación de las políticas de seguridad internas, debido a que de nada serviría cuidar la información de la organización de ataques externos, cuando existen vulnerabilidades y amenazas internas. Por ejemplo, cuando un usuario usa un dispositivo de almacenamiento infectado con virus, este puede contagiar a las demás estaciones de trabajo de la red interna.

En su publicación (Vega Velasco, n.d.) define a una política de seguridad como: "un conjunto de reglas que se deben seguir para obtener acceso a la información y los recursos". Los documentos de política de seguridad deben ser dinámicos, lo que significa que deben ajustarse y mejorarse constantemente en respuesta a los cambios en los contextos en los que se establecieron.

Las políticas de seguridad se crean para proteger la información y los sistemas de una empresa u organización y, al mismo tiempo, garantizar la integridad, confidencialidad y disponibilidad de la información. Los documentos de políticas de seguridad deben incluir mecanismos para implementar las regulaciones, así como deberes en todos los niveles, en estos documentos deben estar explícitamente descritos: El objetivo, los responsables y las acciones que se tomaran en caso de que estas sean incumplidas.

2.7.2 Sistemas de Gestión la Seguridad de la Información

Un sistema de gestión de la seguridad de la información (SGSI) es un conjunto de políticas y procedimientos para gestionar sistemáticamente los datos confidenciales de una organización. El objetivo de un SGSI es minimizar el riesgo y garantizar la continuidad del negocio limitando proactivamente el impacto de una brecha de seguridad (Yasar, 2021).

2.7.2.1 ISO/IEC 27001:2013

Es el estándar internacional definido para la seguridad de la información. Delimita los requisitos para un sistema de gestión de seguridad de la información (SGSI), así como de los sistemas que la procesan.

La orientación de mejores prácticas de ISO 27001 ayuda a las organizaciones a administrar la seguridad de la información al abordar personas, procesos y tecnología. Además, permite la evaluación de riesgos y la aplicación de controles necesarios para mitigar o eliminar los conflictos de seguridad informática (IT Governance, n.d.).

Capítulo III: Diseño y Desarrollo

3.1 Metodología

Para el desarrollo de este sistema se ha planteado la integración del modelo iterativo el cual tiene un enfoque de desarrollo de sistemas que se basa en la repetición de un ciclo de desarrollo para mejorar continuamente el producto. El modelo iterativo permite una mayor flexibilidad en el proceso de desarrollo del sistema. Esto se debe a que las iteraciones permiten que el equipo de desarrollo pueda adaptarse rápidamente a los cambios en los requisitos del proyecto y ajustarlo sobre la marcha. Las etapas del modelo iterativo son las siguientes:

- **Planificación:** En esta etapa se define el alcance del proyecto, se establecen los objetivos y se planifican las iteraciones del proceso de desarrollo.

- **Análisis de requerimientos:** Se recopilan y analizan los requisitos del sistema, se identifican las funcionalidades necesarias y se establecen los criterios de aceptación.

- **Diseño:** En esta etapa se define la arquitectura del sistema, se diseñan los componentes y se establecen las interfaces entre ellos.

- **Implementación:** Se lleva a cabo la codificación de los componentes del sistema.

- **Pruebas:** Se realizan pruebas en cada iteración para asegurar que el software funciona correctamente.

- **Evaluación:** En esta etapa se evalúa el software desarrollado en la iteración anterior, se identifican los errores y se realizan mejoras.

- **Retroalimentación:** Se retroalimenta el proceso de desarrollo con las lecciones aprendidas en las iteraciones anteriores, se identifican oportunidades de mejora y se establecen las metas para la siguiente iteración.

El modelo iterativo es un enfoque flexible y adaptable que permite mejorar continuamente el proyecto a medida que se van identificando los requisitos y se van implementando funcionalidades en el sistema.

3.2 Análisis de situación actual

Según un estudio llevado a cabo por Common Sense, se ha constatado un incremento sustancial en el uso de dispositivos móviles por parte de los niños. Este fenómeno se atribuye, en gran medida, a la disminución de la brecha digital, la cual ha resultado en un aumento de la accesibilidad y la asequibilidad de la conexión a internet en todas las áreas geográficas. Además, se ha observado que los niños están familiarizándose con los dispositivos tecnológicos a edades cada vez más tempranas, un fenómeno que ha sido impulsado, en parte, por la pandemia y el rápido proceso de digitalización que se implementó para mantenernos conectados y adaptarnos a una nueva forma de vida (Robb, 2021).

El estudio revela que el acceso equitativo a internet se ha visto favorecido tanto en áreas rurales como urbanas, así como entre grupos socioeconómicos diversos. Esto se ha logrado gracias a la expansión de las infraestructuras de telecomunicaciones y la disponibilidad de planes de datos más asequibles, lo que ha permitido que familias de diferentes regiones y niveles de ingresos puedan brindar a sus hijos el acceso a dispositivos móviles y a la conectividad necesaria.

La pandemia ha desempeñado un papel fundamental en el aumento del uso de dispositivos móviles por parte de los niños. El cierre de las escuelas y la transición hacia la educación a distancia han generado un incremento acelerado en la adopción de tecnología en el ámbito educativo. Los niños se han visto obligados a utilizar dispositivos móviles para acceder a clases en línea, completar tareas escolares y mantenerse en contacto con sus compañeros y profesores.

Asimismo, la rápida digitalización experimentada durante la pandemia también ha producido un cambio en las interacciones sociales de los niños. En lugar de participar en actividades al aire libre o en juegos tradicionales, muchos niños han recurrido a los dispositivos móviles como medio de entretenimiento, comunicación y socialización. Las aplicaciones y plataformas diseñadas específicamente para niños han ganado popularidad, brindando contenido educativo y de entretenimiento adaptado a sus necesidades.

Es importante destacar que, si bien el acceso a la tecnología puede ofrecer beneficios en términos educativos y sociales, también conlleva desafíos y preocupaciones. Los padres y cuidadores deben asumir un papel activo en la supervisión del tiempo que los niños pasan frente a las pantallas, fomentando un uso equilibrado de la tecnología y brindando orientación sobre los posibles riesgos, como el acceso a contenido inapropiado o el acoso en línea.

Con el fin de contrastar la información presentada en el estudio previamente citado, se ha llevado a cabo una encuesta dirigida a los participantes involucrados en el desarrollo de este proyecto la cual se encuentra en el Anexo 1. Mediante este análisis, se busca recopilar datos actualizados que reflejen la situación de los beneficiarios. En la Tabla 1 se proporciona una descripción detallada del método y formato utilizado en la encuesta para la recopilación de la información.

Tabla 1.

Método y formato para levantamiento de datos de situación actual

Método:	Para este proyecto de investigación, se utilizará un enfoque descriptivo que recopila información a través de una encuesta con el fin de comprender las necesidades en las redes domésticas no gestionadas. El objetivo es obtener datos precisos y significativos que permitan identificar las características y requerimientos principales, con el fin de desarrollar estrategias efectivas que mejoren la calidad y seguridad de estas redes.
Formato:	El presente proyecto incorpora una metodología de encuesta analítica con el propósito de recopilar datos empíricos y relevantes sobre la realidad de los beneficiarios, en este caso, los tutores de niños con acceso a internet. Se ha diseñado cuidadosamente un cuestionario estructurado que consta de preguntas cerradas, las cuales facilitarán la obtención de respuestas cuantificables, de fácil tabulación y análisis. Estas preguntas han sido formuladas de manera precisa y técnica, pero al mismo tiempo se ha considerado su comprensión por parte de los participantes, incluso aquellos con un nivel de conocimiento tecnológico limitado. El cuestionario abarca una amplia gama de aspectos relevantes, como la necesidad de implementación, las características físicas del sistema, los dispositivos presentes en la red, los métodos de conexión a internet, los usos que se les dan a los dispositivos y las necesidades específicas de los usuarios, entre otros. Se ha procurado una redacción clara y concisa, a fin de que los encuestados puedan responder de manera efectiva y brindar información detallada. Mediante la aplicación de esta encuesta analítica, se busca obtener una comprensión profunda de la situación actual de los beneficiarios en relación con el acceso a internet y el uso de dispositivos tecnológicos. Los datos recolectados permitirán un análisis íntegro y la formulación de conclusiones sólidas en el contexto del estudio en cuestión.

3.2.1 Análisis de los resultados

Tras la aplicación de la encuesta en línea a una muestra de 10 individuos pertenecientes a diversos hogares utilizando un formulario digital, se han obtenido resultados que proporcionarán una base sólida para el avance y desarrollo de este proyecto. En la sección siguiente, se presentan las conclusiones derivadas del proceso de tabulación de los datos recogidos en las encuestas, los cuales se encuentran detallados en el Anexo 2.

Las preguntas formuladas permiten establecer los requerimientos de usuario para ser implementados en el proyecto de tal forma que todas las funcionalidades se acoplen a

las necesidades de los beneficiarios. De acuerdo con los encuestados los dispositivos más utilizados por los niños en el hogar son los Smartphones seguido por las PCs o laptops. En cuanto al tipo de conexión más habitual se registra que la más común es la inalámbrica.

En cuando a los tipos de contenidos generalmente visitados por los adultos se obtiene que estos ingresan libremente a diversos tipos de sitios web como lo son: redes sociales, juegos en línea, apps de streaming, mensajería, correo electrónico, sitios para adultos y sitios de descarga de contenidos. Así mismo estas personas concuerdan en que no todos estos contenidos son aptos para niños, resaltando que aplicaciones como: sitios web para adultos, redes sociales y sitios de descarga de contenido son lugares no aptos para ellos.

El 90% de los encuestados ha respondido que se debería implementar un sistema de filtrado y control de acceso a contenidos para bloquear y restringir el acceso a los sitios web antes mencionados. El 100% de los encuestados a su vez concuerdan que se debe segmentar las redes de acuerdo con el tipo de usuario, generando redes con permisos y restricciones independientes entre sí.

El 80% opina que se debe contar con credenciales únicas para la vinculación con las redes inalámbricas, de tal modo que se obtenga un mejor monitoreo del contenido que luego accederá cada usuario.

Con respecto a las características físicas y operativas del sistema, el 60% ha coincidido que el sistema debe consumir poca energía eléctrica pero que este debe permanecer activo y operativo las 24 horas del día, los 7 días de la semana.

Para el acceso y gestión del sistema el 80% de los encuestados ha opinado que los tutores de los menores deben poder acceder a las configuraciones del sistema, esto a su

vez apoyado de la implementación de una interfaz gráfica amigable, ya que el 70% ha solicitado que la interfaz debe ser intuitiva y fácil de operar.

En lo que respecta a la generación de informes, los usuarios han solicitado que este tenga la capacidad de mostrar información acerca de las páginas web bloqueadas, páginas web accedidas, amenazas contenidas y el tiempo que los usuarios pasan navegando en la red. Por último, el 60% de los usuarios solicita que el periodo de entrega o difusión de estos informes sea en periodos de 1 vez por semana.

3.3 Introducción al desarrollo del proyecto

Año tras año se ha producido un incremento en el uso de Internet, esto debido a la mayor disponibilidad de conexiones rápidas, dispositivos que necesitan conectarse y mayor penetración de los servicios digitales. Esto incluye el teletrabajo, educación en línea, entretenimiento y comunicación. La seguridad en redes domésticas es esencial para proteger datos personales, prevenir amenazas en línea y garantizar la privacidad. También es fundamental para proteger a los menores de contenido inapropiado y supervisar su acceso. Internet se ha vuelto vital en la vida cotidiana, y la seguridad en redes domésticas es crucial para aprovechar sus beneficios mientras se minimizan los riesgos.

3.3.1 Propósito del sistema

La propuesta del sistema se basa en el monitoreo de redes domésticas para determinar el tipo de tráfico que hay dentro de estas, aplicando métodos de control de tráfico de nueva generación, este busca controlar el tipo de contenido al que los menores pueden acceder cuando no se encuentran bajo la tutela de un adulto, debido a que estos por cuestiones de trabajo no pueden estar todo el tiempo pendientes de lo que los menores realizan en la web y que además en la actualidad prácticamente casi todos los dispositivos del hogar se encuentran conectados a internet.

El sistema planteado al ser un Firewall de Siguiente generación tiene características adicionales a las de un Firewall convencional, lo que le permite tener funciones adicionales como lo son la visualización de las estadísticas de tráfico tanto en tiempo real como el reciente, mismo que se almacena en la base de datos interna del dispositivo y puede ser accedida por el administrador como por el tutor de los menores. Este también tiene la capacidad de validar las firmas y certificados de las páginas web para evitar el acceso a paginas fraudulentas o inseguras, además que mediante la aplicación de los niveles de acceso según el tipo de usuario estos podrán navegar libremente en el caso de los adultos y de forma restringida y controlada en el caso de los niños.

3.3.2 Ámbito del Sistema

El sistema planteado se implementará en una red domestica de área local (LAN) que cuenta con una topología de red de tipo estrella, en donde todos los dispositivos finales (Hosts) se conectan a un punto de acceso central mediante las tecnologías de comunicación inalámbrica Wifi (802.11) o cableada (Ethernet) y que inicialmente no cuenta con un sistema de protección y control.

Al implementar el NGFW se utilizará una topología distinta a la inicial, la cual será en tipo Estrella Extendida debido al uso de VLANs. Las redes que cuentan con VLANs comúnmente implementan este tipo de topología, donde los dispositivos de la red se conectan a un concentrador central o switch. Los switches se utilizan para dividir la red en varias VLANs lógicas, permitiendo la segregación de tráfico, mejorando la seguridad y el rendimiento de la red. Esta topología es popular porque permite la creación de múltiples subredes lógicas en una sola red física, lo que mejora la gestión de la red, la eficiencia del ancho de banda y la implementación de políticas de seguridad y QoS específicas para cada VLAN.

La plataforma del sistema propuesto será desarrollada en Software de código abierto (OPNsense) que se trata de una adaptación de FreeBSD modificada para su uso como Enrutador y Firewall, dentro del cual se planifica implementar módulos adicionales como zenarmor que proporcionan funcionalidades de nueva generación para el control de contenidos. Para una correcta definición de los permisos y capacidades del proyecto este se basará en la definición de políticas de seguridad en redes contemplado en el manual de buenas prácticas bajo el estándar ISO/IEC 27002.

3.3.3 Características de los beneficiarios

Se consideran como beneficiarios a las personas involucradas durante la aplicación del sistema de seguridad y monitoreo a implementarse en las redes domésticas de los interesados. El sistema planteado cuenta con características para análisis y control del tráfico de red, gestión de niveles de acceso y la generación de informes del uso de la red de acuerdo con los dispositivos presentes en la misma. Mediante este proyecto se busca que los tutores de los menores en el hogar puedan estar pendientes de que es lo que realizan los niños en internet en sus diversos dispositivos como: PCs, consolas de videojuegos o demás dispositivos móviles (Tablets o Smartphones).

Mediante el proyecto planteado, se espera que tanto el gestor de la red como el tutor de los menores puedan acceder al sistema mediante sus propias credenciales de acceso para visualizar la actividad de los dispositivos y analizar los informes generados que contaran con graficas que mostraran los sitios web tanto accedidos como bloqueados, así mismo como los dispositivos en los que se realizó dicha actividad. Estos también tendrán la posibilidad de aplicar filtros personalizados automáticamente que sean más permisivos o restrictivos de acuerdo con las necesidades del momento.

3.4 Requerimientos del Proyecto

La definición de los requerimientos es un paso crítico en el proceso de desarrollo del sistema, ya que establece los criterios necesarios para garantizar un funcionamiento adecuado del mismo. A partir de estos requerimientos, se determinan los requisitos específicos que deben ser cumplidos durante la ejecución del proyecto. La definición de los requerimientos se basa en los resultados obtenidos de la encuesta y en los criterios del equipo de desarrollo del proyecto. En este contexto, los requerimientos se establecen en tres grupos principales: de usuario, de sistema y de arquitectura. Cada uno de estos grupos se enfoca en aspectos específicos del sistema y se consideran de gran importancia para garantizar el cumplimiento de las necesidades y expectativas de los stakeholders.

3.4.1 Stakeholders

Son los individuos, grupos u organizaciones que tienen un interés directo o indirecto en el proyecto y pueden influir en sus resultados o ser afectados por ellos. Estas partes interesadas desempeñan roles y tienen responsabilidades específicas en relación con el proyecto, y su participación y satisfacción son fundamentales para el éxito de este. La gestión adecuada de los stakeholders implica identificar, analizar y comprender sus necesidades, expectativas y preocupaciones, y establecer una comunicación efectiva, colaboración y toma de decisiones para garantizar el logro de los objetivos. A continuación, en la Tabla 2 se define la lista de los Stakeholders del proyecto.

Tabla 2.

Lista de Stakeholders

#	Beneficiario	Relación
1	Personas con niños en casa	Usuarios finales
2	MsC. Carlos Vásquez	Director del proyecto de titulación
3	MsC. Luis Suárez	Asesor del proyecto de titulación
4	Sr. Alexander Guanotoa	Desarrollador del Proyecto

3.4.2 Construcción de Atributos de los requerimientos

En la siguiente sección se realiza la construcción de los atributos de los requerimientos, los cuales son: requerimientos de stakeholders, requerimientos de sistema y requerimientos de arquitectura. El cumplimiento de cada uno de estos apartados determinará el desempeño del sistema propuesto.

3.4.2.1 Nomenclatura de los requerimientos

Para lograr una gestión adecuada de los requerimientos, es necesario identificarlos mediante una abreviatura que facilite su gestión y seguimiento. En la Tabla 3 se presentan las abreviaturas utilizadas para el desarrollo de este proyecto.

Tabla 3.
Definición de abreviaturas

Descripción	Abreviatura
Requerimientos de Stakeholders	**StSR**
Requerimientos de Sistema	**SySR**
Requerimientos de Arquitectura	**SrSH**

Durante la fase de construcción de requerimientos, se define la priorización de los requerimientos para establecer su importancia. Esto se debe a que no todos los requerimientos pueden ser implementados en el plazo disponible o con los recursos disponibles. Por lo tanto, es necesario establecer prioridades para decidir cuáles son los requerimientos más importantes y deben ser implementados primero. La priorización de los requerimientos permite centrarse en los objetivos principales del proyecto y a garantizar que el sistema cumpla con las necesidades y expectativas más importantes de los stakeholders.

Los niveles de prioridad pueden basarse en factores como la urgencia, la importancia estratégica, el costo de implementación y el impacto en los usuarios finales. Es crucial que se definan los niveles de prioridad en colaboración con los stakeholders relevantes para asegurar que se consideren todas las perspectivas y necesidades del proyecto. En general, se pueden identificar tres niveles de prioridad: alto, medio y bajo. Los

requerimientos de prioridad alta son aquellos que son esenciales para el funcionamiento del sistema y que no pueden ser pospuestos o ignorados, mientras que los requerimientos de prioridad media y baja pueden ser pospuestos o incluso omitidos en caso de ser necesario. En la Tabla 4 se muestran las prioridades de los requerimientos y la descripción general de cada nivel.

Tabla 4.

Prioridad de los Requerimientos

Prioridad	Descripción
Alta	Este requisito tiene una prioridad crítica y es esencial que se incluya en el proceso de desarrollo del sistema, ya que su omisión podría tener un impacto negativo significativo en la funcionalidad de este. Por lo tanto, es fundamental que este requisito sea considerado como una alta prioridad y se asegure su cumplimiento durante todas las fases del proceso de desarrollo del sistema.
Media	La omisión de este tipo de requerimiento puede influir en la decisión final del sistema, no obstante, en situaciones de fuerza mayor, podría ser posible omitirlo. Es importante tener en cuenta que cualquier decisión de omitir un requerimiento debe ser tomada de manera cuidadosa y justificada, considerando las posibles consecuencias y riesgos asociados con dicha omisión. Además, cualquier excepción a los requerimientos establecidos debe ser documentada y aprobada por los stakeholders relevantes y el equipo de desarrollo del proyecto.
Baja	En caso de que este requerimiento no sea incluido, se estima que su impacto en la decisión final del sistema no será significativo. No obstante, cualquier decisión de omitir un requerimiento debe ser tomada de manera cuidadosa y justificada, considerando las posibles consecuencias y riesgos asociados con dicha omisión. Es importante destacar que cualquier excepción a los requerimientos establecidos debe ser documentada y aprobada por los stakeholders relevantes y el equipo de desarrollo del proyecto.

3.4.3 Requerimientos de Stakeholders

Los requerimientos de stakeholders son aquellas necesidades, objetivos y expectativas que deben ser satisfechas por el sistema en desarrollo. Estos requerimientos deben ser identificados, analizados, documentados y validados adecuadamente a lo largo del ciclo de vida del proyecto. Es importante involucrar a los stakeholders en el proceso de definición de requerimientos y gestionarlos adecuadamente para asegurar que se comprendan y satisfagan sus necesidades y expectativas. A continuación, en la

Tabla 5 se establecen los requerimientos de Stakeholders para los casos operacionales y de usuario.

Tabla 5.

Requerimientos de Stakeholders

Requerimientos de Stakeholders (StSR)					
#	Requerimientos	PRIORIDAD			Relación
		Alta	Media	Baja	
REQUERIMIENTOS OPERACIONALES					
StSR1	El sistema deberá funcionar de forma continua e ininterrumpida.	☑	☐	☐	
StSR2	El sistema debe permitir la identificación y autenticación de los usuarios para el acceso a la red.	☑	☐	☐	
StSR3	El sistema debe contar con capacidades de conexión inalámbrica (WiFi) para los usuarios finales.	☑	☐	☐	
StSR4	El sistema debe contar con capacidades de conexión cableada (Ethernet) para los usuarios finales.	☐	☑	☐	
StSR5	El sistema debe consumir poca energía eléctrica.	☐	☐	☑	
StSR6	El sistema debe segmentar la red física en varias subredes lógicas.	☑	☐	☐	
StSR7	El sistema debe bloquear las amenazas de forma inmediata.	☑	☐	☐	
REQUERIMIENTO DE USUARIOS					
StSR8	El sistema debe ser compacto	☐	☑	☐	
StSR9	El sistema debe proporcionar una interfaz intuitiva para la gestión de permisos de acceso a recursos y servicios de la red.	☑	☐	☐	
StSR10	El sistema debe proporcionar informes claros y detallados de actividad de la red, incluyendo información sobre tráfico de red y eventos de seguridad.	☑	☐	☐	
StSR11	El sistema debe permitir a los usuarios la definición de políticas de seguridad personalizadas para su uso en la red.	☐	☑	☐	
StSR12	Los usuarios deben poder crear y gestionar sus propias cuentas de usuario con permisos específicos.	☐	☑	☐	
StSR13	El sistema debe generar y enviar reportes automáticamente en periodos determinados por el administrador.	☐	☑	☐	
StSR14	El sistema debe contar con soporte técnico y documentación clara para facilitar la configuración y uso del sistema.	☑	☐	☐	

Los requerimientos presentados anteriormente se basan en las necesidades definidas por los stakeholders, a través del uso de encuestas y observación directa. Esto

permite establecer una idea clara del sistema con definiciones precisas para el entorno operativo y las necesidades del usuario.

3.4.4 Requerimientos de Sistema

Los requerimientos del sistema de seguridad se encuentran definidos de acuerdo con las funciones y limitaciones que este debe desempeñar. Se analizan los requerimientos de uso, performance, interfaces, estados y físicos que deben ser coherentes con los requerimientos de los stakeholders. En la Tabla 6 se puede encontrar información detallada de los requerimientos del sistema, los cuales indican sus funcionalidades basándose en la aplicación y en la prioridad del requerimiento.

Tabla 6.

Requerimientos de Sistema

Requerimientos de Sistema (SySR)					
#	Requerimientos	PRIORIDAD			Relación
		Alta	Media	Baja	
REQUERIMIENTOS DE USO					
SySR1	El sistema debe ser fácil de usar y navegar para los usuarios finales	☑	☐	☐	StSR9
SySR2	El sistema debe ser capaz de manejar múltiples usuarios y proporcionar acceso seguro y restringido a diferentes niveles de permisos.	☑	☐	☐	StSR2
SySR3	El sistema debe ser capaz de proporcionar una interfaz intuitiva para la gestión de contenidos, como la adición, edición y eliminación de políticas de seguridad.	☑	☐	☐	StSR9
SySR4	El sistema debe permitir a los usuarios buscar y filtrar información según sus necesidades.	☐	☑	☐	
SySR5	El sistema debe ser capaz de generar informes y estadísticas en tiempo real para los usuarios finales y administradores.	☐	☑	☐	StSR10
REQUERIMIENTO DE INTERFAZ					
SySR6	El sistema debe estar basado en Software de Código Abierto.	☑	☐	☐	
SySR7	El sistema debe mostrar una interfaz gráfica de usuario clara y fácil de usar.	☑	☐	☐	StSR9
SySR8	El sistema debe poder conectarse y comunicarse con otros sistemas y dispositivos de red.	☑	☐	☐	
SySR9	El sistema debe ser compatible con navegadores web estándar y móviles (Chrome, Edge, Firefox)	☑	☐	☐	

SySR10	El sistema debe permitir a los usuarios visualizar los informes de actividad de forma gráfica y resumida.	☑	☐	☐	StSR10
	REQUERIMIENTO DE PERFORMANCE				
SySR11	El sistema debe tener capacidad para procesar y filtrar el tráfico de red sin afectar significativamente el rendimiento de la red.	☑	☐	☐	
SySR12	El sistema debe tener la capacidad para identificar y bloquear contenido no deseado en tiempo real, con un mínimo de falsos positivos.	☑	☐	☐	StSR7
SySR17	El AP debe tener un rango de cobertura de al menos 10 metros.	☐	☑	☐	
	REQUERIMIENTO DE MODO/ESTADO				
SySR17	El sistema debe permanecer activo todo el tiempo.	☑	☐	☐	
SySR18	El sistema debe mostrar mediante los LED incorporados su estado encendido/apagado.	☐	☐	☑	
SySR19	El sistema debe mostrar mediante los LED incorporados el estado de la comunicación.	☐	☐	☑	
	REQUERIMIENTO FÍSICOS				
SySR17	El sistema debe contar con un espacio dedicado para su ubicación.	☑	☐	☐	
SySR18	El sistema debe ser capaz de operar a temperatura ambiente.	☑	☐	☐	
SySR19	El sistema debe ser compacto.	☐	☐	☑	

3.4.5 Requerimientos de Arquitectura

Los requerimientos de arquitectura se enfocan en los diferentes componentes del sistema, como son el hardware, software y componentes eléctricos, y se definen de acuerdo con el funcionamiento que tendrá el sistema. Para garantizar que se cumplan con los requisitos de la arquitectura, se deben considerar los requerimientos lógicos, de diseño, de hardware, software y eléctricos correspondientes. Todos estos requerimientos se encuentran detallados en la

Tabla 7.

Tabla 7.

Requerimientos de Arquitectura

Requerimientos de Arquitectura (SrSH)					
#	Requerimientos	PRIORIDAD			Relación
		Alta	Media	Baja	
	REQUERIMIENTOS LÓGICOS				
SrSH1	El sistema debe ser capaz de monitorear el tráfico de red en tiempo real.	☑	☐	☐	StSR7
SrSH2	El sistema debe ser capaz de permitir la autenticación de usuarios.	☑	☐	☐	StSR2
SrSH3	El sistema debe ser capaz de filtrar el tráfico de red entrante y saliente.	☑	☐	☐	

SrSH4	El sistema debe ser capaz de generar informes detallados sobre el tráfico de red, incluyendo información sobre los intentos de intrusión, los ataques bloqueados y las políticas de seguridad implementadas.	☐	☑	☐	StSR10
	REQUERIMIENTOS DE DISEÑO				
SrSH5	El sistema debe contar con una interfaz de usuario intuitiva.	☐	☑	☐	StSR9
SrSH6	El sistema debe permitir la administración y monitoreo centralizados del sistema para facilitar su administración y mantenimiento.	☑	☐	☐	
SrSH7	El sistema debe permitir la integración con otras soluciones de seguridad como sistemas de detección y prevención de intrusiones, antivirus y filtrado de contenido.	☐	☑	☐	
SrSH8	El sistema debe contar con funcionalidades de inspección profunda de paquetes para identificar y bloquear amenazas avanzadas y malware.	☑	☐	☐	
SrSH9	El sistema debe incluir la capacidad de implementar políticas de seguridad personalizadas para diferentes grupos de usuarios y dispositivos en la red.	☐	☑	☐	
	REQUERIMIENTOS DE HARDWARE				
SrSH10	Interfaces de red: El sistema debe tener la capacidad de brindar conexión inalámbrica con tecnología Wifi.	☑	☐	☐	StSR3
SrSH11	Interfaces de red: El sistema debe tener 1 puerto Ethernet para la conexión WAN.	☑	☐	☐	StSR4
SrSH12	Interfaces de red: El sistema debe tener 1 puerto Ethernet para la conexión con el Access Point.	☑	☐	☐	StSR4
SrSH13	Procesador: El sistema debe tener un procesador de al menos 4 núcleos compatible con arquitectura x86_64.	☐	☑	☐	
SrSH14	Memoria RAM: El sistema debe tener al menos 4Gb de memoria RAM.	☐	☑	☐	
SrSH15	Almacenamiento: El sistema debe poseer almacenamiento de al menos 240Gb para almacenar 30 días de registros en la base de datos interna.	☐	☑	☐	
SrSH16	Access Point: El sistema debe permitir segmentar la red física en diversas redes lógicas (VLANs).	☑	☐	☐	StSR6
	REQUERIMIENTOS DE SOFTWARE				
SrSH17	El Software del sistema debe estar basado en Software de Código Abierto.	☑	☐	☐	SySR6
SrSH18	El sistema debe estar diseñado para Arquitectura x86_64.	☑	☐	☐	
SrSH19	El software debe ser compatible con la base de datos MongoDB	☑	☐	☐	
SrSH20	El sistema debe ser compatible con el protocolo 802.1q (VLANs)	☑	☐	☐	StSR6
SrSH21	El software debe ser capaz de gestionar múltiples usuarios y sesiones simultáneamente.	☐	☑	☐	SySR2
SrSH22	El software debe ser seguro y estar protegido contra posibles amenazas de seguridad.	☑	☐	☐	
	REQUERIMIENTOS ELÉCTRICOS				
SrSH23	El sistema debe contar con protección a descarga y sobrecarga de tensión eléctrica.	☐	☑	☐	
SrSH24	Para el NGFW. Fuente de alimentación de 12V-30W	☑	☐	☐	
SrSH25	Para el AP. Fuente de alimentación de 5V-5W	☑	☐	☐	

3.5 Selección de Hardware y Software

Para la selección tanto del hardware como del software se realiza mediante la comparativa de las especificaciones, propiedades y características de varias alternativas, evaluando el cumplimiento o no de los requerimientos de Stakeholders (StRS, SySR, SrSH), sistema y de arquitectura anteriormente planteados.

3.5.1 Selección de Hardware

En cada tabla se asignará el valor de “1” si se cumple el requisito y de “0” si este no se cumple, tal como se muestra en la Tabla 8. Finalmente se elegirá el componente que obtenga la mayor puntuación siendo este la opción que cubre la mayor cantidad de requerimientos.

Tabla 8

Valor referencial de los requerimientos

Descripción	Valor
Cumple	1
No cumple	0

Para la elección del hardware en donde se montará el NGFW, se establecieron 4 opciones con propiedades y características necesarias para cubrir las necesidades del proyecto. En la Tabla 9 se evalúan requerimientos de Stakeholders (StSR4, StSR5), requerimientos de sistema (SySR19) y los requerimientos de arquitectura (SrSH11, SrSH12, SrSH13, SrSH14, SrSH15). Además, se realiza una breve ampliación acerca de las características del dispositivo seleccionado.

Tabla 9

Elección de Hardware para el NGFW

Hardware / Características	Requerimiento								Val. Total
	StSR4	StSR5	SySR19	SrSH11	SrSH12	SrSH13	SrSH14	SrSH15	
Modelo: Intel NUC **Procesador:** Intel Celeron J4025 (2C/2T) **Conexiones:** 1 Ethernet **Almacenamiento / RAM:** No Incluye **Precio:** 165$	1	1	1	1	0	1	0	0	5
Modelo: OASLOA T8 Pro **Procesador:** Intel Celeron N5105 (4C/4T) **Conexiones:** Dual Gigabit Ethernet **Almacenamiento / RAM:** 256GB / 8GB **Precio:** 160$	1	1	1	1	1	1	1	1	**8**
Modelo: Beelink Mini PC GK55 **Procesador:** Intel Celeron J4125 (4C/4T) **Conexiones:** 1 Ethernet **Almacenamiento / RAM:** 256GB / 8GB Precio: 170$	1	1	1	1	0	1	1	1	7
Modelo: Torre PC ATX **Procesador:** Intel Dual E5700 (2C/2T) **Conexiones:** 1 Ethernet / 1 Gb Ethernet **Almacenamiento / RAM:**128 / 4GB **Precio:** 60$	1	0	0	1	1	1	1	1	6
Elección: La plataforma seleccionada para la implementación del NGFW ha sido la mini-PC OASLOA T8 Pro debido a que cumple con todos los requerimientos además de ser la mejor opción costo-beneficio gracias a la capacidad de su procesador de 11va generación y sus puertos Dual Gigabit Ethernet. Esta es una opción muy compacta y de muy bajo consumo eléctrico al tener un consumo máximo de 20W.									

En la Tabla 10 se amplían las características físicas y técnicas de la mini-PC OASLOA T8 Pro, la cual ha sido seleccionada después de realizar la comparativa técnica de los requerimientos.

Tabla 10

Características del hardware elegido para montar el NGFW

Modelo	
Marca	**OASLOA**
Modelo del producto	T8 PRO
Procesador	
Chip	Celeron N5105
Marca del procesador	Intel
Arquitectura del procesador	x86_64
Cantidad de núcleos	4
Cantidad de subprocesos	4
Frecuencia básica del procesador	2,00 GHz
Frecuencia de Impulso	2,90 GHz
Memoria RAM	
Capacidad	8 GB DDR4
Tipo de memoria del equipo	DDR4 SDRAM
Almacenamiento	
Capacidad	256 GB SSD
Interfaz de la unidad de disco duro	eMMC
Propiedades	
Sistema operativo	Windows 11 Pro
Dimensiones del producto	100x30x90mm
Consumo máximo	20W
Conectividad	
Número de puertos USB 3.0	3
Número de puertos HDMI	3
Número de puertos Gigabit Ethernet	2
Tipo de conexión inalámbrica	802.11a/b/g/n/ac

Para la elección del Access Point el cual brindará la comunicación inalámbrica entre el NGFW y los usuarios finales del sistema se planteó el análisis y comparativa de 4 modelos de distintas marcas que puedan cumplir con los requerimientos de Stakeholders (StSR2 StSR5, StSR6), requerimientos de sistema (SyS2, SySR9) y los requerimientos de arquitectura (SrSH10, SrSH17 SrSH20), en la Tabla 11 se muestran las principales sus principales características tales como el modelo, Sistema Operativo y el precio comercial del producto.

Tabla 11

Elección de Hardware para el Access Point

Hardware / Características	Requerimiento								Val. Total
	StSR2	StSR5	StSR6	SySR2	SySR9	SrSH10	SrSH17	SrSH20	
Marca: Mikrotik **Modelo:** hAP lite TC **OS:** RouterOS **Precio:** 45$	1	1	1	1	1	1	1	1	**8**
Marca: Ubiquiti **Modelo:** Access Point U6 Lite **OS:** UniFi OS **Precio:** 140$	1	0	1	1	1	1	0	1	**6**
Marca: TP Link **Modelo:** EAP610 **OS:** OMADA SDN **Precio:** 110$	1	0	0	1	0	1	0	0	**3**
Marca: CISCO **Modelo:** CBW150AX **OS:** Cisco IOS **Precio:** 150$	1	0	1	1	1	1	0	1	**6**
Elección: El Access Point que cumple con todos los requerimientos planteados se trata del MikroTik hAP lite TC, que gracias a las características de su sistema operativo RouterOS facilita la creación de diversas SSID con capacidad de etiquetado bajo el protocolo 802.1q, además de la versatilidad de configuración para levantar portales cautivos con autenticación desde un directorio activo.									

En la

Tabla 12 se muestra una imagen referencial del producto, así como más detalles técnicos acerca del Access Point MikroTik hAP lite. Este modelo de AP se caracteriza por su bajo costo y bajo consumo y que a su vez gracias a su sistema operativo RouterOS con licencia de Nivel 4 que desbloquea funciones como la creación de VLANs, multiple inicio de sesión para administración y soporte RADIUS.

Tabla 12

Características del Hardware elegido para el Access Point

Modelo	
Marca	Mikrotik
Modelo del producto	RB941-2nD-TC
Procesador	
Chip	QCA9533
Arquitectura del procesador	ARM
Cantidad de núcleos	1
Frecuencia básica del procesador	650 MHz
Memoria RAM	
Capacidad	32 MB
Tipo de memoria del equipo	DDR
Conectividad	
Puertos Ethernet (4)	10/100 Mbit/s Ethernet con Auto-MDI/X
Estándares Inalámbricos	802.11b/g/n
Antena	1.5dBi gain
Propiedades	
Sistema operativo	RouterOS, Level 4 license (AP support)
Dimensiones del producto	124x100x54mm
Consumo Máximo	3W

3.5.2 Selección de Software

Una vez seleccionado el hardware que se utilizará para montar el sistema se procede a realizar un análisis de 5 diferentes alternativas de software comúnmente usados en Firewalls, también se realiza la comparación de los requerimientos de Stakeholders (StSR10, StSR13), requerimientos de sistema (SySR2, SySR6, SySR9, SySR12) y los requerimientos de arquitectura (SrSH1, SrSH4, SrSH5, SrSH6, SrSH8, SrSH9, SrSH19, SrSH21), tal como se muestra en la Tabla 13, lo que permitirá seleccionar la mejor opción para implementar todas las funciones y características planificadas.

Tabla 13

Selección del Software para el NGFW

Software	Requerimiento														Val. Total
	StSR10	StSR13	SySR2	SySR6	SySR9	SySR12	SrSH1	SrSH4	SrSH5	SrSH6	SrSH8	SrSH9	SrSH19	SrSH21	
OPNsense	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**14**
pfSense	0	1	1	1	1	1	1	0	1	1	0	1	1	1	11
IPFire	0	0	0	1	1	1	1	0	0	0	0	0	0	1	5
Zeroshell	0	0	1	1	1	1	1	0	0	1	0	1	0	1	8
Untangle	1	1	0	0	1	0	1	0	1	1	0	1	0	1	8

Elección: Para la elección del software del proyecto se ha optado por OPNsense debido a que es una opción sólida y popular como sistema operativo de firewall y enrutamiento de código abierto. Está basado en FreeBSD, además que cuenta con una interfaz web fácil de usar, actualizaciones automáticas, soporte para redes virtuales, opciones avanzadas de seguridad como VPN y autenticación de dos factores, y una amplia selección de paquetes adicionales para funcionalidad adicional. En comparación con otras alternativas, OPNsense se destaca por su enfoque de seguridad, transparencia y enfoque comunitario. Además, su sistema de plugins y paquetes permite a los usuarios personalizar y escalar fácilmente el sistema para satisfacer sus necesidades.

OPNsense es un sistema operativo libre y de código abierto basado en FreeBSD, que se utiliza como firewall y enrutador de red. Ofrece una amplia gama de características de seguridad, como la prevención de intrusiones basada en firmas y basada en reglas, el filtrado de paquetes, la autenticación de usuarios y la creación de VPN. Además, cuenta con una interfaz web fácil de usar que permite la gestión de las políticas de seguridad y el monitoreo del tráfico de red. OPNsense se enfoca en la seguridad y la privacidad del usuario, y se actualiza constantemente para mantenerse al día con las últimas amenazas y vulnerabilidades (OPNsense, 2023). A continuación, se listan las principales características del sistema operativo:

- Traffic Shaper (Modelador de tráfico de red)
- Autenticación de dos factores para iniciar sesión en la administración del sistema.
- Portal cautivo para el inicio de sesión de los usuarios.

- VPN: incorpora tanto el modo site-to-site como el modo road-warrior, además, es compatible con IPsec y OpenVPN.
- Dispone de HA (High Availability) y hardware failover, para que en caso de caída de un firewall automáticamente entre el siguiente.
- Incorpora IPS (sistema de detección de intrusiones) y también un IDS (sistema de detección de intrusiones).
- Servidor DNS, DNS Forwarder, DHCP server, DHCP relay, Dynamic DNS, etc.
- Permite visualizar en tiempo real gráficos del tráfico, exportar los datos a un servidor remoto.
- Soporta el estándar 802.1Q VLAN para segmentar la red adecuadamente
- Soporte de plugins desarrollados por la comunidad.

3.6 Arquitectura del sistema

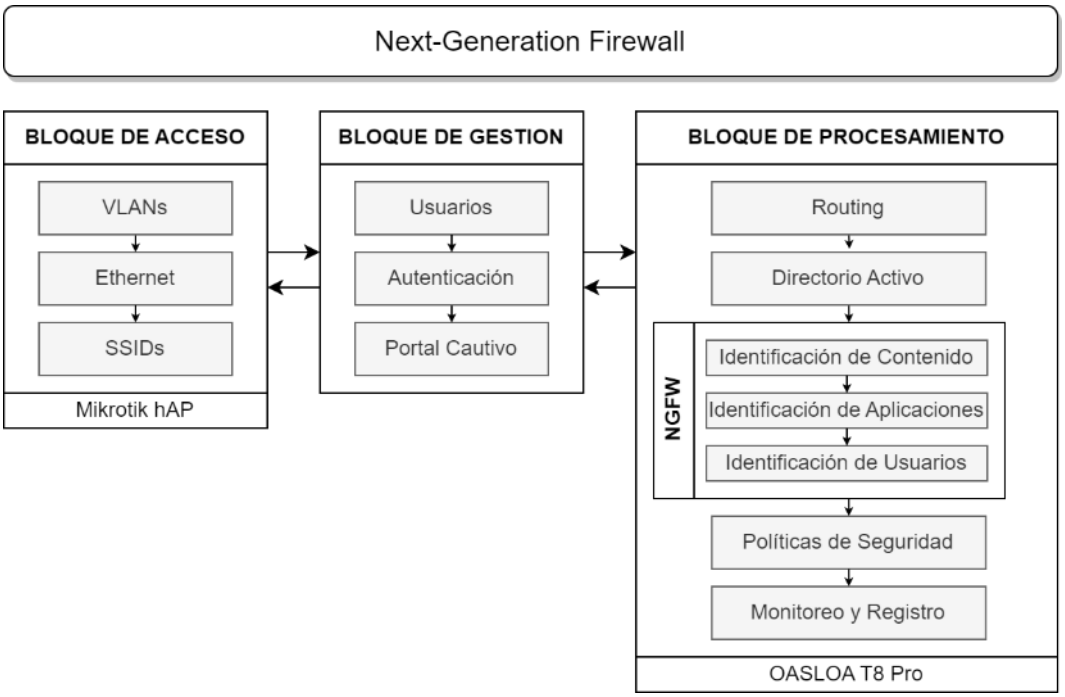
Una vez se han definido los requerimientos y seleccionado los componentes de Hardware y Software para cada componente del sistema, se deben delimitar las funciones y definir la arquitectura de funcionamiento. Esto se lo realiza mediante el diseño de los diagramas de bloque y flujogramas tanto para el esquema general como para cada etapa de funcionamiento. Estos permiten definir correctamente los procesos a seguir y cumplir de acuerdo con la etapa o bloque.

3.6.1 Diagrama de Bloques General del Sistema.

En el siguiente apartado se muestra mediante un diagrama de bloques el sistema de seguridad planteado para el presente proyecto, el cual consta de 3 bloques principales como se observa en la Figura 6, los cuales comprenden funciones y procesos principales de cada etapa, mismos que se puntualizarán más adelante.

Figura 6

Diagrama de bloques general del sistema



3.6.1.1 Bloque de Acceso

Este bloque desempeña un papel fundamental en la provisión de acceso inalámbrico a la red local. En esta etapa, se lleva a cabo la segmentación de la red en tres subredes distintas, cada una de ellas asociada a una VLAN y SSID específica. Esta segmentación permite la asignación de accesos diferenciados a los usuarios finales según su tipo de usuario, brindando un mayor nivel de seguridad y control sobre la red inalámbrica. De esta manera, se garantiza que cada usuario tenga acceso únicamente a la subred y servicios correspondientes a su perfil, mejorando la eficiencia y el cumplimiento de políticas de seguridad en el entorno de red.

3.6.1.2 Bloque de Gestión

Este es el encargado de interactuar entre los bloques de acceso y de procesamiento, este el bloque se encarga de filtrar el acceso de los usuarios a través de la implementación de un portal cautivo, el cual autentica a los usuarios antes de permitir su vinculación a la red. Este proceso de autenticación asegura un nivel adecuado de seguridad

y control en el acceso a los recursos de la red, contribuyendo así a la protección y eficiencia general del sistema. Cabe destacar que las políticas de acceso y las reglas de filtrado se establecerán en el bloque subsiguiente, enmarcando el funcionamiento completo del sistema.

3.6.1.3 Bloque de Procesamiento

En este bloque se definen los componentes físicos y lógicos de la red, tales como las VLANs, las subredes asociadas y los puertos físicos a utilizar. Este bloque además es el encargado del análisis y detección de amenazas mediante la inspección avanzada de los paquetes entrantes, mediante el módulo App-ID que verifica las firmas en la capa aplicación, además decodifica y descifra el tráfico entrante independientemente del puerto, protocolo o tipo de cifrado (SSH o SSL). El módulo Content-ID es el encargado de la prevención de amenazas en tiempo real mediante la implementación de una base de datos de URL que permite distinguir entre sitios confiables y no confiables, además cuenta con características que limitan las transferencias de archivos no seguros, bloqueo de exploits y malware. Por último, el módulo User-ID al combinarlo con las políticas de seguridad permite definir recursos y funciones específicas solo para determinados grupos de usuarios, además de la generación de reportes detallados para analizar tanto las amenazas mitigadas como el comportamiento de los usuarios dentro de la red al conocer los sitios web bloqueados y accedidos por cada usuario en específico.

3.7 Diseño del Sistema

Una vez definida la arquitectura y seleccionados los elementos tanto de hardware como de software necesarios se procede a la realización del diseño del sistema, en los siguientes bloques se describirán los diagramas de conexión del sistema, los diagramas de flujo que establecen la lógica implementada en cada sección y los diagramas de bloque que determinan el flujo de los procesos para cada bloque planteado.

3.7.1 Diagrama General de Conexión

El sistema propuesto consta de dos dispositivos principales: un Access Point para la distribución de la red inalámbrica y un MiniPC encargado de la gestión de la red y las políticas de seguridad. Además, se utiliza un Router principal proporcionado por el Proveedor de Internet para el hogar, el cual debe ser configurado en modo puente para permitir el flujo libre de tráfico y transferir las funciones de enrutamiento al sistema propuesto.

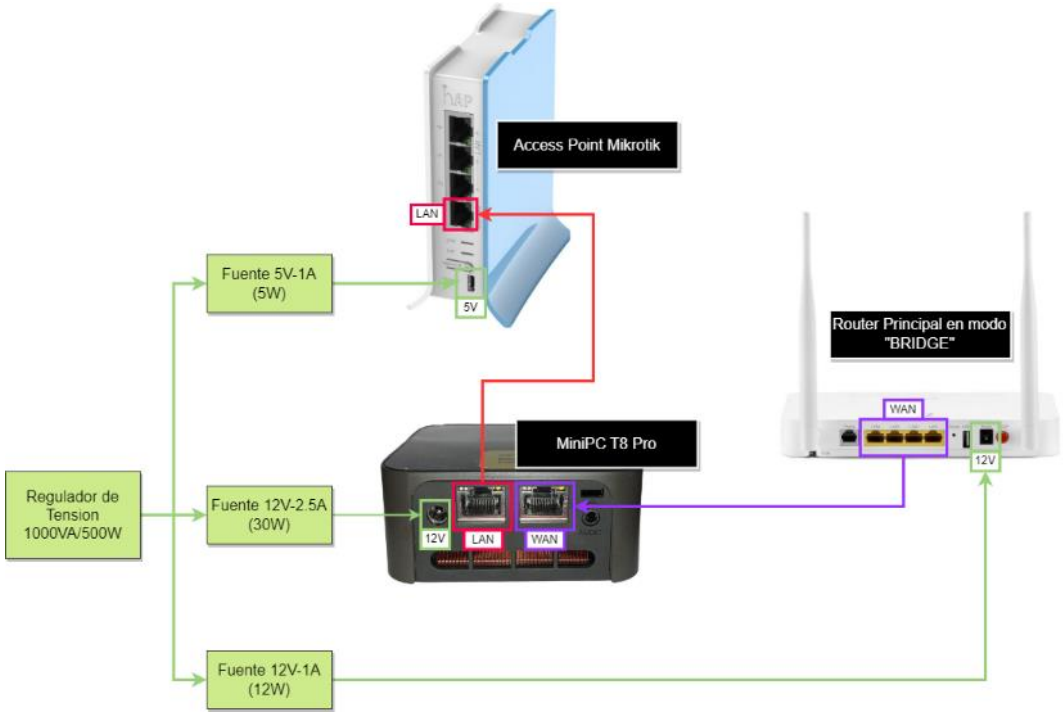
En cuanto al aspecto eléctrico, los tres dispositivos de la red están conectados a un regulador de sobretensión con el fin de prevenir daños causados por fluctuaciones bruscas de voltaje. Además, cada dispositivo cuenta con su propio conversor/adaptador de corriente, el cual proporciona la tensión y potencia adecuadas según las especificaciones de cada equipo.

En cuanto a las conexiones de red, se inicia la conexión desde el Router principal vinculando cualquiera de sus puertos LAN que al estar configurados en modo Bridge se vuelven una extensión del enlace directo con el ISP, el otro extremo del cable ethernet debe ser insertado en el puerto Ethernet 2 del MiniPC que ahora realizará las funciones del puerto antes destinado a la conexión WAN. El puerto Ethernet 1 del MiniPC debe estar conectado con el puerto Ethernet 1 del Access Point para establecer la conexión de área local (LAN).

En la Figura 7 se muestra el diagrama de conexiones que deben realizarse para el correcto funcionamiento del sistema, considerando tanto las conexiones eléctricas las cuales se representan de color verde, como la conexión para la red de área local, representada en color rojo y finalmente la conexión para la salida a internet mostrada en color morado.

Figura 7.

Diagrama de conexión del sistema



3.7.2 Diagrama de Flujo del Proceso General del Sistema

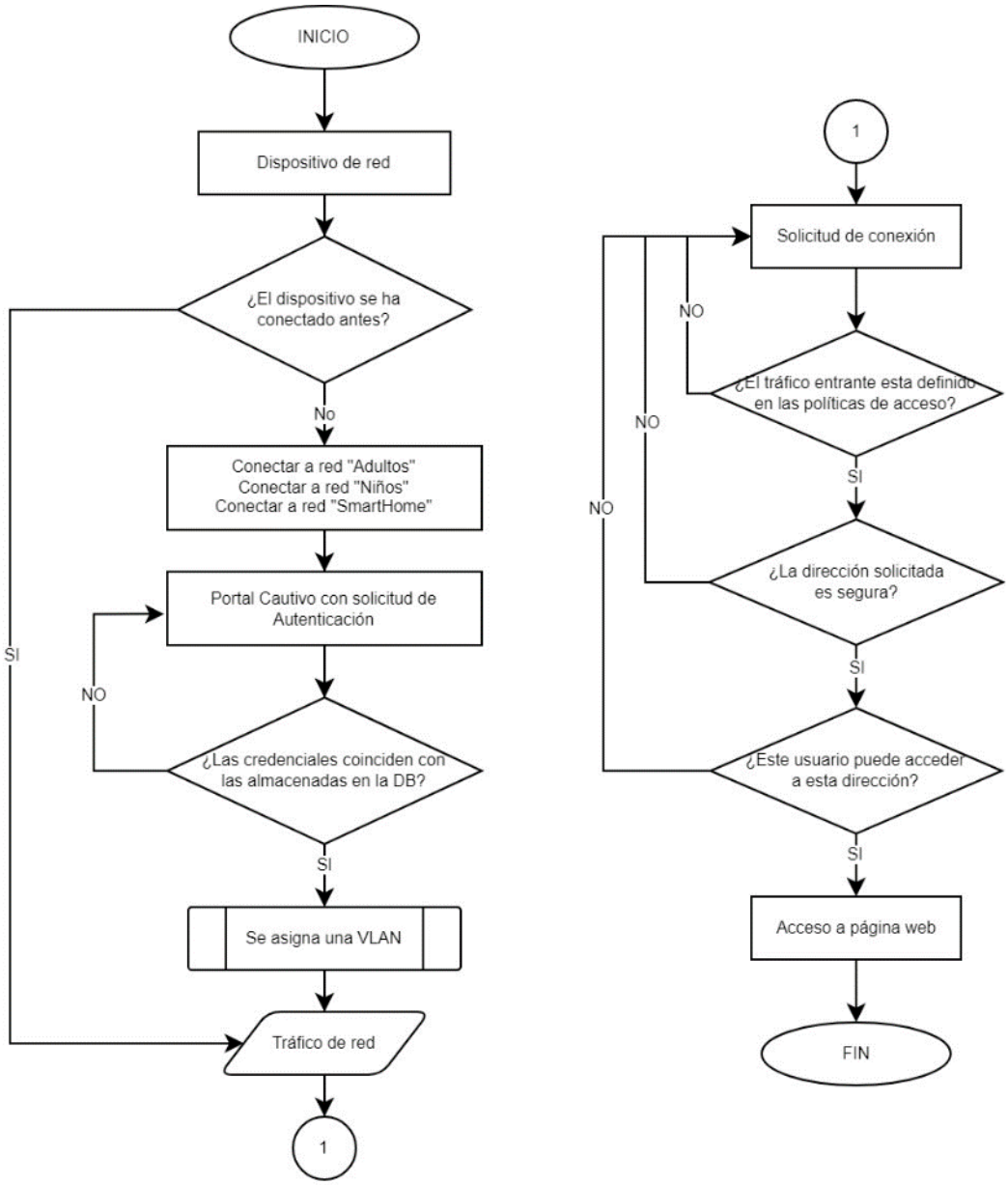
El funcionamiento del sistema desde la perspectiva del cliente comienza cuando un dispositivo de red desea conectarse a una de las redes inalámbricas, las cuales han sido divididas en segmentos según su tipo de uso. El dispositivo muestra al usuario tres opciones de redes inalámbricas identificadas por sus SSID: "Adultos", "Niños" y "SmartHome". El dispositivo se conecta a una de estas redes ingresando una contraseña predefinida. Posteriormente, se muestra una ventana emergente (perteneciente al portal cautivo) que solicita nuevas credenciales, las cuales corresponden a cada usuario. Estas credenciales se almacenan en la base de datos interna del Next-Generation Firewall (NGFW). Si las contraseñas ingresadas coinciden con las almacenadas en el directorio activo, se completa la autenticación y se asigna la VLAN correspondiente a la subred y al usuario.

Una vez que el tráfico ha sido etiquetado y autenticado entra en funcionamiento los módulos de procesamiento del NGFW, empezando por el App-ID que se encarga de permitir o bloquear el tráfico de acuerdo con las aplicaciones configuradas, esto independientemente de los puertos asignados como lo haría un firewall convencional, debido a que este realiza el análisis en una capa superior. Luego el módulo Content-ID es el encargado de desencriptar la información y verificar que el contenido no este contaminado con malware, además compara las firmas para validad que las direcciones origen y destino son seguras. Finalmente, el módulo User-ID registra la actividad asociada al usuario que genero dicho tráfico, almacenando todo en la base de datos interna.

Como se puede observar en el diagrama presente en la Figura 8 una vez que el tráfico generado por determinado dispositivo ha pasado todos los filtros y cumplido con todas las políticas de acceso este finalmente puede acceder a la aplicación o sitio web solicitado.

Figura 8.

Diagrama de flujo del proceso general del sistema



3.7.3 Bloque de Acceso

Dentro de los procesos ejecutados en el bloque de acceso se encuentran la vinculación del dispositivo solicitante a la red inalámbrica, la autenticación de los usuarios a la red y la asignación de las VLANs de al tráfico establecido por el usuario. Una vez completados estos procesos el tráfico avanza al siguiente bloque en donde se realizarán los procesos de red que se detallarán en la siguiente sección.

El proceso de acceso dentro del primer bloque comienza cuando un dispositivo solicita conectarse a la red inalámbrica proporcionada por el Access Point MikroTik, el cual muestra 3 SSIDs, cada uno destinado a un tipo específico de usuario. Para acceder, el usuario debe ingresar la contraseña correspondiente a la red deseada, lo que representa la primera barrera de seguridad.

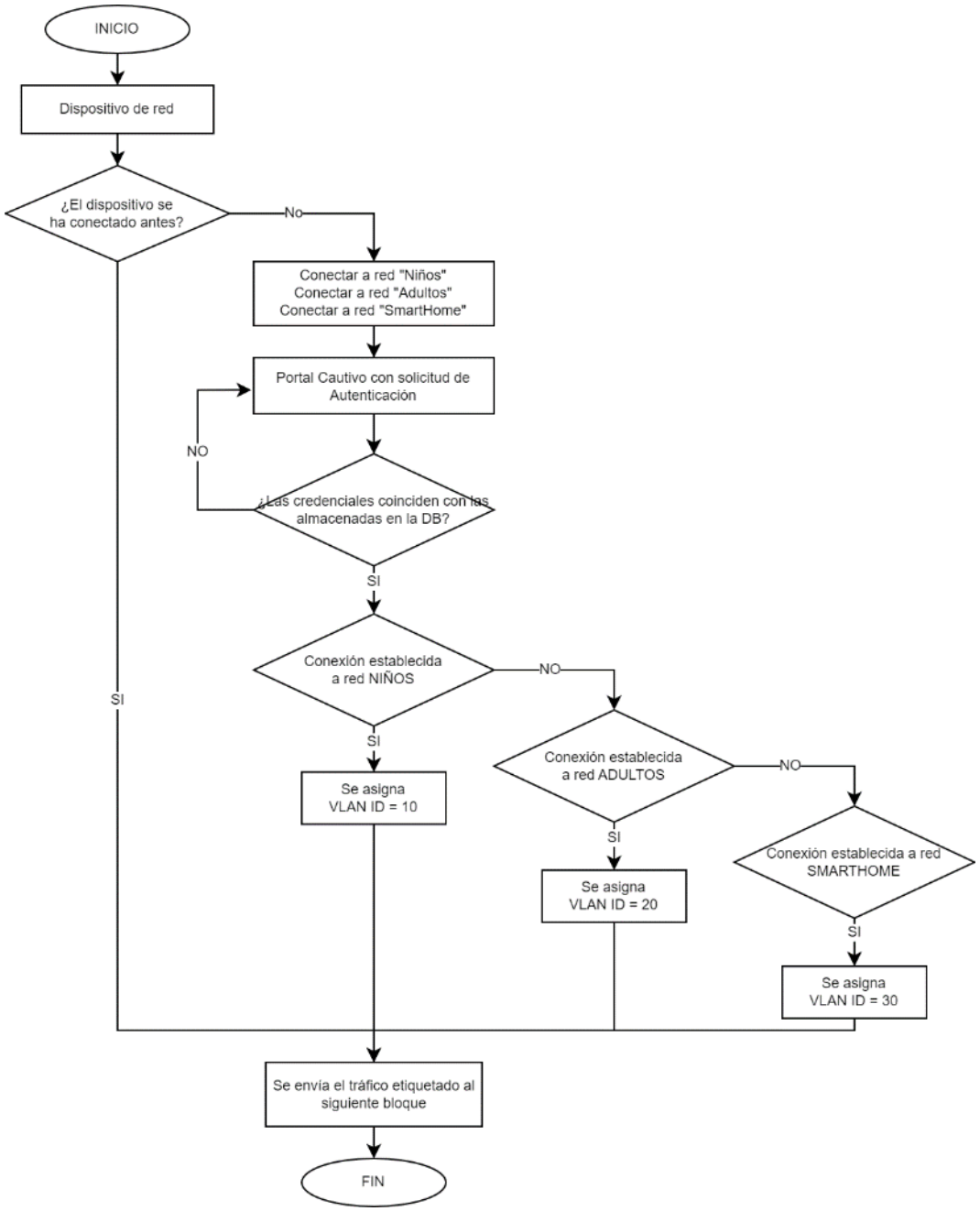
Una vez superada la autenticación inicial, se desplegará un aviso emergente solicitando las credenciales de usuario, las cuales deben estar almacenadas en la base de datos local ubicada en el bloque de gestión. Esta segunda etapa de autenticación permite verificar la identidad del usuario y del dispositivo vinculado, asegurando un nivel adicional de seguridad.

Dado que cada usuario y dispositivo tienen asignados permisos diferenciados en función de su tipo de usuario, se realiza el etiquetado del tráfico correspondiente. Esta etiquetación se lleva a cabo en base a la red inalámbrica a la que se ha vinculado el dispositivo. Asignar etiquetas de VLAN a los flujos de datos permite gestionar el tráfico de manera eficiente y segmentada, asegurando un flujo de datos controlado y protegiendo la integridad y la privacidad de cada tipo de usuario.

El proceso de acceso en el primer bloque implica una doble autenticación: primero, mediante la contraseña de la red inalámbrica, y luego, con las credenciales de usuario almacenadas en la base de datos. Una vez autenticado, el dispositivo es etiquetado para dirigir el tráfico de manera adecuada, garantizando una experiencia segura y optimizada para cada usuario en la red.

Figura 9.

Diagrama de flujo de los procesos ejecutados en el Bloque de Acceso



En la Tabla 14 se presentan los usuarios y las redes inalámbricas a las que están vinculados, junto con el valor de la etiqueta correspondiente a la VLAN y la subred asignada. Cada uno de estos dispositivos obtiene una dirección IP mediante el servidor DHCP presente en el Next-Generation Firewall (NGFW).

Tabla 14.

Tabla de direccionamiento de red.

Usuario	Dispositivos	SSID	VLAN	Subnet	IP
Alexander	▪ Smartphone ▪ PC	Adultos	20	192.168.10.0/24	DHCP
Dayana	▪ Smartphone ▪ Laptop	Adultos	20	192.168.10.0/24	DHCP
Mauricio	▪ Smartphone	Adultos	20	192.168.10.0/24	DHCP
Rosa	▪ Smartphone	Adultos	20	192.168.10.0/24	DHCP
Pamela	▪ Smartphone	Adultos	20	192.168.10.0/24	DHCP
Nicolas	▪ Smartphone ▪ Consola Videojuegos	Niños	10	192.168.20.0/24	DHCP
Valentina	▪ Smartphone ▪ SmartTV	Niños	10	192.168.20.0/24	DHCP

El servidor DHCP es el encargado de asignar automáticamente direcciones IP a los dispositivos de manera dinámica, lo que garantiza que cada dispositivo conectado a la red reciba una dirección única y válida dentro de la subred asignada. Esta funcionalidad facilita la gestión y configuración de la red, ya que los usuarios no necesitan configurar manualmente sus direcciones IP, y el servidor DHCP se encarga de asignarlas de manera eficiente y evitando conflictos de direcciones.

Al adoptar este enfoque, se logra una administración centralizada y simplificada de las direcciones IP en la red inalámbrica, lo que mejora la escalabilidad y la flexibilidad del sistema. Los usuarios pueden acceder a la red de manera rápida y sencilla, sin preocuparse por configuraciones complejas, mientras que el NGFW se encarga de asignar y administrar adecuadamente tanto las direcciones IP como las VLANs con la finalidad de garantizar un funcionamiento eficiente y confiable de la red.

3.7.4 Bloque de Gestión

Los procesos llevados a cabo en el bloque de gestión se inician con el dispositivo solicitante, que realiza una petición para acceder a los recursos de la red. Esta solicitud implica una autenticación al servidor, donde se verifican las credenciales almacenadas en la

base de datos correspondientes a los usuarios registrados y autorizados para acceder a la red.

Una vez que el dispositivo selecciona una SSID e ingresa la contraseña correspondiente, debe superar el segundo filtro de seguridad. Este filtro vincula el dispositivo con el usuario específico a través de un portal cautivo, en el cual se solicita el nombre de usuario y su contraseña única.

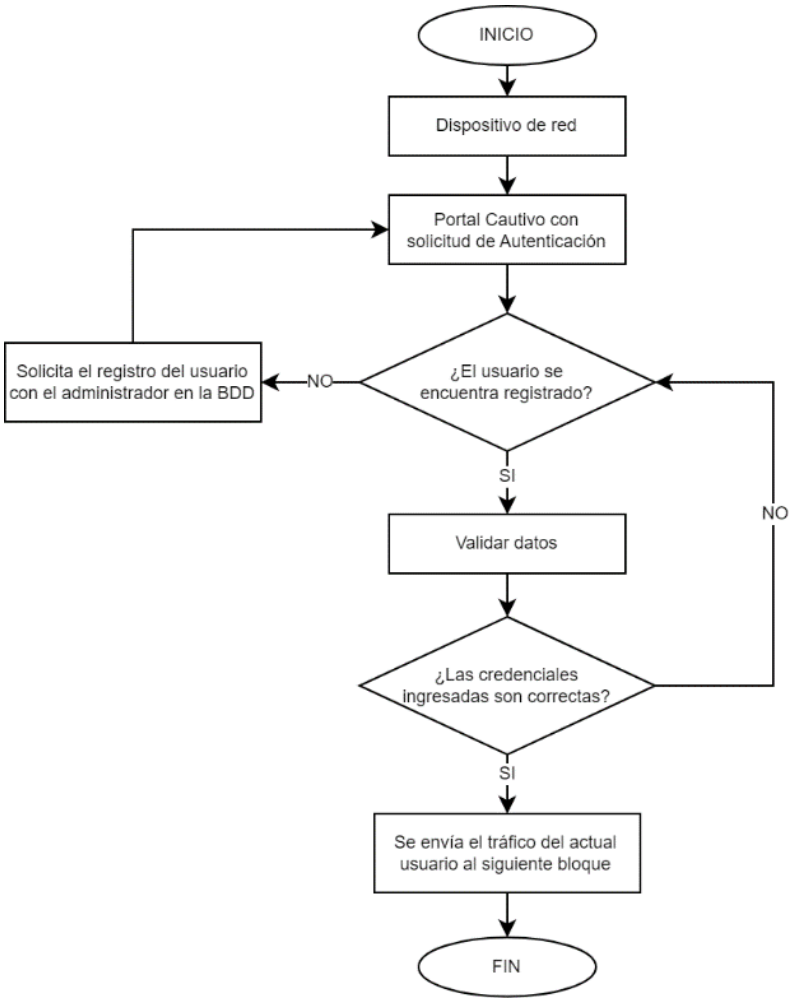
El Next-Generation Firewall (NGFW), a través de su módulo de autenticación, se encarga de realizar una comprobación y una negociación con la base de datos para establecer la conexión. Si la información ingresada coincide con la almacenada en la base de datos, se permite el acceso a la red. Este proceso garantiza que solo los usuarios autorizados puedan conectarse a la red y acceder a los recursos correspondientes.

Una vez que el proceso de autenticación ha sido completado con éxito, el tráfico del dispositivo es gestionado por el siguiente bloque, el cual se encarga de aplicar las políticas de seguridad y calidad de servicio establecidas para cada tipo de usuario y red inalámbrica.

El bloque de gestión es fundamental para asegurar la autenticación y vinculación adecuada de los dispositivos con los usuarios autorizados, proporcionando un nivel adicional de seguridad y control en el acceso a la red. Como se observa en la Figura 10, una vez verificada la identidad del usuario el tráfico es dirigido al siguiente bloque para su correcto manejo y optimización en función de las políticas establecidas posteriormente.

Figura 10.

Diagrama de flujo de los procesos ejecutados en el Bloque de Gestión



3.7.5 Bloque de Procesamiento

El bloque de procesamiento es el responsable de clasificar el tráfico en función de las VLANs asignadas y aplicar las reglas de filtrado correspondientes a cada tipo de usuario en la red. Este bloque emplea varios procesos para garantizar una protección integral y efectiva de la red.

El primer proceso es el App-ID, que verifica si el tráfico entrante está permitido en la capa de aplicación, sin importar el protocolo o puerto utilizado. Este enfoque es altamente efectivo para evitar intentos de evasión de las políticas de seguridad establecidas, ya que puede detectar incluso tráfico cifrado. La capacidad del App-ID de inspeccionar el tráfico a

nivel de aplicación asegura un control granular y preciso sobre los recursos y servicios a los que los usuarios pueden acceder.

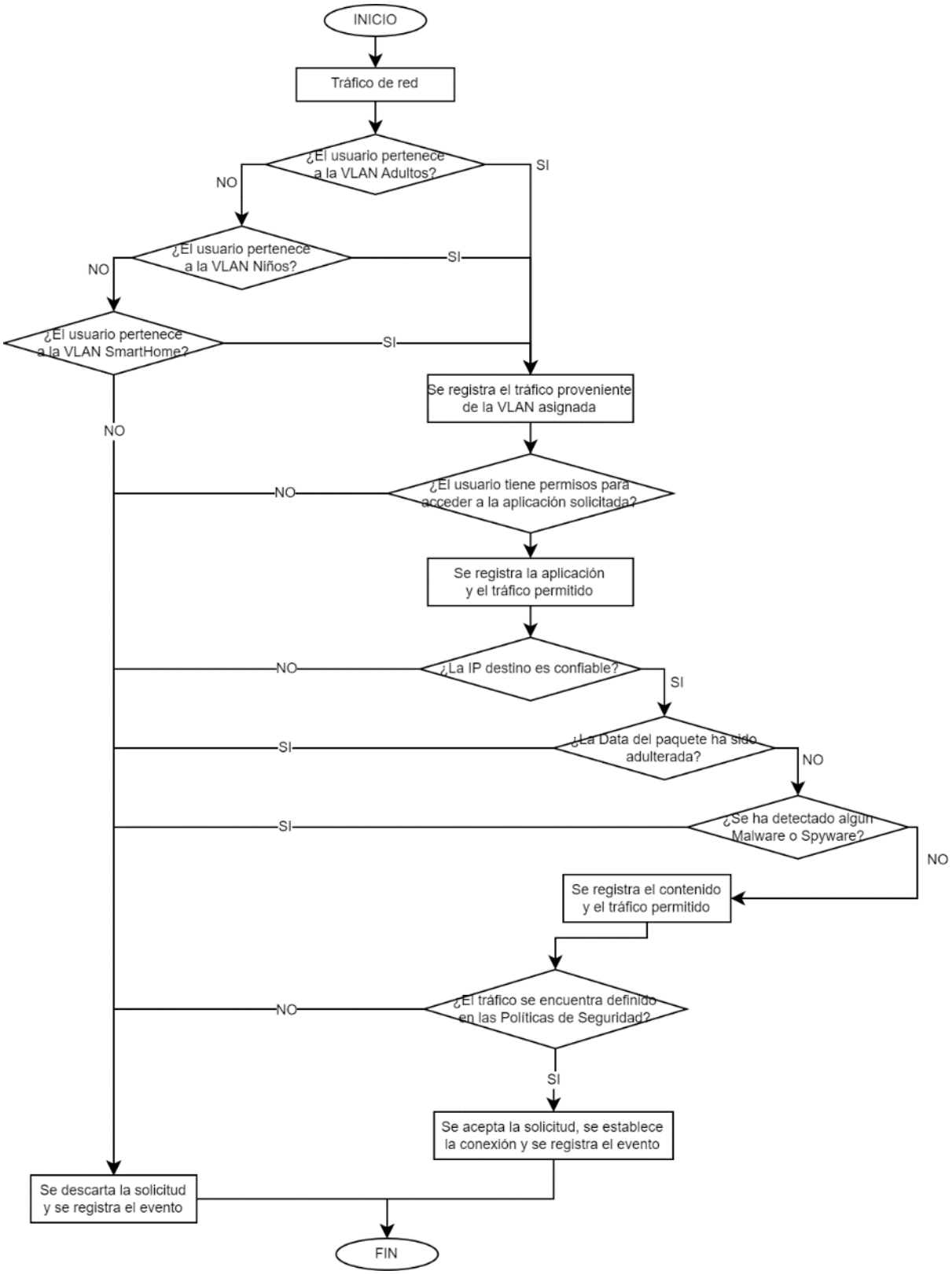
A continuación, el Content-ID entra en acción al conectarse con servidores dedicados proporcionados por Zenarmor. Este proceso realiza un análisis basado en direcciones web clasificadas como seguras, lo que permite filtrar en tiempo real el tráfico entrante. Dado que esta base de datos se actualiza constantemente gracias a la retroalimentación de la comunidad, representa una barrera sólida frente a sitios web reportados como inseguros, fortaleciendo la seguridad y la prevención de amenazas en la red.

El proceso siguiente es llevado a cabo por el User-ID, que realiza el último filtrado del tráfico de acuerdo con las políticas internas definidas en las políticas de seguridad específicas para cada tipo de usuario. Además de este importante papel en el filtrado, el User-ID ofrece funciones avanzadas de visualización y generación de informes en tiempo real. Esto permite un análisis exhaustivo de la red, facilita la identificación de posibles anomalías y proporciona informes detallados sobre las conexiones, lo que permite una supervisión activa y una respuesta rápida ante cualquier incidente de seguridad.

En conjunto, estos procesos del bloque de procesamiento que se muestran de forma gráfica en la Figura 11 garantizan una protección completa y efectiva de la red, asegurando que el tráfico sea adecuadamente clasificado, filtrado y monitorizado para mantener la seguridad y la integridad del sistema en todo momento.

Figura 11.

Diagrama de flujo de los procesos ejecutados en el Bloque de Procesamiento



3.8 Implementación

En la siguiente sección, se procede a describir en detalle los procedimientos realizados para llevar a cabo la implementación tanto del software como del hardware en cada uno de los bloques del sistema. Estos procesos son fundamentales para lograr la ejecución exitosa de todas las operaciones planificadas previamente. La puesta en marcha de estos componentes constituye un hito clave en el desarrollo del proyecto, ya que marca la transición desde la fase de diseño y planificación hacia la operatividad efectiva del sistema. Cada paso y decisión tomados durante esta etapa juega un papel crucial en la capacidad del sistema para cumplir con todos los requerimientos y objetivos del proyecto.

3.8.1 Implementación de Software

En la fase de implementación del software, se profundiza en las consideraciones técnicas de diseño que guían la estructuración de cada componente, junto con las configuraciones meticulosamente aplicadas en todos los dispositivos interconectados dentro de la red del sistema propuesto. Estas consideraciones abarcan desde la arquitectura global del sistema hasta los detalles de las interfaces y protocolos empleados. Cada configuración adoptada se ajusta a las necesidades específicas del sistema y contribuye a la creación de un entorno coherente y funcional.

3.8.1.1 Bloque de Acceso

Para la implementación del software en el bloque de acceso se ha considerado la segmentación de la red mediante VLANs, el establecimiento de las SSID para las diferentes subredes, así como la personalización de sus perfiles de seguridad, aquí además se configuran las interfaces físicas y se crean las subinterfaces lógicas que se implementaran en el Access Point, aquí se habilitan los protocolos necesarios para la conexión e intercomunicación con los bloques subsecuentes.

3.8.1.1.1 Segmentación de la red con VLANs

Como se muestra en la Tabla 15 se planteó la segmentación de la red mediante VLANs asociadas a las redes inalámbricas con el objetivo de gestionar el tráfico de acuerdo con el tipo de usuario vinculado. Para ello, se establecieron las siguientes subredes:

Tabla 15.
VLAN tag asignadas a las subredes planificadas

Interfaz	Subnet	VLAN	Descripción
alc0_vlan10	192.168.10.0/24	10	VLAN dedicada para el tráfico del contenido de los niños
alc0_vlan20	192.168.20.0/24	20	VLAN con libre acceso a la Web y a las aplicaciones.
alc0_vlan30	192.168.30.0/24	30	VLAN dedicada al tráfico de dispositivos SmartHome (SmarTVs, Alexa, Google Home)

- **Subred "Niños":** Esta subred está diseñada para usuarios infantiles y se asigna una VLAN particular (10). Se implementan medidas de filtrado y control de contenidos para asegurar un entorno seguro y apropiado para los niños.

- **Subred "Adultos":** Esta subred está destinada a usuarios adultos y se configura con una VLAN específica (20). Se aplican políticas de seguridad y restricciones de acceso para garantizar la privacidad y seguridad de los usuarios en esta red.

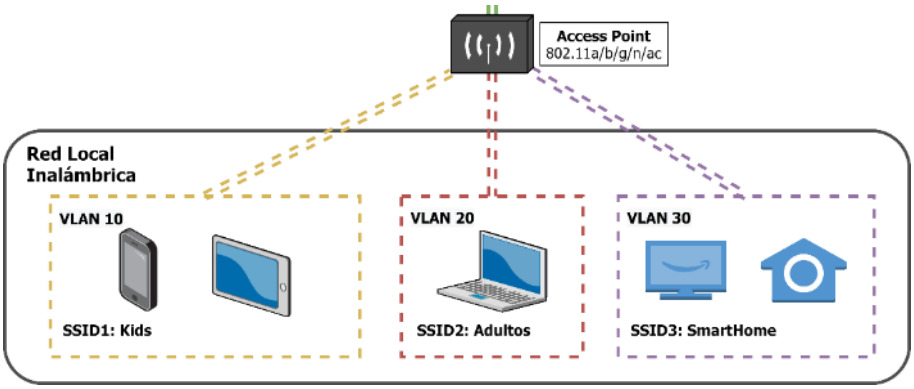
- **Subred "SmartHome":** Esta subred se utiliza para dispositivos y sistemas domésticos inteligentes. Se les asigna una VLAN (30) para gestionar el tráfico relacionado con la automatización del hogar, como luces, termostatos y asistentes de voz.

Cada subred VLAN se configura con políticas de seguridad adecuadas para optimizar, proteger y garantizar una experiencia de usuario óptima en cada segmento. Esta

segmentación basada en VLANs permite una gestión eficiente del tráfico y una mayor seguridad en el sistema global de la red inalámbrica debido a que como se muestra en la Figura 12 aísla el tráfico presente en cada subred, evitando que se acceda a recursos no autorizados o se propague cualquier anomalía de un segmento a otro.

Figura 12.

Subredes de la red Local Inalámbrica.

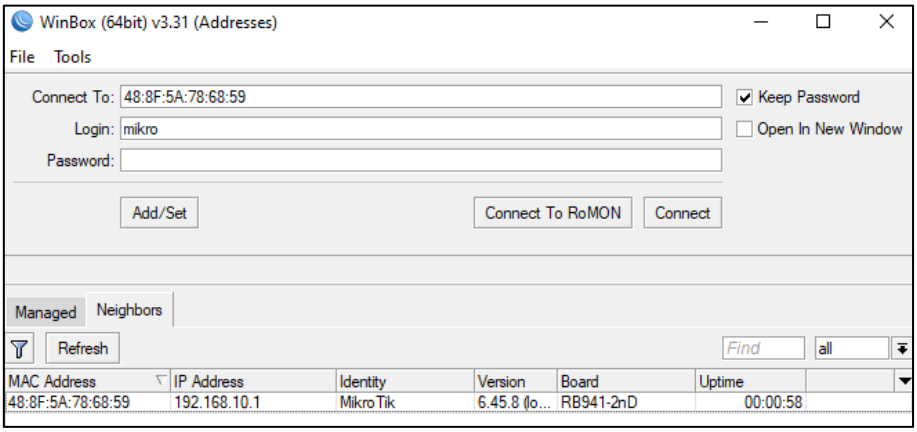


3.8.1.1.2 Configuración inicial del Access Point

Para llevar a cabo las configuraciones necesarias en el Access Point, es necesario eliminar cualquier rastro de configuración previa, incluidas las predeterminadas. Este procedimiento se realiza a través de la aplicación WinBox, donde se escanea los dispositivos de la red y se selecciona el deseado tal como se muestra en la Figura 13, luego se inicia sesión en el hAP de MikroTik utilizando la contraseña predeterminada.

Figura 13.

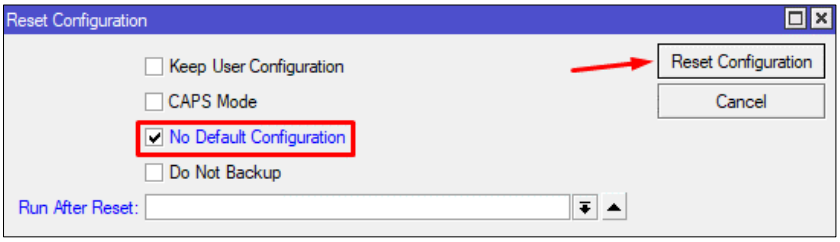
Interfaz de administración Winbox



Una vez se ha ingresado al dispositivo mediante la aplicación Winbox se debe dirigir a la sección “System/Reset Configuration” en donde se muestra una ventana emergente Figura 14 con varias opciones, se debe marcar la opción “No Default Configuration” para que de esta forma el dispositivo elimine todas las configuraciones presentes, pero además no aplique ninguna configuración predeterminada para algún tipo de operación por defecto.

Figura 14.

Restablecimiento del dispositivo



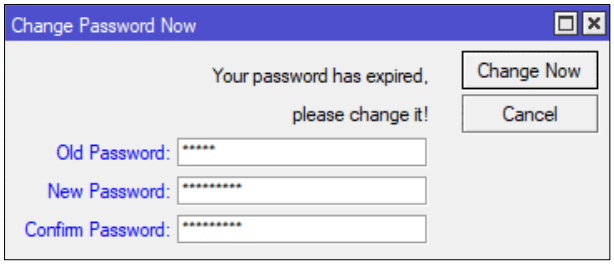
3.8.1.1.3 Cambio de contraseña predeterminada

Al reestablecerse el dispositivo a su configuración inicial cuando se ingrese por primera vez se solicitará el cambio de contraseña predeterminada como se observa en la Figura 15 debido a que se vuelve inseguro mantener las contraseñas predeterminadas, se debe seleccionar una nueva contraseña que sea segura combinando letras mayúsculas,

minúsculas, dígitos numéricos y caracteres especiales, además de la contraseña la únicamente la debe conocer el administrador del sistema.

Figura 15.

Cambio de contraseña predeterminada

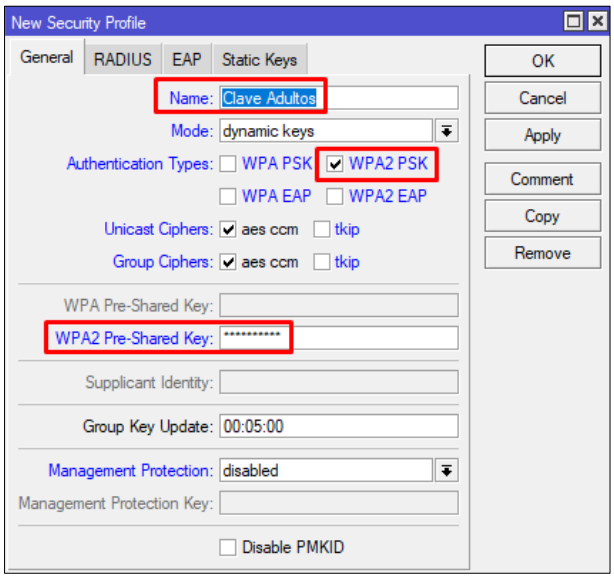


3.8.1.1.4 Establecimiento de perfiles de seguridad

Debido a que se utilizarán diversas SSIDs en la red se crean los diversos perfiles de seguridad para aplicarlos a las redes inalámbricas, como se muestra en la Figura 16 se aplica un nombre para el perfil de seguridad, el modo de operación en “dynamic key”, el tipo de autenticación en “WPA2 PSK” y se crea una contraseña segura para el perfil.

Figura 16.

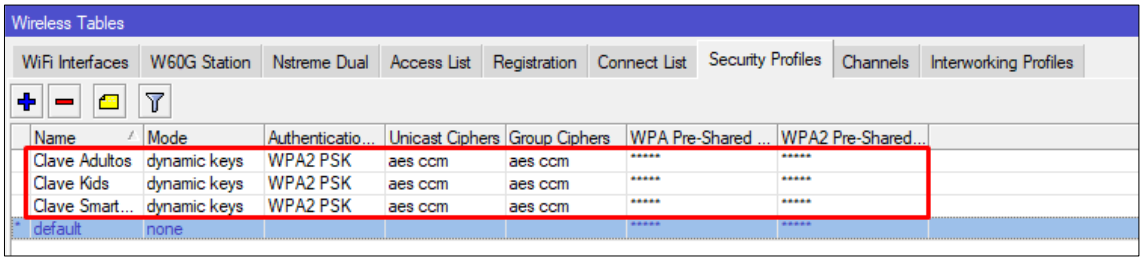
Creación de credenciales para perfiles de seguridad



Se crean los 3 perfiles de seguridad que luego serán asignados a cada una de las redes inalámbricas tal como se observa en la Figura 17, estos permitirán que cada SSID cuente con sus propias credenciales de autenticación a la red inalámbrica seleccionada.

Figura 17.

Perfiles de seguridad creados en el AP

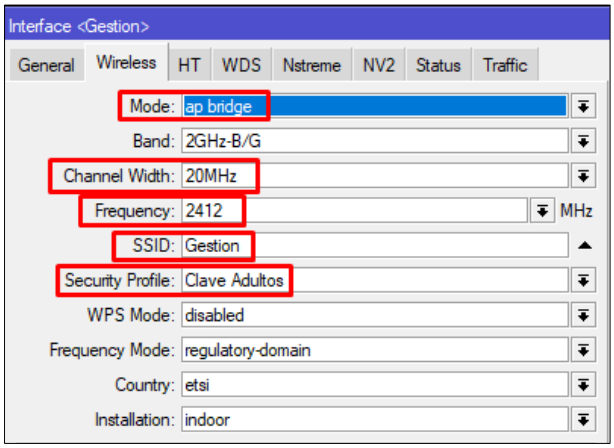


3.8.1.1.5 Creación de las SSID

Para llevar a cabo la creación de las redes inalámbricas, como se observa en la Figura 18 se inicia habilitando una interfaz inalámbrica de tipo Master, que posteriormente se vinculará con las demás subredes que se creen. Como red principal se ha designado la denominada GESTION. En este contexto, se elige el modo de operación "ap bridge", se define el ancho del canal y la frecuencia de operación. Asimismo, se asigna un identificador de conjunto de servicios (SSID). Adicionalmente, se selecciona el perfil de seguridad previamente configurado y se finaliza el proceso mediante la aplicación de los cambios correspondientes.

Figura 18.

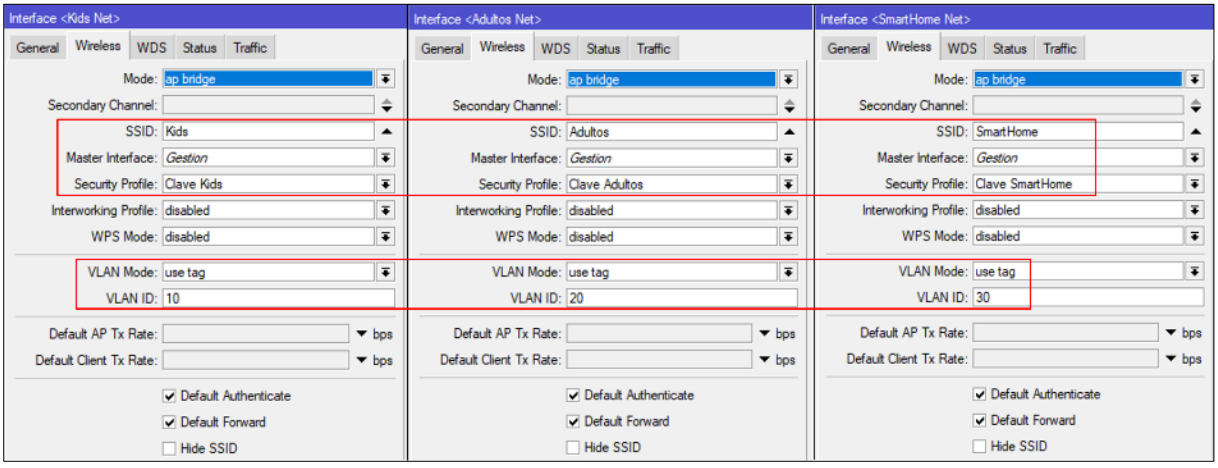
Configuración de los parámetros de la red inalámbrica.



A partir de la interfaz MASTER, se procede a la creación de las subredes adicionales las cuales son: Niños, Adultos y SmartHome, cada una con su correspondiente SSID. En este proceso, se selecciona la interfaz principal a la cual estas subredes están vinculadas (GESTION). Un aspecto crucial es que estas subredes hacen uso del protocolo 802.1q para llevar a cabo la etiquetación de su tráfico y lograr así la segmentación efectiva de la red en distintas VLANs. Como se muestra en la Figura 19, se asignan las etiquetas pertinentes a cada subred, asegurando la correcta separación de los flujos de datos y contribuyendo a la organización y seguridad de la red en su conjunto.

Figura 19.

Creación de las subredes ancladas a la red MASTER

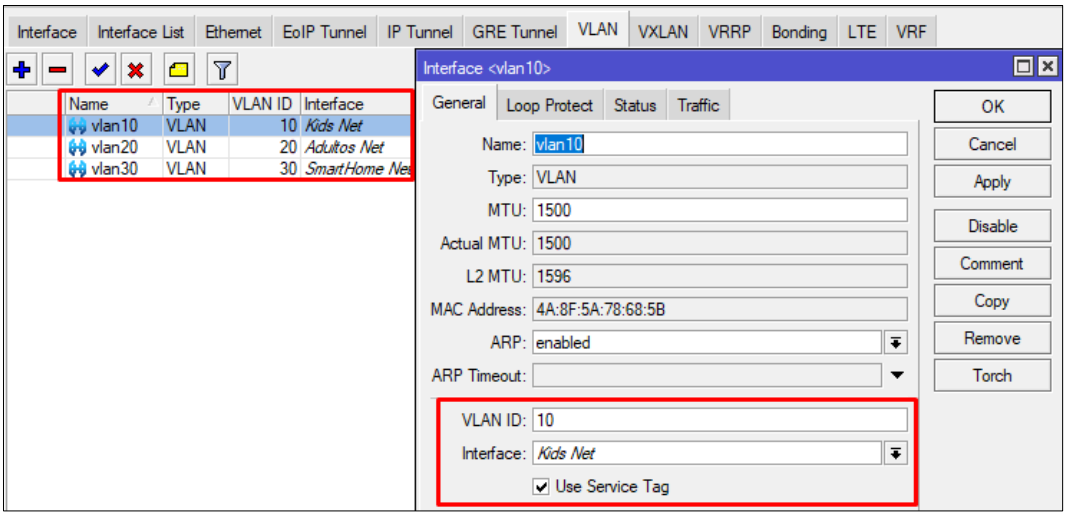


3.8.1.1.6 Creación de las VLANs

En el proceso de segmentación de la red, se procede a la creación de las tres interfaces virtuales (VLAN) que serán empleadas con este propósito. Como se muestra en la Figura 20, cada VLAN recibe un nombre distintivo para su identificación, se selecciona un ID que se asocia a la interfaz específica correspondiente. Esta asignación de ID garantiza una separación clara y ordenada de las redes virtuales dentro de la infraestructura, permitiendo un control preciso y eficiente del tráfico y los recursos en función de las necesidades y políticas de la red.

Figura 20.

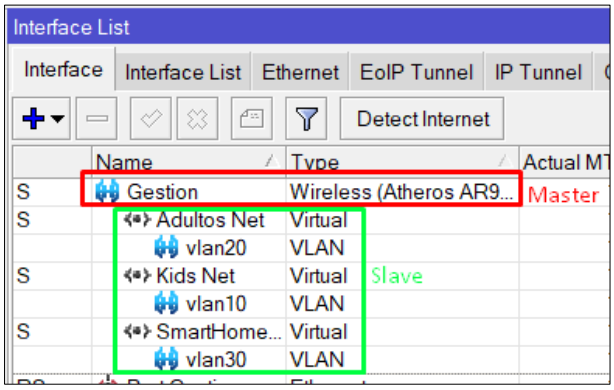
Verificación de las VLAN creadas



Luego de la configuración, se procede a verificar la correcta asociación de las redes inalámbricas de tipo "slave" (Adultos, Niños y SmartHome) con la red principal de tipo "Master" denominada GESTIÓN. Como se muestra en la Figura 21 mediante esta comprobación el administrador se asegura que la interconexión entre las redes sea efectiva y que la segmentación planificada funcione según lo previsto.

Figura 21.

Jerarquía de las redes inalámbricas.

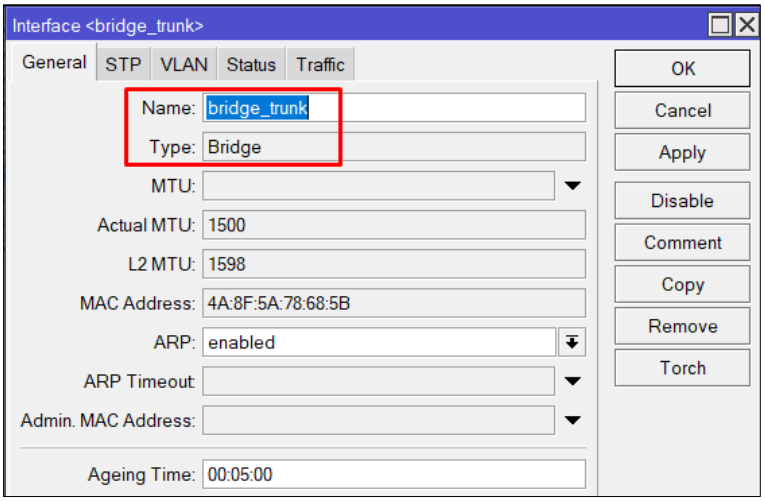


3.8.1.1.7 Configuración de interfaces Bridge

En la Figura 22 se realiza la creación de una interfaz virtual del tipo puente, comúnmente conocida como "bridge", con el propósito de consolidar la gestión del flujo de datos en la red. Esta interfaz actúa como un nodo central al cual se conectan tanto las interfaces virtuales como las físicas, posibilitando una integración fluida del tráfico entre ellas. La consolidación de estas conexiones en una única interfaz conlleva la optimización de la administración de datos, simplificando la gestión de la red.

Figura 22.

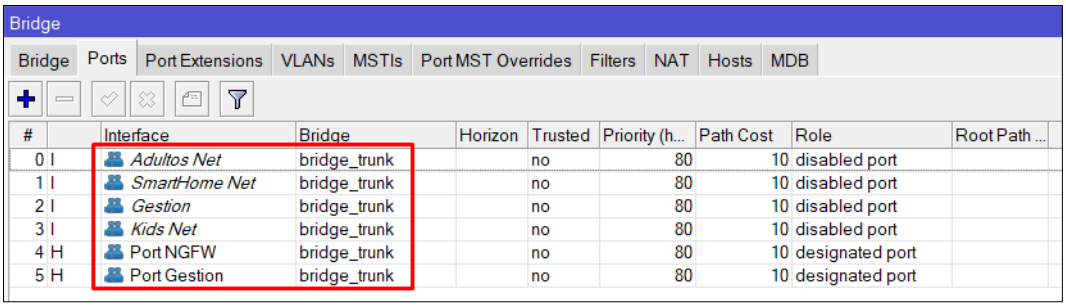
Creación de interfaz tipo puente.



En la Figura 23 se procede a asociar todas las interfaces configuradas, tanto físicas como virtuales en el Access Point al puente creado. Esta acción tiene como objetivo establecer una conectividad integral entre las interfaces y el NGFW. Al fusionar estas interfaces en el puente, se propicia un canal de comunicación uniforme y continuo con el NGFW, posibilitando un monitoreo y control eficiente de la circulación de datos. Esta sincronización asegura que el tráfico proveniente de diversas fuentes, tanto virtuales como físicas, sea dirigido hacia el NGFW para su análisis y filtrado, fortaleciendo así las capacidades de seguridad y regulación en la red.

Figura 23.

Interfaces asociadas al puente



3.8.1.2 Bloque de Gestión

Este bloque constituye el enlace necesario para la operatividad entre el bloque de acceso y el bloque de procesamiento, aquí se realizan las configuraciones en el NGFW tales como: El levantamiento y configuración del Portal Cautivo, la creación de los usuarios del sistema, la gestión de los permisos y niveles de acceso para cada tipo de usuario y la agrupación de los usuarios en grupos con permisos diferenciados.

3.8.1.2.1 Levantamiento de portal Cautivo

Para levantar el portal cautivo dentro OPNsense hay que hacerlo ingresando a “Services/Captive Portal/Administration” ya que el sistema cuenta por defecto con esta característica sin embargo hay que habilitarla tal como se muestra en la Figura 24.

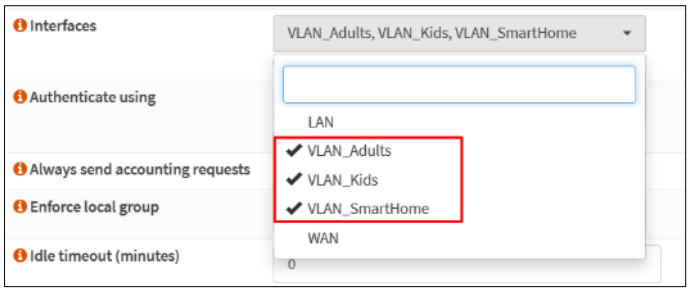
Figura 24.

Habilitación del portal cautivo

La Figura 25 ilustra cómo el portal cautivo puede ser implementado de manera selectiva en las subredes según su necesidad. En este contexto particular, las VLANs vinculadas a las subredes Adultos, Kids y SmartHome son las que han sido seleccionadas para aplicar el portal cautivo. No obstante, la interfaz LAN no es parte de esta selección, ya que se destinará para funcionar como enlace troncal. Esta elección asegura que el portal cautivo sea implementado únicamente en las áreas donde sea requerido.

Figura 25.

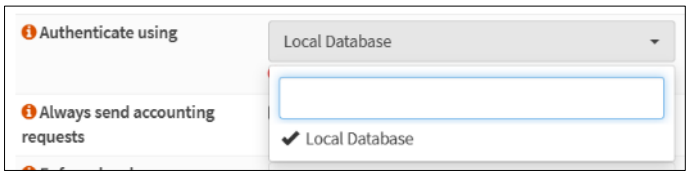
Redes con acceso al Portal Cautivo



El NGFW cuenta con una BDD local la cual almacena los usuarios que tendrán acceso tanto a las configuraciones del sistema como para el ingreso a la red. Como se observa en la Figura 26 se selecciona esta BDD como opción predeterminada para el proceso de autenticación de los usuarios finales.

Figura 26.

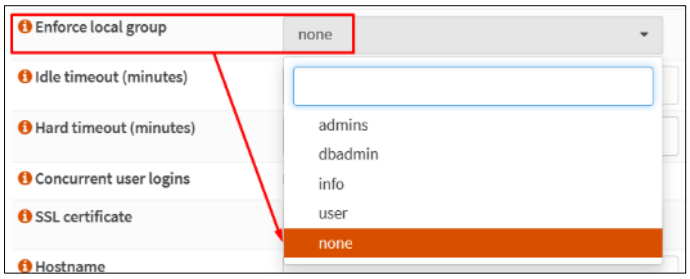
Selección de la BDD en la que se almacenan los usuarios



En el marco de sus funcionalidades, el portal presenta la capacidad de limitar el acceso para un grupo específico de usuarios en situaciones que lo requieran. En este contexto particular, como se muestra en la Figura 27 se ha optado por seleccionar la opción "ninguno", lo que implica que la solicitud se extienda a todos los usuarios sin distinción de sus permisos individuales.

Figura 27.

Exclusión de autenticación para los grupos de usuarios



3.8.1.2.2 Creación de usuarios

Dentro del contexto del sistema propuesto, se identifica la presencia de múltiples personas, quienes son los principales usuarios de la red en el entorno residencial a lo largo de cada jornada. En la Tabla 16 se presenta un listado que incluye todos los usuarios que forman parte de la red en la cual se implementará este sistema. Este registro detallado ofrece una visión completa y estructurada de los usuarios involucrados, facilitando así la administración y el monitoreo de las actividades y accesos en el sistema.

Tabla 16.

Usuarios de la red

Nombre de usuario	Persona asociada
amguanotoa	Alexander Guanotoa
miguantoa	Mauricio Guanotoa
jdhuera	Dayana Huera
jpguanotoa	Pamela Guanotoa
efguanotoa	Edy Guanotoa
ejguanotoa	Joel Guanotoa
enguanotoa	Nicolas Guanotoa
svreyes	Valentina Reyes

La Figura 28 proporciona una representación visual de la finalización exitosa de la creación y configuración de todos los usuarios planificados. En este proceso, a cada usuario se le ha asignado un nombre de usuario exclusivo, con el propósito de distinguirlo de otros en el sistema. Además, se ha proporcionado a cada usuario una contraseña única que garantiza su acceso seguro a la red. Además de estas credenciales, a cada usuario se le ha asignado un identificador, el cual corresponde a su nombre completo. Este proceso de configuración contribuye a la individualización de los usuarios y a una administración precisa y segura de sus accesos en el entorno de la red, reforzando así la integridad y la eficiencia del sistema implementado.

Figura 28.

Usuarios almacenados en la BDD

3.8.1.2.3 Asignación de usuarios a grupo

Dado que se prevé que cada usuario tendrá niveles de acceso diferenciados, se procede a realizar una clasificación detallada de los usuarios y asignarlos a uno o varios grupos tal como se observa en la Tabla 17. Cada uno de estos grupos poseerá permisos distintos, los cuales se ajustan según las necesidades y roles específicos de cada tipo de usuario. Estos permisos abarcan un espectro variado, que incluye la autorización para acceder a la red, ingresar a la Base de Datos (BDD), visualizar información, gestionar los permisos del sistema, efectuar cambios en las configuraciones y otras funciones relevantes. Esta segmentación y asignación de permisos garantiza un acceso controlado y una administración eficiente en función de las responsabilidades y requerimientos de cada usuario, promoviendo la seguridad y la gestión efectiva de los recursos del sistema.

Tabla 17.

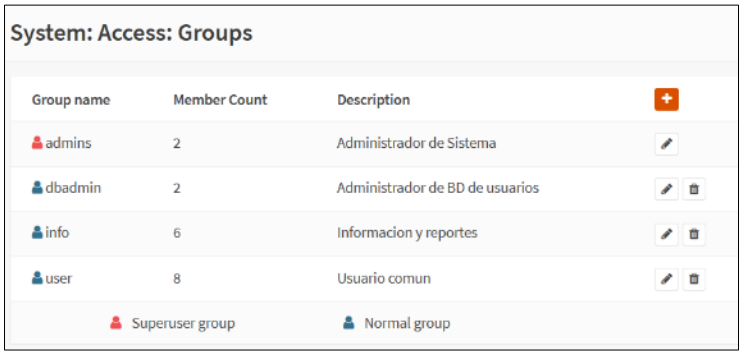
Grupos asociados a los tipos de usuario

Usuario	Grupo			
	admins	**dbadmin**	**info**	**user**
amguanotoa	☑	☑	☑	☑
miguantoa	☐	☐	☑	☑
jdhuera	☐	☑	☑	☑
jpguanotoa	☐	☐	☑	☑
efguanotoa	☐	☐	☐	☑
ejguanotoa	☐	☐	☐	☑
enguanotoa	☐	☐	☐	☑
svreyes	☐	☐	☐	☑

En la Figura 29 se muestran los grupos creados dentro del sistema, la cantidad de usuarios pertenecientes a cada grupo y la descripción general de las características del grupo, además mediante un icono se puede observar fácilmente si se trata de un grupo con permisos limitados (Grupo normal) o un grupo con permisos extendidos (Grupo de superusuarios).

Figura 29.

Grupos asociados a los tipos de usuario en la BDD



3.8.1.2.1 Niveles de gestión y acceso

En la etapa final, se procede a asignar los permisos correspondientes a cada grupo de usuarios. Los administradores del sistema (admins) se les otorga un control total sobre el sistema, lo que les permite ejercer funciones de supervisión y gestión exhaustiva. Por otro lado, los administradores de la Base de Datos (dbadmin) se les confiere la capacidad de agregar, modificar y eliminar usuarios en la base de datos, con el objetivo de administrar eficazmente los registros de usuario.

En una línea similar, el grupo de visualizadores de información (info) adquiere la capacidad de visualizar el estado de interfaces y servicios, así como acceder a gráficas que presentan información crucial sobre amenazas mitigadas, conexiones establecidas y usuarios enlazados a la red. Por último, los usuarios comunes (user) son asignados con permisos limitados, restringidos al acceso al servicio de autenticación del portal cautivo. Estos usuarios no poseen privilegios de visualización ni de gestión del sistema, focalizándose exclusivamente en la autenticación a través del portal cautivo implementado. Estos roles y permisos cuidadosamente asignados conforman un sistema de control de acceso robusto y personalizado que garantiza la seguridad y la funcionalidad adecuada del sistema en su totalidad. En la Tabla 18 se muestra a detalle todos los permisos asociados a cada grupo.

Tabla 18.

Permisos de los grupos de usuario

Permisos	Grupo			
	admins	dbadmin	info	user
Dashboard (all)	☑	☑	☑	☐
Dashboard (widgets only)	☑	☑	☑	☐
Diagnostics: Configuration History	☑	☐	☐	☐
Diagnostics: Factory defaults	☑	☐	☐	☐
Diagnostics: Firewall sessions	☑	☐	☐	☐
Diagnostics: Firewall statistics	☑	☐	☐	☐
Diagnostics: Reboot System	☑	☐	☐	☐
Diagnostics: Routing tables	☑	☐	☐	☐
Firewall: Rules	☑	☐	☐	☐
Interfaces: Assign network ports	☑	☐	☐	☐
Interfaces: Configuration network ports	☑	☐	☐	☐
Lobby: Login / Logout / Dashboard	☑	☑	☑	☑
Services: Captive Portal	☑	☐	☐	☐
Services: DHCP server	☑	☐	☐	☐
Services: Intrusion Detection	☑	☐	☐	☐
Status: DHCP leases	☑	☐	☑	☐
Status: Interfaces	☑	☐	☑	☐
Status: Services	☑	☐	☑	☐
Status: Traffic Graph	☑	☐	☑	☐
System: Advanced: Admin Access Page	☑	☐	☐	☐
System: Advanced: Firewall and NAT	☑	☐	☐	☐
System: Advanced: Network	☑	☐	☐	☐
System: Authentication Servers	☑	☐	☐	☐
System: Firmware	☑	☐	☐	☐
System: General Setup	☑	☐	☐	☐
System: Group manager	☑	☐	☐	☐
System: Static Routes	☑	☐	☐	☐
System: Status	☑	☑	☑	☐
System: User Manager	☑	☑	☐	☐
System: User Password Manager	☑	☑	☐	☐

3.8.1.3 Bloque de Procesamiento

Dentro del bloque de procesamiento se efectúan los procesos más importantes del sistema, debido a que en este están contenidos los módulos de identificación de usuarios, control de aplicaciones y generación de información. Durante la configuración de las características de este bloque se realizó: la configuración de las interfaces físicas y lógicas,

habilitación del protocolo de etiquetado para las VLANs mediante el protocolo 802.1Q, levantamiento de los servicios de DHCP, aplicación de las reglas de filtrado, establecimiento de las zonas, configuración del generador de reportes de incidencias detectadas y personalización de las políticas de seguridad para cada tipo de usuario.

3.8.1.3.1 Creación de las Interfaces Virtuales

Para la configuración de las VLANs, se implementó un proceso en el cual se asigna un nombre a cada subinterfaz, el cual también funge como una descripción del correspondiente VLAN ID asociado a dicha subinterfaz. Este nombre puede personalizarse según las necesidades, siempre siguiendo un formato que incluya un prefijo y caracteres numéricos separados por puntos. Además, en el campo VLAN tag se especifica un valor numérico dentro del rango de 1 a 4094, el cual será utilizado posteriormente para etiquetar el tráfico correspondiente a la subred en cuestión. La Figura 30 presenta de manera visual la configuración realizada específicamente para la subred denominada "Kids", brindando así una representación concisa y detallada del proceso implementado para definir la estructura de VLANs y etiquetas VLAN en la red.

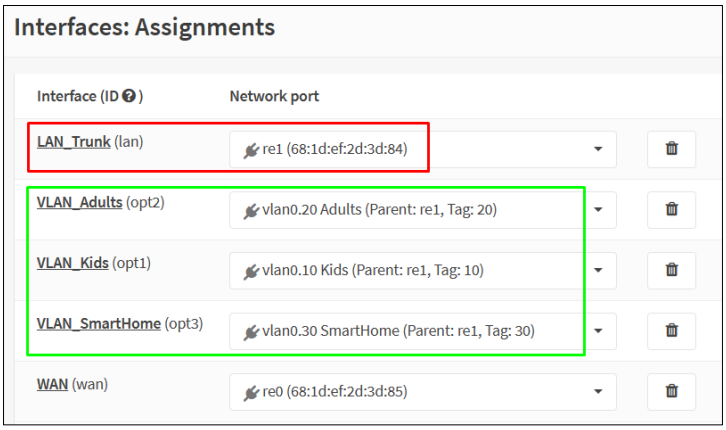
Figura 30.
Creación de interfaces VLAN en el NGFW

3.8.1.3.2 Asignación y vinculación de las Subinterfaces

Después de establecer las subinterfaces, se procede a vincularlas a la interfaz física principal, que se encuentra resaltada en color rojo en la Figura 31. Esta interfaz principal asumirá la responsabilidad de transportar todo el tráfico a través de la implementación del protocolo 802.1Q. Mediante esta conexión se habilita la transferencia eficiente de datos entre las subinterfaces y la interfaz principal. La aplicación del protocolo 802.1Q posibilita la segmentación y etiquetado de paquetes, lo que contribuye a una gestión ordenada y segura del tráfico en la red.

Figura 31.

Asignación de las Interfaces y subinterfaces.

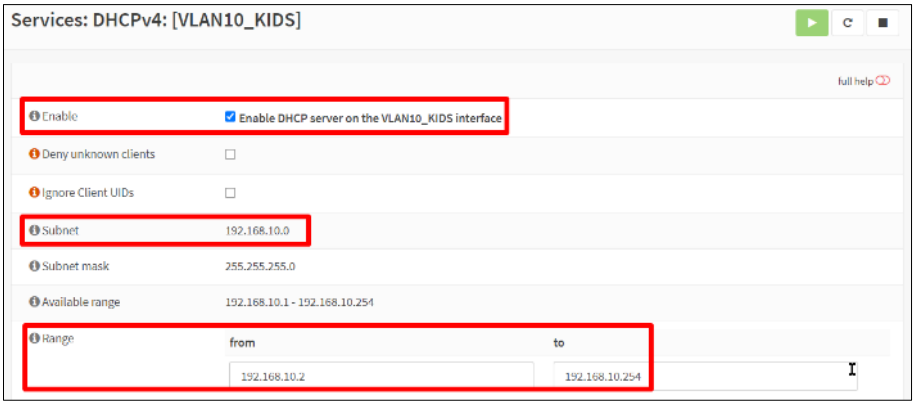


3.8.1.3.3 Configuración de servicio DHCP en las subinterfaces

Luego de establecer y asignar las VLANs a sus respectivas interfaces, se procede a activar el servicio de DHCP. Esta funcionalidad posibilita que los dispositivos clientes que se conecten a la red puedan adquirir de manera automática una dirección IP dentro del rango de la subred correspondiente. Adicionalmente, se proporciona un Gateway predeterminado y se asignan los servidores DNS específicos asociados a la VLAN en cuestión. Este proceso asegura una conectividad fluida y simplificada para los dispositivos en la red, permitiéndoles obtener las configuraciones de red necesarias sin intervención manual. En la Figura 32 se detalla la configuración de una de las interfaces.

Figura 32.

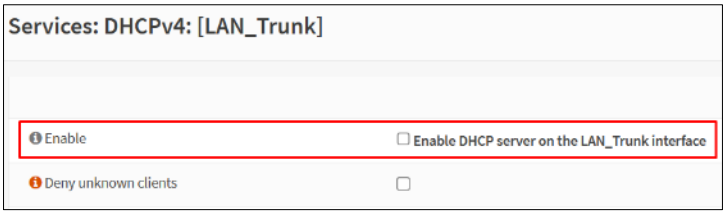
Configuración del servicio DHCP para las subredes



Con el propósito de prevenir la asignación de direcciones IP en la interfaz troncal que a su vez funciona como la interfaz de gestión, se lleva a cabo la inhabilitación del servicio DHCP. Como se observa en la Figura 33 en esta interfaz, se opta por no habilitar ninguna VLAN en particular. Esta medida garantiza que la interfaz troncal, que cumple una función crítica en la administración y gestión de la red, no participe en el proceso de asignación automática de direcciones IP. De esta manera, se asegura una segregación adecuada de funciones y se evita cualquier conflicto que pueda surgir al asignar direcciones IP en la interfaz de gestión.

Figura 33.

Desactivación del servicio DHCP en la interfaz física



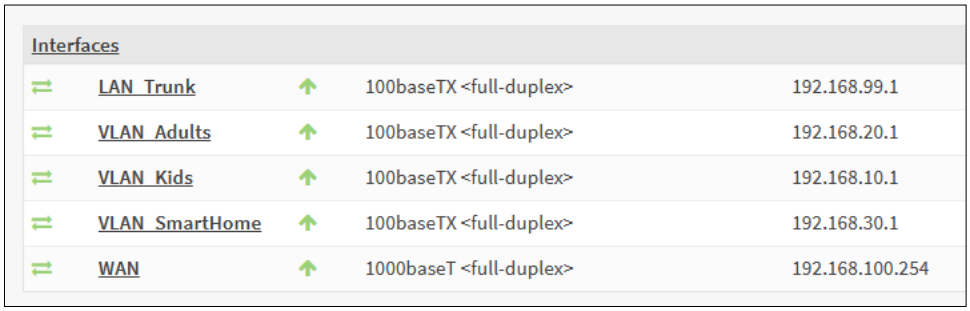
3.8.1.3.4 Verificación del estado de las interfaces físicas y virtuales.

Una vez completada la configuración, se procede a la verificación del estado de todas las interfaces. En la Figura 34, los iconos con flechas verdes indican las interfaces

que se encuentran habilitadas y operativas. Esta visualización gráfica facilita una evaluación rápida y eficiente del estado de cada interfaz en el sistema. Adicionalmente, en esta figura se exhiben las direcciones IP asignadas a cada una de las interfaces habilitadas, proporcionando una referencia visual para la identificación de las direcciones IP asociadas a cada punto de acceso y segmento de la red.

Figura 34.

Interfaces físicas y lógicas configuradas en el sistema

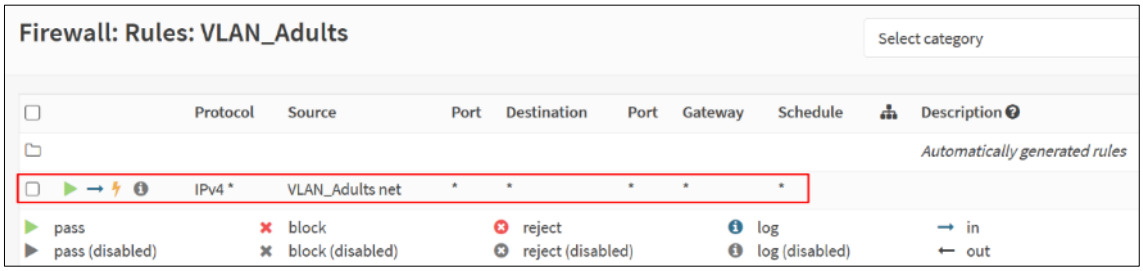


3.8.1.3.1 Reglas de filtrado para el flujo de tráfico TCP/UDP

Para garantizar la conectividad de las VLANs con Internet, se requiere la implementación de reglas de tráfico dentro del Firewall. Como se observa en la Figura 35 en cada VLAN se configura una regla que permite que el tráfico TCP/UDP, tanto entrante como saliente, tenga un acceso sin restricciones hacia la web. La selección de esta configuración obedece a la consideración de que el control de tráfico se llevará a cabo de manera directa a través del módulo de filtrado avanzado (Zenarmor) presente en el Firewall de Siguiente Generación.

Figura 35.

Configuración de reglas básicas de filtrado en el Firewall



3.8.1.3.2 Reputación en la Nube y Categorización Web

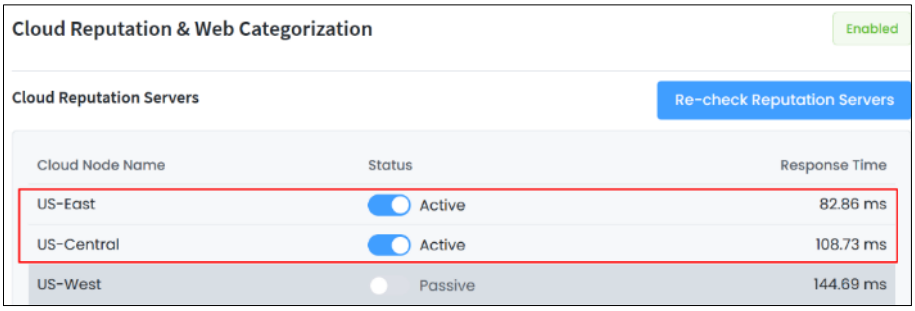
La función de reputación en la nube y categorización web se ejecuta en el módulo de Identificación de contenido (Content-ID), el cual realiza consultas en tiempo real a múltiples servidores disponibles que almacenan información acerca de la reputación y seguridad para más de 300 millones de sitios web que son actualizados constantemente, este servicio se lo conoce como SVN Cloud el cual permite responder de forma inmediata a amenazas de malware y brotes de virus en tiempo real.

Los datos de SVN Cloud se verifican en tiempo real cada vez que Zenarmor detecta un dispositivo tratando de establecer una conexión en la red protegida de una organización. Luego, el motor de paquetes procesa estos flujos, los consulta a los servidores en la nube más cercanos y toma decisiones sobre la legitimidad de los flujos según la información proporcionada en la nube y las configuraciones de políticas del sistema.

La comunicación entre los servidores Zenarmor y SVN Cloud utiliza un protocolo cifrado propietario que se transmite a través de los puertos UDP 5355 y 5356. Es importante destacar que se seleccionan al menos 2 servidores en función de su tiempo de respuesta para minimizar la latencia en la comunicación, como se ilustra en la Figura 36.

Figura 36.

Servidores elegidos como Base de Datos en tiempo real

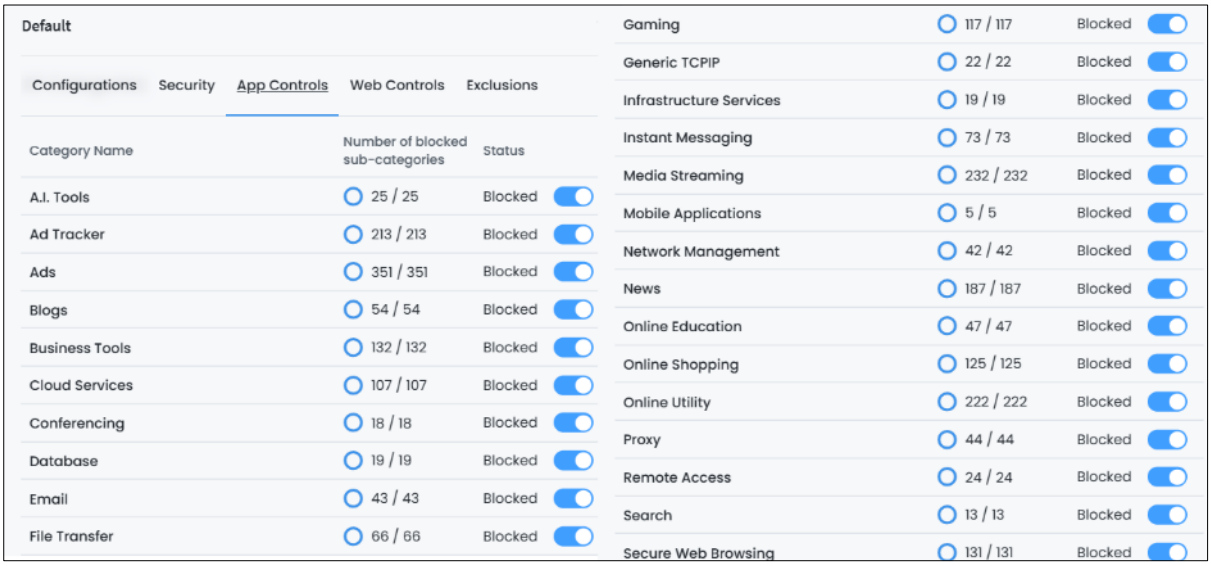


3.8.1.3.3 Políticas de tráfico de red

Se establece una política por defecto que rechace todo el tráfico tanto entrante como saliente, debido a que posteriormente se aplicaran políticas personalizadas basado en el tipo de usuario, esto permite que todo el tráfico que no esté establecido dentro de las políticas determinadas para cada subred sea rechazado y descartado. En la Figura 37 se muestra todas las aplicaciones seleccionadas para ser bloqueadas, en donde se han seleccionado la totalidad de las aplicaciones disponibles.

Figura 37.

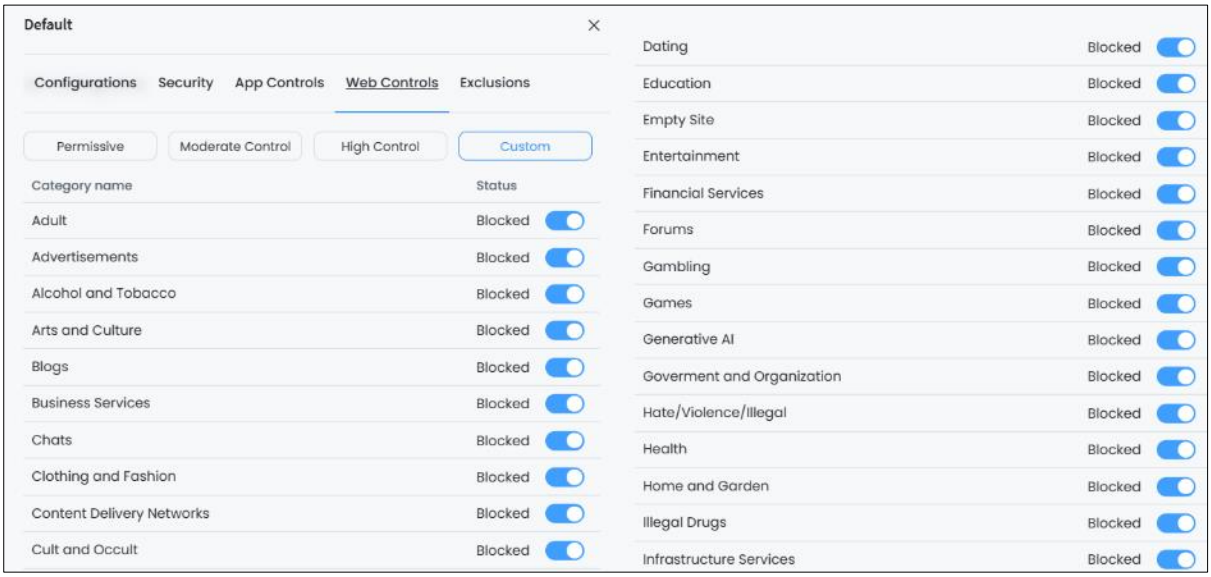
Aplicaciones Bloqueadas por la política Default



El NGFW también cuenta con un apartado para el bloqueo de sitios web el cual se distribuye por categorías, dentro de este apartado se tiene la posibilidad de establecer ajustes predeterminados para aplicar niveles de bloque, los cuales pueden ser más o menos permisivos, debido a que en la política por defecto se busca denegar todo tipo de acceso en este también se bloquea las categorías en su totalidad tal como se muestra en la Figura 38 mediante una lista personalizada.

Figura 38.

Páginas Web Bloqueadas por la política Default



Una vez configurada la política por defecto se añadieron 2 políticas adicionales como se muestra en la Figura 39, las cuales son Niños y Adultos/SmartHome. Estas contaran con permisos personalizados en base al tipo de usuario y a la subred perteneciente.

Figura 39.

Políticas del NGFW configuradas

3.8.1.3.4 Políticas de Seguridad Esenciales

Zenarmor cuenta con varias categorías de filtrado de contenido para aumentar la seguridad de los usuarios, se habilitó todas las funciones de seguridad tanto para la política por defecto como para los usuarios debido a que estas protegen tanto al usuario de forma independiente como a toda la red de posibles infecciones de malware que se propaga de

diversas formas a través de internet, en la Figura 40 se muestran las categorías habilitadas en el sistema.

Figura 40.

Políticas de Seguridad Esenciales

Cada categoría habilitada cumple una función en específico, habilitando filtros concretos para cada tipo de distribución de contenido no seseado, en la Tabla 19 de detallan brevemente cada las funciones que cumple cada categoría habilitada.

Tabla 19.

Descripción de las categorías del Módulo de Seguridad Esencial

Categoría	Descripción
Firstly Seen Sites	Mejora la seguridad al bloquear el acceso a sitios no categorizados previamente, evitando amenazas potenciales al interactuar con sitios desconocidos.
Hacking Sites	Bloquea el acceso a sitios web conocidos por distribuir contenido relacionado con la piratería y el delito cibernético. Esto refuerza la seguridad de la red y previene actividades no autorizadas y el acceso a recursos maliciosos.
Malware Activity	Bloquea sitios web que alojan malware, fortaleciendo las defensas contra esta amenaza. Al hacerlo, protege contra violaciones de datos y vulnerabilidades del sistema al prevenir el acceso a sitios contaminados por malware.
Parked Domains	Protege la red contra amenazas al limitar el acceso a sitios web llenos de anuncios que a menudo ocultan contenido dudoso o malicioso. Esto previene interacciones inadvertidas con anuncios dañinos o páginas infectadas, mejorando la seguridad en línea.
Phishing Servers	Bloquea sitios conocidos por alojar software malicioso utilizado en ataques de phishing. Esto mejora la seguridad al prevenir la interacción con dominios peligrosos que podrían comprometer datos o credenciales de usuarios.
Potentially Dangerous Sites	Bloquea sitios con actividades sospechosas similares a sitios maliciosos, aunque no se confirme su malicia. Esta función refuerza la seguridad de la red al prevenir el acceso a sitios que podrían ser riesgosos.

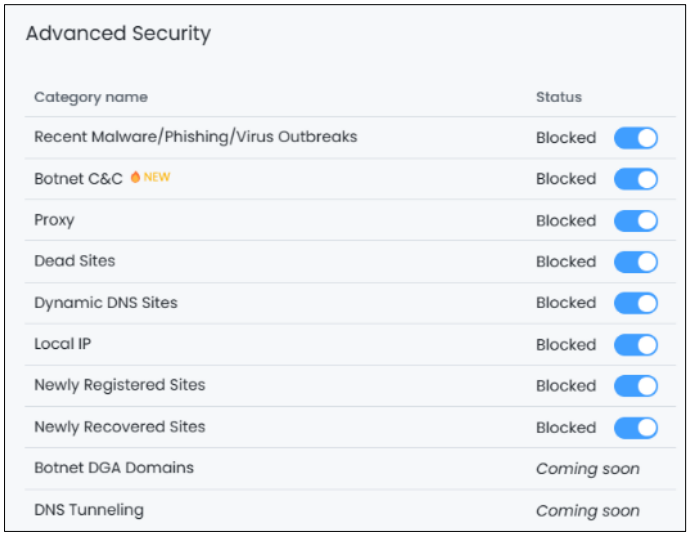
Spam Sites	Bloquea el acceso a sitios que distribuyen correo no deseado. Esto protege la red de contenido no solicitado y riesgos de seguridad asociados, mejorando la eficiencia y reduciendo amenazas de phishing o malware.

3.8.1.3.5 Políticas de Seguridad Avanzadas

Las políticas de seguridad avanzadas elevan la seguridad de la red bloqueando de forma proactiva dominios sospechosos, incluyendo dominios comprometidos, caducados y recién registrados, que a menudo son utilizados por ciberdelincuentes. El sistema cuenta con diversas funciones de seguridad avanzada tal como se muestra en la Figura 41 que contrarrestan las tácticas cambiantes de los ciberdelincuentes, ofreciendo una defensa completa que anticipa, identifica y neutraliza amenazas antes de causar daños. Con estas funcionalidades, los usuarios pueden navegar con confianza sabiendo que su red está protegida contra diversas amenazas.

Figura 41.

Políticas de Seguridad Avanzadas



La Tabla 20 describe las funciones de cada una de las características de seguridad avanzada presentes en el sistema.

Tabla 20.

Descripción de las categorías del Módulo de Seguridad Avanzada

Categoría	Descripción
Botnet C&C	Bloquea Centros de Control y Comando de Botnets, una medida esencial para defenderse contra botnets que pueden lanzar ataques masivos, propagar malware y robar datos. Esta función protege la red y sus operaciones en línea.
Dead Sites	Bloquea el acceso a dominios cuyos registros han caducado, una medida necesaria ya que los ciberdelincuentes los aprovechan para actividades maliciosas. Esto protege la red y sus usuarios de posibles amenazas.
Dynamic DNS Sites	Bloquea el acceso a sitios web que utilizan servicios de DNS dinámico, previniendo posibles amenazas. Los hackers a menudo emplean este método para ocultar sus actividades al lanzar ataques. Los sitios de DNS dinámico, que cambian continuamente sus direcciones IP, son difíciles de vigilar y categorizar, sin embargo, Zenarmor lo hace posible, disminuyendo el riesgo para la red y los usuarios.
Recent Malware/Phishing/ Virus Outbreaks	Fortalece la defensa de la red contra ataques recientes. Detecta y previene software malicioso, intentos de phishing y acciones de infección recientes sin necesidad de actualizar bases de datos. Al activar esta opción se logra bloquear amenazas que han surgido en las últimas 0 a 2 semanas, mejorando la seguridad de la red.
Newly Registered Sites	Fortalece las defensas de la red contra amenazas recientes al prevenir el acceso a dominios recién registrados, que a menudo son utilizados por hackers en durante ataques maliciosos.
Proxy	Bloquea preventivamente el acceso a sitios proxy utilizados por atacantes para mantener el anonimato. Esto impide que los usuarios de la red utilicen estos intermediarios para evitar medidas de seguridad. Zenarmor fortalece así las defensas contra amenazas anónimas.

3.8.1.3.6 Políticas de Control de Aplicaciones

El bloqueo por aplicaciones se basa en una base de datos de firmas de aplicaciones actualizada que permite al NGFW identificar miles de aplicaciones, desde aplicaciones comerciales legítimas hasta aplicaciones potencialmente maliciosas. Cuando el tráfico de red pasa por el NGFW, este examina los paquetes de datos para determinar qué aplicación se está utilizando y luego aplica políticas de seguridad específicas para esa aplicación.

En el sistema propuesto, se implementan políticas de acceso personalizadas en función de la identidad del usuario y la red a la que están conectados. Estas políticas se aplican en relación con categorías de aplicaciones a las que los usuarios pueden o no pueden acceder. En la Tabla 21, se enumeran todas las categorías disponibles para el control de aplicaciones, junto con las restricciones aplicadas a cada tipo de usuario.

Específicamente, se han establecido restricciones más estrictas para el grupo de usuarios designado como "niños". Estas restricciones incluyen el bloqueo de aplicaciones que se consideran inapropiadas o no adecuadas para este grupo demográfico. La selección de estas categorías se basa en los resultados de una encuesta realizada a los beneficiarios, que se describe en detalle en el Anexo 2, en la pregunta 6.

Tabla 21.

Políticas de Control de Aplicaciones

	Usuario	
Categoría	**Niños**	**Adultos**
Herramientas de I.A.	☐	☐
Rastreador de anuncios	☑	☑
Anuncios	☑	☑
Blogs	☐	☐
Herramientas empresariales	☑	☐
Servicios en la nube	☐	☐
Conferencias	☐	☐
Base de datos	☐	☐
Correo electrónico	☑	☐
Transferencia de archivos	☑	☐
Juego	☐	☐
TCP/IP genérico	☐	☐
Servicios de infraestructura	☑	☐
Mensajería instantánea	☐	☐
Transmisión de medios	☐	☐
Gestión de redes	☑	☐
Educación en línea	☐	☐
Compras en línea	☑	☐
Utilidad en línea	☑	☐
Proxy	☑	☐
Acceso remoto	☑	☐
Buscar	☐	☐
Navegación web segura	☐	☐
Red Social	☑	☐
Actualizaciones de software	☐	☐
Almacenamiento y copia de seguridad	☐	☐
Sistema y sistema operativo	☐	☐
VOIP	☑	☐
Navegación Web	☐	☐

Esta estrategia garantiza que los usuarios más jóvenes tengan un entorno en línea seguro y apropiado para su edad, al tiempo que permite a otros grupos de usuarios acceder a una gama más amplia de aplicaciones de acuerdo con sus necesidades y requisitos específicos.

3.8.1.3.7 Políticas de control Web

El bloqueo web consiste en la capacidad del firewall para controlar y restringir el acceso a sitios web específicos o categorías de sitios web en función de políticas de seguridad predefinidas. Esto se hace con el objetivo de proteger la red y a los usuarios contra amenazas, garantizar el cumplimiento de políticas de uso de Internet y prevenir el acceso a contenido no deseado o peligroso.

En base a los resultados de la encuesta descrita en el Anexo 2 – Pregunta 6 se ha diseñado la

Tabla 22 en donde se detalla las categorías de las páginas web bloqueadas para los usuarios pertenecientes al grupo “niños”, estos filtros impiden que estos accedan a sitios determinados como prohibidos los cuales son: Sitios para adultos, anuncios web, sitios relacionados a sustancias ilegales, salas de chat, sitios de descargas, armas, entre otros. La tabla también muestra las categorías bloqueadas para los usuarios pertenecientes al grupo “Adultos” que son más permisivas, sin embargo, se ha optado por el bloqueo de categorías como: anuncios, ilegal, drogas y warez debido a que en estos sitios principalmente se muestra publicidad maliciosa la cual muchas veces contiene malware y sirve como una puerta abierta para la recolección de datos de los usuarios

Tabla 22.

Políticas de control Web

	Usuario	
Categoría	**Niños**	**Adultos**
Adulto	☑	☐
Anuncios	☑	☑
Alcohol y tabaco	☑	☐
Arte y Cultura	☐	☐
Blogs	☑	☐
Chats	☑	☐
Ropa y moda	☐	☐
Redes de entrega de contenido	☐	☐
Culto y ocultismo	☐	☐
Educación	☐	☐
Sitio vacío	☐	☐
Diversión	☐	☐
Servicios financieros	☐	☐
Foros	☑	☐
Juegos	☑	☐
Gobierno y Organización	☐	☐
Odio/Violencia/Ilegal	☑	☑
Salud	☐	☐
Drogas ilegales	☑	☑
Servicios de infraestructura	☐	☐
Niños	☐	☐
Productos de cannabis bajos en THC	☐	☐
Música	☐	☐
Almacenamiento en línea	☑	☐
Video en línea	☑	☐
Pornografía	☑	☐
Bien inmueble	☐	☐
Religión	☐	☐
Buscadores	☐	☐
Autolesiones	☐	☐
Compras	☐	☐
Redes Sociales	☑	☐
Sociedad	☐	☐
Descargas de software	☑	☐
Tecnología e Informática	☐	☐
Vacaciones y Viajes	☐	☐
Vehículos	☐	☐
Warez	☑	☑
Armas y Fuerzas Armadas	☑	☐

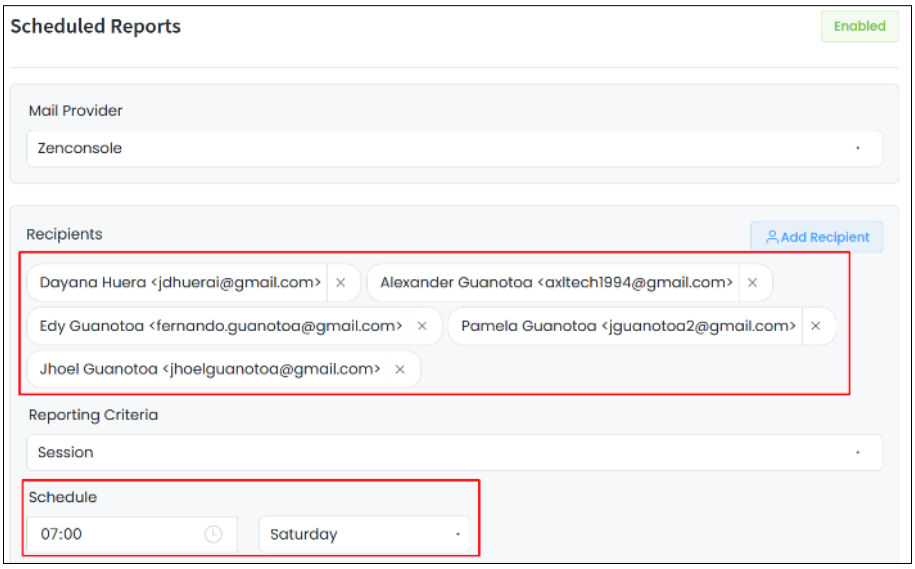
La principal diferencia entre el bloqueo web y el bloqueo por aplicaciones en un NGFW es la naturaleza del tráfico que controlan. El bloqueo web se centra en sitios web y

URLs, mientras que el bloqueo por aplicaciones se enfoca en aplicaciones específicas, ya sean basadas en web o de escritorio. Ambas características son esenciales para una estrategia integral de seguridad de red, ya que permiten personalizar las políticas de seguridad según necesidades específicas.

3.8.1.3.8 Informes Programados

En base al requerimiento planteado por los usuarios en el Anexo 2 – Pregunta 16 y 17 el sistema debe contar con la capacidad de generar reportes de usuario personalizados, en donde se muestre al menos: las aplicaciones utilizadas, los sitios web bloqueados y accedidos, las amenazas mitigadas y los usuarios asociados a los eventos registrados. Como se observa en la Figura 42 se ha programado el envío automático de reportes semanales, mismos que serán entregados los sábados a todos los usuarios pertenecientes al grupo “info”.

Figura 42.
Programación del envío de reportes

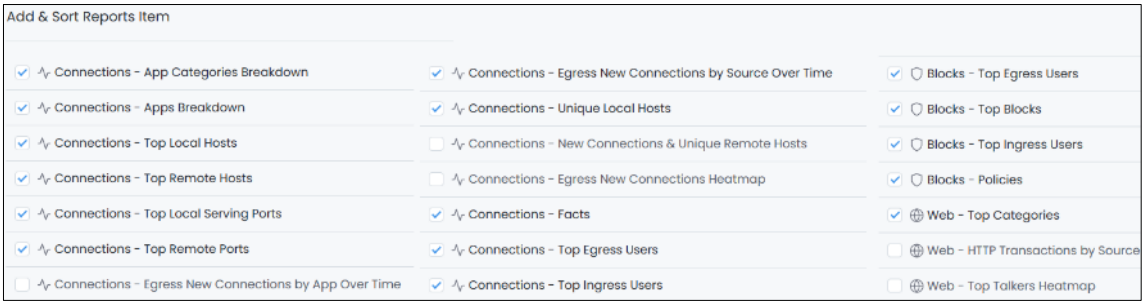


El servicio de programación de reportes automatizados permite la selección de las categorías de acuerdo con lo que se requiera, como se observa en la Figura 43 se han seleccionado los elementos relacionados a los requerimientos solicitados por los usuarios

en el Anexo 2 – Pregunta 16. En donde se incluirán en los informes las categorías de aplicaciones más utilizadas, la cantidad de sesiones establecidas por aplicación, el porcentaje de uso de la red por usuario autenticado, las estadísticas de aplicaciones bloqueadas y las amenazas detectadas y mitigadas.

Figura 43.

Elementos a incluir en los informes



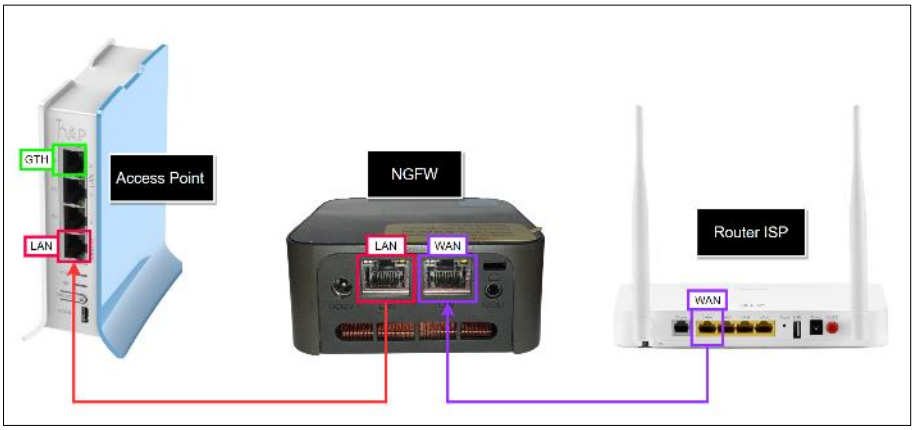
3.8.1 Implementación de Hardware

Para la implementación del hardware de sistema se ha designado un espacio físico dentro del hogar, el cual debe estar en un lugar centrado para poder distribuir las redes inalámbricas a todos los sitios de forma eficiente, este debe ser además un sitio elevado, con ventilación y sin obstrucciones.

Los dispositivos necesarios para el funcionamiento del sistema se han colocado uno junto a otro en una repisa con suficiente espacio para su libre ubicación. En la Figura 44 se muestran las conexiones que deben realizarse para la intercomunicación y funcionamiento de los dispositivos.

Figura 44.

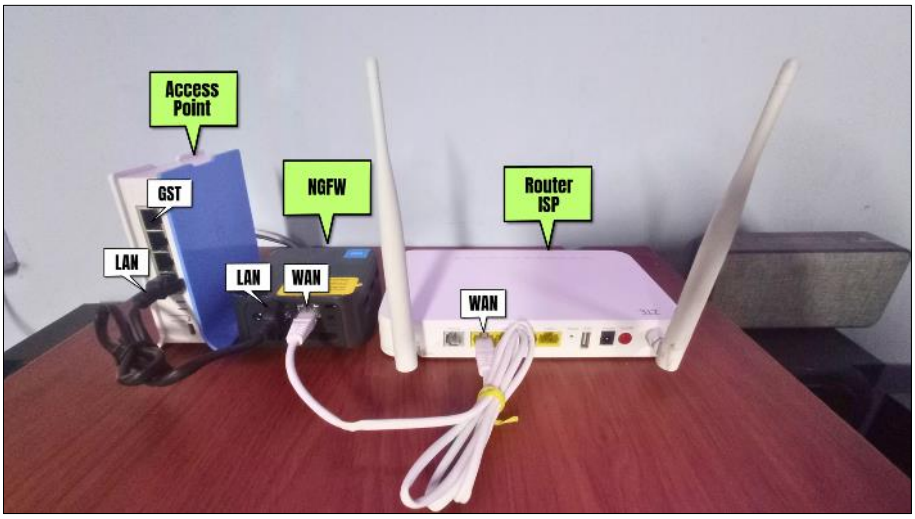
Diagrama de conexión de los puertos de red



La Figura 45 muestra la vista posterior de los dispositivos junto a las conexiones físicas llevadas a cabo durante la implementación del sistema, se han obviado las conexiones de los puertos eléctricos para facilitar la visualización de los cables asociados a cada puerto de red.

Figura 45.

Vista posterior que muestra la conexión de los puertos del sistema



En la Figura 46 se muestra una vista frontal superior del sistema ubicado en su sitio definitivo, los dispositivos han sido colocados de esta forma debido a que cada uno realiza procesos independientes en su procesador los cuales generan calor, estos al estar

separados el uno del otro impide que calor generado por los dispositivos se acumule y genere una baja de rendimiento a nivel de procesamiento.

Figura 46.

Vista frontal del sistema implementado

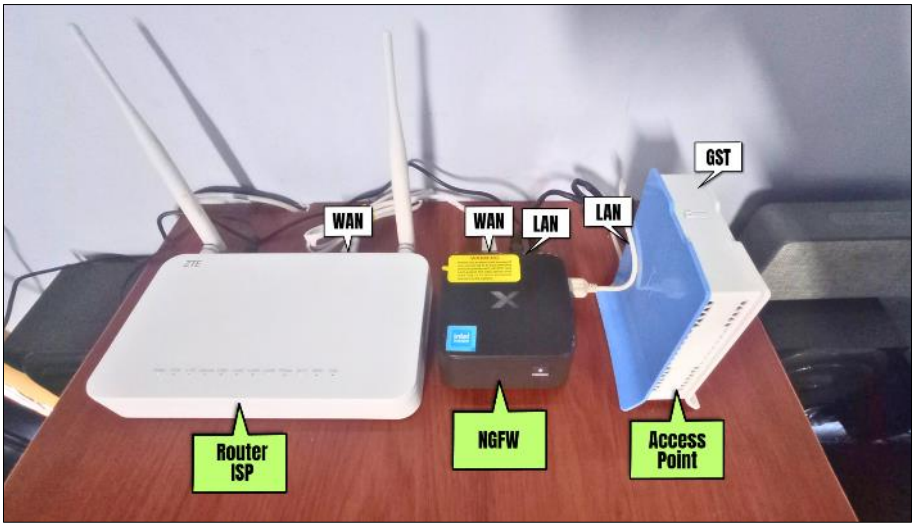


Tabla 23.

Especificación de las funciones asignadas a los puertos de cada dispositivo

Dispositivo	Puerto	Función
Router ISP	*WAN*	Puerto habilitado como Bridge que sirve para la conexión y salida a Internet del sistema de seguridad.
NGFW	*WAN*	Puerto que permite la salida a Internet a los Hosts conectados al sistema de seguridad (NGFW).
	LAN	Puerto designado para la intercomunicación entre el Access Point y el NGFW (Trunk Port), este puerto tiene habilitado el protocolo 802.1Q para el libre flujo del tráfico perteneciente a las VLANs
Access Point	*LAN*	Puerto designado para la intercomunicación entre el Access Point y el NGFW (Trunk Port), este puerto tiene habilitado el protocolo 802.1Q para el libre flujo del tráfico perteneciente a las VLANs
	GST	Puerto que se utilizará para gestionar tanto el Access Point de MikroTik mediante Winbox como para acceder a la WebUI de las configuraciones del NGFW mediante el explorador de internet.

Capítulo IV: Pruebas de Funcionamiento

En este capítulo, se ejecutan las pruebas de funcionamiento del sistema de seguridad en cada uno de los bloques propuestos en la arquitectura. El propósito fundamental de llevar a cabo este proceso de verificación es obtener evidencia objetiva y técnica que confirme que el sistema satisface los requisitos solicitados por los stakeholders, así como las funcionalidades implementadas en el capítulo anterior. Estas pruebas son esenciales para garantizar la operatividad efectiva y la integridad de todo el sistema, brindando la confianza necesaria en su desempeño ante posibles amenazas y escenarios del mundo real.

4.1 Pruebas de cumplimiento

Las pruebas consisten en la evaluación de los parámetros del proyecto mediante una lista de verificación en la que se tienen en cuenta todos los atributos definidos durante la fase de construcción de requerimientos. Se llevaron a cabo tres evaluaciones de acuerdo con su tipo, y las pruebas de cumplimiento se definen a partir de los requerimientos de las partes interesadas (stakeholders), los requerimientos del sistema y los requerimientos de la arquitectura.

4.1.1 Cumplimiento de requerimientos de Stakeholders

Se valida el cumplimiento de los requerimientos de Stakeholders planteados para el sistema, en la Tabla 24 se muestran los identificadores asociados a cada parámetro planteado en la etapa de diseño en donde se indica si el ítem fue implementado con éxito.

Tabla 24.

Cumplimiento de Requerimientos de Stakeholders

Requerimientos de Stakeholders		StSR1	StSR2	StSR3	StSR4	StSR5	StSR6	StSR7	StSR8	StSR9	StSR10	StSR11	StSR12	StSR13	StSR14
Cumple	Si	☑	☑	☑	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
	No	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Para los requerimientos de stakeholders después de la evaluación realizada se ha cumplido con la mayoría de los parámetros solicitados por los beneficiarios, teniendo como punto no cumplido el requerimiento StSR4 de prioridad MEDIA el cual corresponde a la implementación de interfaces cableadas para los usuarios cableados, este requerimiento no ha podido ser cumplido debido a la limitación de cantidad de puertos en el Access Point ya que son necesarios 3 puertos disponibles para esta aplicación (uno para cada VLAN) y luego del diseño y la definición de los puertos a utilizarse únicamente se contó con 2 puertos libres.

4.1.2 Cumplimiento de requerimientos de Sistema

Se valida el cumplimiento de los requerimientos de Sistema planificados para el proyecto, en la Tabla 25 se muestran los identificadores asociados a cada parámetro establecido en la etapa de desarrollo en donde se indica si el ítem fue implementado con éxito o no.

Tabla 25.

Cumplimiento de Requerimientos de Sistema

Requerimientos de Sistema		SySR1	SySR2	SySR3	SySR4	SySR5	SySR6	SySR7	SySR8	SySR9	SySR10	SySR11	SySR12	SySR13	SySR14	SySR15	SySR16	SySR17	SySR18	SySR19
Cumple	Si	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
	No	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

En la evaluación de cumplimiento de los requerimientos de sistema planificados se logrado cumplir con el 100% de los parámetros evaluados, los cuales constan de: Requerimientos, Requerimientos de interfaz, Requerimientos de performance, Requerimientos de modo/estado y Requerimientos físicos.

4.1.3 Cumplimiento de requerimientos de Arquitectura

Se valida el cumplimiento de los requerimientos de Arquitectura planificados para el sistema, en la Tabla 26 se muestran los identificadores asociados a cada parámetro establecido en la etapa de desarrollo en donde se indica si el requerimiento fue implementado con éxito o no.

Tabla 26.

Cumplimiento de Requerimientos de Arquitectura

Requerimientos de Arquitectura		SrSH1	SrSH2	SrSH3	SrSH4	SrSH5	SrSH6	SrSH7	SrSH8	SrSH9	SrSH10	SrSH11	SrSH12	SrSH13	SrSH14	SrSH15	SrSH16	SrSH17	SrSH18	SrSH19	SrSH20	SrSH21	SrSH22	SrSH23
Cumple	Si	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
	No	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Para los requerimientos de arquitectura establecidos se ha cumplido con el 100% de los parámetros evaluados, los cuales constan de: Requerimientos Lógicos, Requerimientos de Diseño, Requerimientos de Hardware, Requerimientos de Software y Requerimientos Eléctricos.

4.2 Pruebas de Funcionalidad

El objetivo de las pruebas de funcionamiento realizadas es verificar que el sistema, cumple con precisión los requisitos y las especificaciones establecidas, garantizando el funcionamiento correcto y eficiente de todas las características requeridas por los beneficiarios.

4.2.1 Bloque de Acceso

En la siguiente sección se muestran las pruebas efectuadas en el bloque de acceso tanto con el sistema en funcionamiento como sin activarlo, a continuación, se detallan y muestran los procesos llevados a cabo para la validación y comparación de los resultados.

4.2.1.1 Test de Red Inalámbrica

Para el bloque de acceso se verifica la distribución de las redes inalámbricas mediante un test que permita visualizar el modo de operación, la jerarquía de las redes y el SSID de difusión. En la Tabla 27 se detalla el proceso llevado a cabo durante la primera prueba de validación de resultados.

Tabla 27.
Test de Red Inalámbrica

Test de Red Inalámbrica	
Bloque de prueba	Bloque de Acceso
Descripción	Prueba para el funcionamiento de la red inalámbrica
Prerrequisitos: ▪ Access Point MikroTik hAP ▪ Smartphone	

- Wifi Analyzer
- Winbox
- Interfaz Inalámbrica

Pasos:

- Verificar la difusión de red MASTER
- Verificar las subredes asociadas
- Verificar el modo de operación
- Verificar el protocolo de transmisión
- Verificar el protocolo de encriptación

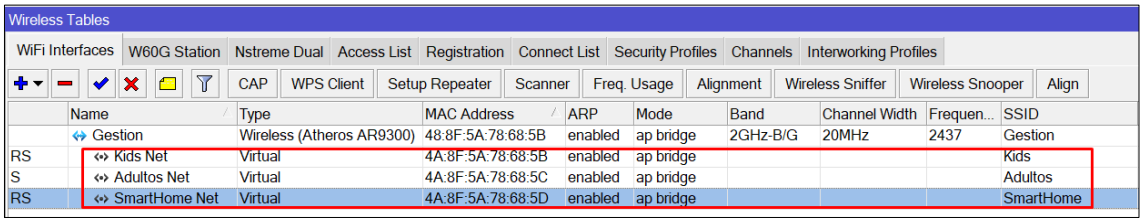
Resultados esperados: Difusión de las redes y subredes inalámbricas por parte del AP y visualización de las redes inalámbricas desde un cliente final.

Resultados Obtenidos: En el proceso de configuración de las redes inalámbricas, se ha trabajado meticulosamente para asegurar su correcto desempeño y accesibilidad. Estas redes han sido configuradas de manera que puedan ser detectadas y utilizadas desde cualquier dispositivo con una interfaz Wi-Fi compatible con el protocolo 802.11g, el cual opera en la banda de 2.4 GHz. Esta configuración proporciona una amplia compatibilidad, permitiendo que diversos dispositivos, como computadoras portátiles, teléfonos inteligentes y dispositivos IoT, puedan acceder y utilizar la red de manera efectiva.

La Figura 47 representa la tabla de interfaces inalámbricas que se encuentra desplegada en el software Winbox. En este contexto, se destacan las redes inalámbricas denominadas "Kids," "Adultos," y "SmartHome," las cuales se han resaltado mediante el color rojo para su fácil identificación. Estas redes inalámbricas están enlazadas de manera directa a la interfaz master designada como "Gestion," lo que permite un manejo centralizado de todas estas redes. Es importante señalar que todas estas redes inalámbricas esclavas operan en el mismo canal, banda y frecuencia determinada por la interfaz Master. Esta configuración se implementa con el propósito de optimizar el rendimiento de las redes inalámbricas y minimizar posibles interferencias y conflictos de canal en el entorno de implementación.

Figura 47.

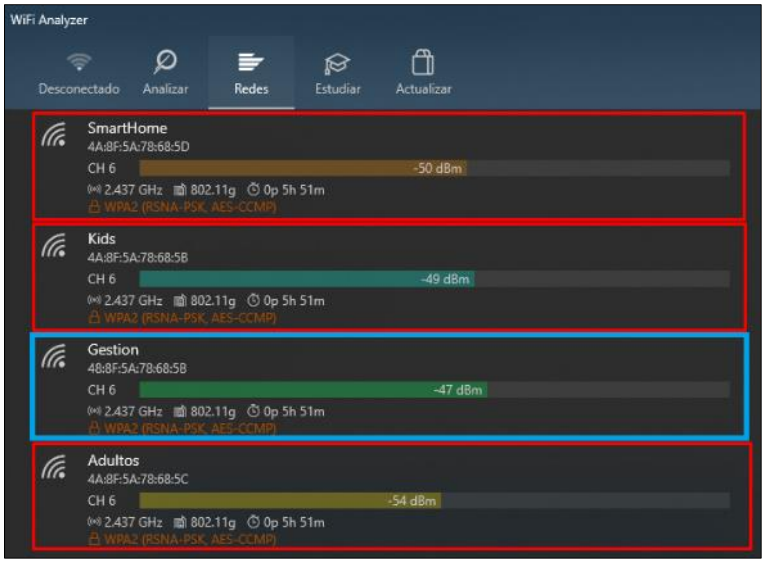
Visualización de las WLAN configuradas en el AP



Mediante el software Wifi Analyzer y un adaptador inalámbrico USB se escanearon las redes difundidas en el medio, teniendo como resultado las redes mostradas en la Figura 48, en donde se puede observar más detalles de las redes inalámbricas, tales como el Protocolo de encriptación de las contraseñas implementadas en las WLAN, el canal de operación de la red, la dirección MAC asociada a la SSID y la potencia de transmisión. En color azul se encuentra resaltada la red Master y en color rojo las subredes ancladas a la misma.

Figura 48.

Análisis de las redes difundidas inalámbricamente por el NGFW



4.2.1.2 Test de Etiquetado de Tráfico

Durante esta etapa, se implementaron medidas específicas para garantizar que el etiquetado 802.1Q se llevara a cabo de manera precisa y efectiva en la red. Esto implicó

configuraciones detalladas en los dispositivos de red para asegurar que los paquetes se etiquetaran adecuadamente al ingresar y salir de las VLAN. La inspección de los encabezados Ethernet desempeñó un papel crucial en la verificación de que el etiquetado se realizara de acuerdo con las especificaciones requeridas, contribuyendo así a la correcta segmentación y gestión del tráfico en la red. En la Tabla 28 se detalla el proceso llevado a cabo durante la segunda prueba de validación de resultados.

Tabla 28.

Test de Etiquetado de Tráfico

Test de Etiquetado de Tráfico	
Bloque de prueba	Bloque de Acceso
Descripción	Prueba para el funcionamiento del protocolo 802.1q (Etiquetado VLAN)
Prerrequisitos: ▪ Access Point MikroTik hAP ▪ Puerto con función MIRROR activada ▪ NGFW con subinterfaces VLAN habilitadas ▪ Hosts Clientes enlazados a las subredes ▪ Wireshark ▪ Winbox	
Pasos: ▪ Habilitar función MIRROR en puerto de gestión del dispositivo MikroTik ▪ Generar tráfico con los hosts conectados a las distintas VLANs ▪ Capturar paquetes de la interfaz troncal mediante el puerto designado como MIRROR ▪ Filtrar paquetes capturados que contengan las etiquetas del protocolo 802.1q	
Resultados esperados: Flujo de paquetes encapsulados con el protocolo 802.1q en donde se muestren las diferentes etiquetas correspondientes al identificador de VLAN asociado a cada subred.	

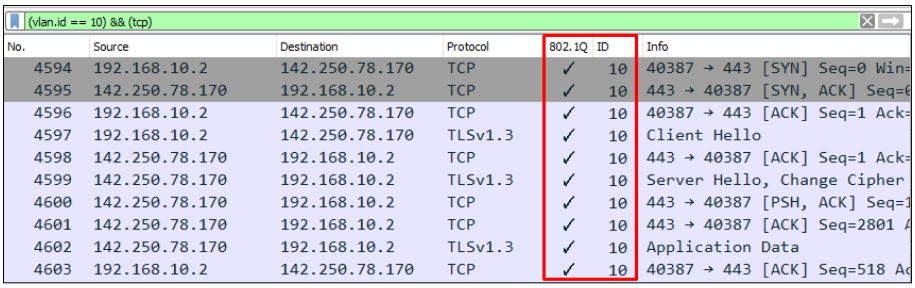
Resultados obtenidos: Mediante la función MIRROR habilitada en el AP MikroTik fue posible clonar todo el tráfico de red presente en el puerto eth0 el cual corresponde a la interfaz utilizada como puerto troncal, que es el que se encarga de transportar todo el tráfico tanto etiquetado como sin etiquetar entre el AP y el NGFW, de esta forma mediante la captura de paquetes con el Software Wireshark fue posible identificar que los paquetes

etiquetados mediante el protocolo 802.1q pueden ser transportados sin novedad entre el Access Point y el Firewall.

En la Figura 49 se muestra la captura de los paquetes TCP pertenecientes a la VLAN Kids con etiqueta (Vlan Tag) = 10, estos corresponden a una solicitud de conexión a una página web realizada por el host con IP = 192.168.10.2.

Figura 49.

Paquetes capturados pertenecientes a la VLAN Kids

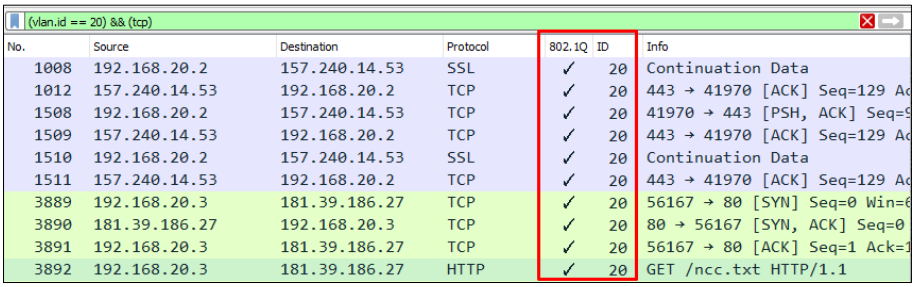


No.	Source	Destination	Protocol	802.1Q	ID	Info
4594	192.168.10.2	142.250.78.170	TCP	✓	10	40387 → 443 [SYN] Seq=0 Win=
4595	142.250.78.170	192.168.10.2	TCP	✓	10	443 → 40387 [SYN, ACK] Seq=0
4596	192.168.10.2	142.250.78.170	TCP	✓	10	40387 → 443 [ACK] Seq=1 Ack=
4597	192.168.10.2	142.250.78.170	TLSv1.3	✓	10	Client Hello
4598	142.250.78.170	192.168.10.2	TCP	✓	10	443 → 40387 [ACK] Seq=1 Ack=
4599	142.250.78.170	192.168.10.2	TLSv1.3	✓	10	Server Hello, Change Cipher
4600	142.250.78.170	192.168.10.2	TCP	✓	10	443 → 40387 [PSH, ACK] Seq=1
4601	142.250.78.170	192.168.10.2	TCP	✓	10	443 → 40387 [ACK] Seq=2801 A
4602	142.250.78.170	192.168.10.2	TLSv1.3	✓	10	Application Data
4603	192.168.10.2	142.250.78.170	TCP	✓	10	40387 → 443 [ACK] Seq=518 Ac

En la Figura 50 se muestra la captura del flujo de paquetes TCP pertenecientes a la VLAN Adultos con etiqueta (Vlan Tag) = 20, estos corresponden a una solicitud de conexión a una página web realizada por el host con IP = 192.168.10.2.

Figura 50.

Paquetes capturados pertenecientes a la VLAN Adultos

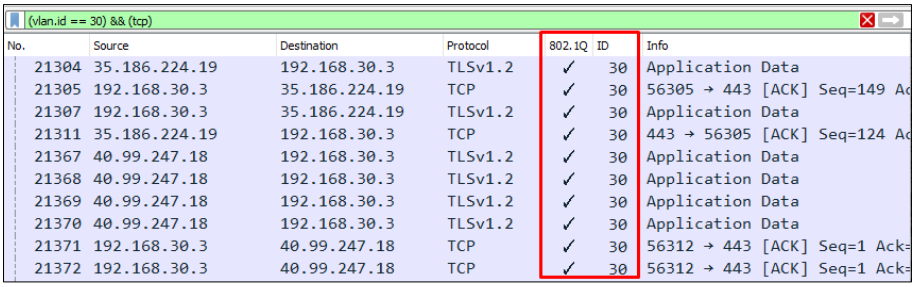


No.	Source	Destination	Protocol	802.1Q	ID	Info
1008	192.168.20.2	157.240.14.53	SSL	✓	20	Continuation Data
1012	157.240.14.53	192.168.20.2	TCP	✓	20	443 → 41970 [ACK] Seq=129 Ac
1508	192.168.20.2	157.240.14.53	TCP	✓	20	41970 → 443 [PSH, ACK] Seq=9
1509	157.240.14.53	192.168.20.2	TCP	✓	20	443 → 41970 [ACK] Seq=129 Ac
1510	192.168.20.2	157.240.14.53	SSL	✓	20	Continuation Data
1511	157.240.14.53	192.168.20.2	TCP	✓	20	443 → 41970 [ACK] Seq=129 Ac
3889	192.168.20.3	181.39.186.27	TCP	✓	20	56167 → 80 [SYN] Seq=0 Win=6
3890	181.39.186.27	192.168.20.3	TCP	✓	20	80 → 56167 [SYN, ACK] Seq=0
3891	192.168.20.3	181.39.186.27	TCP	✓	20	56167 → 80 [ACK] Seq=1 Ack=1
3892	192.168.20.3	181.39.186.27	HTTP	✓	20	GET /ncc.txt HTTP/1.1

En la Figura 51 se muestra la captura del flujo de paquetes TCP pertenecientes a la VLAN SmartHome con etiqueta (Vlan Tag) = 30, estos corresponden a una negociación de conexión entre una página web y el host con IP = 192.168.30.3.

Figura 51.

Paquetes capturados pertenecientes a la VLAN SmartHome



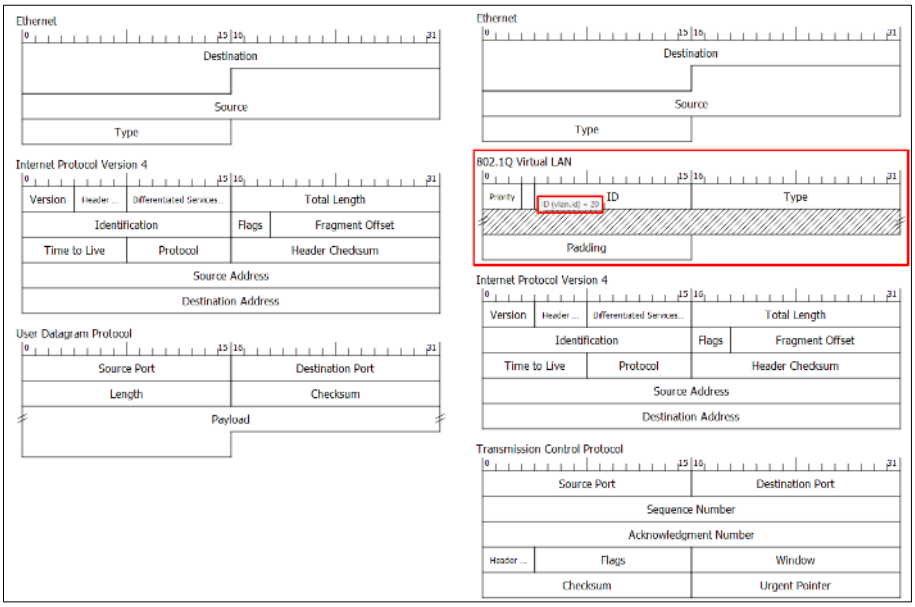
(vlan.id == 30) && (tcp)

No.	Source	Destination	Protocol	802.1Q	ID	Info
21304	35.186.224.19	192.168.30.3	TLSv1.2	✓	30	Application Data
21305	192.168.30.3	35.186.224.19	TCP	✓	30	56305 → 443 [ACK] Seq=149 Ac
21307	192.168.30.3	35.186.224.19	TLSv1.2	✓	30	Application Data
21311	35.186.224.19	192.168.30.3	TCP	✓	30	443 → 56305 [ACK] Seq=124 Ac
21367	40.99.247.18	192.168.30.3	TLSv1.2	✓	30	Application Data
21368	40.99.247.18	192.168.30.3	TLSv1.2	✓	30	Application Data
21369	40.99.247.18	192.168.30.3	TLSv1.2	✓	30	Application Data
21370	40.99.247.18	192.168.30.3	TLSv1.2	✓	30	Application Data
21371	192.168.30.3	40.99.247.18	TCP	✓	30	56312 → 443 [ACK] Seq=1 Ack=
21372	192.168.30.3	40.99.247.18	TCP	✓	30	56312 → 443 [ACK] Seq=1 Ack=

La Figura 52 presenta una comparativa entre dos tramas capturadas. En la trama ubicada a la izquierda, se aprecia una trama Ethernet que no está asignada a ninguna VLAN específica. Por otro lado, a la derecha se muestra otra trama capturada en la misma interfaz, pero con la diferencia de que a esta segunda trama se le ha agregado un campo en la cabecera denominado "802.1Q Virtual LAN."

Figura 52.

Inserción de la etiqueta 802.1Q en una trama Ethernet



Estos resultados son indicativos de que, dentro de la misma interfaz, la implementación del protocolo 802.1Q posibilita la compartición de un mismo medio físico sin

que se produzcan interferencias entre subredes. Este protocolo permite la segmentación y etiquetado de tramas Ethernet, lo que a su vez facilita la segregación y gestión eficiente del tráfico de datos en redes que comparten una infraestructura física común. De esta manera, se logra mantener la integridad de las subredes, evitando colisiones y conflictos en el tráfico de datos.

4.2.2 Bloque de Gestión

En la siguiente sección se muestran las pruebas efectuadas en el bloque de gestión en donde se detallan y muestran los procesos llevados a cabo para la validación de los resultados.

4.2.2.1 Test de Autenticación mediante Portal Cautivo

Para el bloque de gestión se verificó que el portal cautivo autenticara a los usuarios de manera efectiva antes de permitirles el acceso a la red. Esta verificación abarcó la comprobación de credenciales, incluyendo nombres de usuario y contraseñas, para garantizar un proceso de autenticación seguro y eficaz. En la Tabla 29 se detallan las consideraciones para la realización de la prueba.

Tabla 29.
Test de Autenticación de Portal Cautivo

Test de Autenticación de Portal Cautivo	
Bloque de prueba	Bloque de Gestión
Descripción	Prueba para el funcionamiento de autenticación al portal cautivo
Prerrequisitos: ▪ Usuarios añadidos a la Base de Datos del sistema ▪ Usuarios vinculados a los grupos de trabajo ▪ Hosts Clientes ▪ Access Point MikroTik hAP ▪ MiniPC con OPNSense	
Pasos: ▪ Verificar la existencia de los usuarios en la Base de Datos ▪ Validar la autenticación al portal mediante los logs del sistema	

Resultados esperados: Autenticación de los usuarios del sistema a la red mediante el uso del portal cautivo implementado como segundo factor de autenticación.

Resultados obtenidos: La base de datos local que almacena los usuarios puede interactuar con el portal cautivo permitiendo la autenticación de los usuarios, esta además permite visualizar el registro de los eventos asociados al portal cautivo como usuarios autenticados y solicitudes rechazadas.

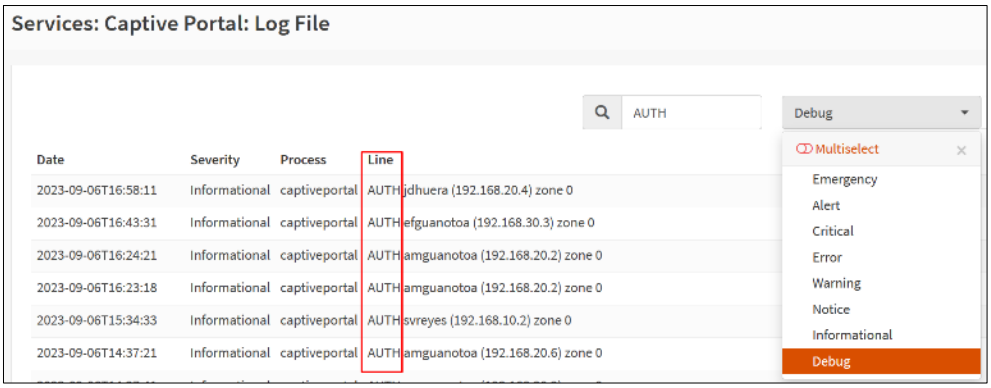
Para la validación del funcionamiento el usuario selecciona la red a la cual desea vincularse, ingresa la contraseña de la red inalámbrica e inmediatamente salta una ventana emergente como la mostrada en la Figura 53, esta sirve como un segundo factor de autenticación al sistema, la primera autenticación vincula al dispositivo a una VLAN especifica mientras que la segunda autenticación vincula un usuario especifico al dispositivo. De esta forma se vuelve más sofisticada y eficiente la implementación de control de tráfico y aplicaciones desde el punto de vista del administrador y más complicada la evasión de los controles aplicados desde el punto de vista del usuario final.

Figura 53.
Ventana emergente que solicita el ingreso de credenciales

El portal cautivo implementa un servicio de registro de todos los eventos llevados a cabo en él, mediante el modo “Debug” y aplicando el filtro “AUTH” se muestra en la Figura 54 todos los eventos correspondientes a la autenticación de forma exitosa de los usuarios al portal cautivo. Además, se puede conocer la hora exacta en la cual el usuario se autenticó con éxito, la dirección IP asignada al dispositivo y la zona a la cual el portal cautivo pertenece.

Figura 54.

Log de eventos que muestra las autenticaciones exitosas



La Figura 55 muestra los intentos fallidos durante la autenticación de un usuario, estos eventos se registran cuando se ingresa datos incorrectos en los campos usuario o contraseña debido a que no se encuentran coincidencias entre los datos ingresados y los datos almacenados en la base de datos.

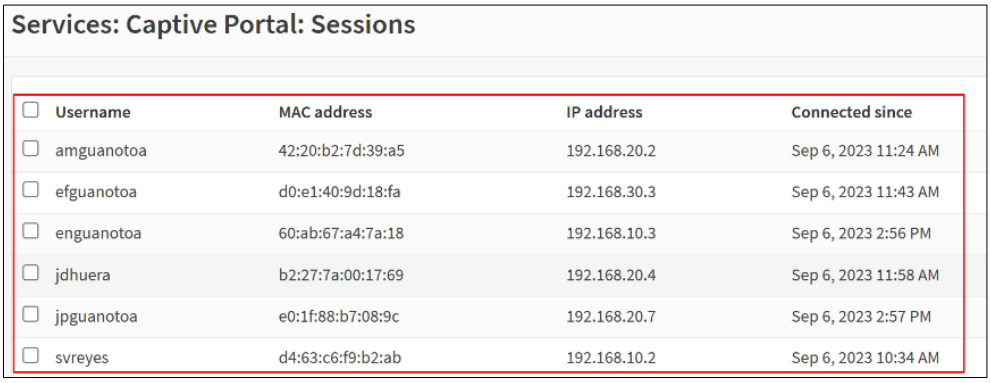
Figura 55.

Log de eventos que muestra las autenticaciones fallidas

Finalmente, en la Figura 56 se muestran los usuarios con sesiones activas en el portal cautivo, la dirección MAC del dispositivo asociado, la dirección IP y el registro de la hora desde el cual el usuario se encuentra asociado.

Figura 56.

Sesiones registradas en el Portal Cautivo



4.2.2.2 Test de Políticas de Acceso

Para la siguiente prueba en el bloque de acceso se comprobó que las políticas de acceso se aplicaran correctamente de acuerdo con los roles de usuario y las políticas de seguridad previamente definidas. Esta comprobación implicó la restricción de acceso a recursos o servicios específicos del NGFW, asegurando así una implementación precisa y efectiva de las políticas de seguridad y de acceso en el sistema. En la Tabla 30 de detallan las consideraciones y pasos a seguir para la validación de los resultados.

Tabla 30.

Test de Políticas de Acceso

Test de Políticas de Acceso	
Bloque de prueba	Bloque de Gestión
Descripción	Prueba para el funcionamiento de las políticas de acceso
Prerrequisitos: ▪ Usuarios añadidos a la Base de Datos del sistema ▪ Usuarios vinculados a los grupos de trabajo ▪ Hosts Clientes ▪ Access Point MikroTik hAP	

- MiniPC con OPNSense

Pasos:

- Ingresar a la herramienta de validación de credenciales de usuario
- Validar las credenciales de los usuarios
- Validar las categorías disponibles para cada grupo de usuario

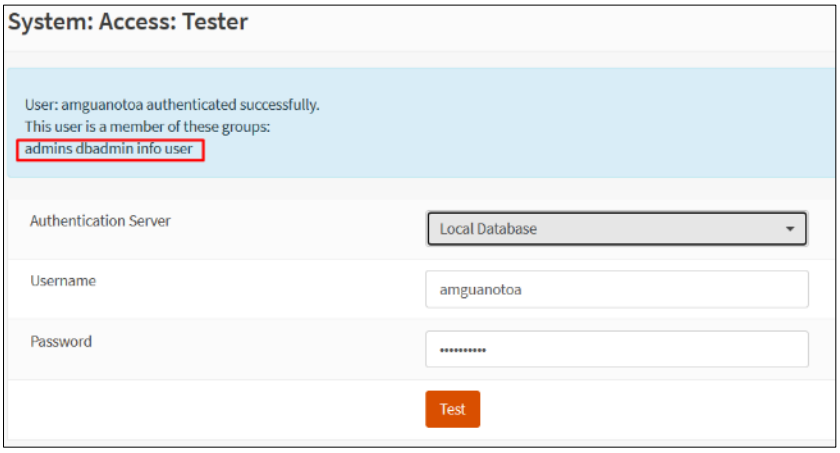
Resultados esperados: Verificación de la validez de las credenciales asignadas a los usuarios del sistema y visualización de las categorías, recursos y funciones específicas en base al tipo de usuario autenticado.

Resultados obtenidos: Cada usuario logró acceder a las categorías y funciones asignadas a sus respectivos grupos, gracias a la implementación exitosa de permisos específicos que regulan su capacidad de visualización y acceso en la plataforma. Esto aseguró una experiencia de usuario personalizada y protegió los datos y funciones sensibles, permitiendo únicamente el acceso a usuarios autorizados.

Para la validación de las credenciales de usuario se utilizó la funcionalidad Tester presente en el Firewall el cual permite verificar las coincidencias de las credenciales ingresadas en los campos con las almacenadas en la base de datos, como se observa en la Figura 57 se ingresó las credenciales del usuario “amguanotoa” en donde se muestra un mensaje que indica que el usuario en cuestión ha sido autenticado con éxito, además de muestra un mensaje adicional que indica los grupos a los cuales este pertenece, cada uno de estos grupos cuenta con permisos específicos para la gestión y visualización de funciones específicas en el sistema.

Figura 57.

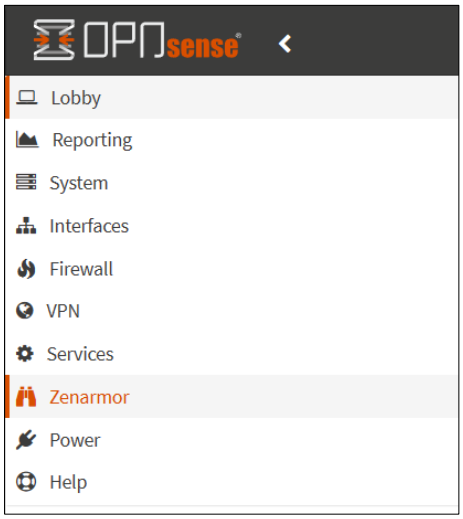
Testeo de la contraseña y permisos del usuario amguanotoa



Para comprobar la visualización de las categorías a las cuales el anterior usuario tiene acceso se ingresa al sistema desde la dirección http://192.168.99.1 y se introduce las credenciales correspondientes, una vez dentro del sistema se muestran únicamente las categorías a las cuales el usuario autenticado puede acceder, como se observa en la Figura 58 se trata de un usuario con permisos de administrador por lo cual se muestran todas las categorías disponibles.

Figura 58.

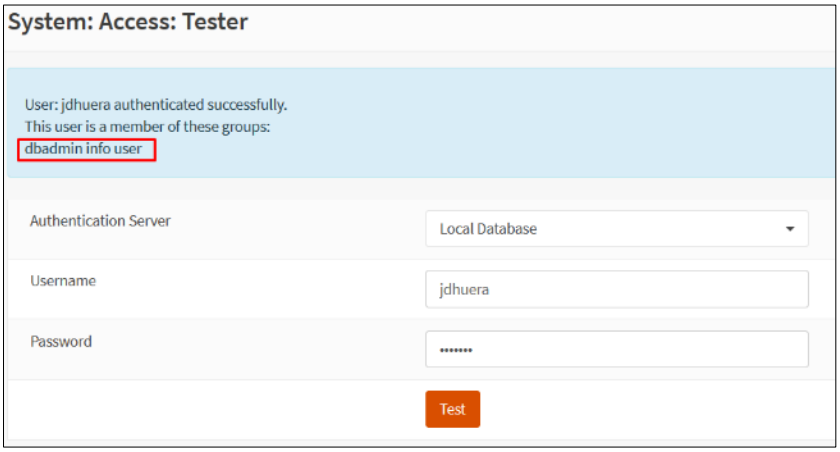
Panel de control de las categorías con permiso de visualización



La Figura 59 muestra la validación de las credenciales para el usuario jdhuera, además de los grupos a los que este pertenece, como se observa en el recuadro rojo este cuenta con menos permisos en comparación del anterior, estos le permiten al usuario únicamente ingresar al sistema para poder agregar nuevos usuarios a la base de datos y visualizar información acerca del monitoreo del sistema y los reportes de uso de la red.

Figura 59.

Testeo de la contraseña y permisos del usuario jdhuera



La Figura 60 muestra las categorías a las cuales el usuario jdhuera tiene acceso, como se puede observar en comparación con el usuario anterior este presenta menos categorías disponibles una vez a ingresado al sistema, estas categorías le permiten al usuario únicamente acceder al módulo de reportes, a la visualización de eventos del sistema, al estado de las interfaces y a los registros de los servicios tales como el portal cautivo y las direcciones asignadas por el servidor DHCP, es decir únicamente funciones de monitoreo de la red.

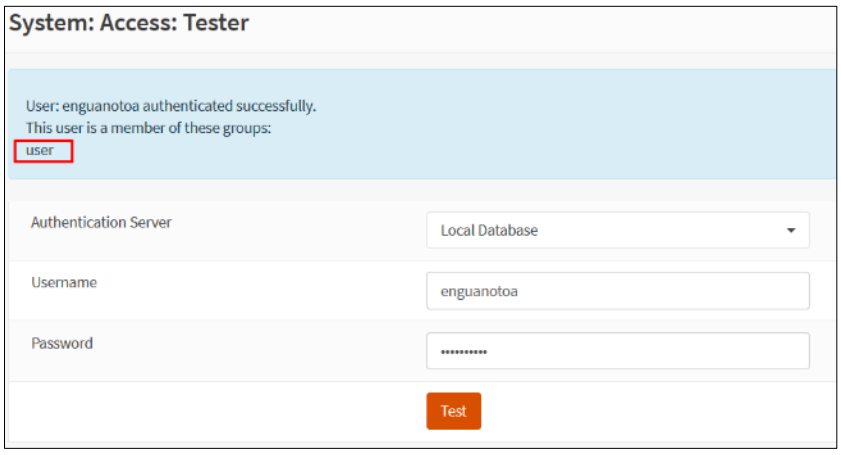
Figura 60.

Panel de control de las categorías con permiso de visualización

Finalmente se realiza la autenticación del usuario enguanotoa, el cual como se observa en la Figura 61 únicamente cuenta con permisos de usuario final, estos usuarios únicamente tienen acceso al lobby sistema en donde pueden iniciar sesión en el portal cautivo o desloguearse.

Figura 61.

Testeo de la contraseña y permisos del usuario enguanotoa



La Figura 62 muestra como el usuario anteriormente mencionado al ingresar al sistema únicamente cuenta con los permisos de grupo de usuario denominado “user” el cual tiene permitido únicamente el acceso al Lobby del sistema.

Figura 62.

Panel de control de las categorías con permiso de visualización

Mediante las pruebas realizadas para los distintos tipos de usuarios se puede determinar la efectividad de las políticas de control de acceso al sistema, en donde en base a los permisos previamente definidos se restringe el acceso a recursos y servicios específicos del sistema.

4.2.3 Bloque de Procesamiento

En la siguiente sección se muestran las pruebas efectuadas en el bloque de procesamiento en donde se detallan y muestran los procesos llevados a cabo para la validación de los resultados.

4.2.3.1 Test de Firewall

Para evaluar la efectividad del Firewall se realizaron pruebas de acceso o restricción a contenidos web y aplicaciones desde los dispositivos finales vinculados a las redes inalámbricas, estos eventos fueron registrados en la Base de Datos del sistema para el análisis de cumplimiento de las políticas implementadas. En la Tabla 31 se detallan los procesos a llevarse a cabo durante la prueba a realizar.

Tabla 31.

Test de Firewall

Test de Firewall	
Bloque de prueba	Bloque de Procesamiento
Descripción	Prueba para el funcionamiento de políticas de Firewall
Prerrequisitos: ▪ Access Point MikroTik hAP	

- MiniPC con OPNSense
- Hosts Clientes
- Usuarios vinculados y autenticados
- Políticas de filtrado de aplicaciones
- Políticas de filtrado web

Pasos:

- Generar tráfico web desde los hosts vinculados a las VLANs
- Visualizar el registro de conexiones
- Aplicar los filtros de visualización en los reportes

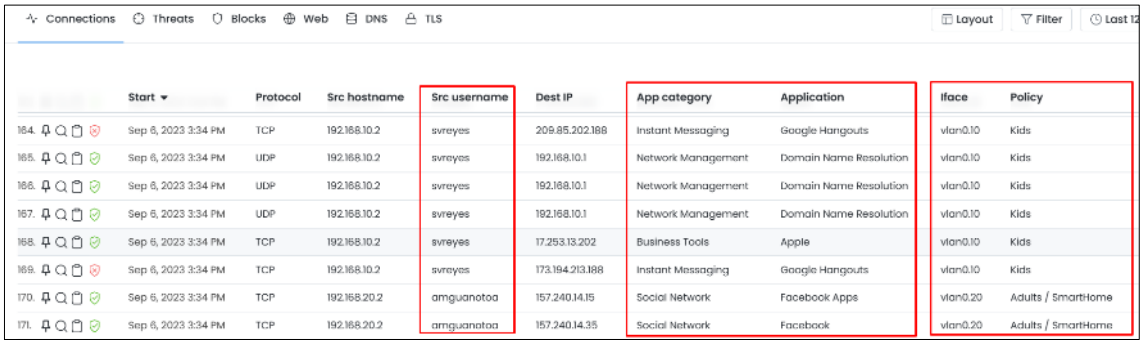
Resultados esperados: Cumplimiento de las políticas de firewall establecidas para cada subred y tipo de usuario vinculado al sistema, visualización de los eventos y las acciones ejecutadas por los módulos del sistema.

Resultados Obtenidos: Se ha logrado el cumplimiento de los objetivos establecidos al implementar políticas que operan de manera efectiva. Estas políticas se han ajustado para ser restrictivas en el caso del grupo de usuarios pertenecientes a la VLAN "Kids," al mismo tiempo que han demostrado ser más permisivas para el resto de los usuarios. Este enfoque ha permitido crear un entorno seguro y adecuado para el grupo de usuarios en cuestión, al tiempo que proporciona una experiencia más flexible para otros usuarios en la red. La correcta configuración de estas políticas ha garantizado un equilibrio exitoso entre seguridad y accesibilidad en la red.

La Figura 63 muestra de forma detallada mediante la visualización del historial de eventos como se aplican las políticas de firewall para cada usuario perteneciente a una subred en específico, además se ha resaltado en la imagen la aplicación que ha sido aceptada o rechazada, así como la categoría a la que pertenece dicha conexión, esto permite validar el funcionamiento y cumplimiento de las políticas implementadas.

Figura 63.

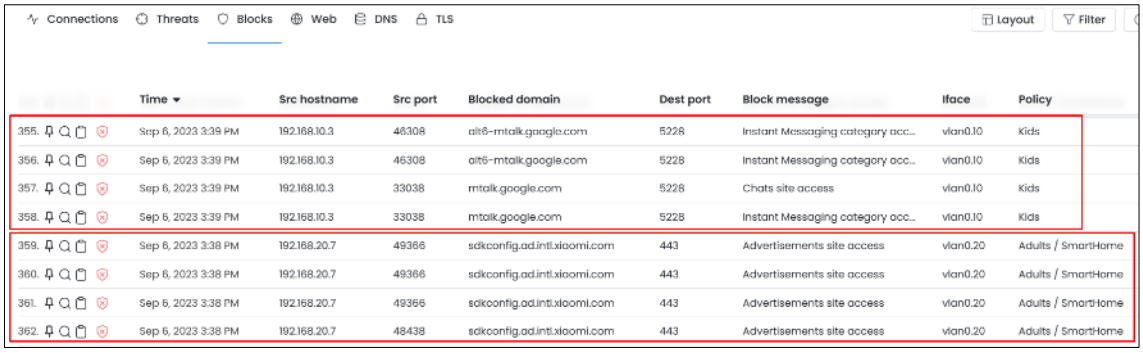
Historial de eventos registrados por el NGFW



La Figura 64 muestra el detalle de las solicitudes rechazadas, en el primer recuadro resaltado se muestran las solicitudes denegadas pertenecientes a la VLAN 10 que se encuentran definidas en la política del firewall denominada “Kids”, mientras que en el segundo recuadro se resaltan las conexiones denegadas para la VLAN 20 perteneciente a las políticas establecidas en la política “Adults / SmartHome”.

Figura 64.

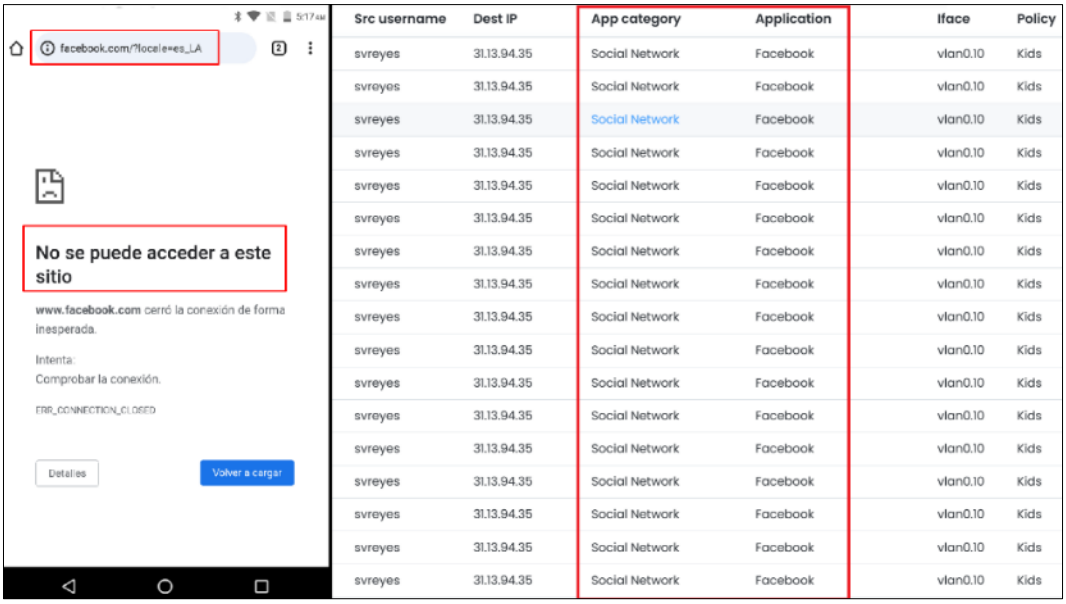
Historial de bloqueos web registrados por el NGFW



La Figura 65 muestra en el lado izquierdo el bloqueo al intentar ingresar a la página web FACEBOOK debido a que este sitio se encuentra contemplado como RESTRINGIDO dentro de las políticas establecidas para los usuarios KIDS. Mientras que al lado derecho se muestra el historial de eventos registrados en el Firewall, aquí se puede ver a detalle la política aplicada al usuario “svreyes”, así como la interfaz desde la cual se solicitó la conexión.

Figura 65.

Visualización del Bloqueo en el Host y detalles de la política aplicada



Src username	Dest IP	App category	Application	Iface	Policy
svreyes	31.13.94.35	Social Network	Facebook	vlan0.10	Kids
svreyes	31.13.94.35	Social Network	Facebook	vlan0.10	Kids
svreyes	31.13.94.35	Social Network	Facebook	vlan0.10	Kids
svreyes	31.13.94.35	Social Network	Facebook	vlan0.10	Kids
svreyes	31.13.94.35	Social Network	Facebook	vlan0.10	Kids
svreyes	31.13.94.35	Social Network	Facebook	vlan0.10	Kids
svreyes	31.13.94.35	Social Network	Facebook	vlan0.10	Kids
svreyes	31.13.94.35	Social Network	Facebook	vlan0.10	Kids
svreyes	31.13.94.35	Social Network	Facebook	vlan0.10	Kids
svreyes	31.13.94.35	Social Network	Facebook	vlan0.10	Kids
svreyes	31.13.94.35	Social Network	Facebook	vlan0.10	Kids
svreyes	31.13.94.35	Social Network	Facebook	vlan0.10	Kids
svreyes	31.13.94.35	Social Network	Facebook	vlan0.10	Kids
svreyes	31.13.94.35	Social Network	Facebook	vlan0.10	Kids
svreyes	31.13.94.35	Social Network	Facebook	vlan0.10	Kids
svreyes	31.13.94.35	Social Network	Facebook	vlan0.10	Kids
svreyes	31.13.94.35	Social Network	Facebook	vlan0.10	Kids
svreyes	31.13.94.35	Social Network	Facebook	vlan0.10	Kids
svreyes	31.13.94.35	Social Network	Facebook	vlan0.10	Kids

4.2.3.2 Test de Monitoreo y Registro

El sistema cuenta con un módulo de generación de reportes que permite mostrar de manera gráfica los reportes de conexiones, amenazas, bloqueos o acceso web, permitiendo aplicar filtros específicos para generar graficas que detallen la información de acuerdo con las necesidades de los beneficiarios del sistema. En la Tabla 32 se detallan las consideraciones para la realización de esta prueba.

Tabla 32.

Test de Monitoreo y Registro

Test de Monitoreo y Registro	
Bloque de prueba	Bloque de Procesamiento
Descripción	Prueba para el funcionamiento del Monitoreo y Registro
Prerrequisitos: ▪ Access Point MikroTik hAP ▪ MiniPC con OPNSense ▪ Hosts Clientes ▪ Tráfico almacenado en la BDD ▪ Correo electrónico vinculado al servicio de programación de informes	

Pasos:

- Especificar un periodo de análisis
- Generar reporte de conexiones
- Analizar las gráficas obtenidas
- Confirmar la entrega de reportes por correo electrónico

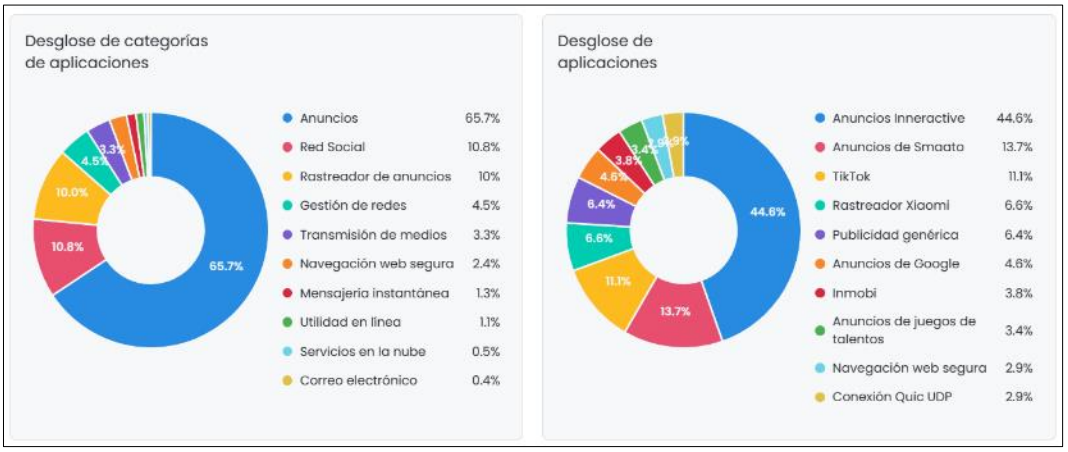
Resultados esperados: Obtener gráficas que detallen las conexiones efectuadas por medio del NGFW, obtener estadísticas de amenazas mitigadas, obtener reportes de aplicación de las políticas de filtrado, recibir el informe programado por en el correo electrónico.

Resultados obtenidos: El sistema tiene la capacidad de mostrar informes fáciles de visualizar e interpretar, etiquetando y segmentando las categorías mostradas, además se verificó que el sistema realiza la entrega programada de informes según el periodo establecido.

En la parte izquierda de la Figura 66 se muestra las categorías de aplicaciones distribuidas por porcentajes en una gráfica de pastel, en donde se puede constatar que las sesiones que más se han establecido para el total de conexiones son las correspondientes a aplicaciones de visualización de anuncios con un 66% del total, seguido por un 10,8% de uso de redes sociales y en tercer lugar se encuentran las conexiones pertenecientes a aplicaciones de rastreo de anuncios. En la gráfica de la derecha se muestran los porcentajes pertenecientes a cada aplicación especifica de las categorías registradas.

Figura 66.

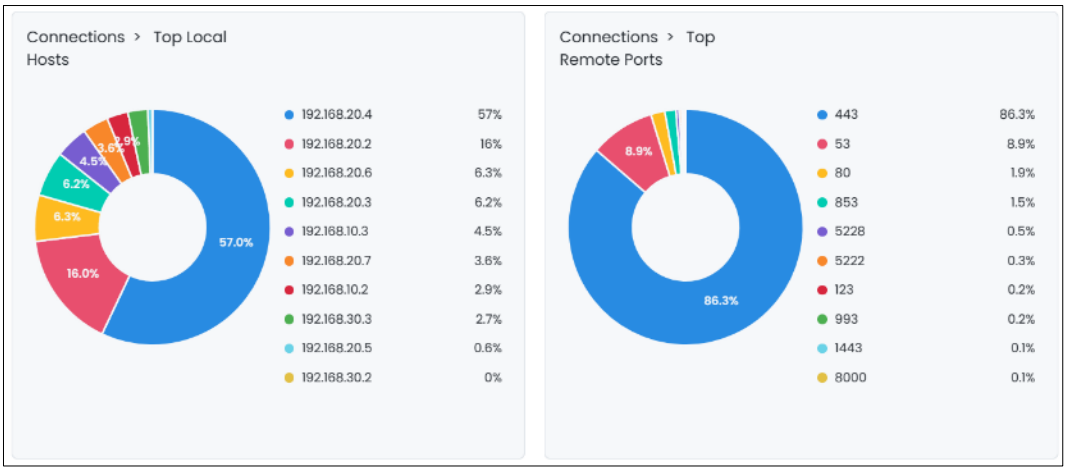
Sesiones registradas de aplicaciones y categorías de aplicaciones



En la gráfica de la derecha mostrada en la Figura 67 se muestra el porcentaje de conexiones establecidas por host representado con la dirección IP asociada al dispositivo, mientras que en la gráfica de la derecha se muestran los puertos utilizados para dichas conexiones, teniendo como resultados que el puerto más utilizado es el 443 que corresponde a comunicaciones web encriptadas.

Figura 67.

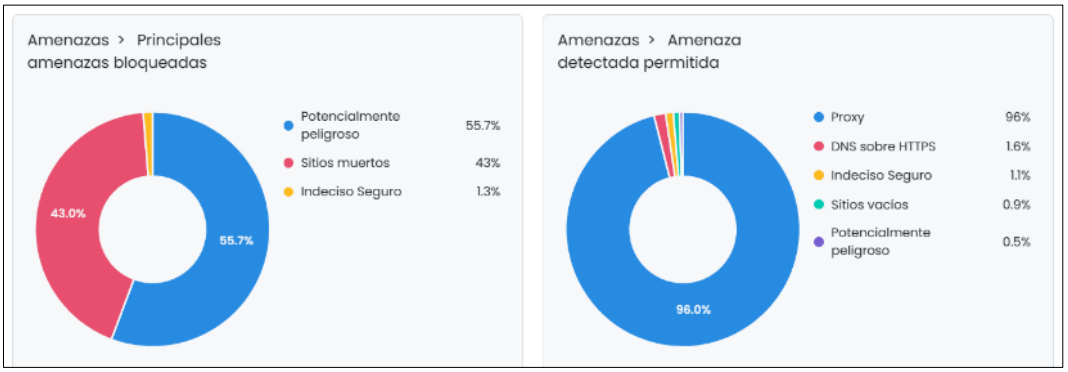
Host locales y puertos remotos más usados.



En la gráfica de la derecha presente en la Figura 68 se muestra la distribución de los porcentajes pertenecientes a las principales amenazas bloqueadas por el NGFW, validando que un 55.7% de las comunicaciones bloqueadas perteneces a sitios considerados potencialmente peligrosos, seguido por un 43% correspondiente a sitios “muertos”. En la gráfica de la derecha se muestra el porcentaje de comunicaciones consideradas como falsos positivos, encabezados por sesiones Proxy con un 96% del total del tráfico analizado.

Figura 68.

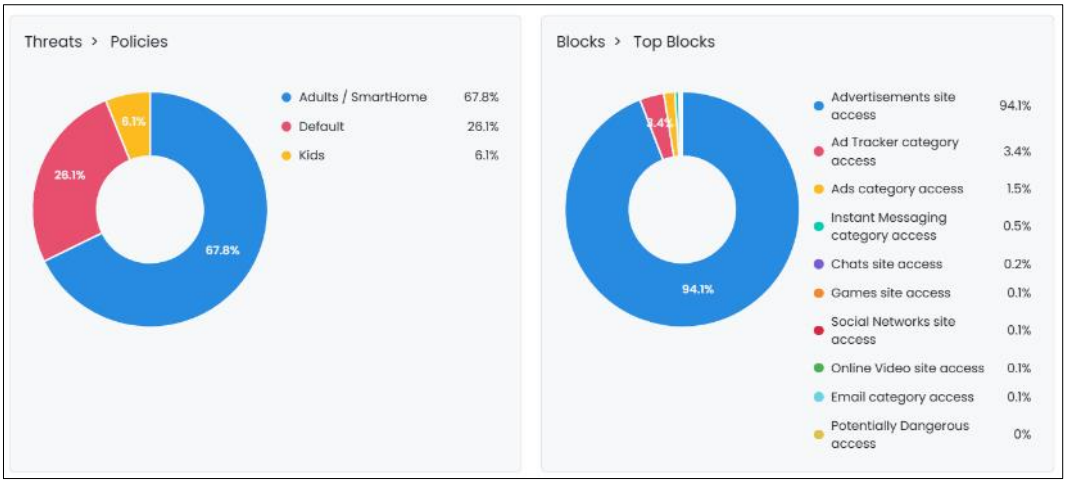
Amenazas detectadas y bloqueadas



La Figura 69 corresponde a la aplicación de las políticas de filtrado, en el gráfico de la izquierda se puede observar que del tráfico total analizado el 67.8% es tráfico al cual se aplicaron las políticas establecidas en las reglas “Adults / SmartHome”, seguidas por un 28.1% de conexiones que fueron rechazadas por la política por defecto la cual fue configurada con parámetros “Deny All” y por último se muestra con un 6.1% el total de conexiones que implementaron la política “Kids”. Por su parte la gráfica de la derecha muestra la distribución de las aplicaciones bloqueadas por las políticas definidas en el firewall, teniendo como principal resultado que el 94% de las conexiones bloqueadas pertenecen a aplicaciones relacionadas a la distribución de publicidad.

Figura 69.

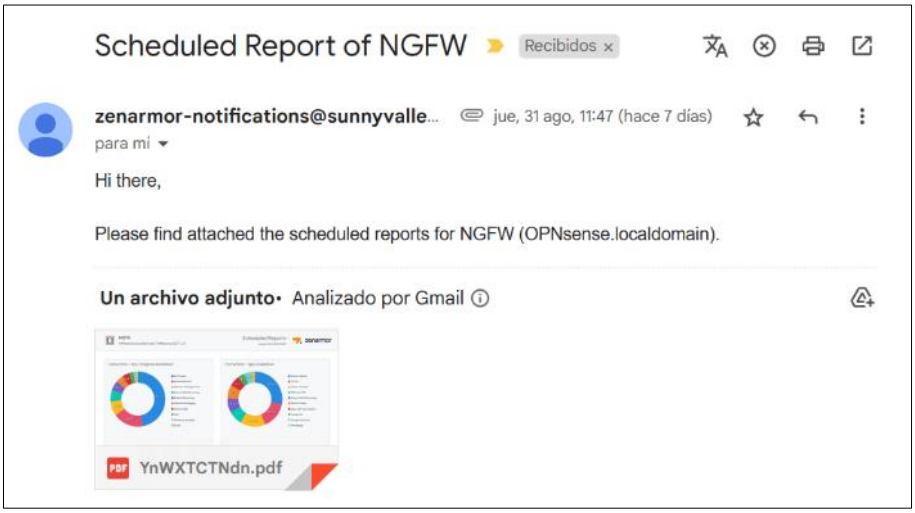
Políticas aplicadas y categorías bloqueadas



Finalmente, en la Figura 70 se verifica el funcionamiento del servicio programado de entrega de reportes por correo electrónico, validando que se ha recibido un correo electrónico entregado por el NGFW con un correo adjunto el cual contiene todos los datos recolectados durante el periodo de una semana organizado por categorías y detallando el tipo de acciones aplicadas.

Figura 70.

Reporte semanal programado entregado al administrador del sistema



4.3 Evaluación de la Eficacia del Sistema

Para determinar la eficacia del software, se llevó a cabo un análisis basado en los objetivos establecidos por los stakeholders antes del desarrollo del sistema. A continuación, se procederá a evaluar el sistema según los parámetros definidos en la norma ISO/IEC 9126, que incluyen Funcionalidad, Fiabilidad, Usabilidad, Mantenibilidad, Portabilidad y Calidad de uso. Cada uno de estos parámetros contiene a varias subcaracterísticas, en donde la conformidad es una sub-característica de la funcionalidad, así como el parámetro de seguridad.

4.3.1 Parámetro de Conformidad de Funcionalidad

El parámetro de conformidad de funcionalidad se refiere a una sub-característica de funcionalidad contenido en la norma ISO/IEC 9126, aquí se establecen las funciones prioritarias del sistema de acuerdo con los usuarios de este. Los usuarios prioritarios son tanto el administrador como los usuarios con acceso a funciones de gestión. En la Tabla 33 se detallan a los beneficiarios.

Tabla 33.
Usuarios del sistema

Nombre	Rol en el Sistema
Sr. Alexander Guanotoa	Administrador
Sra**.** Dayana Huera	Usuario

Con la finalidad de evaluar los distintos parámetros, se ha establecido la Tabla 34 que contiene los criterios de evaluación y su valor correspondiente.

Tabla 34.
Criterio y valoración

Criterio	Valor
Pobre	1
Justo	2
Bueno	3
Excelente	4

Además de determinar el nivel de cumplimiento de los objetivos planificados, evaluar el parámetro de conformidad implica analizar detalladamente las funciones específicas del sistema y asignarles un nivel de aceptación. Esto permite identificar áreas donde el sistema puede no estar cumpliendo con los requisitos establecidos y facilita la toma de decisiones para realizar ajustes o mejoras necesarias. A continuación, en la Tabla 35 se detallan las funciones y los resultados de evaluación pertenecientes al administrador del sistema.

Tabla 35.

Valoración de funciones de conformidad de funcionalidad (Admin)

Nro	Función	Criterio	Valor
1	Visualización de las redes	Excelente	4
2	Vinculación a las redes inalámbricas	Excelente	4
3	Autenticación al sistema	Bueno	3
4	Registro de usuarios	Excelente	4
5	Asignación de usuarios a grupos	Excelente	4
6	Asignación de niveles de acceso	Excelente	4
7	Segmentación del tráfico	Excelente	4
8	Bloqueo de aplicaciones	Excelente	4
9	Bloqueo de dominios	Excelente	4
10	Bloqueo de amenazas	Excelente	4
11	Registro de reglas permisivas	Excelente	4
12	Registro de reglas restrictivas	Excelente	4
13	Reporte de uso	Bueno	3
14	Reporte de estado	Bueno	3
	Total		**53**
	Porcentaje		**95%**

Una vez recopilados y tabulados los resultados se puede determinó que la aceptación de funcionalidad por parte del administrador fue del 95%. En la Tabla 36 se detallan los porcentajes asociados a cada criterio en específico.

Tabla 36.

Porcentajes de valoración de conformidad de funcionalidad (Admin)

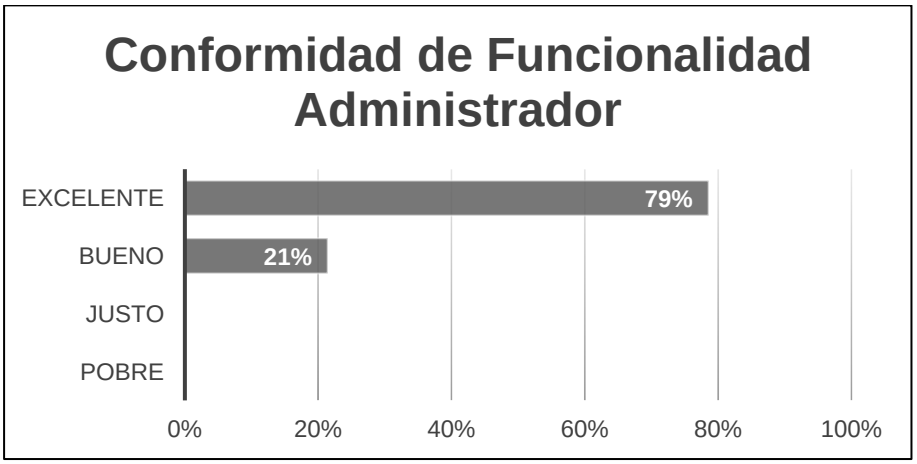
Cantidad	Criterio	Porcentaje
0	Pobre	0%
0	Justo	0%
3	Bueno	21%
11	Excelente	79%

De acuerdo con el análisis del parámetro, se determina que el 79% de las funciones han obtenido una aceptación determinada como “Excelente”, mientras que el 21% del total de las funciones han calificado como “Bueno”. Los criterios “Pobre” y “Justo” han tenido una representación del 0%, lo que significa que la conformidad del sistema es mayormente

positiva estableciendo que se han cumplido con éxito la mayoría de las funciones evaluadas. En la Figura 71 se muestra los porcentajes de conformidad de acuerdo a cada criterio de evaluación.

Figura 71.

Conformidad de Funcionalidad para Administrador



De la misma forma se realizó un análisis de conformidad de funcionalidad para el rol "Usuario", quien en base a su experiencia con el uso del sistema asigno los valores en cada una de las funciones, las cuales se detallan en la Tabla 37.

Tabla 37.

Valoración de funciones de conformidad de funcionalidad (User)

Nro	Función	Criterio	Valor
1	Visualización de las redes	Bueno	3
2	Vinculación a las redes inalámbricas	Excelente	4
3	Autenticación al sistema	Excelente	4
4	Registro de usuarios	Bueno	3
5	Asignación de usuarios a grupos	Bueno	3
6	Asignación de niveles de acceso	Excelente	4
7	Segmentación del tráfico	Bueno	3
8	Bloqueo de aplicaciones	Excelente	4
9	Bloqueo de dominios	Excelente	4
10	Bloqueo de amenazas	Excelente	4
11	Registro de reglas permisivas	Bueno	3
12	Registro de reglas restrictivas	Bueno	3

13	Reporte de uso	Bueno	3
14	Reporte de estado	Justo	2
	Total		**47**
	Porcentaje		**84%**

La conformidad de funcionalidad del sistema fue de un 84% para el rol “Usuario”, en la Tabla 38 se detallan los porcentajes ligados a cada criterio.

Tabla 38.

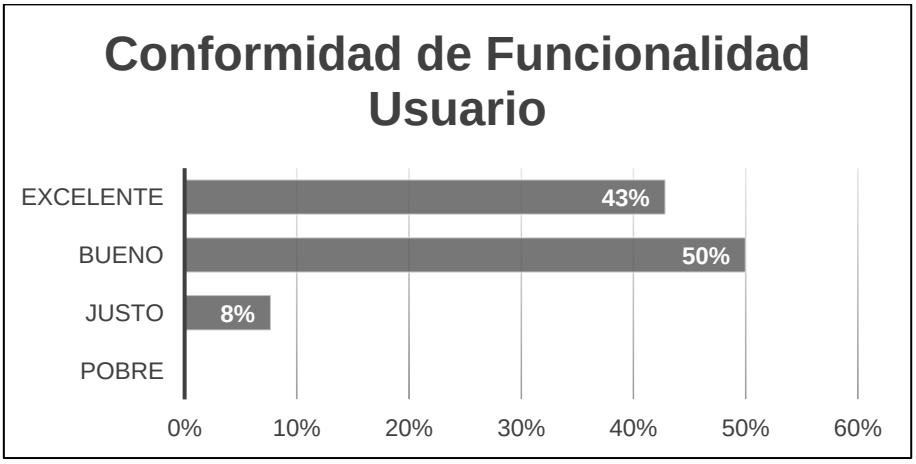
Porcentajes de valoración de conformidad de funcionalidad (User)

Cantidad	Criterio	Porcentaje
0	Pobre	0%
1	Justo	8%
7	Bueno	50%
6	Excelente	43%

Luego del análisis se ha obtenido como resultados que el 43% de los parámetros evaluados han sido asignados como “Excelente”, el 50% como “Bueno” lo que confirma la alta funcionalidad del sistema, el 8% se ha definido como “Justo” y 0% de parámetros se han definido como “Pobre” tal como se muestra en la Figura 72.

Figura 72.

Conformidad de Funcionalidad para Usuario



Una vez tabulada la información se obtiene como resultados los presentados en la Tabla 39, en donde se puede observar que para el “Administrador” el porcentaje de

aceptación representa un 96%, mientras que para el “Usuario” representa un 84%, teniendo una media de aceptación del 90% respecto a la conformidad del sistema.

Tabla 39.
Resultados de conformidad de funcionalidad

Rol	Valor	Porcentaje
Administrador	53	96%
Usuario	47	84%
Promedio		**90%**

4.3.2 Parámetro de Evaluación de Seguridad

El parámetro de seguridad constituye una sub-característica de vital importancia dentro del marco de evaluación de la funcionalidad establecido por la norma ISO/IEC 9126. Con el propósito de analizar este parámetro, se llevó a cabo una comparativa entre la aceptación de las funciones relacionadas con la seguridad de los beneficiarios, tanto con el sistema habilitado como deshabilitado. Este proceso se llevó a cabo con el objetivo de evaluar el nivel de contribución del Next-Generation Firewall (NGFW) a la seguridad de la red doméstica.

Con la finalidad de evaluar los parámetros y funciones de seguridad se ha propuesto los siguientes criterios contenidos en la Tabla 40, en donde se asignan valores de 1 a 4 para establecer los criterios de aceptación.

Tabla 40.
Criterio y valoración

Criterio	Valor
Pobre	1
Justo	2
Bueno	3
Excelente	4

El parámetro de seguridad constituye una sub-característica de vital importancia dentro del marco de evaluación de la funcionalidad establecido por la norma ISO/IEC 9126. Con el propósito de analizar este parámetro, se llevó a cabo una comparativa entre la aceptación de las funciones relacionadas con la seguridad de los beneficiarios tal como se muestra en la Tabla 41 tanto con el sistema habilitado como deshabilitado. Este proceso se llevó a cabo con el objetivo de evaluar el nivel de contribución del Next-Generation Firewall (NGFW) a la seguridad de la red en la que se implementó.

Tabla 41.

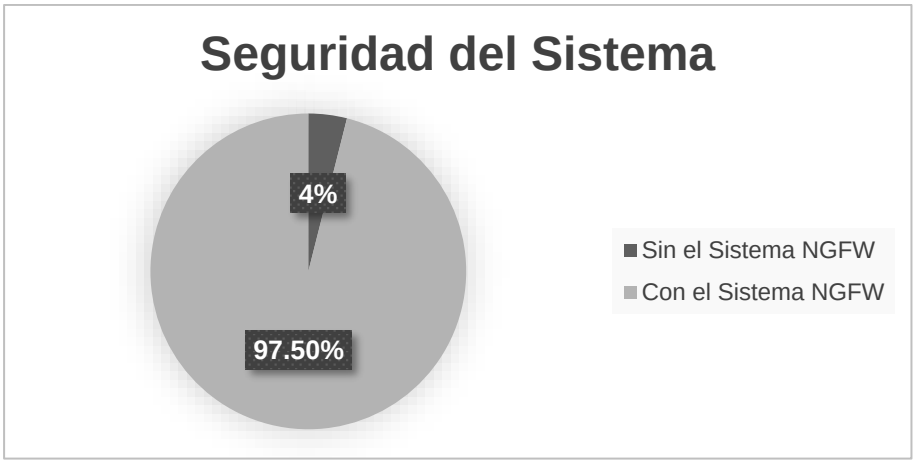
Valoración de funciones de evaluación de seguridad

Nro	Función	Sin el Sistema NGFW	Con el Sistema NGFW	Porcentaje de mejora
1	Autenticación de doble factor	1	4	100%
2	Niveles de acceso	1	4	100%
3	Identificación de usuarios	1	4	100%
4	Detección de amenazas	1	4	100%
5	Bloqueo de amenazas	1	3	75%
6	Filtrado de Contenido	1	4	100%
7	Inspección SSL/TLS	1	4	100%
8	Control de Aplicaciones y Políticas	1	4	100%
9	Visibilidad de la Red y Análisis de Tráfico	1	4	100%
10	Gestión Centralizada y Automatización	1	4	100%
	Total	**10**	**39**	
	Porcentaje	**4%**	**97,5%**	**93,5%**

Como se observa en la Figura 73, el porcentaje asociado a la seguridad del sistema sin habilitar las funciones específicas es apenas del 4%, utilizando únicamente funciones básicas de acceso. Sin embargo, al activar el sistema, la seguridad se incrementa significativamente hasta alcanzar un 97.5%. Esto representa una mejora del 93.5% en la seguridad de la red doméstica después de aplicar las funciones, lo que demuestra la efectividad del sistema para fortalecer la protección del entorno.

Figura 73.

Porcentaje de funcionalidad en la seguridad del sistema



CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

La digitalización impulsada por la pandemia del 2019 incrementó la penetración del uso de internet en los hogares, lo que a su vez aumentó los riesgos al navegar en línea, especialmente para los niños y adolescentes. La falta de control en la navegación en Internet expuso a estos grupos a amenazas como el ciberacoso, la pornografía infantil, el sexting, la explotación sexual en línea y el libre acceso a contenido inapropiado en general. La implementación de este proyecto al ser dotado de características avanzadas propias de un NGFW ofrece una solución a esta problemática, ya que los dispositivos de red doméstica a menudo carecen de capacidades de control de tráfico, dejando la responsabilidad de protección en manos de los usuarios finales.

La definición y aplicación de políticas para el Firewall de Nueva Generación en un entorno controlado de simulación representó una etapa fundamental durante el desarrollo. En este entorno, se llevaron a cabo las primeras evaluaciones de funcionalidad, incluyendo el filtrado de tráfico, el control de acceso de usuarios y la detección de amenazas. Este proceso constituye un paso previo dentro del modelo de desarrollo, ya que los requerimientos del sistema se van complementando de manera progresiva hasta estar listos para ser implementados en un entorno más complejo, como una red física con clientes reales. Mediante estas evaluaciones iniciales en un entorno simulado, se garantiza que el firewall cumpla con los estándares de seguridad necesarios antes de su despliegue en un entorno de producción, lo que contribuye significativamente a la eficacia y fiabilidad del sistema final.

El uso del modelo iterativo ha permitido desarrollar de manera efectiva el diseño del sistema, tanto en hardware como en software. Este enfoque se basa en la planificación detallada, la definición precisa de los requisitos, la evaluación continua de su cumplimiento y la corrección o complementación de etapas anteriores si los objetivos no se cumplen en su

totalidad. Esta metodología ha resultado en una combinación ideal de funcionalidades necesarias para cubrir los requisitos del sistema, así como en la selección de componentes adecuados para las necesidades de la red y los usuarios.

La implementación de niveles diferenciados de acceso para cada usuario, junto con políticas de seguridad sólidas, establecen una estructura de control robusta en el sistema. Esta estrategia no solo garantiza la seguridad y la integridad del sistema, sino que también promueve una gestión eficiente de los recursos, asegurando que cada usuario tenga acceso solo a lo necesario para cumplir sus responsabilidades. El control preciso sobre el acceso a la red y el bloqueo de aplicaciones y sitios web por categorías contribuyeron significativamente a mejorar la seguridad general de la red y prevenir posibles amenazas y vulnerabilidades.

El sistema alcanzó el objetivo de generar informes personalizados de manera automática. Estos informes incluyen datos sobre el uso de aplicaciones, actividades web, amenazas detectadas y estadísticas de uso de la red, mismos que son entregados vía correo electrónico de forma periódica a los usuarios asignados con los permisos de visualización y monitoreo dentro del sistema. Esta funcionalidad mejora la capacidad de supervisión y toma de decisiones relacionadas con la seguridad y el rendimiento de la red.

5.2 Recomendaciones

A pesar de que este sistema cuenta con capacidades de análisis y protección avanzadas, es importante resaltar que la supervisión activa por parte de los tutores o adultos responsables sigue siendo una práctica fundamental. Se aconseja encarecidamente que los tutores de los menores no dejen a los niños sin supervisión mientras utilizan dispositivos electrónicos, incluso cuando se cuenta con medidas de seguridad en su lugar. La supervisión continua permite a los adultos monitorear las actividades en línea de los

niños, guiarlos en el uso responsable de la tecnología y estar alerta ante cualquier contenido inapropiado o situaciones de riesgo que puedan surgir.

Debido a la diversidad de escenarios de implementación que pueden surgir, es esencial enfocarse en el dimensionamiento adecuado del alcance del Access Point para garantizar una cobertura efectiva de las redes inalámbricas en todo el entorno. Esto implica considerar factores como el tamaño físico del área a cubrir, la disposición de las paredes y obstáculos, la densidad de usuarios y dispositivos, así como la capacidad de transmisión y la calidad de señal requerida.

El cuidado y la protección de las credenciales de acceso al sistema son de suma importancia, ya que estas credenciales son el mecanismo principal que determina los permisos de acceso tanto a la conexión a Internet como a las configuraciones del sistema. Si estas credenciales caen en manos equivocadas o son utilizadas por un usuario no autorizado, se otorgan automáticamente permisos que no le corresponden, lo que puede dar lugar a problemas de seguridad y violaciones de privacidad. Por lo tanto, se recomienda que las credenciales de acceso se mantengan confidenciales y que solo se compartan con usuarios autorizados.

La revisión periódica de los informes proporcionados por el sistema es una práctica fundamental para mantener la seguridad y la integridad de la red. Estos informes contienen datos valiosos que pueden revelar eventos de seguridad importantes, como amenazas filtradas o accesos no autorizados. Al llevar a cabo una lectura y análisis regular de estos informes, los administradores de red pueden identificar patrones y tendencias en el comportamiento de la red que podrían indicar actividades sospechosas. Además, esta revisión permite tomar medidas preventivas y correctivas de manera oportuna para abordar cualquier incidente de seguridad que pueda surgir. El monitoreo constante de los informes

contribuye significativamente a mantener un entorno de red seguro y protegido contra amenazas cibernéticas.

Bibliografía

Agencia de Regulación y Control de las Telecomunicaciones. (2020). *Por un internet seguro para niños, niñas y adolescentes*. https://www.arcotel.gob.ec/por-un-internet-seguro-para-ninos-ninas-y-adolescentes/

Alabdan, R. (n.d.). *future internet Phishing Attacks Survey: Types, Vectors, and Technical Approaches*. https://doi.org/10.3390/fi12100168

Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security*, *74*, 144–166. https://doi.org/10.1016/J.COSE.2018.01.001

AO Kaspersky Lab. (2022). *What Is an IP Address & What does it mean?* https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address

Aroyo, A. M., Rea, F., Sandini, G., & Sciutti, A. (2018). Trust and Social Engineering in Human Robot Interaction: Will a Robot Make You Disclose Sensitive Information, Conform to Its Recommendations or Gamble? *IEEE ROBOTICS AND AUTOMATION LETTERS*, *3*(4), 3701. https://doi.org/10.1109/LRA.2018.2856272

Arrate, A., González-Cabañas, J., Cuevas, Á., & Cuevas, R. (2020). Malvertising in Facebook: Analysis, Quantification and Solution. *Electronics 2020, Vol. 9, Page 1332*, *9*(8), 1332. https://doi.org/10.3390/ELECTRONICS9081332

Ashtari, H. (2022, March 10). *Network Topology Diagrams and Selection Best Practices for 2022*. Network Topology Is the Physical Arrangement of the Endpoints and Links in an Enterprise Network. https://www.spiceworks.com/tech/networking/articles/what-is-network-topology/

Aslan, O., & Samet, R. (2020). A Comprehensive Review on Malware Detection Approaches. *IEEE Access*, *8*, 6249–6271. https://doi.org/10.1109/ACCESS.2019.2963724

Barracuda Networks. (2021). *What is a Network Perimeter?* https://www.barracuda.com/glossary/network-perimeter

Consejo Nacional para la Igualdad Intergeneracional. (2020, September 2). *Ecuador es el primer país de la región en contar con una política pública por una internet segura para niñas, niños y adolescentes*. https://www.igualdad.gob.ec/ecuador-es-el-primer-pais-en-contar-con-una-politica-publica-por-una-internet-segura-para-ninas-ninos-y-adolescentes/

Cordón. (2021, May 31). *¿Qué son las ciberamenazas? Principales tipos*. Cordón Asesores Independientes. https://seguroscibernéticos.es/que-son-las-ciberamenazas-principales-tipos/

Cortés Aldana, D. Geovanny. (2016). *Firewalls de Nueva Generación: La Seguridad Informática Vanguardista*. Universidad Piloto de Colombia.

Eby, K. (2019, January 2). *The Power of Iterative Design and Process*. https://www.smartsheet.com/iterative-process-guide

El Universo. (2021, December 7). *Recomendaciones para escoger un proveedor de internet adecuado*. https://www.eluniverso.com/larevista/tecnologia/recomendaciones-para-escoger-un-proveedor-de-internet-adecuado-nota/

Eliyan, L. F., & Di Pietro, R. (2021). DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. *Future Generation Computer Systems*, *122*, 149–171. https://doi.org/10.1016/J.FUTURE.2021.03.011

English, J. (2022, April 22). *An introduction to 8 types of network devices*. TechTarget. https://www.techtarget.com/searchnetworking/tip/An-introduction-to-8-types-of-network-devices

Fortinet. (2021). *What Is a Wireless Network? Wi-Fi and Networking*. https://www.fortinet.com/resources/cyberglossary/wireless-network

Foss, W., & Grant, K. (2020, May). *Key Objectives of Perimeter Security*. Perimeter Security Partners. https://perimetersecuritypartners.com/in-the-know/post-title-3/

Fruhlinger, J. (2022, May 25). *What is an IP address? And what is your IP address?* Network World. https://www.networkworld.com/article/3588315/what-is-an-ip-address-and-what-is-your-ip-address.html

Gillis, A. (2020). *Intrusion prevention system (IPS)*. https://www.techtarget.com/searchsecurity/definition/intrusion-prevention

Gillis, A. (2021). *What is a Computer Network?* TechTarget. https://www.techtarget.com/searchnetworking/definition/network

Goralski, W. (2017). User Datagram Protocol. *The Illustrated Network*, 289–306. https://doi.org/10.1016/B978-0-12-811027-0.00011-4

Haber, L. (2021, January 5). *What is a port number?* https://www.techtarget.com/searchnetworking/definition/port-number

Herbst, J. (2017, August 30). *VLANs: 5 Types and Benefits*. https://www.summit360.com/2017/08/30/vlans-types-benefits/

Hitron Technologies Americas. (2020, October 30). *What is the Difference Between ONT & ONU?* https://us.hitrontech.com/learn/what-is-the-difference-between-ont-onu

IBM. (2022, November 15). *TCP/IP terminology - IBM Documentation*. AIX 7.3. https://www.ibm.com/docs/en/aix/7.3?topic=protocol-tcpip-terminology

Instituto Nacional de Estadística y Censos. (2020). *Tecnologías de la Información y Comunicación-TIC*. https://www.ecuadorencifras.gob.ec/tecnologias-de-la-informacion-y-comunicacion-tic/

IT Governance. (n.d.). *ISO/IEC 27001. Implement, Certify & Comply*. Retrieved November 30, 2022, from https://www.itgovernance.co.uk/iso27001

IT Governance. (2019). *What is Cyber Security? Definition & Best Practices*. https://www.itgovernance.co.uk/what-is-cybersecurity

Juniper Networks. (2018, October 18). *Understanding the IEEE 802.11 Standard for Wireless Networks*. https://www.juniper.net/documentation/en_US/junos-space-apps/network-director4.0/topics/concept/wireless-80211.html

Jyotiyana, P., & Maheshwari, S. (2016). A literature survey on malware and online advertisement hidden hazards. *Advances in Intelligent Systems and Computing*, *530*, 449–460. https://doi.org/10.1007/978-3-319-47952-1_35/COVER/

Kanade, V. (2022, February 10). *What Is Network Hardware? Definition, Architecture, Challenges, and Best Practices*. Spiceworks Tech. https://www.spiceworks.com/tech/networking/articles/what-is-network-hardware/

Link, J. (2021, January 16). *What's a MAC Address and how do I find it?* The Ohio State University. https://slts.osu.edu/articles/whats-a-mac-address-and-how-do-i-find-it/

Lutkevich, B. (2021). *What is an intrusion detection system (IDS)? Definition from SearchSecurity*. https://www.techtarget.com/searchsecurity/definition/intrusion-detection-system

Macy, D. (2022, January 7). *What Is Perimeter Security In Cybersecurity?* Security Foward. https://www.securityforward.com/what-is-perimeter-security-in-cybersecurity/

Ministerio de Inclusión Económica y Social, Ministerio de Telecomunicaciones y Sociedad de la Información, & Consejo Nacional para la Igualdad Intergeneracional. (2020, September). *Política pública por una internet segura para niños, niñas y adolescentes*. https://www.igualdad.gob.ec/wp-content/uploads/downloads/2020/09/pol%C3%ADtica_publica_internet_segura.pdf

Mostak, T. (2021, March 15). *What is a Data Network?* HEAVY.AI. https://www.heavy.ai/technical-glossary/data-network

OPNsense. (2023). *About OPNsense - High-end Security Made Easy™*. https://opnsense.org/about/about-opnsense/

Oracle. (2018). *Oracle Agile Engineering Data Management/Security Guide for Agile, Release e6.2.1.0*. https://docs.oracle.com/cd/E89228_03/otn/pdf/install/html_edmsc/output/title.htm

Orange Cyberdefense. (2017, December 7). *WAF vs NGFW*. https://orangecyberdefense.com/be/blog/infrastructure/waf-vs-ngfw/

Pokrovskaia, N. N., & Snisarenko, S. O. (n.d.). *Social Engineering and Digital Technologies for the Security of the Social Capital'development*.

Puerta, G., Piñeros, S., & Franco, A. (2008). *Temas de psiquiatría infantil y del adolescente desde el modelo biopsicosocial. (3ª cartilla)*. Bogotá: Universidad El Bosque.

Robb, M. (2021). *Los niños usan cada vez más los dispositivos móviles: nuevo estudio de Common Sense*. Common Sense Media. https://www.commonsensemedia.org/es/articulos/los-ninos-usan-cada-vez-mas-los-dispositivos-moviles-nuevo-estudio-de-common-sense

Salahdine, F., & Kaabouch, N. (n.d.). *future internet Social Engineering Attacks: A Survey*. https://doi.org/10.3390/fi11040089

Shah, N. (2021, July 30). *Redefining Next-Generation Firewalls*. https://www.fortinet.com/blog/business-and-technology/redefining-next-generation-firewalls

Shea, S. (2021). *Software-Defined Perimeter (SDP)*. Network Securit. https://www.techtarget.com/searchcloudcomputing/definition/software-defined-perimeter-SDP

Shea, S., Gillis, A., & Clark, C. (2021, August 2). *What is Cybersecurity? Everything You Need to Know*. TechTarget. https://www.techtarget.com/searchsecurity/definition/cybersecurity

Slattery, T., & Burke, J. (2020). *What is a VLAN (Virtual LAN)?* Techtarget. https://www.techtarget.com/searchnetworking/definition/virtual-LAN

SolarWinds. (2021). *What Is a Network Node?* IT Glossary . https://www.solarwinds.com/resources/it-glossary/network-node

Sunney Valley Networks. (2020, June). *What is a Next-Generation Firewall (NGFW)*. https://www.sunnyvalley.io/docs/network-security-tutorials/next-generation-firewall

Tanenbaum, A. S. (2003). *Redes de computadoras*. Pearson educación.

UNIR. (2020, July 30). *Seguridad perimetral informática: objetivos y plataformas recomendables*. UNIR REVISTA. https://www.unir.net/ingenieria/revista/seguridad-perimetral-informatica/

UNISERVE. (2020). *Securing Your Network Perimeter*. Uniserve IT Solutions. https://uniserveit.com/blog/securing-your-network-perimeter

Vega Velasco, W. (n.d.). *POLITICAS Y SEGURIDAD DE LA INFORMACION*.

Wong, H., & Luo, T. (2020). *Man-in-the-Middle Attacks on MQTT-based IoT Using BERT Based Adversarial Message Generation.* https://github.com/HenryCWong/adversarialBERTMessages

World Wide Technology. (2021, September 20). *What Is a Data Network? Understanding the Types and Benefits of Data Networks*. https://www.wwt.com/article/what-is-a-data-network

Yasar, K. (2021, July 23). *Information Security Management System (ISMS)*. https://www.techtarget.com/whatis/definition/information-security-management-system-ISMS

Anexos

Anexo 1. Encuesta aplicada

1) ¿Considera factible el desarrollo de un sistema que minimice el riesgo que corren los menores al navegar por internet dentro de su red domestica?
    - Si
    - No

2) ¿Considera que implementar un sistema de protección (Dispositivo Firewall de Siguiente Generación) dentro de su red domestica ayudará a monitorear y controlar lo que los menores hacen en Internet cuando no están bajo su supervisión?
    - Si
    - No

3) En cuanto al tipo de dispositivos con acceso a Internet que los menores en su hogar utilizan. ¿Cuáles son?
    - Smartphone
    - Tablet
    - Consola de Videojuegos
    - SmartTV
    - PC o Laptop
    - Ninguno

4) En cuanto al tipo de conexión que los dispositivos utilizan en su domicilio. ¿Cuáles de las siguientes opciones usted utiliza?
    - Red Inalámbrica (Wifi)
    - Red Cableada (Ethernet)
    - Datos Móviles
    - Ninguna

5) En cuanto al tipo de actividad (Navegación Web) que se realiza en su domicilio. ¿Cuál de las siguientes opciones se visitan con frecuencia?
    - Redes Sociales (Facebook, Instagram, TikTok, etc)
    - Juegos en Línea (Roblox, Minecraft, Free Fire, etc)
    - Sitios Educativos (Teams, Google Classroom, Zoom, etc)
    - Correo Electrónico (Outlook, Gmail, etc)
    - Aplicaciones de Streaming (Netflix, HBO Max, Disney+, Youtube, etc)
    - Salas de Chat (Omegle, ChatRandom, ChatRoulette, etc)
    - App de mensajería (Messenger, Whattsapp, Telegram, etc)
    - Sitios web para adultos. (Xvideos, PornHub, CAM4, etc)
    - Sitios de descarga de contenido (Software crackeado, juegos piratas, series y películas)

6) En cuanto al tipo de actividad (Navegación Web) que se realiza en su domicilio. ¿Cuál de las siguientes opciones considera no son aptas para los menores mientras navegan en Internet?
    - Redes Sociales (Facebook, Instagram, TikTok, etc)
    - Juegos en Línea (Roblox, Minecraft, Free Fire, etc)
    - Sitios Educativos (Teams, Google Classroom, Zoom, etc)
    - Correo Electrónico (Outlook, Gmail, etc)
    - Aplicaciones de Streaming (Netflix, HBO Max, Disney+, Youtube, etc)
    - Salas de Chat (Omegle, ChatRandom, ChatRoulette, etc)
    - App de mensajería (Messenger, Whattsapp, Telegram, etc)
    - Sitios web para adultos. (Xvideos, PornHub, CAM4, etc)

- Sitios de descarga de contenido (Software crackeado, juegos piratas, series y películas)

7) Considera usted importante la implementación del Filtrado y Control de Acceso a Contenidos para permitir o bloquear el ingreso a sitios web de adultos, redes sociales o sitios web específicos de acuerdo con el tipo de usuario dentro de su red (menores o adultos).
   - Si
   - No

8) Considera usted que se deben crear redes inalámbricas para cada tipo de usuario (Red Wifi para menores con contenidos bloqueados y red Wifi para adultos con libre acceso a cualquier sitio web).
   - Si
   - No

9) Considera usted que cada usuario disponga de sus propias credenciales de acceso (Usuario y contraseña) para conectarse a la red.
   - Si
   - No

10) En cuanto al tamaño del dispositivo. ¿Cuál de las siguientes opciones usted considera como adecuada?
   - Debe ser pequeño (Como un Router aproximadamente)
   - Debe ser mediano (Como un MiniPC aproximadamente)
   - Debe ser grande (Como un Gabinete de PC Aproximadamente)
   - El tamaño del dispositivo me es indiferente.

11) En cuanto al consumo de energía. ¿Cuál de las siguientes opciones usted considera como adecuada?
   - Debe consumir poca energía
   - Debe consumir la energía que sea necesaria
   - El consumo de energía me es indiferente.

12) En cuanto al tiempo de funcionamiento del sistema. ¿Cuál de las siguientes opciones usted considera como adecuada?
   - Debe funcionar solo en la mañana
   - Debe funcionar solo en la tarde
   - Debe funcionar solo en la noche
   - Debe funcionar todo el tiempo

13) En cuanto a la gestión del sistema. ¿Cuál de las siguientes opciones usted considera como adecuada?
   - Solo el administrador del sistema puede aplicar cambios en el funcionamiento del dispositivo.
   - El padre de familia o la persona a cargo de los menores puede aplicar cambios en el funcionamiento del dispositivo.

14) En cuanto a la interfaz gráfica del sistema. ¿Cuál de las siguientes opciones usted considera como adecuada?
   - Debe ser intuitiva de usar para cualquier usuario.
   - Debe poder visualizarse desde cualquier dispositivo con un navegador web (Chrome, Edge, Firefox, Safari)
   - No deseo acceder a las configuraciones del sistema.

15) En cuanto al uso y configuración del sistema. ¿Considera usted que se le deberían proporcionar manuales de usuario para la configuración de las funciones del sistema, tales como: bloqueo y desbloqueo de sitios web, cambio de contraseñas, ¿gestión de usuarios?
    - Si
    - No

16) En cuanto a los informes generados por el sistema. ¿Que desearía usted poder conocer acerca de la actividad en su red?
    - Amenazas Bloqueadas
    - Páginas Web Accedidas
    - Páginas Web Bloqueadas
    - Tiempo de navegación por usuario

17) En cuanto a la frecuencia de los informes generados por el sistema (Páginas web accedidas o bloqueadas, tiempo de uso de internet). ¿Cuál de las siguientes opciones usted considera como adecuada?
    - Diarios
    - Semanales
    - Quincenales
    - Mensuales
    - Solo cuando se los requiera

Anexo 2. Resultados y Análisis de la encuesta

Pregunta 1. En la primera pregunta realizada el resultado obtenido demostró que el 100% de los encuestados consideran factible el desarrollo del proyecto propuesto. La Figura 74 muestra la tabulación de los datos obtenidos.

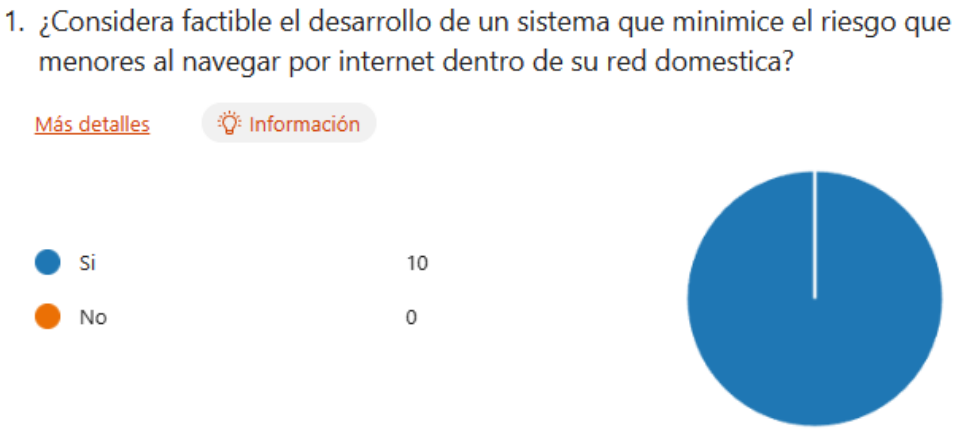


Figura 74. Resultados de la 1ra pregunta de la encuesta

Fuente: Autor del proyecto

Pregunta 2. En la segunda pregunta realizada el resultado obtenido demostró que el 100% de los encuestados consideran que implementar un sistema de protección ayudará a controlar y monitorear lo que hacen los menores en la red. La Figura 75 muestra la tabulación de los datos obtenidos.

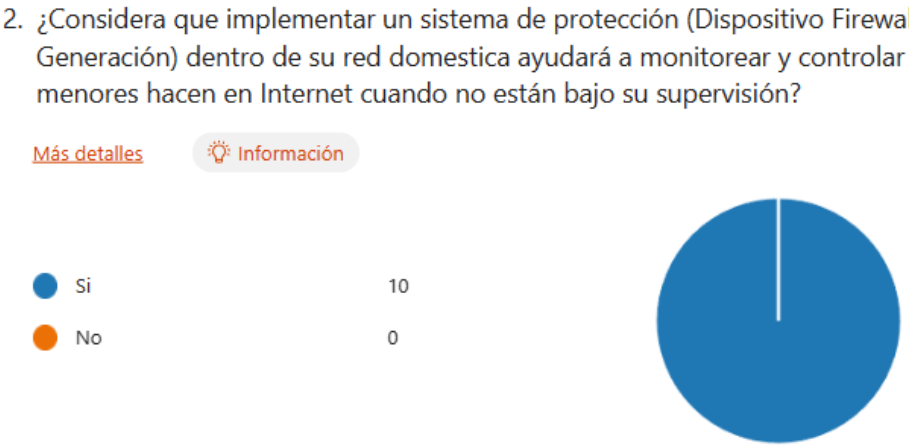


Figura 75. Resultados de la 2da pregunta de la encuesta

Fuente: Autor del proyecto

Pregunta 3. En la tercera pregunta realizada el resultado obtenido demostró que el 100% de los encuestados consideran factible el desarrollo del proyecto propuesto. La Figura 74 muestra la tabulación de los datos obtenidos.

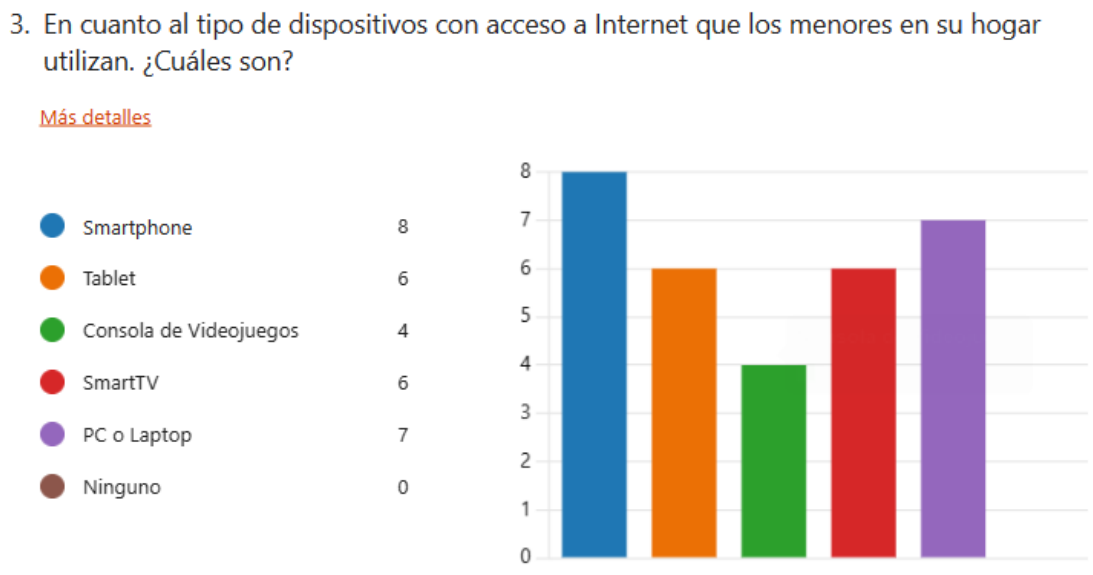


Figura 76. Resultados de la 3ra pregunta de la encuesta

Fuente: Autor del proyecto

Pregunta 4. En la cuarta pregunta realizada el resultado obtenido demostró que el 100% de los encuestados utiliza una conexión a internet de tipo inalámbrica para sus dispositivos, seguido por 8 que eligen una conexión cableada. La Figura 77 muestra la tabulación de los datos obtenidos.

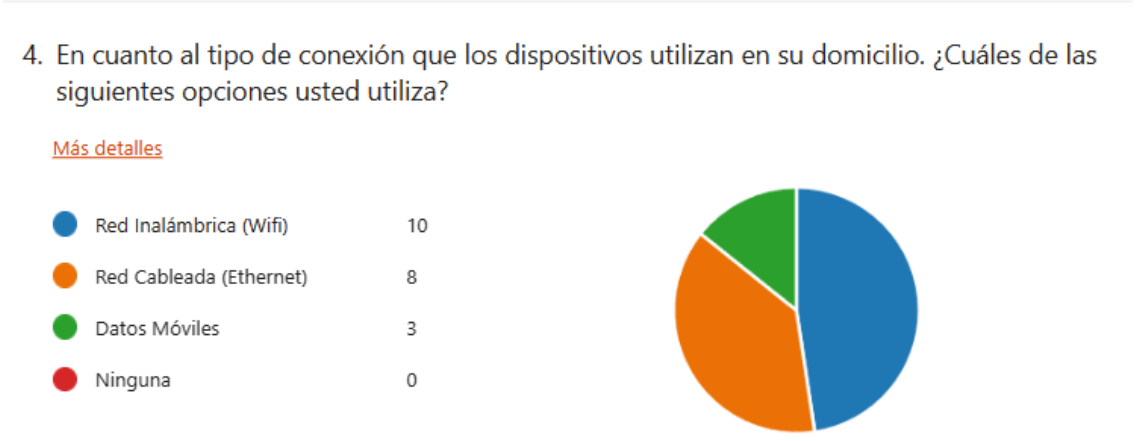


Figura 77. Resultados de la 4ta pregunta de la encuesta

Fuente: Autor del proyecto

Pregunta 5. En la quinta pregunta realizada el resultado de la encuesta mostró que el tipo de actividad más frecuente en los usuarios encuestados es para redes sociales juegos en línea, aplicaciones de streaming y mensajería, mientras que los menos frecuentes son los sitios web para contenido adulto o sitios de descargas. La Figura 78 muestra la tabulación de los datos obtenidos.

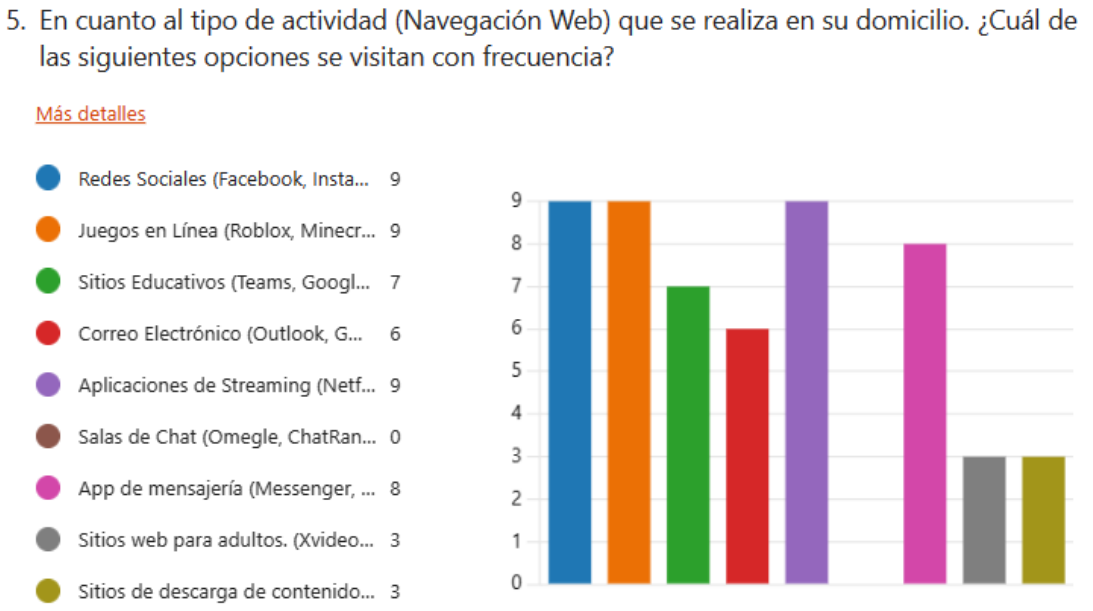


Figura 78. Resultados de la 5ta pregunta de la encuesta

Fuente: Autor del proyecto

Pregunta 6. En la sexta pregunta realizada los resultados muestran que la mayoría de los encuestados concuerdan que paginas como redes sociales, salas de chat, sitios para adultos y sitios de descargas no son páginas aptas para niños que tienen acceso a internet. La Figura 79 muestra la tabulación de los datos obtenidos.

Figura 79. Resultados de la 6ta pregunta de la encuesta

Fuente: Autor del proyecto

Pregunta 7. En la séptima pregunta realizada en la encuesta se determinó que 9 de los 10 encuestados considera importante la implementación de un sistema de filtrado y control de acceso en la red para monitorear la actividad de los menores en el hogar. La Figura 80 muestra la tabulación de los datos obtenidos.

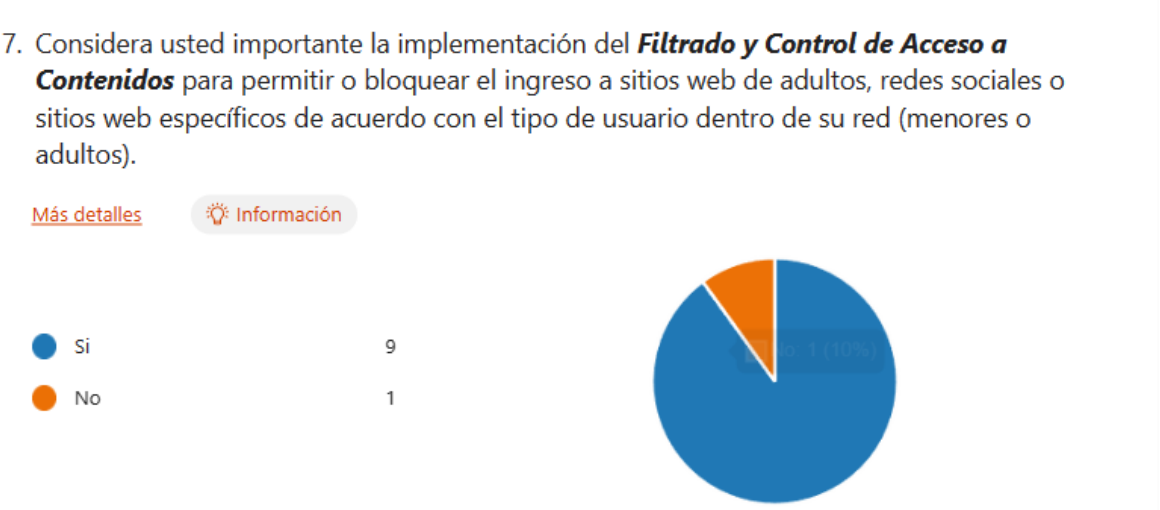


Figura 80. Resultados de la 7ma pregunta de la encuesta

Fuente: Autor del proyecto

Pregunta 8. En la octava pregunta realizada en la encuesta el 100% de los encuestados está de acuerdo con que se deben crear redes inalámbricas independientes para cada tipo de usuario, en donde solo se brinde acceso libre o restringido de acuerdo a la red vinculada. La Figura 81 muestra la tabulación de los datos obtenidos.

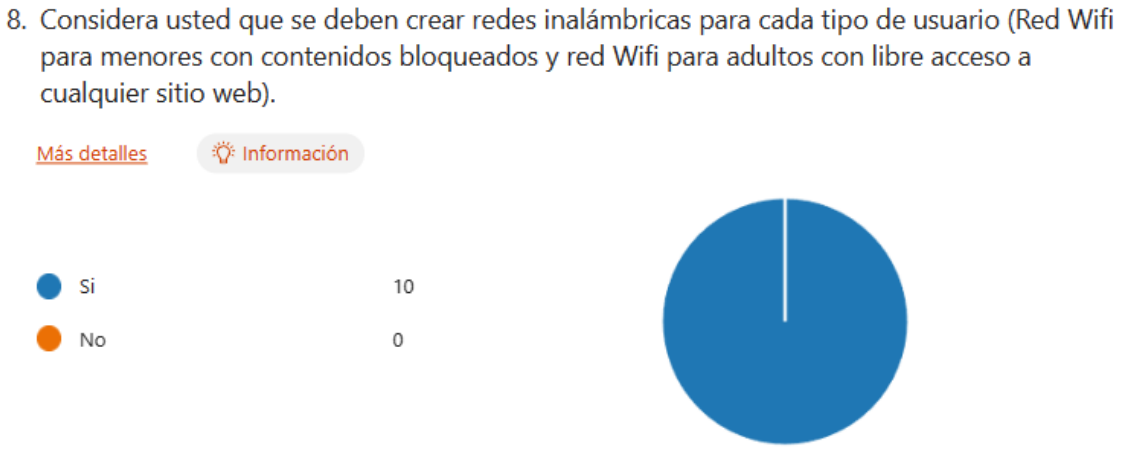


Figura 81. Resultados de la 8va pregunta de la encuesta

Fuente: Autor del proyecto

Pregunta 9. En la novena pregunta realizada en la encuesta el 80% concuerda que cada usuario debe contar con credenciales de usuario únicas para el acceso a la red, mientras que el 20% restante no está de acuerdo. La Figura 82 muestra la tabulación de los datos obtenidos.

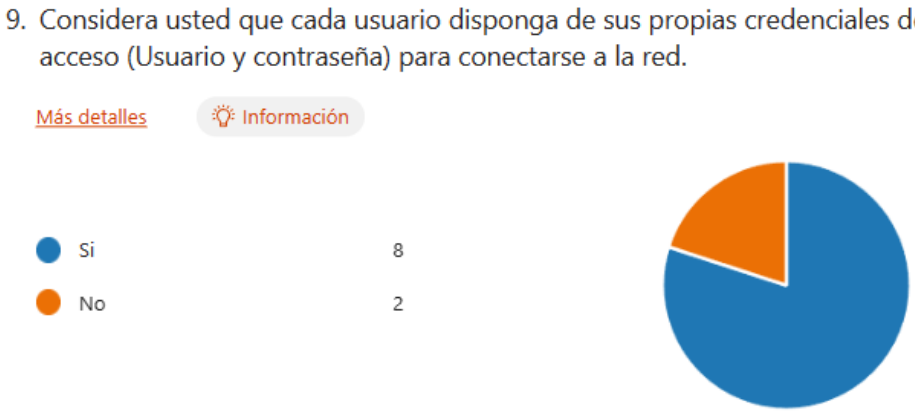


Figura 82. Resultados de la 9na pregunta de la encuesta

Fuente: Autor del proyecto

Pregunta 10. En la décima pregunta realizada en la encuesta el 50% de los encuestados opinan que el dispositivo debe ser compacto, mientras que el 30% le es indiferente el tamaño del dispositivo. La Figura 83 muestra la tabulación de los datos obtenidos.

Figura 83. Resultados de la 10ma pregunta de la encuesta

Fuente: Autor del proyecto

Pregunta 11. En la onceaba pregunta realizada en la encuesta, 6 de los 10 encuestados concuerda que el dispositivo implementado debe consumir poca energía eléctrica, mientras que 3 opinan que debe consumir la energía necesaria y 1 de los encuestados opina que le es indiferente el consumo total del dispositivo. La Figura 84 muestra la tabulación de los datos obtenidos.

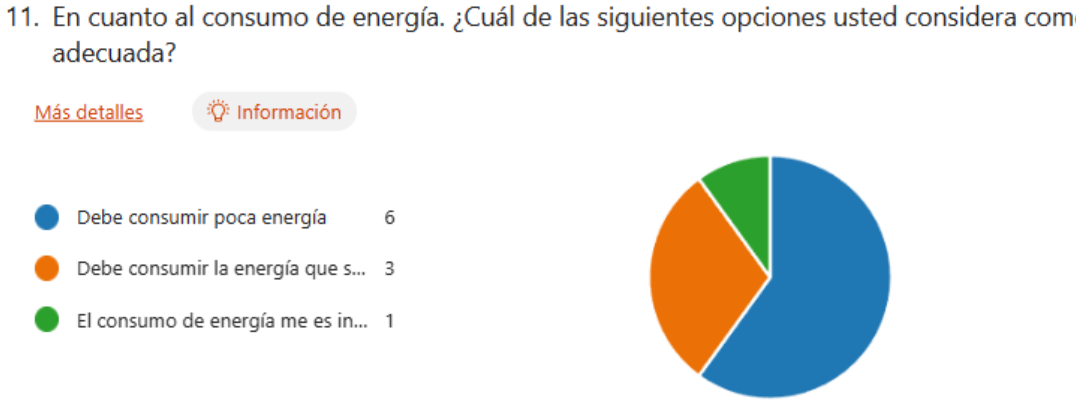


Figura 84. Resultados de la 11va pregunta de la encuesta

Fuente: Autor del proyecto

Pregunta 12. En la doceava pregunta realizada en la encuesta el 100% de los encuestados coincide en que el sistema debe permanecer en funcionamiento las 24 horas del día ininterrumpidamente. La Figura 85 muestra la tabulación de los datos obtenidos.

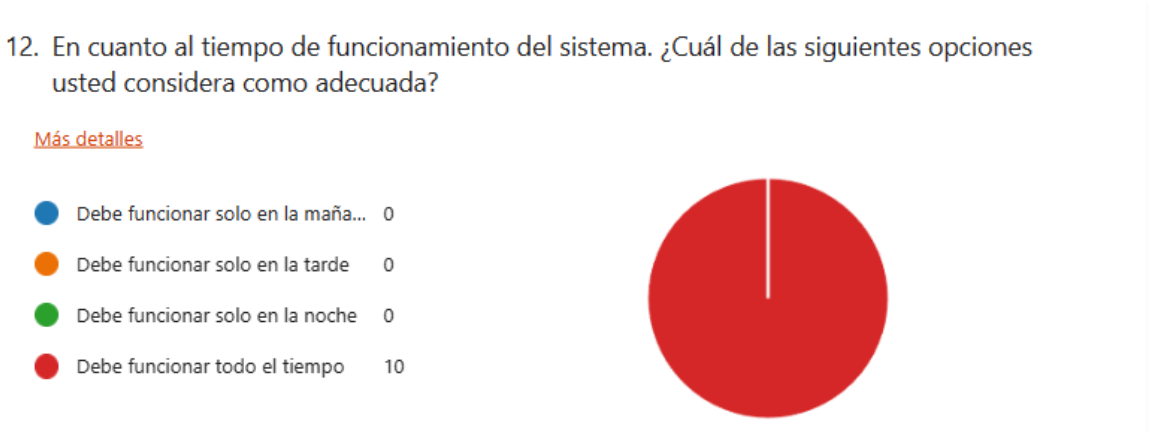


Figura 85. Resultados de la 12va pregunta de la encuesta

Fuente: Autor del proyecto

Pregunta 13. En la decimotercera pregunta realizada en la encuesta los resultados muestran que el 80% de los encuestados necesitan poder acceder a la administración del dispositivo por cuenta propia, mientras que el 20% dice que únicamente el administrador del sistema debería poder modificar las configuraciones. La Figura 86 muestra la tabulación de los datos obtenidos.

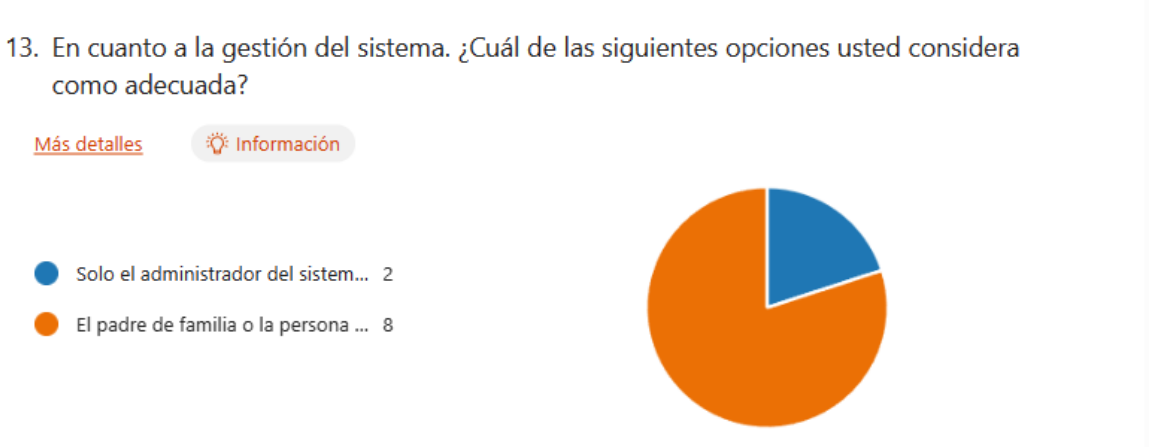


Figura 86. Resultados de la 13va pregunta de la encuesta

Fuente: Autor del proyecto

Pregunta 14. En la decimocuarta pregunta realizada en la encuesta 7 de los 10 de los encuestados dice que la interfaz de usuario del sistema debe ser intuitiva y fácil de usar, 4 de los 10 plantea que esta debe poder visualizarse desde cualquier dispositivo independiente de la plataforma o sistema operativo y 2 de los 10 dicen que no desean ingresar a las configuraciones del sistema. La Figura 87 muestra la tabulación de los datos obtenidos.

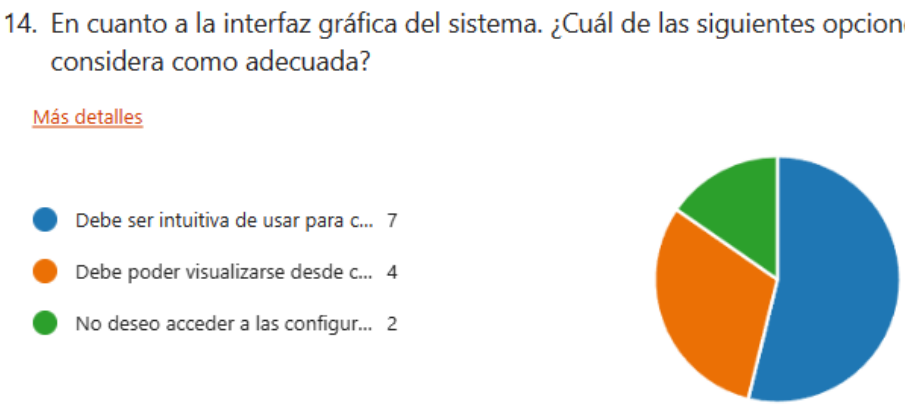


Figura 87. Resultados de la 14va pregunta de la encuesta

Fuente: Autor del proyecto

Pregunta 15. En la decimoquinta pregunta realizada en la encuesta el 100% de los encuestados requiere que se le proporcionen manuales de usuario para la configuración de las funciones básicas y elementales del sistema para un correcto uso. La Figura 88 muestra la tabulación de los datos obtenidos.

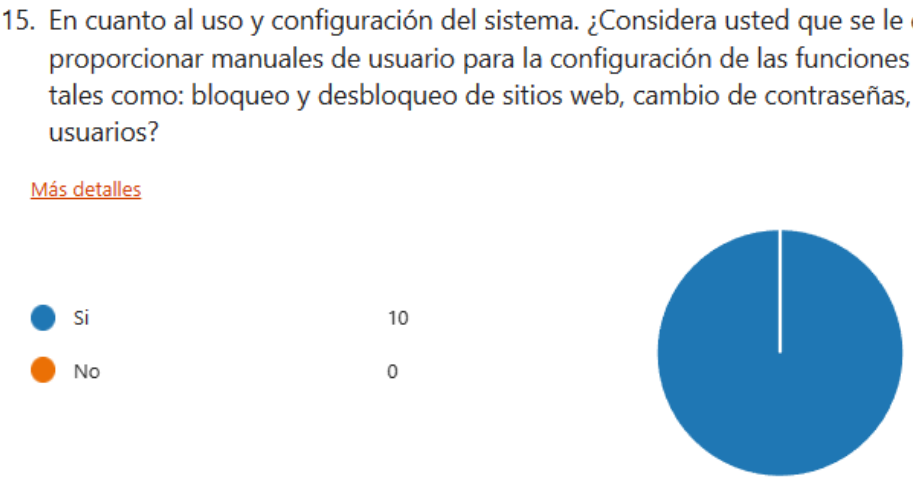


Figura 88. Resultados de la 15va pregunta de la encuesta

Fuente: Autor del proyecto

Pregunta 16. En la decimosexta pregunta realizada en la encuesta 8 de los 10 encuestados necesitan conocer en los informes generados las amenazas y páginas web que han sido bloqueadas luego de un intento de acceso, mientras que 6 de los 10 encuestados quieren conocer a que páginas si tuvieron acceso, por último 5 de 10 encuestados quieren conocer el tiempo de navegación de los usuarios. La Figura 89 muestra la tabulación de los datos obtenidos.

Figura 89. Resultados de la 16va pregunta de la encuesta

Fuente: Autor del proyecto

Pregunta 17. En la decimoséptima pregunta realizada en la encuesta el 60% de los encuestados necesitan que se realice informes de actividad semanales, mientras que el 30% dice que estos deben ser generados únicamente cuando el usuario los requiera. La Figura 90 muestra la tabulación de los datos obtenidos.

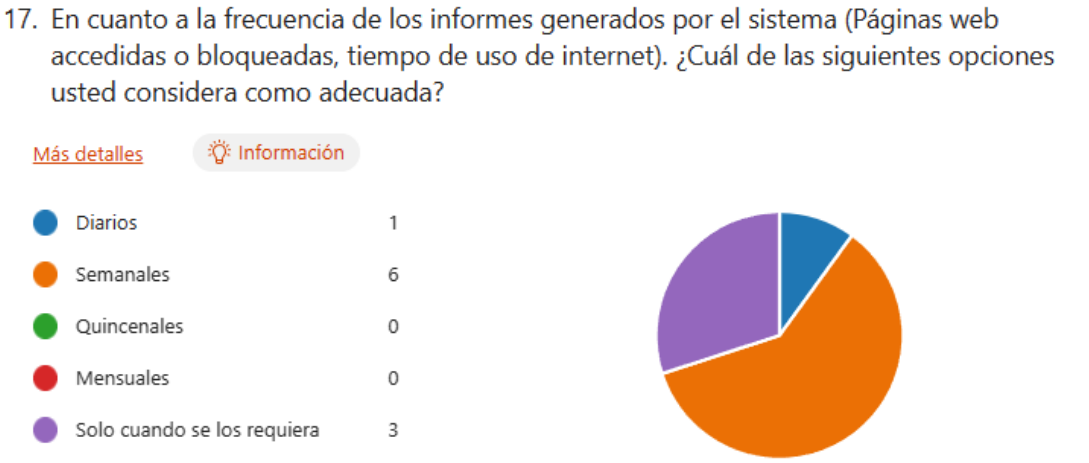


Figura 90. Resultados de la 17va pregunta de la encuesta

Fuente: Autor del proyecto