UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE INFORMÁTICA

TRABAJO DE TITULACIÓN

Propuesta Tecnológica, previo a la obtención del Título de:

INGENIERO EN SISTEMA

"Implementación del Software de control de tráfico de red "NM Traffic" para que detecte los posibles problemas de comunicación alámbrica o inalámbrica aplicable al área de Tecnología en la empresa AGUAPEN EP"

AUTOR
ISAAC EMANUEL RIVERA SUÁREZ

PROFESOR O TUTOR
LSI. DANIEL QUIRUMBAY YAGUAL, MSIA

LA LIBERTAD – ECUADOR
2017

AGRADECIMIENTO

El autor de este presente trabajo desea agradecer a:

En primer lugar le agradezco de todo corazón a Dios por darme las fuerzas, la inteligencia, el valor y el coraje para seguir adelante y permitirme terminar este camino de todos los obstáculos que se me presentarón para alcanzar esta meta.

Un especial agradecimiento a mis padres quienes han sido el pilar fundamental en mi vida, mi querida madre, Sila Suárez, porque ella busca lo mejor para mí, y además me hizo una persona de valores y principios para mi vida. A mí querido padre, Placido Rivera, porque me brindó una oportunidad de realizar los estudios y de una u otra manera me ayudó cada día para poder alcanzar este objetivo.

De la misma forma un agradecimiento muy especial a mi querida novia, Evelyn Rodríguez, por quererme, ayudarme siempre, por apoyarme, por su preocupación siempre de una manera muy especial.

Gracias a todas las personas que me ayudarón de alguna manera u otra alcanzar y cumplir mi meta: amigos, docentes y autoridades de esta prestigiosa institución y específicamente a la gran ayuda del Lsi. Daniel Quirumbay, que me colaboró en la realización de este trabajo.

Y por último le agradezco a la Empresa AGUAPEN EP que me abrió sus puertas y me brindó su confianza para poder realizar este trabajo de titulación.

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del trabajo de investigación, "IMPLEMENTACIÓN DEL SOFTWARE DE CONTROL DE TRÁFICO DE RED "NM TRAFFIC" QUE DETECTE LOS POSIBLES PROBLEMAS DE COMUNICACIÓN ALÁMBRICA O INALÁMBRICA APLICABLE AL ÁREA DE TECNOLOGÍA EN LA EMPRESA AGUAPEN EP", elaborado por el Sr. **ISAAC EMANUEL RIVERA SUÁREZ**, egresado de la Carrera de Informática, Escuela de Informática, Facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena, previo a la obtención del Título de Ingeniero en Sistemas, me permito declarar que luego de haber orientado, estudiado y revisado, la Apruebo en todas sus partes.

La Libertad, 06 de Marzo del 2017

…….

Lsi. Daniel Quirumbay Yagual, Msia

TRIBUNAL DE GRADO

Ing. Mariuxi de la Cruz, MSIG **Decana Facultad Sistemas y Telecomunicaciones**	Ing. Shrendry Rosero Vásquez, MSc **Director Carrera de Informática**
Lsi. Daniel Quirumbay Yagual, MSIA **Profesor Tutor**	Ing. Iván Coronel Suárez, MSIA **Profesor Área**

Abg. Brenda Reyes Tómala, MSc.
Secretaria General

RESUMEN

El presente trabajo propone la creación de un sistema de monitoreo, control de tráfico de red y el apoyo a un manejo óptimo del ancho de banda con la ayuda de lenguaje de programación y en conjunto con una base de datos para permitir el uso de la interfaz visual a ser utilizada por los administradores, donde se podrá observar información relacionada al tráfico de la red, monitoreo de equipos y sondeos de canales WIFI como: capturas en tiempo real del tráfico de los paquetes de datos, detección de direcciones IP y MAC y conocer los canales de los Access Point por medio de texto o de forma gráfica. El aplicativo contará también con un módulo de administración para controlar la información de los usuarios y administradores, es decir, poder tener un acceso a la creación, modificación, eliminación de los mismos.

La información capturada del tráfico de la red será almacenada en una base de datos, con esta información registrada se podrá realizar reportes de forma estadística para que el administrador haga su propio análisis para la toma de decisiones.

Para la creación de este proyecto se utilizó lenguaje de programación Visual Studio 2015 junto con una base de datos MySQL Workbench, este software será desarrollado bajo aplicativo de escritorio, es decir, solo será utilizado en ambiente de Windows, para llevar a cabo este software se harpa uso de librerías relacionadas al tráfico como: Pcap y WinPcap que ayudarán a obtener los paquetes de información.

La aplicación será destinada al Área de Tecnología de la empresa AGUAPEN EP, esta herramienta servirá de apoyo, porque además de realizar un escaneo de tráfico de red contiene otras funciones para los administradores que conforman este departamento y que harán uso de ella, este software como se mencionó no solo ayudará a realizar un monitoreo de tráfico sino también de escanear los equipos, niveles de ancho de banda y canales de las redes inalámbricas. Este aplicativo tendrá una interfaz sumamente interactiva, amigable y fácil comprensión para que el usuario pueda navegar de manera sencilla y rápida.

ABSTRACT

This project consists of the design and implementation of an application for monitoring, network traffic control, optimal bandwidth management for the company AGUAPEN EP, the application will be able to provide real-time captures of the traffic of information packets By means of text or graphics, as well as providing other options such as the scanning of computers that will serve to know the PCs that are connected to the local network and that will help to be able to filter the traffic through this information obtained, also includes the Scanning of the visible and near WIFI wireless networks to know in which channel it is working and finally, the query function of both the upload and download bandwidth levels of the local computer. The network traffic capture will be stored in the database in case the user chooses this storage option, this information will be displayed in a statistical way for the user to make their own analysis for decision making.

For the creation of this project was used programming language Visual Studio 2015, this software will be developed under desktop application because it will only be used in Windows environment, to carry out this process will be added and will use libraries such as Pcap and WinPcap that will help In order to obtain the data packets, in terms of storage will be used MySQL Workbench database.

The application will be destined to the Technology Area of the company AGUAPEN EP, this tool will serve as support, because in addition to performing a scan of network traffic contains other functions for the user and for the administrators that make up this department and that will make use of it , This software as mentioned will not only help to perform a traffic monitoring but also to scan the equipment, bandwidth levels and channels of the wireless networks. This application will have an extremely interactive interface, friendly and easy to understand so that the user can navigate easily and quickly.

DECLARACIÓN

El contenido del presente Trabajo de Graduación es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.

Isaac Emanuel Rivera Suárez

TABLA DE CONTENIDOS

ÍNDICE DE GRÁFICOS

ITEM DESCRIPCIÓN PÁGINA

ÍNDICE DE TABLAS

ITEM DESCRIPCIÓN **PÁGINA**

LISTA DE ANEXOS

N.- DESCRIPCIÓN

ABREVIATURAS

ACK: Acknowledgement, Acuse de Recibo

AIM: AOL Instant Messenger

ARP: Address Resolution Protocol, Protocolo de Resolución de Direcciones

ASCII: American Standard Code for Information Interchange, Código Estadounidense Estándar para el Intercambio de Información

DHCP: Dynamic Host Configuration Protocol, Protocolo de Configuración Dinámica de Host

DNS: Domain Name System, Sistema de Nombres de Dominio

DoS: Denegation of Service**,** Denegación de Servicio

FTP: File Transfer Protocol, Protocolo de transferencia de archivos

HTML: HyperText Markup Language, Lenguaje de Marcado de Hipertexto.

HTTP: Hypertext Transfer Protocol, Protocolo de Transferencia de Hipertexto

HTTPS: Hyper Text Transfer Protocol Secure, Protocolo Seguro de Transferencia de Hipertexto

ICMP: Internet Control Message Protocol, Protocolo de Mensajes de Control de Internet

IDE: Integrated Development Environment, Entorno de Desarrollo Integrado.

IEEE: Institute of Electrical and Electronics Engineers, Instituto de Ingenieros Eléctricos y Electrónicos

IGMP: Internet Group Management Protocol

IMAP: Internet Message Access Protocol, Protocolo de red de acceso a mensajes electrónicos

IPv4: Internet Protocol version 4, Protocolo de Internet versión 4

SSPD: Simple Service Discovery Protocol, Protocolo Simple de Descubrimiento de Servicios

NBNS: Nombre de Servicios NetBIOS

INTRODUCCIÓN

El administrador de la red hoy en día debe preocuparse en mantener de forma correcta el tráfico generado por los equipos conectados, realizando diferentes monitoreos, pero por falta de tiempo, recursos o por desconocimiento en tecnologías de software apropiados, se llega a enfrentar en muchas ocasiones a la pérdida de rendimiento por diferentes causas o motivos: ingreso de intrusos, lentitud o virus, trayendo así complicaciones como colapsos, congestionamientos o pérdidas de información. En una red WIFI, cada vez que existe interferencia se debe a que el canal está cubierto por otras redes inalámbricas. El administrador tiene la responsabilidad de colocar a cada red inalámbrica en un canal diferente, de acuerdo a los estándares que recomienda la red Wireless 802.11 para así evitar problemas: no tener acceso a la red, pérdida de información y navegación al internet, etc.

En el departamento de Tecnología de la empresa AGUAPEN EP, existen herramientas para el monitoreo y control del tráfico de la red, cada uno de estos softwares contiene una única función, el administrador tiene que hacer un análisis y observación a fondo de cada resultado obtenido para llegar a una sola conclusión para la toma de decisiones. Cada una de estas herramientas tiene su forma de interpretar el tráfico de la red o escaneo de equipos, gráficamente o por texto pero no es amigable ni entendible para el administrador. Además dentro del departamento no cuentan con una herramienta de escritorio para monitorear las redes inalámbricas y saber en qué canal están trabajando cada una de ellas.

Debido a lo anteriormente mencionado se requiere desarrollar e implementar una herramienta para analizar el tráfico de la red, monitoreo de equipos conectados, escaneo de canales de las redes inalámbricas Wireless 802.11, utilizando tecnologías de desarrollo y librerías que ayudarán a realizar un nuevo aplicativo de apoyo, para poder llevar los proceso de monitoreo, control de tráfico en la red, manejo óptimo del ancho de banda y control de canales de las redes WIFI para los miembros del área de tecnología de la empresa AGUAPEN EP.

CAPÍTULO I

INTRODUCCIÓN

1.1 Antecedentes

En la Empresa AGUAPEN EP, en el Departamento de TIC donde se realizán los monitoreos, controles y sondeos de todos los paquetes de información que transitan a través de la red que son generados por los equipos conectados en los diferentes departamentos, el administrador se enfrenta a esta situación de llevar la responsabilidad de que se genere un tráfico correcto y fluido en la red. En muchas ocasiones por falta de tiempo, recursos o desconocimiento de herramientas de monitoreo no se puede llegar a entender y encontrar las causas del problema trayendo complicaciones como perdida de rendimiento, lentitud, congestionamiento, cuellos de botellas y problemas de virus. Hoy en día existen nuevos avances en tecnología de software para llevar acabo estos procesos, pero para obtener todos los beneficios o servicios del aplicativo se debe hacer un pago por la licencia, en muchas ocasiones dejan de utilizar estas aplicaciones debido a que se vence el tiempo de gratuidad o porque solo posee un modo de texto no amigable ni entendible para el usuario y este debe estar observando y analizando para llegar a comprender dónde está el problema en la red, siendo estas las razones fundamentales por la cual dejan de llevar un monitoreo.

Además estas herramientas que se utilizan no llevan un registro de almacenaje de información de todos los usuarios y del equipo que está usando. Para llevar un control de que quien está provocando inconvenientes en la red, se debe utilizar varias herramienta de monitoreo para solo ver qué dirección IP es el que ocasiona el problema, eso lleva tiempo porque debe realizar una consulta en los documentos históricos que en muchos de los casos se llevan en papel.

El responsable de la red actualmente posee 2 o 3 herramientas para realizar los diferentes monitoreos, análisis, detección de errores y sondeos del tráfico. Cada una de estas herramientas genera un solo resultado y en conjunto es analizado esta información para llegar a una sola conclusión y poder tomar las decisiones respectivas para corregir el problema que se presentó en la red, además estos aplicativo no posee un módulo en donde se puedan registrar los empleados con su respectivo equipo de trabajo en donde incluye la dirección IP, dirección MAC y responsable que son los más importante, este proceso se realiza de forma manual y en el momento de realizar una verificación de IP y de usuario lleva tiempo realizarlo este proceso porque se debe ir verificando cada dirección IP hasta llegar al que se está requiriendo.

Además el encargado de la red no posee una herramienta, la cual ayude a observar en que canal están trabajando sus redes inalámbricas WIFI, lo que podría causar interferencias en las demás, y esto lleva a tener un mal rendimiento en el internet como la velocidad de navegación o conexión lenta y problema de acceso a la red.

Es por eso que se propone como una posible solución, el desarrollo de un sistema de monitoreo, control de tráfico de la red local donde se pueda visualizar en forma sencilla toda la información de los paquetes trasportados, para así detectar posibles inconvenientes en la red en los diferentes departamentos de la empresa AGUAPEN EP, y además de integrar otra función como es el módulo de control de los canales de las redes WIFI.

Para realizar una mejora la herramienta delimitará un módulo específico para el ingreso de información del personal que hará uso de la red local evitando pérdida de tiempo en buscar a través de la dirección IP. El sistema contará con una base de datos la cual llevará almacenada esta información de cada una de esta persona con su respectivo equipo de trabajo solucionando los inconveniente a la hora de realizar una búsqueda y optimizar el tiempo de respuesta, y de manera inmediata da a conocer al usuario que se requiere o que está haciendo mal uso de la red y del internet.

1.2 Descripción del proyecto

El presente proyecto de titulación “Sistema de control de tráfico de red que detecte los posibles problemas de comunicación alámbrica o inalámbrica” la cual ayudará a la empresa AGUAPEN EP a mantener el tráfico de la red de forma correcta y fluida para evitar problemas que se puedan presentar en la misma, además llevar un control del equipo de trabajo de cada uno de los empleados que se encuentre conectado a la red y de los canales de cada una de los Access Point.

En este presente proyecto se plantea como solución el diseño y desarrollo de un aplicativo para el monitoreo y análisis de tráfico de red para el Departamento de Tecnología, teniendo como objetivo principal llevar un control de los equipos de cada uno de los usuarios que hacen uso de ellas, además de mantener de forma correcta los diferentes canales que posee cada una de las redes inalámbrica WIFI, logrando una optimización, tanto para el tráfico como para el acceso al internet para la satisfacción de la empresa.

Con el desarrollo de este proyecto de monitoreo y control de tráfico de red se pretende que el usuario pueda observar los paquetes de información en tiempo real desde su propia pc, además esta información será almacenada en una base de datos para luego realizar reportes estadísticos diarios, quincenales o mensuales para la toma de decisiones. Con este proyecto se busca obtener una solución y mejora en el monitoreo, análisis y sondeo del tráfico de acuerdo a la problemática analizada, sus causas y sus objetivos que son los que ayudarán a dar una mejora en la actual forma de que llevan estos procesos.

Para la construcción de la aplicación de escritorio se necesita utilizar las siguientes tecnologías en software que se detallan a continuación:

- Sistema Operativo Windows 7
- Microsoft Visual Studio 2015
- Base de Datos MySQL

- WinPcap 4.1.3

1.3 Objetivos

1.3.1 Objetivo General

Implementar un sistema de control de tráfico de red que detecte los posibles problemas de comunicación alámbrica o inalámbrica para la empresa AGUAPEN EP con la ayuda de la plataforma de desarrollo Visual .Net 2015.

1.3.2 Objetivos Específicos

- Aplicar conceptos de seguridad en redes al momento de la creación de la herramienta de monitoreo y análisis de tráfico de red.
- Diseñar interfaz gráfica amigable que permita al usuario adaptarse de una forma rápida y sencilla con la aplicación.
- Diseñar reportes basado en la captura de información del análisis de tráfico de paquetes transportados en la red local.
- Realizar pruebas de diagnóstico para verificación del correcto funcionamiento de la herramienta.

1.4 Justificación

A pesar de las diversas formas que se han integrado a la red local para mejorar el rendimiento del tráfico o problemas de solapamientos en antenas inalámbricas en la empresa AGUAPEN EP, siempre existirán los avances en tecnologías en hardware como los dispositivos inalámbricos de alta frecuencia y cableado de alta velocidad para transmitir.

Estas tecnologías en hardware permiten regular el tráfico en la red, sin embargo, cuando un dispositivo inalámbrico o cable de red falle ya sea por estar desconectado, que supere el ancho de banda requerido o que se encuentre en mal estado, puede llegar a generar muchos inconvenientes como el bajo rendimiento del servicio de internet, colapsos en el tráfico de datos, solapamiento en las WIFI y pérdida de información.

El administrador es la persona encargada de mantener de manera fluida el tráfico de la red, control en los equipos de trabajo, conexiones a la red y canales de puntos de acceso al internet con la ayuda de diferentes herramientas para el monitoreo, análisis y sondeos de datos para encontrar y evitar las posibles falencias que se puedan presentar dentro de ella, pero por falta de tiempo, desconocimiento en tecnología en software o en la forma de mostrar los resultados la herramienta de manera en un texto no amigable dejan de hacer usos de ellas sin poder comprender y encontrar donde se generó dicho problema en la red, además esta persona lleva un control de registro de los equipos de trabajo y para realizar una consulta toma tiempo porque debe buscar en sus fuentes históricas hasta encontrarlo.

Es por esto que este proyecto se originó con el fin de detectar los problemas que se puedan originar en la red de la empresa AGUAPEN EP para que el administrador pueda tomar sus decisiones, dar soluciones a dichas fallas encontradas y mejorar el rendimiento del tráfico, conexiones y canales de puntos de acceso, además podrá optimizar los tiempos de respuestas para llevar un mejor control en los equipos de trabajo.

La herramienta que se va a desarrollar solo será de uso de la persona o personal encargado de administrar la red local. La necesidad de una aplicación de escritorio se da debido a que se monitoreará a todos los equipos conectados a la red, y que solo trabajan bajo ambiente de Windows.

Esta herramienta facilitará al encargado del departamento TIC y beneficiará a la empresa de que todos los usuarios conectados a la red lleven un buen uso de ella haciendo que el tráfico sea más fluido para evitar interrupciones en los procesos que realizán, además ayudará al administrador en mantener un buen uso del internet y de los canales de las redes WIFI.

Para una mejor perspectiva es necesario llevar un monitoreo de tráfico de paquetes de información, realizando reportes de forma digital cada día, quincenal o mensualmente para el análisis y que ayudarán a realizar auditorías de la red local e identificar fallas o problemas dentro de la misma ocasionadas por software o hardware. Además con esto permitirá al administrador saber con exactitud donde se generó dicha falla, problema o interferencia y de quien usuario está causando esto de que exista un tráfico no deseado en la red.

Esto beneficiará a la empresa y al encargado que hará uso de este servicio de llevar un buen uso de su red local además que los usuarios puedan ejercer sus procesos de trabajos de manera correcta.

1.5 Metodología

El presente trabajo de titulación efectuará una investigación exploratoria, debido a que ella permite basarse desde una problemática, hallar los datos más relevantes de esta y crear diferentes procesos o procedimientos de acuerdo a líneas de investigación, con la finalidad de resolver dicho problema. Además también se realizará una investigación de campo, debido a que esta investigación viene de la mano con el método de campo la cual posee técnicas que ayudaran a la recolección de información en el lugar de los hechos donde acontece el fenómeno para llevar a cabo en si el aplicativo de monitoreo de tráfico de la red de datos, sondeos de canales de redes WIFI y control de direcciones IP de cada equipo de acuerdo a los requerimientos que el usuario desee, estas técnicas que posee este método es la de observación, entrevistas y encuesta.

Técnicas e instrumentos de recolección de datos

El proceso para el desarrollo de este software se obtendrá mediante la técnica entrevista, la cual nos ayudará a reunir información relevante y necesaria mediante una conversación profesional para que ayuden a sustentar los procesos que se vayan a resolver y poder llegar a desarrollar el prototipo deseado.

Se aplicará otra técnica de recopilación de información al grupo del área de tecnología de la Empresa AGUAPEN EP, esta técnica documental definida como cuestionario, la cual nos ayudará a adquirir información, para ello se elaborará un respectivo cuestionario con preguntas relacionada al tráfico en la red y ancho de banda, como resultado de esto se podrá conocer la opinión, interés o criterio de este problema.

Se diseñará un modelo o formato de entrevista la cual ayudará a sacar conclusiones específicas, para evaluar el conocimiento y utilización de software analizadores de redes que realicen control y monitoreo de la red local.

Población

El tamaño de la población de investigación está constituido por los trabajadores que conforman el departamento de TI de la empresa AGUAPEN EP con un total de 5 personas, y se describen a continuación:

TI	Cantidad
Jefe de Sistema	1
Administrador	1
Programadores	2
Soporte Técnico	1

Tabla 1: Personal de TI

Con este total de 5 personas, son los que se trabajará, sin embargo las personas beneficiarias indirectas serán todas las personas que conforma la empresa AGUAPEN

EP y los beneficiarios directos serán las 5 personas a la que se realizará la entrevista porque son ellos quienes manejarán y harán uso del aplicativo de monitoreo.

La entrevista está dirigida a la empresa AGUAPEN EP en el departamento de Tecnología que posee infraestructura básica y adecuada para realizar las pruebas con la herramienta NM Traffic:

Evaluación de resultados

Para el análisis de este trabajo se ha considerado evaluar los siguientes cuestionamientos:

- ¿Cuáles son las consecuencias del control óptimo del tráfico, congestionamiento de la red en la empresa AGUAPEN EP?
- ¿Cuáles son las consecuencias del control óptimo del ancho de banda para el servicio de la red en la empresa AGUAPEN EP?

1.6 Tabulación y análisis de la encuesta

Este cuestionario está dirigido al personal del departamento de tecnología de información y comunicación con el fin de obtener información real y relevante para cumplir con los requerimientos de este proyecto.

Por tal motivo se consideró como información más relevante de proyecto evidenciar las siguientes preguntas resumidas a continuación.

1. **Cuánto tiempo se demora en carga o descargar un archivo debido a la lentitud del servicio de internet de acuerdo a su conexión cableado o inalámbrico.**

N.	Descripción	Cantidad
1	0 – 15 Min.	4
2	16 – 30 Min.	0

3	31 – 54 Min.	0
4	46 – 60 Min.	0
5	Más de 1 hora	1
Total de la encuesta		**5**

Tabla 2: Carga o descarga de un archivo

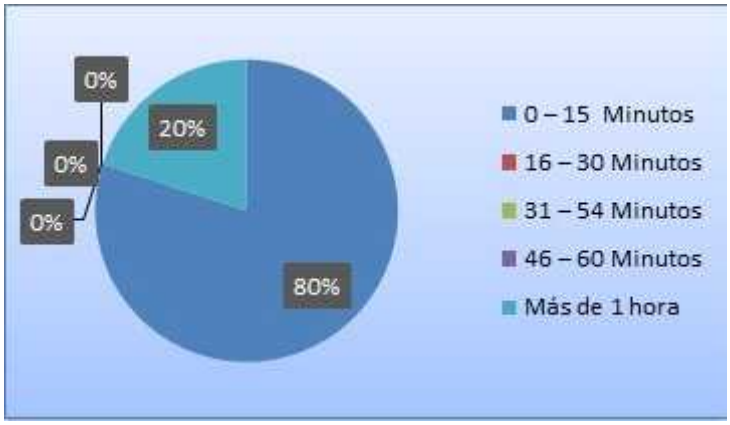


Gráfico 1: Carga o descarga de un archivo

De acuerdo a los resultados encuestados, existe un gran porcentaje (80%) que corresponde a las personas que ha dicho que el tiempo para cargar o descargar un archivo se toma un tiempo de 0 a 15 minutos, su ancho de banda ha de ser favorable para ellos para llegar a tener este tiempo, por otra parte el 20% ha indicado que se toma un tiempo de más de hora para obtener el archivo correspondiente, su ancho de banda debe ser no tan bueno o lento el servicio de internet para llegar a cabo esta operación y demorar mucho más tiempo que otras personas para subir o descargar un archivo, siendo este pequeño grupo de persona para llevar a cabo la encuesta para el estudio del presente proyecto de titulación.

2. ¿Con que frecuencia usted debe reiniciar el dispositivo WIFI debido a no tener acceso a la red?

N.	Descripción	Cantidad
1	Siempre	0
2	Casi Siempre	2

3	Algunas Veces	1
4	Muy Pocas Veces	2
5	Nunca	0
Total de la encuesta		**5**

Tabla 3: Reinicio del dispositivo WIFI

Gráfico 2: Reinicio del dispositivo WIFI

Existe un 40% de las personas encuestada que casi siempre debe reiniciar su dispositivo WIFI para que los demás empleados puedan tener acceso a ella y llevar a cabo sus diferentes actividades en la empresa, esto se debe que existe problemas en la red inalámbrica, por otra parte hay también un 40% de empleados que dice que algunas veces debe reiniciar su Access Point para poder seguir con sus actividades y un 20% aunque no tenga acceso a la red no realiza ningún reset al dispositivo WIFI, en muchas ocasiones por falta de tiempo o de los recursos no se llega a realizar ningún mantenimiento a los dispositivos inalámbricos lo que con lleva a tener interferencias, mala señal, no tener acceso a internet o a la red.

3. **¿Cuantas veces usted debe reiniciar su equipo de trabajo debido a que las aplicaciones son lentas y a veces tardan mucho tiempo en responder a que el tráfico en la red es muy lento?**

N.	Descripción	Cantidad
1	Siempre	0
2	Casi Siempre	0

3	Algunas Veces	1
4	Muy Pocas Veces	2
5	Nunca	2
Total de la encuesta		**5**

Tabla 4: Reinicio de su equipo de trabajo

Gráfico 3: Reinicio de su equipo de trabajo

Del total de personas encuestada un 20% ha tenido que reiniciar algunas veces su equipo de trabajo debido a que las aplicaciones que tienen acceso a internet o a otros servicios dentro de la misma red tardan mucho tiempo en responder, es ahí donde se presenta problemas de lentitud o que el equipo se tarde en responder, también puede dar fallas en el tráfico de la red que no sea tan fluido y que exista congestionamiento, en muchas ocasiones las consecuencias son graves porque se llega a tener pérdida de información muy importante y relevante para el empleado, por otra parte hay también un 40% que solo muy pocas veces reinicia su equipo de trabajo y un 40% nunca realiza esta operación por falta de tiempo o de desconocimiento de que puede estar provocando el problema.

4. **¿Cuantas veces le ha pasado que su dispositivo detecta el Access Point pero no se puede conectar a la red inalámbrica?**

N.	Descripción	Cantidad
1	Todos los días	0
2	Frecuentemente	3

3	De vez en cuando	1
4	Rara vez	0
5	Nunca	1
Total de la encuesta		**5**

Tabla 5: Detección y conexión al Access Point

Gráfico 4: Detección y conexión al Access Point

El 60% de las personas han respondido que frecuentemente al momento de conectarse por medio de un teléfono inteligente, una laptop o una pc no pueden realizar una conexión satisfactoria debido a que el Access Point no está debidamente colocado en un lugar preciso y adecuado en donde todos puedan tener acceso a ella, o por alguna restricción del administrador o que sus configuraciones no son los más recomendables y adecuados para que se realice una conexión correcta para que los usuarios que están cercanos puedan hacer uso de ella, también hay 20% que de vez en cuando por alguna razón no se puede conectar a la red inalámbrica y dejan de realizar sus actividades y 20% ha dicho que nunca le ocurre este problema.

5. **¿Con que frecuencia usted debe configurar el canal de la red inalámbrica WIFI debido a las interferencias o solapamiento que se presenta por otras redes inalámbricas?**

N.	Descripción	Cantidad
1	Siempre	0

2	Casi Siempre	0
3	Algunas Veces	3
4	Muy Pocas Veces	1
5	Nunca	1
Total de la encuesta		**5**

Tabla 6: Configuración del canal de la antena inalámbrica (Access Point)

Gráfico 5: Configuración del canal de la antena inalámbrica (Access Point)

El 60% de las personas han respondido que si hay algunas veces en la que se necesita configurar el canal del router debido a que está debajo de otras redes inalámbricas para evitar problemas de interferencias, o por solapamientos de las redes cercanas, y esto es lo que ocasiona que se pueda perder la conexión, pérdida de información, lentitud en el acceso a internet, el 20% ha dicho que son muy pocas veces en las que tiene que configurar su router o punto de acceso y el otro 20% nunca realiza este proceso de configuración en el canal del Access Point tal vez sea porque no le sucede este problema o que todo esté bien configurado o por falta tiempo, desconocimiento de este tipo de falla.

CAPITULO II

LA PROPUESTA

2.1 MARCO CONTEXTUAL

2.1.1 Descripción del ámbito del proyecto

Actualmente el departamento de Tecnología de AGUAPEN EP, no cuenta con una herramienta que lleve el control de los equipos que están conectados a la red local, además este departamento utiliza diferentes software para realizar los procesos de monitoreo, análisis y control del tráfico, de las redes WIFI o de los equipos conectados.

Los principales beneficiarios serán el administrador y sus ayudantes que conforman el departamento de Tecnología, el beneficiario en general será la empresa AGUAPEN EP, esta herramienta será capaz de realizar no solamente un monitoreo de tráfico sino también monitoreo de equipos y canales de redes WIFI, ancho de banda tanto de subida como de bajada del equipo local. Adicionalmente los miembros que conforman el departamento podrán llevar el respectivo registro de equipos y que ayuden a minimizar los tiempos de respuestas en el momento de realizar una búsqueda, con el objetivo de llevar un historial en caso que se lo requiera para la toma de decisiones.

Ante lo mencionado es de vital importancia la aceptación de un sistema que realice y que cumpla con los diferentes procesos presentados. Se desarrollará el aplicativo de monitoreo de tráfico de red, sondeos de equipos, canales de redes WIFI y ancho de banda bajo las herramientas con distribución libre, además con la ayuda de las diferentes librerías externar e internas que darán las funcionalidades y diferentes utilidades al software.

2.1.2 Alcances y limitaciones del proyecto

El presente proyecto tiene como alcance implementar un sistema de monitoreo que realice el control de tráfico de red y que permita ayudar a detectar los posibles problemas de comunicación. Esta herramienta será otorgado a los miembros del Departamento de Tecnología de la empresa AGUAPEN EP de acuerdo a lo establecido en la Sección 1.2 del Capítulo 1, la cual servirá de apoyo para realizar los diferentes monitoreo en caso de que la red local o inalámbrica pueda perder rendimiento por causas de colapsos, congestionamiento o perdidas de información, por lo cual se creará una aplicación de escritorio útil, con el fin de ayudar en estos diferentes procesos de llevar un monitoreo de tráfico, control de usuarios, análisis de los canales de las redes WIFI y ancho de banda del equipo local y detectar fallas que se puedan presentar.

La aplicación de escritorio a desarrollar solo funcionará en ambiente de Windows debido a que los equipos de la empresa poseen este sistema operativo, además que solo se llevara un monitoreo en dichos equipos y no en servidores. Este aplicativo tendrá un diseño interactivo y de fácil uso para que el usuario pueda navegar libremente por cada uno de los componentes que está conformada la interfaz, para ello el computador donde será instalada esta herramienta deberá poseer los requisitos necesarios para que funcione de manera correcta.

El administrador que hará uso de este aplicativo podrá registrar a los diferentes usuarios que tendrán acceso al mismo, ingresando los datos que se requiere en la interfaz de registro, además pueda usar las diferentes funciones que brinda esta herramienta. Mientras la aplicación esté activa el usuario podrá monitorear y analizar el tráfico que pasa por la red, ver los equipos conectados a la misma, además de observar los canales en la que están trabajando las redes inalámbricas WIFI.

Toda esta información tanto del tráfico de la red como el registro de los equipos será almacenada en la base datos, al momento de hacer un escaneo de PCs pueda observar que usuarios están conectados a la red.

Las contraseñas de cada usuario que se registre en la base de datos poseerán un método de encriptación de contraseña, para mantener con un alto nivel la seguridad de la herramienta y proteger a los usuarios frente a algún atacante sino también frente a los propios empleados que hacen uso de la aplicación, y de esta manera evitar que alguien pueda acceder a la base de datos y conseguir averiguar la contraseña de dicho usuario.

Los reportes que se generen servirán de ayuda al administrador para llevar un control de toda la información del tráfico de la red y se presentarán de forma estadística, por medio de esto se podrá hacer un análisis para la toma de decisiones.

El sistema constará con los siguientes módulos que serán útiles para el administrador para llevar a cabo los procesos de monitoreo, ingreso de información del equipo que se encuentra conectado a la red y del usuario que utilizará la aplicación, los módulos se detallan a continuación:

- **Validación Administrador/Usuarios:**

El aplicativo solo se instalará si el equipo está en modo administrador para la seguridad.

- **Registro de Equipos:**

El administrador del departamento se encargará de registrar los equipos que están conectados a la red local para mantener un control correcto de las direcciones IPs y a que usuario está asignada dicha dirección IP además de conocer su tráfico de paquetes de información.

Ingreso de nuevos equipos: se ingresará el nombre completo del usuario, dirección IP, Dirección MAC.

Modificación de equipos: se modificará el equipo en caso de que requiera de una nueva información.

Eliminación de equipos: se eliminará de forma lógica al equipo que no tenga acceso a la red.

- **Control de Usuarios:**

El administrador del departamento se encargará de llevar un registro de las personas que serán administradores y usuarios, a través de este proceso dar privilegios en la herramienta de monitoreo.

Se utilizará un inicio de sesión, porque cada usuario que ingrese no tendrá los mismo privilegios, algunas opciones no estarán disponibles para los tipos usuarios.

Ingreso de nuevos administradores o usuarios: se ingresara el nombre completo, nombre del departamento, usuario y contraseña, correo electrónico.

Inicio de sesión: se iniciará sesión al usuario que estará registrado en la base de datos.

- **Monitoreo, Canales WIFI o Tráfico de la red:**

Escaneo de host conectados a la red

El administrador podrá ingresar un rango de IPs o se realizará de forma automática de acuerdo a la red a la que está conectado, esto ayudará a realizar un escaneo de forma rápida para observar las máquinas conectadas con su respectiva información.

Monitoreo en tiempo real a través de gráficos

El administrador observará de forma gráfica el uso del tráfico de manera general o través de un host generado en la red.

Ancho de banda

El administrador podrá observar los niveles de ancho de banda que se genera en tiempo real.

Canales y SSID de red WIFI

El administrador podrá observar los canales más usados o congestionados por los usuarios conectados a la red.

Modo Sniffer

El administrador observará el tráfico de forma general que generan las máquinas conectadas a la red donde incluye toda la información necesaria para realizar las auditorias respectivas que llevarán a la toma de decisiones y dar solución a los problemas que se puedan presentar.

Modo Sniffer por host

El administrador solo observará el tráfico del equipo seleccionado a la que se le quiere realizar un control.

- **Módulo de Reportes:**

En este módulo se generará los reportes necesarios para realizar las diferentes auditorías para que se pueda tomar las respectivas decisiones y realizar las correcciones a los problemas que se puedan presentar, en esta parte de este módulo ayudará a que el tráfico de la red local este optimizado y mantenerlo de forma fluida para obtener el paquete de información correcto.

  - Reporte del tráfico general diario, quincenal o mensual.
  - Reporte del tráfico por host por día, quincenal o mensual.
  - Reporte de protocolos más usados por los usuarios.
  - Reporte de los puertos accedidos por los usuarios.
  - Reporte por filtro y general de todas las IPs escaneadas cada una con su debida información de los usuarios registrado.
  - Reporte de URLs accedidas por los usuarios.
  - Reporte de seguimientos de equipos.

El aplicativo permitirá escoger los protocolos de filtro de tráfico tanto TCP o UDP o ambos para el monitoreo.

Se generaran dos manuales el de instalación y el de usuario para la persona que va a hacer uso de la herramienta “NM Traffic” pueda comprender y entender la instalación, características y funcionalidades de cada componente y de las interfaces.

El presente proyecto va a ser desarrollado en lenguaje de programación Microsoft Visual Studio 2015. El mismo que podrá ser ejecutado en sistemas operativos Windows. Sin embargo el software tendrá limitaciones, es decir, no posee la capacidad de bloquear o manipular el tráfico generado por otros programas en la misma máquina o remota. Por esta razón no puede ser usado en aplicaciones como limitadores de tráfico, y firewalls personales.

Para realizar los diferentes monitoreos no se utilizará la tarjeta inalámbrica que viene incluida en la Notebook Pc debido a que esta antena es sorda para este tipo de trabajo, es decir no puede visualizar y obtener todas las redes que están alrededor del área en la que se encuentra ubicada la pc, no brinda un nivel de señal alto. Se utilizará una antena externa alfa WIFI alterna de respaldo que servirá de apoyo para realizar y llevar a cabo estos procesos debido a que ella provee una mejor señal y rendimiento para obtener mejores resultados.

Para el escaneo de las redes inalámbricas y observar sus diferentes canales en que están trabajando cada una de ella, solo se hará uso bajo el estándar 802.11g en la frecuencia de 2.4 Ghz, no se utilizará bajo la frecuencia 5 Ghz debido a que algunos equipos disponen de esta tecnología.

2.1.3 MARCO CONCEPTUAL

En este proyecto tiene como objetivo la implementación de un aplicativo que sirva como herramienta de apoyo que ayude a los administradores del Departamento de Tecnología de AGUAPEN EP en el monitoreo, análisis de tráfico de red, sondeos de equipos y visualización de canales en la que están trabajando las redes inalámbricas.

En esta sección se procederá a definir los diferentes conceptos de seguridad en redes que se indicarón en el proceso del anteproyecto, se citarán las respectivas referencias bibliográficas a la que representa cada uno de los siguientes párrafo o texto descriptivo.

2.1.4 Modelo OSI y Modelo TCP IP

Modelo OSI

La Organización Internacional para la Estandarización ISO, en el año de 1840 aceptó la necesidad de crear un modelo para las redes de computadoras, para facilitar a los distintos fabricantes en la creación de diversas implementaciones que sean interoperables y abiertas.[1]

Así nace este modelo, llamado OSI, este modelo fué creado debido al crecimiento de las redes de datos; y esto implicó a que no se pueda intercambiar información de un punto a otro.

El modelo OSI presenta una arquitectura de red, la cual se entiende como viaja y se transportán la información de los paquetes a través de ella, y está formada por 7 capas o niveles enumerados.

Gráfico 6: Capas del modelo OSI.

Aplicación (Capa 7).- Se encarga de suministrar servicios de red a las aplicaciones del usuario final. Estos servicios de red incluyen acceso a archivos, aplicaciones, etc.[2]

Presentación (Capa 6).- Se encarga de la presentación de los datos transmitidos, es decir cada ordenador puede tener su propia forma de presentación interna de los datos, por lo que es necesario tener acuerdos y convenciones para poder asegurar el entendimiento entre diferentes ordenadores.[2]

Sesión (Capa 5).- Esta capa de sesión establece, mantiene y administra conversaciones, denominadas sesiones, entre dos o más aplicaciones de distintas computadoras. La capa de sesión se encarga de mantener las líneas abiertas durante la sesión y de desconectaría cuando concluyen.[2]

Transporte (Capa 4).- Esta capa toma el archivo de datos y lo divide en segmentos para facilitar la transmisión. Su principal objetivo es garantizar una comunicación fiable y eficiente entre dos computadoras, con independencia de los medios empleados para su interconexión. Para conseguir este objetivo se emplea protocolos de transporte.[2]

Red (Capa 3).- La capa de red agrega direcciones lógicas o de red, como las direcciones de Protocolo de Internet (IP), a la información que pasa por ella. Con la adición de esta información de direccionamiento, los segmentos en esta etapa se denominan paquetes. Esta capa determina la mejor ruta para transferir los datos de una red a otra.[2]

Enlace de datos (Capa 2).- La capa de enlace de datos administra la notificación de errores, la topología y el control de flujo. Reconoce identificadores especiales que son únicos para cada host, tales como las direcciones de control de acceso a medios (MAC). Los paquetes de la Capa 3 se colocan en tramas que contienen esas direcciones físicas (MAC) de cada host origen y de destino.[2]

Física (Capa 1).- Esta capa incluye los medios, como cable de par trenzado, cable coaxial y cable de fibra óptica para transmitir las tramas de datos. Además se define los medios electrónicos y mecánicos; el procedimiento y las funciones para activar, mantener y desactivar el enlace físico entre sistemas finales.[2]

Por lo tanto cada capa debe tener funciones específicas además de seguir estándares internacionales, cada capa posee una interfaz la cual esta interconectada con la capa superior. Se entiende por interfaz al conjunto de procedimientos que definen al servicio que la capa está en condiciones de realizar para entregar a quien lo necesite.

Cuando un computador A (origen) desea enviar información a otro computador B (destino), empezando en el origen, conforme los datos se desplazan atravesando las diferentes capas del modelo OSI, cada capa va agregando información de control a los datos, es decir los datos se empaquetan por medio de un proceso que se denomina ***encapsulamiento***. En el destino cada capa analiza y va eliminando la información de control de los datos.[1]

Gráfico 7: Encapsulamiento en el modelo OSI.

Modelo TCP IP

El departamento de Defensa de EE.UU. (DoD) desarrolló el modelo de referencia TCP/IP que es un conjunto de reglas para que equipos compartan información en una red en cualquier tipo de medio. TCP/IP se creó como un estándar abierto que permita un desarrollo acelerado del mismo.[2]

El modelo TCP/IP tiene las siguientes cuatro capas:

Aplicación (Capa 4).- Esta capa se encarga de manejar aspectos de representación, codificación y control de diálogo.[2].

Transporte (Capa 3).- Esta capa se encarga de aspectos como control de flujo, calidad del servicio, corrección de errores, segmentación y re ensamble de datos en la comunicación. El protocolo principal de esta capa es el de control de transmisión (TCP), definido en la RFC.793; es un protocolo orientado a conexión, es decir mantiene una conexión lógica entre sus extremos. Además está el protocolo de datagrama de usuario (UDP) definido en la RFC-768; que es un protocolo no orientado a conexión y se lo utiliza cuando la aplicación necesita un tiempo de respuesta menor dado a que su cabecera es muy simplificada por lo cual no consume muchos recursos en su trasmisión.[2]

Internet (Capa 2).- El propósito de la capa internet es utilizar los datos de las capas superiores, es decir, los segmentos TCP o UDP empaquetarlos y enviados en la red. En este caso el protocolo Internet (IP) definido en la RFC-791 es el que permite que los paquetes lleguen a su destino independientemente de la ruta que utilizaron para llegar allí.[2]

Acceso a la red (Capa 1).- En esta capa se refiere a cualquier tecnología utilizada en una red. Esto incluye a todas las tecnológicas de la capa física y enlace de datos del modelo OSI.[2]

2.1.5 Red

Una red de computadoras, también llamada red de ordenadores o red informática, es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos con la finalidad de compartir información y recursos.[3]

La finalidad principal para la creación de una red de computadoras es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el coste general de estas acciones.[3]

2.1.6 Paquetes de Datos

Un paquete de datos es una unidad fundamental de transporte de información en todas las redes de computadoras modernas.[4]

Un paquete está generalmente compuesto de tres elementos: una cabecera contiene la generalmente la información necesaria para trasladar el paquete desde el emisor hasta el receptor, el área de datos que contiene los datos que se desean trasladar, y la cola, que comúnmente incluye código de detección de errores.[3]

2.1.7 Protocolos

Las redes modernas se componen de una variedad de sistemas que se ejecutan en diferentes plataformas. Para facilitar esta comunicación, se utiliza un conjunto de lenguajes comunes llamados protocolos. [3]

- Protocolo de Control de Transmisión (TCP).
- Protocolo de internet (IP).
- Address Resolution Protocol (ARP).
- Dynamic Host Configuration Protocol (DHCP).

Una pila de protocolos es una agrupación lógica de los protocolos que trabajan juntos. Los protocolos trabajan en gran parte del mismo modo, lo que nos permite definir el número de paquetes que deben ser colocados, como iniciar una conexión y la forma de asegurar el recibimiento de los datos.

Un protocolo puede ser muy simple o muy completo, dependiendo de su función.[3]

2.1.8 Cuellos de Botella

Un cuello de botella o embudo es un fenómeno que limita la capacidad de transferir la información de un sistema o de una conexión, es decir puede reducir el rendimiento del tráfico y esto lleva a la sobrecarga. Se da cuando las solicitudes no son atendidas en el mismo tiempo creando una fila de espera hasta llegar a un punto en donde ya no se pueda atender más solicitudes saturando la conexión y terminando los procesos.

2.1.9 Programas Analizadores de Red

Los tipos de Analizadores de tráfico de red se describen a continuación:

TCPDUMP Permite monitorizar el tráfico de red en tiempo real. Los filtros que se pueden crear para mostrar tan sólo la información que nos interesa, hacen de TCPDUMP una herramienta muy potente para el análisis de tráfico en redes de comunicaciones.[4]

NWATCH Se puede entender como un analizador de puertos pasivo, que está solamente interesado en tráfico IP y organiza los resultados como un explorador de puertos. Para la seguridad de la red NWatch es un complemento excelente al barrido de puertos regular de sus redes. Por defecto, NWatch permanece activo indefinidamente hasta que recibe un aviso de cierre.[4]

NMAP: Nmap se define como una suite de herramientas de descubrimiento de redes de código abierto, ha sido utilizada desde hace mucho tiempo en procesos de auditorías de seguridad ya que la misma permite determinar los puntos de acceso de una red y logra extraer grandes y útiles cantidades de información de la misma.[13]

WIRESHARK: es un analizador que captura paquetes de información que circulan a través de una red en tiempo real. Un analizador de paquetes de red intenta capturar paquetes en la red e intenta visualizar los datos de esos paquetes tan detalladamente como sea posible. Se puede pensar en un analizador de paquetes de red como un

dispositivo de medida usado para examinar que está pasando al interior de un cable de red.[14]

IP TRAFFIC MONITOR: PRTG monitoriza su red y no requiere de otros programas externos para que pueda funcionar de manera correcta. Además en su misma infraestructura esta herramienta puede monitorizar ordenadores y equipos de red.

2.1.10 Socket

Los sockets no son más que puntos o mecanismos de comunicación entre procesos de ordenadores que permiten que uno de ellos hable (emita o reciba información) con otro, incluso estando estos en distintas maquinas. Esta característica de interconectividad entre maquinas hace que el concepto de socket nos sirva de gran utilidad.[5]

Un socket es al sistema de comunicación entre ordenadores, la forma de referenciar un socket por los procesos implicados es mediante un descriptor del mismo tipo que es utilizado para referenciar ficheros. Debido a esta característica, se podrá realizar redirecciones de los archivos de E/S estándar (descriptores 0, 1 y 2) a los sockets y así combinar entre ellos aplicaciones de la red. Todo nuevo proceso creado heredará, por tanto, los descriptores de sockets de su padre.[5]

2.1.11 Congestionamiento

La congestión es un fenómeno producido en una red, se produce cuando el número de paquetes de información que se trasfieren en dicha red supera límite de tráfico que esta puede soportar, existen varias causas de la congestión y son:

- Insuficiente memoria en los conmutadores.
- Insuficiente CPU en los nodos.
- Insuficiente velocidad en las líneas.

2.1.12 Lenguaje de Programación Visual Studio

Visual Studio es un conjunto completo de herramientas de desarrollo para la generación de aplicaciones web ASP.NET, Servicios Web XML, aplicaciones de escritorio y aplicaciones móviles. Visual Basic, Visual C# y Visual C++ utilizán todos el mismo entorno de desarrollo integrado (IDE), que habilita el uso compartido de herramientas y facilita la creación de soluciones en varios lenguajes. Asimismo, dichos lenguajes utilizán las funciones de .NET Framework, las cuales ofrecen acceso a tecnologías clave para simplificar el desarrollo de aplicaciones web ASP y Servicios Web XML.[6]

Visual Studio es un entorno de desarrollo integrado para crear aplicaciones web, escritorio, etc. Además es la que utilizaremos para llevar a cabo el desarrollo del aplicativo bajo entorno C# con ayuda de sus librerías y complementos disponibles para que se logre un buen funcionamiento de esta herramienta de escritorio para el monitoreo de red, solo servirá bajo ambiente de Windows.

2.1.13 Seguridad de la Información

La seguridad de información se define como la protección de cantidades de información en cuanto a autorización y acceso a datos, modificación, eliminación de manera intencional o accidental.

La seguridad de la red depende mucho de esas medidas, y deben ser tomadas para mantener protegida la red del acceso no autorizado, de la destrucción y modificación de información relevante, hackeo accidental o mal intencionado con operaciones normales, inclusive para la protección del software.

2.1.14 Control de Tráfico

El término control de tráfico hace referencia al subsistema de colas de paquetes en una red o dispositivo de red. El control de tráfico consiste de diversas operaciones.[7]

- *Clasification*.- Es el mecanismo por el cual se identifican los paquetes y se los coloca en flujos o clases individuales.[7]
- *Policing*.- Es el mecanismo por el cual se limita la cantidad de paquetes o bytes en un flujo que corresponda a una clasificación particular.[7]
- *Scheduling*.- Es el proceso de decisión a través del cual se ordenan los paquetes para ser transmitidos.[7]
- *Shaping*.- Es el proceso a través del cual los paquetes son demorados y transmitidos para producir un flujo predecible.[7]

Estas características del sistema de control de flujo pueden combinarse de tal forma de reservar un determinado ancho de banda para un flujo de datos determinado (o una aplicación), o para limitar el ancho de banda disponible para un flujo o aplicación en particular.[7]

El siguiente listado no pretende ser exhaustivo de las soluciones disponibles para los usuarios mediante el uso de control de tráfico, pero introduce los tipos de problemas que pueden ser sorteados usando los mecanismos de control de tráfico para maximizar la usabilidad de un enlace de red.[7]

- Limitar el ancho de banda total disponible a un valor fijo conocido.
- Limitar el ancho de banda de un usuario, servicio o cliente en particular.
- Reservar ancho de banda para un usuario, servicio o cliente en particular.
- Realizar una administración y distribución equitativa del ancho de banda disponible.
- Filtrar un tipo particular de tráfico. Este caso muestra que el control de tráfico está relacionado con el concepto de *firewalling*, y que existen casos donde el primero puede realizar parcialmente las tareas del segundo.[7]

2.1.15 .NET Framework

.NET Framework es un entorno de ejecución runtime que administra aplicaciones cuyo destino es .NET Framework. Incorpora Common Language Runtime, que

proporciona administración de la memoria y otros servicios del sistema, y una biblioteca de clases completa, que permite a los programadores aprovechar el código sólido y confiable de todas las áreas principales del desarrollo de aplicaciones.[8]

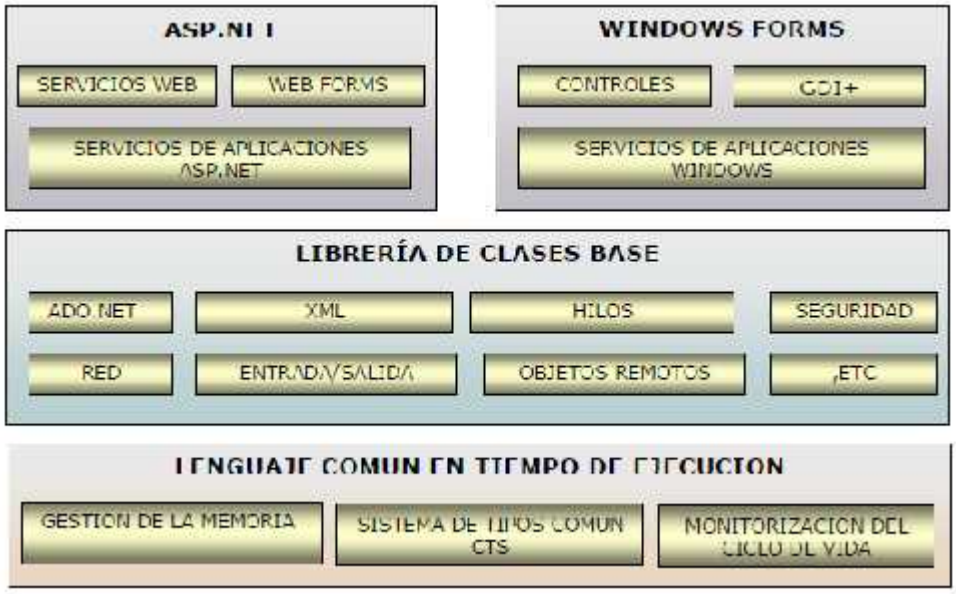


Gráfico 8: Esquema del Framework .Net

2.1.16 Base Datos

Una base de datos es un conjunto de datos **organizados** e **interrelacionados** que se organizan y relacionan entre sí de manera **sistemática**, esto es, siguiendo unas determinadas reglas.[10]

2.1.17 MySQL

MySQL es un sistema de administración de bases de datos relacionales rápido sólido y flexible. Es ideal para crear bases de datos con acceso desde páginas web dinámicas, para la creación de sistemas de transacciones *on-line* o para cualquier otra solución profesional que implique almacenar datos, teniendo la posibilidad de realizar múltiples y rápidas consultas.[9]

MySQL ofrece varias ventajas respecto a otros sistemas gestores de base de datos:

- Tiene licencia pública, permitiendo no solo la utilización del programa sino también la consulta y modificación de su código fuente. Resulta por tanto fácil de personalizar y adaptar a las necesidades concretas.[9]
- Puede ser descargado gratuitamente de internet (http://www.mysql.com) haciendo uso de su licencia GPL.[9]

2.1.18 Wireless IEEE 802.11

IEEE 802.11 es un estándar creado por el Instituto de Ingenieros Eléctricos y Electrónicos para Ethernet inalámbrica lanzado en 1997. Posee un método de acceso llamado CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) la cual es muy eficaz porque sacrifica el ancho de banda para asegurar los datos de la transmisión sea confiable.

Estándares de la IEEE 802.11

Existen diferentes estándares definidos por la IEEE, estas están basadas a todo tipo de WIFI y han evolucionado según las necesidades del usuario.

Los más usados y aceptados son los estándares 802.11g y 802.11n, los dos trabajan en ancho de banda 2.4 GHz pero se diferencia en la velocidad de transmitir. El 802.11n puede alcanzar un rango mayor pero depende también si no hay interferencias.

El estándar más utilizado es el 802.11n debido a su mayor velocidad en transferencias y es uso de la tecnología MIMO.

El nuevo estándar 802.11ac en las redes inalámbricas es la última tecnología y evolucionado del estándar 802.11n, esta tecnología funciona exclusivamente en frecuencia de 5Ghz la cual permite conectar más dispositivos a mayor velocidad superando a las redes por cable Ethernet, tiene menor congestionamiento y mínima interferencia que la 2.4Ghz. Esta tecnología nació debido al gran crecimiento de los dispositivos inalámbricos y la extrema saturación de la frecuencia 2.4Ghz y esto da

como resultado un cuello de botella, es decir la mayoría de los dispositivos y routers trabajan bajo la frecuencia de 2.4Ghz lo que conlleva a que estos equipos no sean compatibles con la nueva tecnología 5Ghz. Algunos dispositivos como Móviles, routers son compatible porque ya viene incorporado la tecnología Wireless 802.11ac, además esta tecnología soporta a los estándares anteriores.

La Wireless 802.11ac viene incorporado un ancho de canal de 80Mhz incluso puede llegar a soporta 160Mhz aumentando la velocidad en trasmisión de datos, posee una modulación de amplitud en cuadrática y además soporta trasmisión simultánea de múltiples usuarios.

Canales en banda ancha 2.4 Ghz

Los canales 1, 6, 11 son los más óptimos para eliminar el solapamiento y minimizar las interferencias, estos ayudán a evitar que se superponga las redes WIFI, es decir que no estén debajo de otras redes cercanas, además hay que mantenerlos separados los puntos de acceso para evitar problemas como los mencionados, estos canales son los que recomienda la Wireless 802.11.

Características de una red WIFI

Essid.- Es el nombre con que se identifica la red.
Bssid.- Es la dirección MAC del Access Point a la que nos conectamos.
Rssid.- Nivel de potencia recibida de un dispositivo inalámbrico.
Canal.- número en la que está trabajando el dispositivo inalámbrico.

2.1.19 Aspectos Éticos y Legales

Leyes y normas que regulan la protección de datos en el Ecuador

- **La Ley del Sistema Nacional de Registro de Datos Públicos indica en:**

El artículo 66, numerales 19 y 28 garantizan los derechos a la identidad colectiva y personal y a la protección de datos de carácter personal, el cual incluye el acceso y la

decisión sobre información de este carácter, así como su correspondiente protección. [12]

- **Ley de Comercio Electrónico, Firmas y Mensajes de Datos en su Art. 9 establece:**

Protección de datos.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de estos, quien podrá seleccionar la información a compartirse con terceros.[12]

- **Ley Orgánica de Transferencia y Acceso a la Información Pública considera Información Confidencial:**

Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la Republica.[12]

El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes.[12]

Existen Leyes penales contra los delitos informáticos. Los siguientes artículos del Código Orgánico Integral Penal juzgan:

Art. 202.- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.[12]

Art. 262.- Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa

fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubiere sido comendados sin razón de su cargo.[12]

Art. 415.-

Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.[12]

Entre los estándares de seguridad de la información tenemos:

Entre los estándares existen: "Las normas publicadas bajo la serie ISO 27000 son entandares alineados con el conjunto de normas publicadas por ISO (Internacional Organization for Standardization) e IEC (International Electrotechnical Commission) actuales o futuras y que son desarrolladas mediante comités técnicos específicos" (Normas ISO 27000, 2009).

La norma ISO 27001: "Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización".[12]

De la familia de normas ISO 27000 existe otro estándar para la seguridad de la información. ISO 27002 que:

La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que solo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso

son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran).[12]

Proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.[12]

Aspecto Ético

De acuerdo a los estándares legales esta aplicación solo será uso de la empresa AGUAPEN EP y de sus empleados que son parte del departamento de Tecnología, la cual podrá obtener solo información dentro de ella, no se podrá realizar monitoreo y obtener datos de forma externa.

Aspecto Legal

En el COIP se sancionan los delitos informáticos, cuyos actos se comenten con el uso de tecnología para violentar la confidencialidad y la disponibilidad de datos personales. Estos actos que se registran a través de la Internet son: fraude, robo, falsificaciones, suplantación de identidad, espionaje, clonación de tarjetas de crédito, entre otros.[15]

El delito de interceptación ilegal de datos consta en el artículo 230 del COIP. Este sanciona con tres a cinco años de pena privativa de libertad a quienes utilicen estos datos y los difundan.[15]

La aplicación tiene como objetivo realizar los diferentes procesos como es la captura, análisis, monitoreo o control del tráfico de la red por medio de cableado o forma inalámbrico para obtener información relevante y que están dentro de la empresa, no se obtendrán datos confidenciales como cuentas o contraseñas que son de propiedad de cada usuario. El usuario administrador quien hará uso de esta herramienta lo debe realizar con responsabilidad, de manera correcta y no usarlo para fines de mal intenciones porque será penalizado de acuerdo al artículo 230 del COIP.

2.3 MARCO TEÓRICO

En esta sección de este capítulo se describirán información de los siguientes conceptos acerca de los fundamentos teóricos escritos en el trabajo de investigación, que ayudarán a entender cómo opera un analizador de red y además de estudios e investigación sobre el desarrollo e implementación de este aplicativo.

2.3.1 SISTEMA DE MONITOREO Y CONTROL DE TRÁFICO DE RED

ANÁLISIS DE PAQUETES DE DATOS

Un análisis es una descomposición de un todo en partes pequeñas para poder estudiar su contenido. Los paquetes de datos contienen información que puede ser analizada y capturada.[4]

Existen herramientas que permiten realizar los diferentes procesos de monitoreo, control, análisis y captura de paquetes de datos que circulan a través de la red de datos.

No todos los paquetes de datos pueden ser interpretados o capturados debido a la implementación adicional de seguridad que tienen, los paquetes de datos que contienen información pueden estar encriptados con claves de acceso.[4]

ANALIZADOR DE TRÁFICO DE RED

Un analizador de red es un programa especializado en el monitoreo, análisis y captura de tramas o paquetes que pasan a través de la red de datos.[4]

Es un software informático que puede interceptar y registrar tráfico de paquetes pasando sobre una red de datos. Mientras el flujo de datos va y viene en la red, el husmeador captura cada unidad de datos del protocolo y puede decodificar y analizar su contenido, de acuerdo a la especificación del programa.[4]
Su uso varía desde la detección de un cuello de botella en una red hasta el análisis de fallas en las redes, aunque también es habitual su uso para fines maliciosos, como

robo de contraseñas, interceptar mensajes de correo electrónico, espiar conversaciones de chat, obtener datos personales entre ellos.[4]

¿QUIÉNES UTILIZAN UN ANALIZADOR DE RED?

Los administradores de sistemas, ingenieros de redes, ingenieros de seguridad, operadores de sistemas y los programadores usan los analizadores de red, que son herramientas muy valiosas para el diagnóstico y resolver problemas de red, problemas de configuración del sistema y las dificultades de aplicación.[3]

El arte del análisis de redes es un arma de doble filo. Mientras que los profesionales de la seguridad hacen uso para la solución de problemas y el control de la red, intrusos utilizan el análisis de la red para propósitos dañinos. Un analizador de red es una herramienta, y como todas las herramientas, puede ser utilizado para fines tanto buenos como malos.[3]

UN ANALIZADOR DE RED SE UTILIZA PARA:

- La conversión de los datos binarios a un formato legible.
- Resolución de problemas en la red.
- Analizar el rendimiento de una red para descubrir cuellos de botella.
- Detección de intrusos en la red.
- Registro de tráfico de red para la argumentación y las pruebas.
- El análisis de las operaciones de las aplicaciones.
- El descubrimiento de tarjetas de red defectuosas.
- Descubrir el origen de los brotes de virus o de la denegación de servicio (DoS).
- Validar el cumplimiento de las políticas de seguridad de la empresa.
- Como un recurso educativo en el aprendizaje acerca de los protocolos.

LOS INTRUSOS UTILIZAN LOS ANALIZADORES DE REDES PARA:

- La captura de nombres de usuario y contraseñas de texto plano.

- El descubrimiento de los patrones de uso de los usuarios en una red.
- Comprometer información confidencial.
- Captura y reproducción de voz sobre IP conversaciones telefónicas (VoIP).
- Mapeo de la distribución de la red.

2.3.2 SNIFFER

Un sniffer es un dispositivo o una aplicación que permite capturar los datos o información que pasan a través de una red, que no precisamente van dirigidos hacia él, por lo tanto es un tráfico de información al que no debería tener acceso.[11]

¿SON PELIGROSOS LOS SNIFFERS?

Resulta bastante obvio suponer que los sniffers presentan un riesgo de seguridad tanto en una sola máquina como en una red, debido a la facilidad con la que cuenta para poder capturar información.[11]

Lamentablemente viaja por la red una cantidad innumerable de información confidencial sin contar con ningún tipo de cifrado o método de encriptación, entre las que se puede mencionar: contraseñas, correo confidencial, números de tarjetas de crédito, registros de bases de datos, cookies con información de autenticación, entre otros.[11]

Es de vital importancia realizar una inspección de detección de sniffers en la red no solo para detectar el daño que pueda, sino también para darse cuenta que los niveles de seguridad pueden ser violados y que se deben tomar medidas.[11]

¿PARA QUE USAN LOS INTRUSOS UN PROGRAMA DE SNIFFER?

Es utilizado por personas malintencionadas, los sniffers pueden representar una amenaza significativa para la seguridad de la red. Los intrusos de la red utilizan sniffers para capturar información confidencial.[3] Un sniffer es útil siempre y cuando sea utilizado de forma correcta y autorizada por el administrador de la red o

por los usuarios a los que se requieren obtener información: contraseñas, tanto correo electrónico, como para acceso a zonas WIFI restringidas.

Si el caso se utiliza de forma ilegítima un sniffer, se le considera como un ataque pasivo debido que no está autorizado para monitorear, analizar y obtener información confidencial o relevante en la red, en cambio sí se está utilizando este sniffer de forma legítima es porque está autorizada por una institución o administrador que solo hará uso dentro de ella para realizar diferentes procesos.

DEFENSA CONTRA SNIFFER

Hoy en día existen software como NEPED, SNIFFDET, ANTISNIFF para encontrar sniffer que son difíciles de detectar debido a que se encuentra de forma pasiva y ocupan menos espacio de memoria en el ordenador para no dejar rastros.

FUNCIONAMIENTO GENERAL DE UN SNIFFER

Para poder capturar el tráfico de la red a la que estamos conectados se debe colocar la tarjeta de red en "*modo promiscuo*". El modo promiscuo por definición consiste en que "todos los adaptadores de red reciben los paquetes que son para ellos, (filtran por IP), pero el colocar el adaptador de red en modo promiscuo hace que no filtre, y vea todo el tráfico que está en la red".[11]

Un sniffer es más efectivo es en una red LAN que maneja la topología tipo Bus; otro entorno de los sniffers es una máquina víctima.[11]

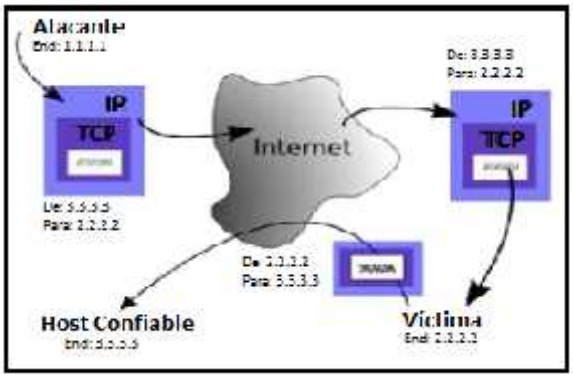


Gráfico 9: Sniffer en un equipo

2.4 DESARROLLO

2.4.1 Componente de la Propuestas

Software

Para desarrollar el aplicativo se utilizaron software con distribución libre, lo que significa que se pueden descargar libremente desde el internet de su respectivo sitio web oficial.

Valoración	Denominación
1	Microsoft Visual Studio 2010
1	Microsoft Visual Studio 2015
1	MySQL Workbench 6.0 CE
1	WinPcap 4.1.3
1	SQL Power Architect 1.0.6
1	Microsoft Office 2010

Tabla 7: Requerimientos de Software.

Hardware

Los recursos que se utilizaron para la presente propuesta tecnológica son los siguientes y se describen a continuación:

Valoración	Denominación
1	Laptop HP Intel Core I3, 3Gb
1	PC Escritorio HP Intel Duo Core, 4Gb
1	Celular Samsung Galaxy J5 SM-J500M
1	Pendrive 4 Gb
1	Antena Alfa Network
1	Impresora Canon Pixma MG2400

1	Resmas de Papel A4

Tabla 8: Requerimientos de Hardware.

2.4.2 Diseño de la Propuesta

Se describirán a continuación los diagramas de casos de uso y esquemas para que el usuario final de quien va hacer uso de esta herramienta, pueda observar, entender, comprender y analizar de cómo se lleva a cabo cada uno de los diferentes procesos y funcionalidades de los componentes e interfaces y base de datos que comprende el aplicativo en si (Monitoreo y Control de Tráfico de red, escaneo de direcciones IPs con su respectivo información de equipo y niveles de ancho de banda).

Esquema de la aplicación

En el siguiente esquema que se muestra a continuación se observa el proceso y las fases posteriores para realizar el escaneo del tráfico en una red, además de filtrar por host.

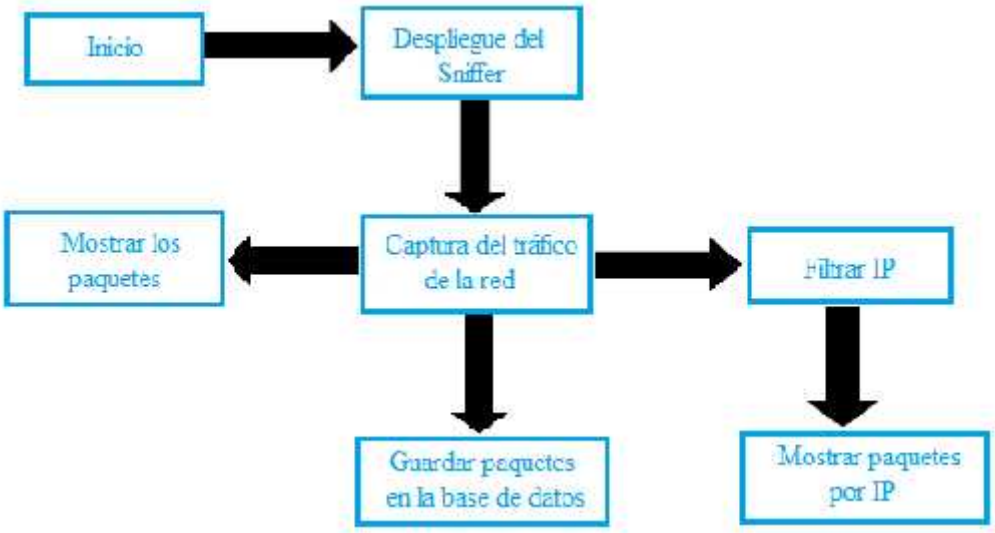


Gráfico 10: Esquema del Escaneo de Tráfico de red.

En el siguiente esquema que muestra a continuación describirá de cómo se realiza un escaneo de equipos conectados a la red a través de una ping ARP, esto se lo hace con un filtro de rango de IP.

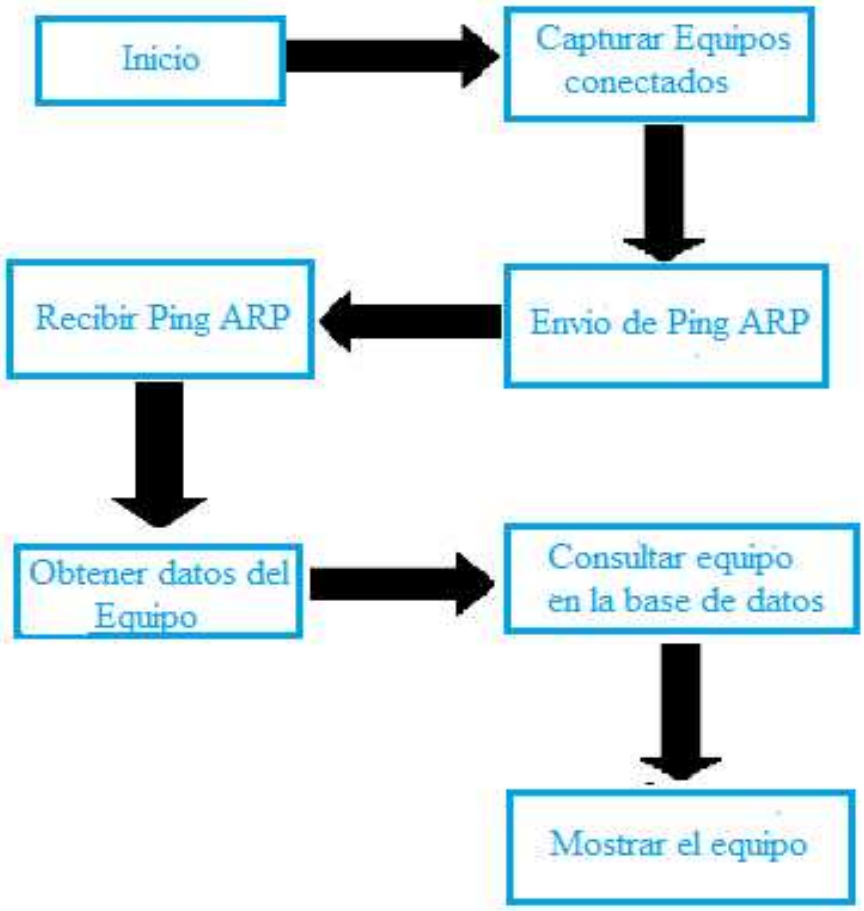


Gráfico 11: Esquema del Escaneo de Equipos.

En el caso del ancho de banda solo se realizará una consulta a una respectiva dirección web la cual realiza este proceso y que otorgará de manera inmediata los niveles de subida como de bajada (descarga) de internet, y en el caso de las redes inalámbricas no agregaremos una arquitectura porque no posee tantas fases, solo se realiza una consulta de todos los routers cercanos para obtener su respectiva información.

2.4.3 Diagramas de casos de uso

En esta gráfica de casos de usos se determinará las funcionalidades o procesos de cada una de la persona que interactuará con este aplicativo, además de cómo se lleva a cabo de manera sencilla las diferentes funciones y procesos que comprenden esta

herramienta monitoreo, análisis de tráfico de red, sondeos de equipos y canales de redes inalámbricas.

Caso de Uso Inicio de Sesión

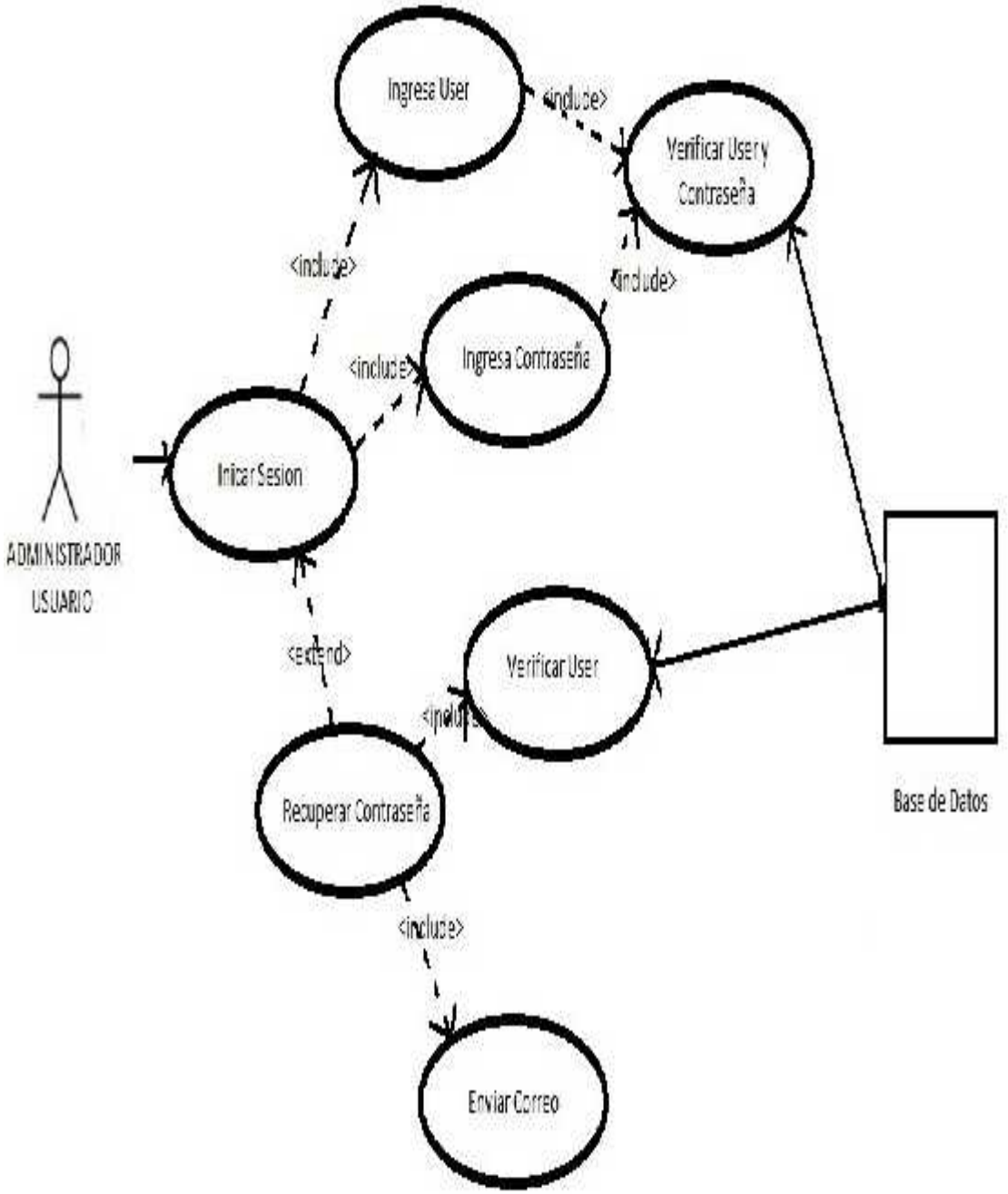


Gráfico 12: Diagrama de caso de uso Inicio de Sesión.

Caso de Uso Registro de Usuario

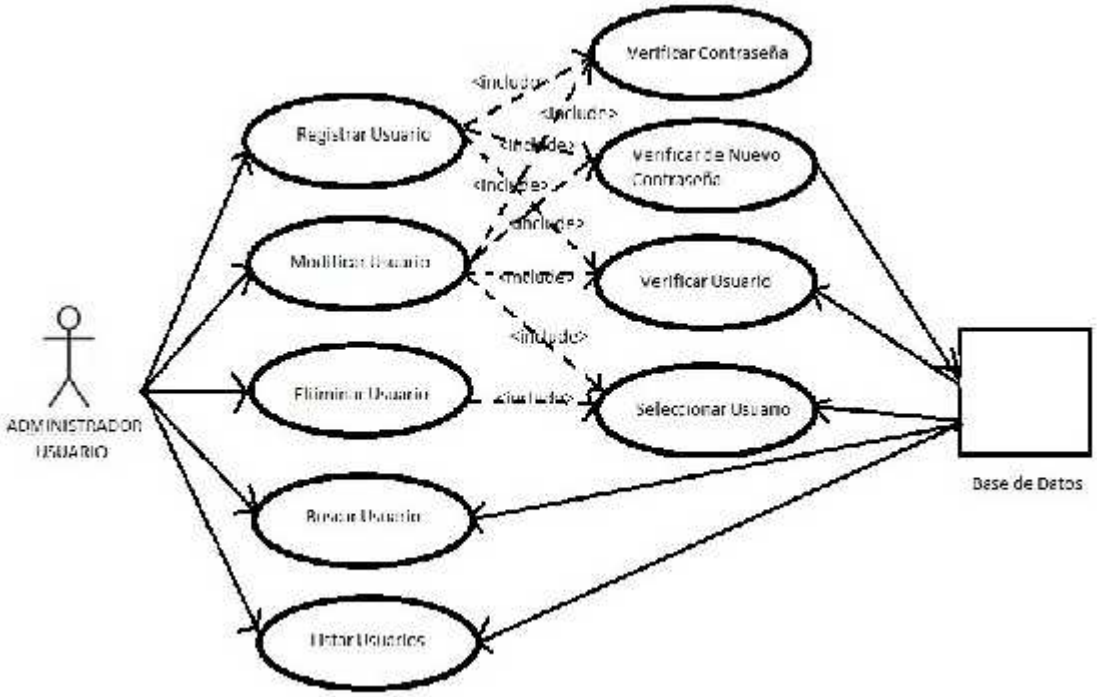


Gráfico 13: Diagrama de caso de uso Registro de Usuario.

Caso de Uso Registro de Equipo

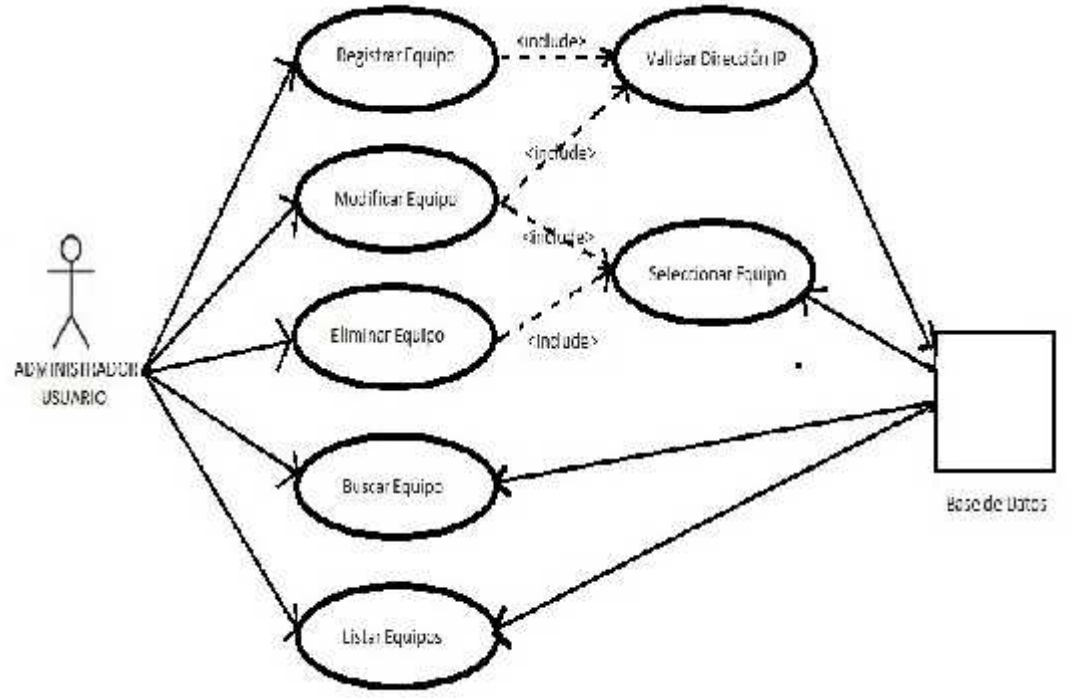


Gráfico 14: Diagrama de caso de uso Registro de Equipo.

Caso de Uso Escaneo de Equipo

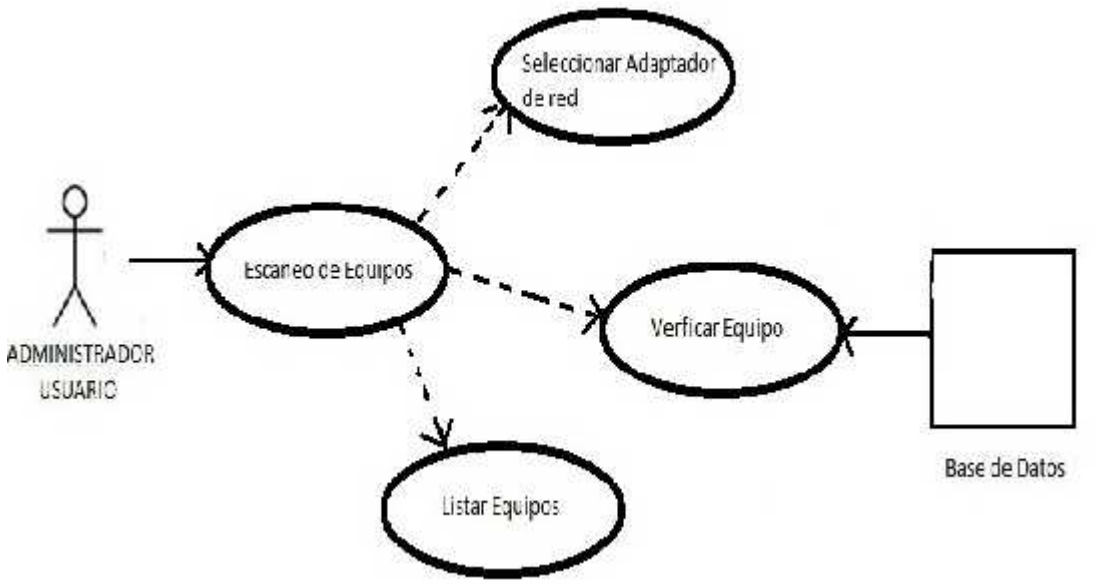


Gráfico 15: Diagrama de caso de uso Escaneo de Equipos.

Caso de Uso Tráfico de Red General y Por Host

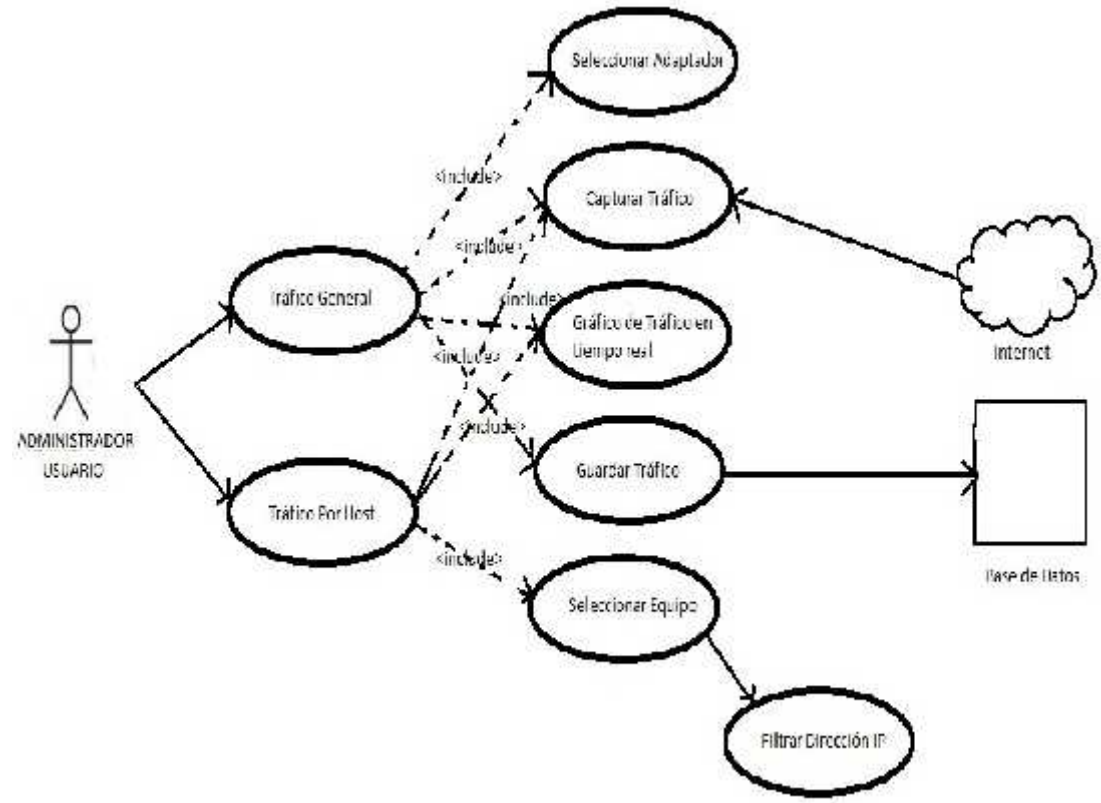


Gráfico 16: Diagrama de caso de uso Tráfico de red General y Por Host.

Caso de Uso Niveles Ancho de Banda, Canales de Redes WIFI y Reportes

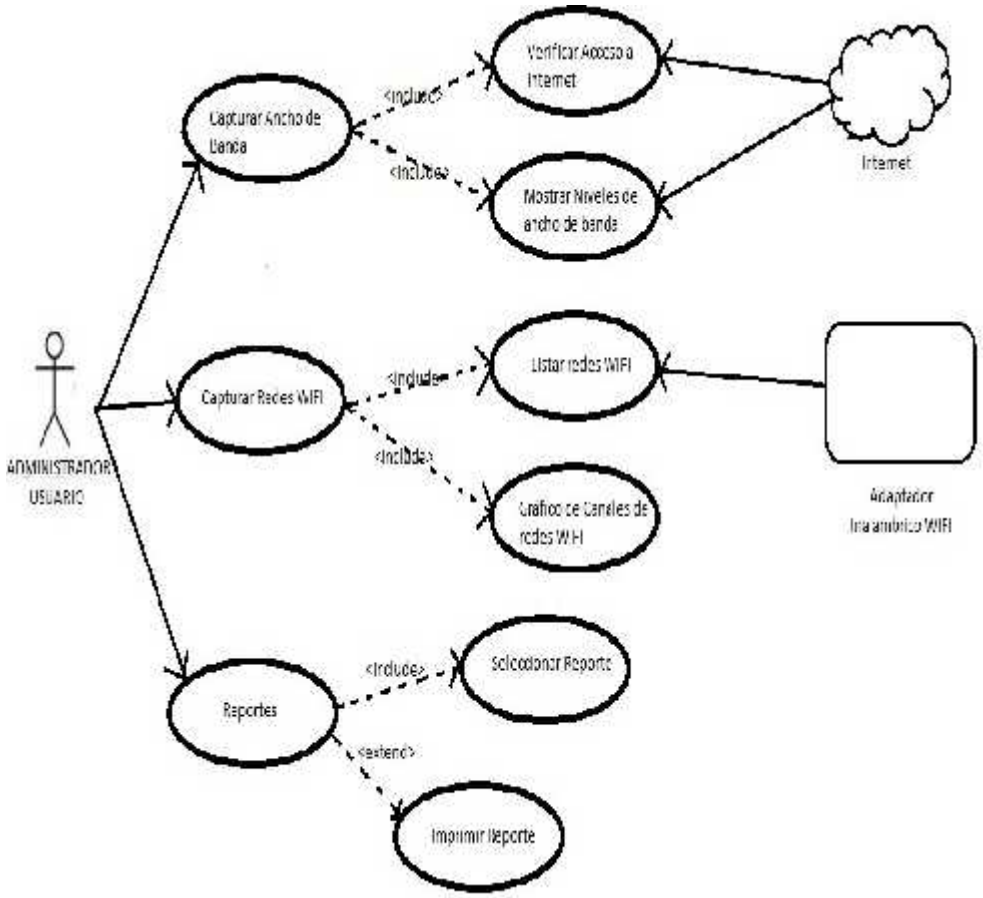


Gráfico 17: Diagrama de caso de uso Ancho de Banda, Canales WIFI y Reportes.

Casos de uso formato extendido

Para el aplicativo de Monitoreo, Control de tráfico de red y manejo óptimo del ancho de banda tendrá los siguientes casos de uso, y se describen a continuación en las siguientes tablas:

Caso de uso #1

En este primer caso de uso el administrador podrá registrar los usuarios que desee y quienes van hacer uso de esta herramienta, en la siguiente tabla se detallará más fondo de este caso.

Registrar Usuario, Caso de uso extendido.

CASO DE USO	Registrar Usuario
ACTOR(ES)	Administrador
PROPÓSITO	Todos los usuarios podrán iniciar sesión desde el aplicativo con sus datos registrados y otorgados por el administrador.
DESCRIPCIÓN	Iniciará cuando el administrador llene todo los datos que se requiera en el formulario de registro de usuario.
PRECONDICIÓN	Instalar el software y tener los datos del usuario.
ACTOR(ES) 1.- Abre la aplicación para iniciar sesión. 3.- Selecciona la opción de Usuarios. 5.- Selección registrar nuevo usuario. 7.- Se rellena los campos del formulario con los datos del usuario nuevo. 8.- Presiona el botón Guardar.	**APLICACIÓN** 2.- La aplicación abrirá el formulario de inicio de sesión de forma automática. 4.- La aplicación abrirá el formulario de usuario. 6.- La aplicación abrirá el formulario de registro de usuario. 9.- Confirmación y registrado en la base de datos.
CURSO ALTERNO	
POSTCONDICIÓN	Un mensaje notificando que la inserción se ha efectuado de manera correcta.

Tabla 9: Registro de Usuario, Caso de Uso Extendido**.**

Caso de uso #2

En este segundo caso el usuario podrá iniciar sesión para tener acceso al aplicativo y hacer uso de ella, en la siguiente tabla se detallará más fondo de este caso.

Inicio de sesión, Caso de uso.

CASO DE USO	Inicio de Sesión
ACTOR(ES)	Administrador
PROPÓSITO	El administrador podrá hacer uso de la herramienta y de sus funciones.
DESCRIPCIÓN	Iniciará cuando el usuario llene los campos de inicio de sesión.
PRECONDICIÓN	Estar registrado en la base de datos.
ACTOR(ES) 1.- Abre la aplicación para iniciar sesión. 3.- Rellenar los campos del formulario con los datos correctos. 4.- Presiona el botón Aceptar.	**APLICACIÓN** 2.- La aplicación abrirá el formulario de inicio de sesión de forma automática. 5.- la aplicación abrirá el formulario principal, si no enviara un mensaje de error de usuario o contraseña incorrectas.
CURSO ALTERNO	
POSTCONDICIÓN	Inicio de sesión de manera exitosa e ingreso al aplicativo.

Tabla 10: Inicio de Sesión, Caso de Uso Extendido.

Caso de uso #3

En este tercer caso el administrador o usuario podrá registrar, modificar o eliminar un equipo según lo requiera para llevar un mejor control de los mismos, en la siguiente tabla se detallará más fondo de este caso.

Registrar Equipo, Caso de uso extendido.

CASO DE USO	Registrar Equipo
ACTOR(ES)	Administrador, Usuario
PROPÓSITO	Mostrar los equipos conectados con su debida información registrada en caso de que esté conectado o no a la red.
DESCRIPCIÓN	Iniciará cuando el administrador o usuario llene todo los datos que se requiera en el formulario de registro de equipo.
PRECONDICIÓN	Haber iniciado sesión y tener los datos correctos del equipo.
ACTOR(ES) 1.- Abre la aplicación para iniciar sesión. 3.- Selecciona la opción de Equipo. 5.- Selección registrar nuevo equipo. 7.- Se rellena los campos del formulario con los datos del usuario equipo. 8.- Presiona el botón Guardar.	**APLICACIÓN** 2.- La aplicación abrirá el formulario de inicio de sesión de forma automática. 4.- La aplicación abrirá el formulario de Equipo. 6.- La aplicación abrirá el formulario de registro de equipo. 9.- Confirmación y registrado en la base de datos.
CURSO ALTERNO	El usuario podrá registrar, modificar o eliminar los equipos registrados.
POSTCONDICIÓN	Un mensaje notificando que la operación de inserción se ha efectuado de manera exitosa.

Tabla 11: Registro de Equipo, Caso de Uso Extendido.

Caso de uso #4

En este cuarto caso el administrador o usuario podrá realizar el escaneo de los equipos conectados en la red y ser visualizados, en la siguiente tabla se detallará más a fondo este caso.

Escaneo de PCs, Caso de uso extendido.

CASO DE USO	Escaneo de PCs
ACTOR(ES)	Administrador, Usuario
PROPÓSITO	Mostrar los equipos conectados de la red.
DESCRIPCIÓN	Iniciará cuando el administrador o usuario despliegue y seleccione un adaptador de red.
PRECONDICIÓN	Haber iniciado sesión y estar conectado a la red local o inalámbrica.
ACTOR(ES) 1.- Abre la aplicación para iniciar sesión. 3.- Estar colocado en la opción de PCs. 4.- Selecciona un adaptador de red 5.- Presionar el botón de iniciar. 7.- Presionar el botón Parar.	**APLICACIÓN** 2.- La aplicación abrirá el formulario de inicio de sesión de forma automática. 6.- La aplicación escaneara y mostrará todas las PCs conectadas a la red. 8.- La aplicación parará el escaneo.
CURSO ALTERNO	
POSTCONDICIÓN	Lista de PCs conectadas exitoso.

Tabla 12: Escaneo de PCs, Caso de Uso Extendido.

Caso de uso #5

En este quinto caso el administrador o usuario seleccionará un adaptador de red para poder realizar el escaneo del tráfico y mostrarla de forma de texto y en gráficas en tiempo real, en la siguiente tabla se detallará más fondo este caso.

Escaneo de Tráfico de red, Caso de uso extendido.

CASO DE USO	Escaneo de Tráfico de red
ACTOR(ES)	Administrador, Usuario
PROPÓSITO	Mostrar el mensaje y cada atributo del paquete que transmitió en la red.
DESCRIPCIÓN	Iniciará cuando el administrador o usuario despliegue y seleccione un adaptador de red.
PRECONDICIÓN	Haber iniciado sesión y estar conectado a la red local o inalámbrica.
ACTOR(ES) 1.- Abre la aplicación para iniciar sesión. 3.- Estar colocado en la opción de Modo Sniffer. 4.- Selecciona un adaptador de red 5.- Presionar el botón de iniciar. 7.- Presionar el botón Parar.	**APLICACIÓN** 2.- La aplicación abrirá el formulario de inicio de sesión de forma automática. 6.- La aplicación escaneara y mostrará los paquetes enviados y recibidos de los diferentes equipos conectados a la red. 8.- La aplicación parará el escaneo de manera automática.
CURSO ALTERNO	
POSTCONDICIÓN	Mostrar paquetes de información.

Tabla 13: Escaneo de tráfico de red, Caso de Uso Extendido.

Caso de uso #6

En este sexto caso el administrador o usuario seleccionará un equipo escaneado y conectado a la red para poder realizar el proceso respectivo del tráfico y mostrarlo de la misma forma de texto o en gráficas en tiempo real, en la siguiente tabla se detallará más fondo este caso.

Escaneo de Tráfico de red por IP, Caso de uso extendido.

CASO DE USO	Escaneo de Tráfico de red por IP
ACTOR(ES)	Administrador, Usuario
PROPÓSITO	Mostrar el mensaje y cada atributo del paquete enviado y recibo en la red.
DESCRIPCIÓN	Iniciará cuando el administrador o usuario despliegue y seleccione un adaptador de red.
PRECONDICIÓN	Haber iniciado sesión, estar conectado a la red local o inalámbrica y seleccionar un host para el escaneo.
ACTOR(ES) 1.- Abre la aplicación para iniciar sesión. 3.- Estar colocado en la opción de Modo Sniffer por Host. 4.- Selecciona un adaptador de red para escanear. 5.- Presionar el botón de iniciar.	**APLICACIÓN** 2.- La aplicación abrirá el formulario de inicio de sesión de forma automática. 6.- La aplicación escaneará y mostrará los paquetes enviados y recibidos del equipo filtrado a través de la IP correspondiente y seccionada correspondiente conectado a la red.

7.- Presionar el botón Parar.	8.- La aplicación parará el escaneo.
CURSO ALTERNO	
POSTCONDICIÓN	Mostrar paquetes con éxito.

Tabla 14: Escaneo de tráfico de red por Host, Caso de Uso Extendido.

Caso de uso #7

En este séptimo caso el administrador o usuario deberá tener acceso a internet para poder consultar su nivel de ancho de banda desde una página registrada por defecto para consultar estos niveles, en la siguiente tabla se detallará más fondo de este caso.

Consulta de ancho de banda, Caso de uso extendido.

CASO DE USO	Consulta de ancho de banda
ACTOR(ES)	Administrador, Usuario
PROPÓSITO	Mostrar la capacidad de subida y descarga del ancho de banda del ordenador local.
DESCRIPCIÓN	Iniciará cuando el administrador o usuario consulte su ancho de banda.
PRECONDICIÓN	Haber iniciado sesión, tener acceso a internet.
ACTOR(ES) 1.- Abre la aplicación para iniciar sesión. 3.- Estar colocado en la opción Niveles de Ancho de Banda. 4.- Presionar el botón de Actualizar. .	**APLICACIÓN** 2.- La aplicación abrirá el formulario de inicio de sesión de forma automática. 5.- La aplicación cargará la página ingresa por defecto y mostrará los niveles de ancho de banda.

CURSO ALTERNO	
POSTCONDICIÓN	Mostrar niveles de ancho de banda con éxito.

Tabla 15: Consulta de ancho de banda, Caso de Uso Extendido.

Caso de uso #8

En este séptimo caso el administrador o usuario deberá tener una tarjeta o antena inalámbrica insertada en su pc para poder realizar el respectivo escaneo, en la siguiente tabla se detallará más fondo este caso.

Escaneo de SSID WIFI, Caso de uso extendido.

CASO DE USO	Escaneo de SSID WIFI
ACTOR(ES)	Administrador, Usuario
PROPÓSITO	Mostrar las redes inalámbricas con sus características respectivas.
DESCRIPCIÓN	Iniciará cuando el administrador o usuario escanee las redes WIFI.
PRECONDICIÓN	Haber iniciado sesión, tener una tarjeta o antena inalámbrica, estar o no conectado a la red inalámbrica.
ACTOR(ES) 1.- Abre la aplicación para iniciar sesión. 3.- Estar colocado en la opción de SSID_Canales. 3.- Presionar el botón de Refrescar. .	**APLICACIÓN** 2.- La aplicación abrirá el formulario de inicio de sesión de forma automática. 6.- La aplicación escaneará y mostrará en lista todas las redes inalámbricas cercanas.

CURSO ALTERNO	
POSTCONDICIÓN	Mostrar redes inalámbricas con éxito.

Tabla 16: Escaneo de SSID_WIFI, Caso de Uso Extendido.

Caso de uso #9

En este séptimo caso el administrador o usuario podrá realizar los diferentes reportes de tráfico que el aplicativo puede brindar para la toma de decisiones, en la siguiente tabla se detallará más fondo este caso.

Reportes, Caso de uso extendido.

CASO DE USO	Reportes
ACTOR(ES)	Administrador, Usuario
PROPÓSITO	Mostrar estadísticas e informes del tráfico en la red.
DESCRIPCIÓN	Iniciará cuando el administrador o seleccione un reporte.
PRECONDICIÓN	Haber iniciado sesión.
ACTOR(ES) 1.- Abre la aplicación para iniciar sesión. 3.- Estar colocado en la opción de Reportes. 4.- Seleccionar un reporte que desea. 3.- Presionar el botón de generar reporte.	**APLICACIÓN** 2.- La aplicación abrirá el formulario de inicio de sesión de forma automática e iniciar sesión. 5.- La aplicación mostrará el reporte seleccionado con su información respectiva.
CURSO ALTERNO	
POSTCONDICIÓN	Mostrar los reportes con éxito.

Tabla 17: Reportes, Caso de Uso Extendido.

2.4.4 Diagramas de clases

En el siguiente gráfico muestra un diagrama que describe la estructura del sistema de Monitoreo, tráfico de red y el manejo optimo del ancho de banda mostrando las clases, sus atributos, funciones y las relaciones respectivas entre los objetos.

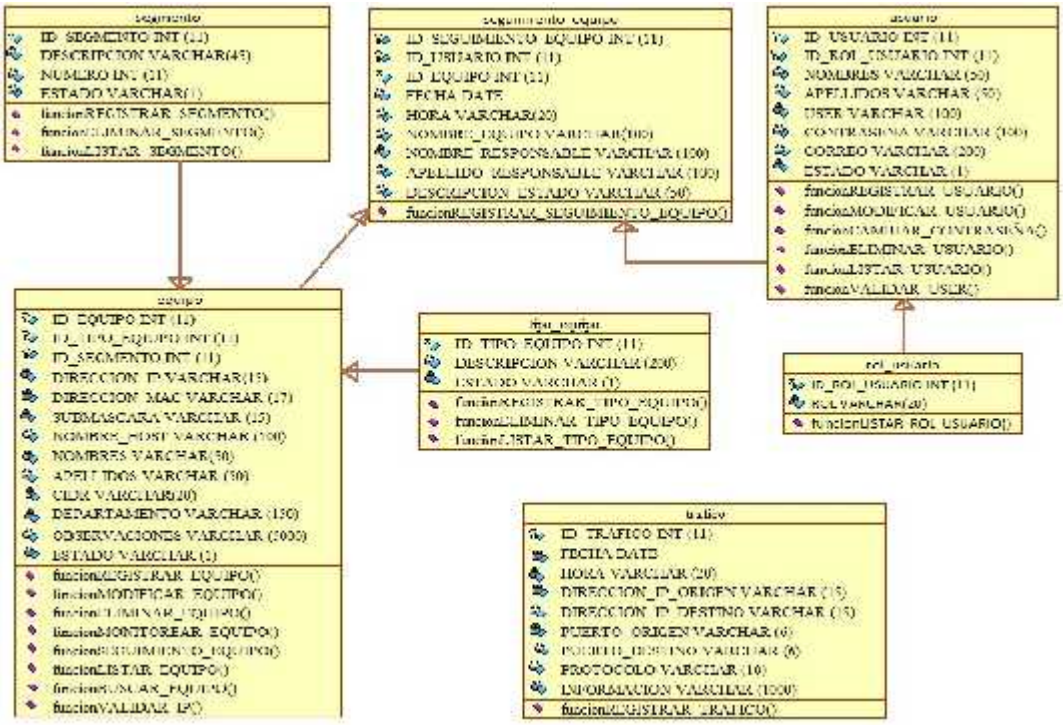


Gráfico 18: Diagrama de clases: NM Traffic.

2.4.5 Estudio de Factibilidad

Después de detallar la descripción del proyecto, objetivos y recursos, se procede a realizar el estudio de factibilidad de la aplicación a desarrollar. Se describirán los costos de hardware, software y gasto varios en relación a la factibilidad financiera.

2.4.5.1 Factibilidad Técnica

Para el desarrollo de la propuesta se realizó el estudio de esta factibilidad y se determinó que el software y el hardware son requeridos a partir de personas naturales o jurídicas para poder llevar a cabo el desarrollo de este aplicativo.

Software: Se considera factible la ejecución de este proyecto porque podemos obtener las herramientas de desarrollo con ambiente de programación desde el internet con licencias libres, y con sus respectivas guías para hacer uso de ellas.

Hardware: También se considera factible porque no se requiere hacer una inversión económica porque se consta con los equipos necesarios para llevar a cabo el desarrollo de la aplicación.

2.4.5.2 Factibilidad Financiera

En el estudio de la factibilidad económica, se determina el presupuesto de costos de los recursos de desarrollo, humanos y los costos de materiales tanto hardware como software para el desarrollo de la aplicación. Los costos del proyecto se describen a continuación:

Personal

En relación al personal solo se requirió un Programador de Sistemas el cual realizó las diferentes tareas para llevar a cabo el desarrollo de este proyecto, se encargó desde la documentación, diseño, desarrollo hasta la respectiva implementación del software de monitoreo.

Duración (Meses)	Descripción	Costo Mensual	Costo Total
6	Programador	$ 600,00	$ 3.600,00
	Total		**$ 3.600,00**

Tabla 18: Personal.

Hardware

En esta propuesta tecnológica el autor fue quien proporciono el hardware porque contaba con estos recursos para que se lleve a cabo la construcción y pruebas del aplicativo.

Valoración	Descripción	Costo
1	Laptop HP – Intel Core i3 – 3Gb Ram	$ 1200,00
1	Antena Wifi Alfa	$ 40,00
Costo Total		**$ 1240,00**

Tabla 19: Hardware, Factibilidad Financiera.

Software

Todos los software que se utilizaron para la presente propuesta tecnológica son de libre distribución (licencia libre) y de código abierto es decir que se puede modificar su código, excepto dos que se necesita obtener su licencia para que se pueda utilizar dentro de la empresa, esto determina que es viable económicamente.

Valoración	Descripción	Costo
1	Microsoft Visual Studio 2010	$ 0,00
1	Microsoft Visual Studio 2015	$ 300,00
1	MySQL Workbench 6.0 CE	$ 200,00
1	WinPcap 4.1.3	$ 0,00
1	SQL Power Architect 1.0.6	$ 0,00
	Costo Total	**$ 5000,00**

Tabla 20: Software, Factibilidad Financiera.

Costo Varios

El proyecto también tendrá costos varios que se detallan a continuación en la siguiente tabla:

Descripción	Costos
Internet	$ 80,00
Viáticos	$ 500,00
Transporte	$ 150,00
Total	**$ 730,00**

Tabla 21: Costo Varios.

Costo Total

A continuación se describirán los costos totales que tendrá que gastarse para realizar este proyecto.

Descripción	Costos
Hardware	$ 1240,00
Software	$ 500,00
Personal	$ 3600,00
Costos Varios	$ 730,00
Total Costos	**$ 6460,00**

Tabla 22: Costo Total, Factibilidad Financiera.

Después de detallar la factibilidad técnica y financiera se determinó que el proyecto de titulación es netamente viable, porque el autor posee los equipos y herramientas necesarias para llevar a cabo esta propuesta tecnológica.

2.4.5.3 Factibilidad Operativa

El aplicativo para el Monitoreo, Control de Tráfico de Red y Manejo Optimo del Ancho de Banda será factible operacionalmente porque será una herramienta muy interactiva, tendrá sus interfaces amigable y de fácil de uso con el usuario ya que podrá interactuar de una mejor manera con ella.

2.4.6 Resultados

En esta sección se detallará de forma gráfica de cómo se visualizará las interfaces del aplicativo de Monitoreo, Control de Tráfico de Red y Manejo Óptimo del Ancho de Banda, además el respectivo análisis de las pruebas de funcionalidad para que de esta manera se pueda comprobar el funcionamiento correcto del mismo.

Diseño del Prototipo

Se diseñará los diferentes bosquejos la cual se asemejarán como la aplicación tendrá la interfaz ante el usuario final y con su respectiva funcionalidad de cada una de ellas.

NM Traffic (Monitoreo, Control de Tráfico de Red y Manejo Óptimo del Ancho de Banda), diseño de Bosquejos del aplicativo.

En el diseño de las interfaces tanto del lado del Administrador como el usuario, son los mismos amigable, interactivo y de fácil uso, en la parte superior se mostrará el menú principal con las diferentes opciones y cierre de sesión, pero para el administrador se le aumentará la opción de Usuarios, en la parte inferior izquierda se mostrará una área en donde se puedan visualizar los equipos (PCs), en la parte central principal se podrá visualizar escaneo de PCs, gráficos en tiempo real, tráfico general o por host, ancho de banda, redes SSID_WIFI, y por último en la parte inferior de la izquierda se mostrará los datos del equipo local , en el centro un conteo de IPs, y en la parte inferior derecha se mostrará el usuario conectado y logoneado en el aplicativo.

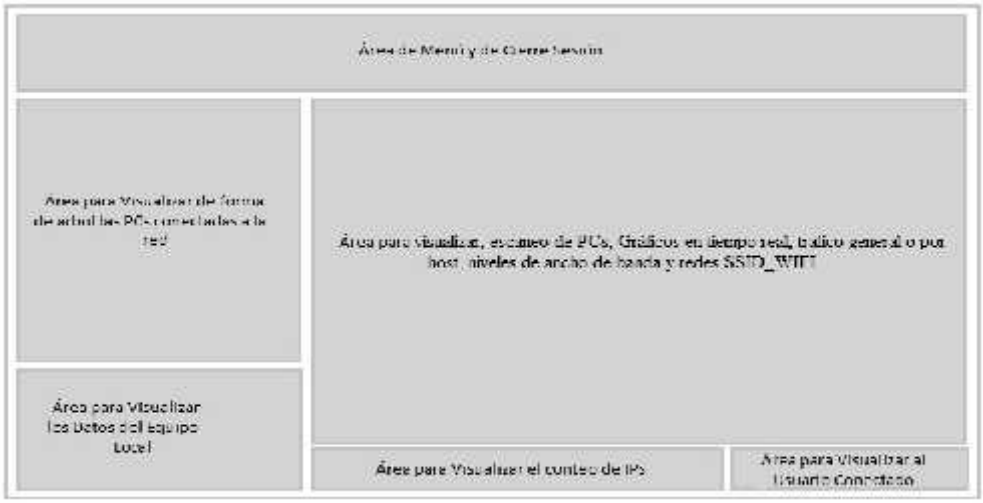


Gráfico 19: Pantalla Principal, Bosquejo

Desarrollo del Prototipo

En relación de los casos de usos y diagrama de clases que se diseñó y que posee el aplicativo de Monitoreo, Control de Tráfico de Red y Manejo Optimo del Ancho de Banda, se desarrolló esta herramienta bajo ambiente de escritorio con la ayuda de la plataforma Visual Studio .Net que sirvió como entorno de programación.

Además se utilizaron librerías y complementos externos debido a que no posee o no vienen por defectos en este software de desarrollo, entre las cuales tenemos librerías

Pcap de *WinPcap* que fueron útiles para poder realizar el escaneo del tráfico en la red, además se utilizó una librería *SpPerfChart* para las gráficas en tiempo real.

Pruebas

En esta sección se procederán a realizar las pruebas correspondientes que ayuden a corroborar que el aplicativo trabaja de una manera correcta y que los usuarios puedan interactuar de manera fácil y rápida, manejando los componentes o las interfaces y poder determinar que el aplicativo es competente para ponerse en marcha y en producción.

Pruebas de funcionalidad

Se realizarán simulaciones de pruebas en el aplicativo de Monitoreo, Control de Tráfico de Red y Manejo Óptimo del Ancho de Banda para detectar y comprobar los posibles defectos que puedan derivarse antes de su uso y productividad, se realizarían pruebas en los diferentes componente que ofrece y comprende la aplicación.

Prueba N° 1: Operaciones de Usuarios	
Objetivo:	Realizar los procesos de registro, modificación y eliminación de usuarios que tienen o no acceso al aplicativo.
Descripción	Verificar las operaciones realizadas.
Nivel de complejidad:	Muy Alta
Caso N° 1: Ingreso de información no duplicadas del nuevo Usuario.	
Datos de entrada	**Datos salida esperados**
Clic en el botón agregar en el formulario de usuario de la aplicación.	Se mostrará el formulario de agregar nuevo registro de usuario.
Ingresar todos los campos obligatorios del formulario.	Se observa y validan que todos los campos que estén ingresados en el formulario.
Clic en el botón guardar	Se mostrará un mensaje de confirmación

	de registro exitoso. Se limpia de forma automática los cuadros de texto para que se pueda ingresar un nuevo usuario en caso de que lo requiera.
Caso N° 2: Ingreso de información duplicada del nuevo Usuario.	
Datos de entrada	**Datos salida esperados**
Dar clic en el botón Nuevo ya iniciada la aplicación. Se Rellena todos los campos del formulario con información duplicada, ejemplo en el campo usuario se ingresa un usuario ya registrado en el sistema. Clic en el botón guardar	Se mostrará el formulario de agregar nuevo registro de usuario. Se observa y validan que todos los campos que estén ingresados en el formulario. Se mostrará un mensaje de datos duplicados.
Caso N° 3: Modificación de información del Usuario.	
Datos de entrada	**Datos salida esperados**
Dar clic en la opción de Usuarios Seleccionar el registro la cual se desea editar. Dar clic en modificar Se procede a editar el registro en cualquier campo. Dar clic en el botón Guardar	Se muestra una lista de todos los usuarios registrados. Se observará el registro que esté seleccionado. Se valida que este seleccionado el registro. Se cargará los datos del registro en el formulario. Se validan que todos los campos estén ingresados. Se presenta un mensaje de confirmación.

Dar clic en SI	Se presenta un mensaje de confirmación de edición exitosa. Se actualiza la lista de los usuarios.
Caso N° 4: Eliminación del Usuario.	
Datos de entrada Dar clic en la opción de Usuarios Seleccionar el registro la cual se desea eliminar. Dar clic en eliminar Dar clic en SI	**Datos salida esperados** Se muestra una lista de todos los usuarios registrados. Se observará el registro que esta seleccionado. Se mostrará un mensaje de confirmación Se eliminara el registro exitosamente. Se actualiza la lista de usuarios registrados.
Responsables implicados:	**Administradores**
Resultados de la Prueba	
Defectos obtenidos	
Proceso en el caso 1, 2, 3 y 4 correctos	**_X_ Ejecución de manera correcta** **____ Ejecución de manera errónea** **____ Ejecución con Detección de errores**

Tabla 23: Pruebas de Funcionalidad Operaciones de Usuarios.

Prueba N° 2: Inicio de Sesión	
Objetivo:	Realizar la operación de iniciar sesión en el aplicativo.
Descripción:	Iniciar sesión de forma correcta.
Nivel de complejidad:	Media
Caso N° 1: Ingreso correcto	

Datos de entrada	**Datos de salida esperados**
Iniciar la aplicación	Se visualizará el formulario de inicio de sesión.
Ingresar su usuario y contraseña registrados.	Se observará y se validan que los campos estén ingresados.
Dar clic en el botón Aceptar	Se mostrará la página principal del aplicativo.
Caso N° 2: Ingreso fallido	
Datos de entrada	**Datos de salida esperados**
Iniciar la aplicación	Se visualizará el formulario de inicio de sesión.
Ingresar su usuario y contraseña.	Se observará y se validan que los campos estén ingresados.
Dar clic en el botón Aceptar	Se mostrará un mensaje de error de usuario o contraseñas incorrectas.
Responsables implicados:	**Administradores y Usuarios**
Resultados de la Prueba	
Defectos obtenidos:	
Proceso en el caso 1 y 2 correctas	**_X_ Ejecución de manera correcta** **____ Ejecución de manera errónea** **____ Ejecución con Detección de errores**

Tabla 24: Pruebas de Funcionalidad Inicio de Sesión.

Prueba N° 3: Operaciones de Equipos	
Objetivo:	Realizar las operaciones de registro,

	modificación y eliminación de los equipos conectados a la red.
Descripción	Verificar de procesos realizados.
Nivel de complejidad:	Alta
Caso N° 1: Ingreso de información no duplicada del nuevo Equipo.	
Datos de entrada	**Datos salida esperados**
Clic en el botón agregar del ítem de equipo iniciada la aplicación. Ingresar todos los campos requeridos del formulario. Clic en el botón Guardar	Se mostrará el formulario de agregar nuevo equipo. Se observa y se validan que todos los campos que estén ingresados en el formulario. Se mostrará un mensaje de confirmación de registro exitoso. Se limpia de forma automática los campos, para que se pueda ingresar un nuevo equipo en caso de que lo requiera.
Caso N° 2: Ingreso de información duplicados del nuevo Equipo.	
Datos de entrada	**Datos salida esperados**
Clic en el botón agregar en ítem de equipos iniciada la aplicación. Se Rellena todos los campos del formulario con información duplicada, ejemplo en el campo dirección IP se ingresa una IP ya registrado en el sistema. Dar clic en el botón guardar	Se mostrará el formulario de agregar nuevo usuario. Se observa y validan que todos los campos que estén ingresados en el formulario. Se mostrará un mensaje de datos duplicados.
Caso N° 3: Modificación de datos del Equipo.	
Datos de entrada	**Datos salida esperados:**

Dar clic en la opción de Equipos Seleccionar el registro la cual se desea editar. Dar clic en modificar Se procede a editar el registro en cualquier campo. Dar clic en el botón Guardar Dar clic en SI	Se muestra una lista de todos los equipos registrados. Se observará el registro que esta seleccionado. Se valida que este seleccionado el registro. Se cargará los datos del registro en el formulario. Se validan que todos los campos estén ingresados. Se presenta un mensaje de confirmación. Se presenta un mensaje de confirmación de edición exitosa. Se actualiza la lista de los equipos.
Caso N° 4: Eliminación de un Equipo.	
Datos de entrada Dar clic en la opción de Equipo Seleccionar el registro la cual se desea eliminar. Dar clic en eliminar Dar clic en SI	**Datos salida esperados** Se muestra una lista de todos los equipos registrados. Se observará el registro que esta seleccionado. Se mostrará un mensaje de confirmación Se eliminará el registro exitosamente. Se actualiza lista de equipos registrados.
Responsables implicados:	**Administradores y Usuarios**
Resultados de la Prueba	
Defectos obtenidos	
Proceso en el caso 1, 2, 3 y 4 correctas	**_X_ Ejecución de manera correcta** **____ Ejecución de manera errónea**

	____ Ejecución con Detección de errores

Tabla 25: Pruebas de Funcionalidad Operaciones de Equipos.

Prueba N° 4: Operaciones de Escaneo de PCs	
Objetivo:	Realizar las operaciones de iniciar y parar escaneo de PCs conectados a la red.
Descripción	Verificar las operaciones realizadas.
Nivel de complejidad:	Alta
Caso N° 1: Iniciar de Escaneo de PCs	
Datos de entrada Seleccionar un adaptador de red ya iniciada la aplicación. Dar clic en el botón Iniciar.	**Datos salida esperados** Se visualizará el rango de ip obtenidas dependiendo a que red a la que esté conectada. Se mostrará un listado con todos los equipos conectados a la red con su debida información.
Caso N° 2: Parar de Escaneo de PCs	
Datos de entrada Dar clic en el botón Parar.	**Datos salida esperados** Se cancelará el escaneo y no se podrá observar los demás equipos conectados o no a la red.
Responsables implicados:	**Administradores y Usuarios**
Resultados de la Prueba	
Defectos obtenidos	
Proceso en el caso 1 y 2 correctas	**_X_ Ejecución de manera correcta** **____ Ejecución de manera errónea** **____ Ejecución con Detección de**

	errores

Tabla 26: Pruebas de Funcionalidad Operaciones de Escaneo de PCs.

Prueba N° 5: Operaciones de Escaneo de Tráfico de red	
Objetivo:	Realizar las operaciones de iniciar y parar escaneo de tráfico de la red local.
Descripción	Verificar las operaciones realizadas.
Nivel de complejidad:	Alta
Caso N° 1: Iniciar de Escaneo de Tráfico de red	
Datos de entrada Seleccionar un adaptador de red y dar clic en iniciar ya iniciada la aplicación.	**Datos salida esperados** Se mostrará un listado con todos los paquetes que circulan a través de la red con su debida información.
Caso N° 2: Parar Escaneo de Tráfico de red	
Datos de entrada Dar clic en el botón Parar.	**Datos salida esperados** Se cancelará el escaneo y no se podrá observar los demás paquetes.
Responsables implicados:	**Administradores y Usuarios**
Resultados de la prueba	
Defectos obtenidos	
Proceso en el caso 1 y 2 correctas	**_X_ Ejecución de manera correcta** **____ Ejecución de manera errónea** **____ Ejecución con Detección de errores**

Tabla 27: Pruebas de Funcionalidad Operaciones Tráfico de red.

Prueba N° 6: Operaciones de Escaneo de Tráfico de red por Host	
Objetivo:	Realizar las operaciones de iniciar y parar

	escaneo de tráfico por host de la red local.
Descripción	Verificar las operaciones realizadas.
Nivel de complejidad:	Alta
Caso N° 1: Iniciar de Escaneo de Tráfico de red por Host	
Datos de entrada: Iniciado el escaneo tráfico de red general y seleccionado un equipo conectado.	Datos salida esperados: Se mostrará sus campos más relevantes en el formulario de escaneo de tráfico por host y comenzará a listar todo sus paquetes filtrados por dicha ip y con su debida información.
Caso N° 2: Parar Escaneo de Tráfico de red por Host	
Datos de entrada Dar clic en el botón Parar.	**Datos salida esperados** Se cancelará el escaneo y no se podrá observar los demás paquetes.
Responsables implicados:	**Administradores y Usuarios**
Resultados de la Prueba	
Defectos obtenidos	
Proceso correcto en el caso 1 y 2	**_X_ Ejecución correcta** **____ Ejecución errónea** ____ Detección de errores

Tabla 28: Pruebas de Funcionalidad Operaciones Tráfico de red por Host.

Prueba N° 7: Consulta de Ancho de Banda	
Objetivo:	Realizar la consulta de los niveles de ancho de banda que posee el equipo.
Descripción	Verificar su ancho de banda de subida y descarga.

Nivel de complejidad:	Media
Caso N° 1: Acceso a Internet	
Datos de entrada Dar clic en Actualizar una vez iniciado el aplicativo.	**Datos salida esperados** Se mostrará una página cargando el medidor de ancho de banda.
Caso N° 2: Sin Acceso a Internet	
Datos de entrada: Dar clic en Actualizar una vez iniciado el aplicativo.	**Datos salida esperados:** Se mostrará una página con mensaje de no tener acceso a internet.
Responsables implicados:	**Administradores y Usuarios**
Resultados de la Prueba	
Defectos obtenidos	
Proceso en el caso 1 y 2 correctas	**_X_ Ejecución de manera correcta** **____ Ejecución de manera errónea** **____ Ejecución con Detección de errores**

Tabla 33: Pruebas de Funcionalidad Consulta de Ancho de Banda.

Prueba N° 8: Escaneo de Redes WIFI SSID	
Objetivo:	Realizar el escaneo de las redes WIFI inalámbricas visibles y saber en qué canal están operando.
Descripción	Verificar el escaneo de los SSID y canales.
Nivel de complejidad:	Media
Caso N° 1: Redes WIFI Visibles	
Datos de entrada:	**Datos salida esperados:**

Dar clic en Actualizar una vez iniciado el aplicativo.	Se mostrará un listado y de manera gráfica todas las redes WIFI con su debida información.
Responsables implicados:	**Administradores y Usuarios**
Resultados de la Prueba	
Defectos obtenidos	
Proceso en el caso 1 correcta	**_X_ Ejecución de manera correcta** **____ Ejecución de manera errónea** **____ Ejecución con Detección de errores**

Tabla 29: Pruebas de Funcionalidad Escaneo de Redes WIFI SSID.

Prueba N° 9: Reportes	
Objetivo:	Generar los reportes respectivos sobre el tráfico de red.
Descripción:	Verificar los procesos realizados
Nivel de complejidad:	Media
Caso N° 1: Generación de reportes con información.	
Datos de entrada: El administrador o usuario deberá haber iniciado sesión. Dar clic en reportes. Dar clic sobre un reporte En caso de poseer parámetros de brusquedad se ingresara o se escogerá.	**Datos de salida esperados** Se desglosa los diferentes reportes. Se generará y observará el reporte seleccionado.
Caso N° 2: Generación de reportes sin información.	
Datos de entrada:	**Datos de salida esperados**

El administrador o usuario deberá haber iniciado sesión. Dar clic en reportes. Dar clic sobre el reporte requerido. En caso de poseer parámetros de brusquedad se ingresará o se escogerá.	Se desglosa los diferentes reportes. Se generará pero no observará el reporte debido a los filtros ingresados porque no se encontraron.
Responsables implicados:	**Administradores y Usuarios**
Resultados de la Prueba	
Defectos obtenidos	
Proceso en el caso 1 y 2 correctas	**_X_ Ejecución de manera correcta** **____ Ejecución de manera errónea** **____ Ejecución con Detección de errores**

Tabla 30: Pruebas en Reportes.

2.4.6.1 Resultados Finales

Las personas que fueron encuestadas son el administrador y demás usuarios que conforman el departamento de Tecnología de la empresa AGUAPEN EP, quienes les pareció de mucho interés en que se implemente un aplicativo que no solo contenga el proceso de analizador de tráfico de red, sino también monitoreo, registros de equipos y análisis de canales de redes inalámbricas, esta herramienta será de gran utilidad y ayuda para ellos.

Se obtuvo un prototipo de acuerdo a los requerimientos y opiniones establecidos por el encargado del departamento, quien dio a conocer las fallas que se presentan y que además no cuenta con una herramienta que realice esos procesos para que pueda encontrar el problema que se está dando.

El uso de la tecnología como lo que es WinPcap que es muy utilizada para analizar una red, porque este complemento brinda información del tráfico que se genera dentro de la red y que será muy útil porque podrá encontrar fallas que se producen en ella. Esta tecnología es utilizada por muchos aplicativos que tienen el mismo objetivo de analizar el tráfico en una red de datos como lo es Wireshark.

El prototipo se desarrolló bajo la plataforma de programación Visual Studio 2015 y de repositorio de base de datos la herramienta MySql Workbench, las cuales son de licencia libre y de distribución gratuita, además estas herramientas posee un sitio online en donde se puede hacer consultas de sus diferentes uso y funcionalidad que ellas brindan.

El aplicativo logra capturar todos los equipos que se encuentran conectados a la red de forma inalámbrica o a través de cable de manera eficaz y rápida, dando a conocer su información respectiva como la dirección IP, segmento de red, nombre del equipo, etc. Además el administrador podrá registrar y consultar esta información de cada uno de estos usuarios y de su equipo de trabajo para poder llevar un control sobre ellos.

En esta herramienta, para llevar a cabo los procesos de monitoreo de datos en la red posee la seguridad respectiva, cuenta con las debidas validaciones necesarias para el proceso de inicio de sesión y restauración de contraseña o cambio de contraseña y así evitar el problema debido a intrusos, la seguridad que el aplicativo brinda es muy eficiente.

Al momento de instalar la aplicación se pudo comprobar que la instalación se llevó a cabo de manera correcta hasta su finalización, debido a que el Sistema Operativo es compatible e indicado para el software.

Durante las pruebas de funcionalidad se pudo comprobar la eficacia y eficiencia del aplicativo, de la misma manera pudo responder a las peticiones que el usuario

realizaba para poder llevar a cabo de forma rápida los procesos de monitoreos y escaneo, cabe destacar que en un ambiente real de trabajo el tráfico será más fluido y así mismo habrá más Access Point para detectar con el aplicativo.

Se realizó las pruebas en el aplicativo en un área de mayores conexiones a los Access Point durante 30 minutos para obtener datos reales, que se pueda observar el comportamiento y nivel de tráfico en la red de datos, que todas las funcionalidades de este proceso se lleven a cabo de manera correcta, así mismo de la misma manera el proceso de escaneo de redes WIFI para conocer su debida información de cada una de ellas y observar en que canales están trabajando.

En el momento del escaneo de equipos se pudo corroborar que todo el rango de IPs fueron escaneadas correctamente, sin embargo toma un cierto tiempo para realizar la consulta en cada una de ellas y poder detectarla, se puede monitorear la cantidad que desee de equipos, el aplicativo donde está instalado debe estar conectada a una red para poder realizar este proceso.

Pruebas en el Área de la Universidad Estatal Península de Santa Elena "UPSE"

En esta área se pudo obtener estos resultados que se muestran a continuación:

Inicio de Sesión

Gráfico 20: Inicio de Sesión

En este proceso el usuario se pudo logonear de manera satisfactoria, quien ingreso su usuario, contraseña y después de lo ingresado se dio clic en el botón ingresar para poder visualizar la siguiente interfaz (interfaz principal).

Datos del Equipo

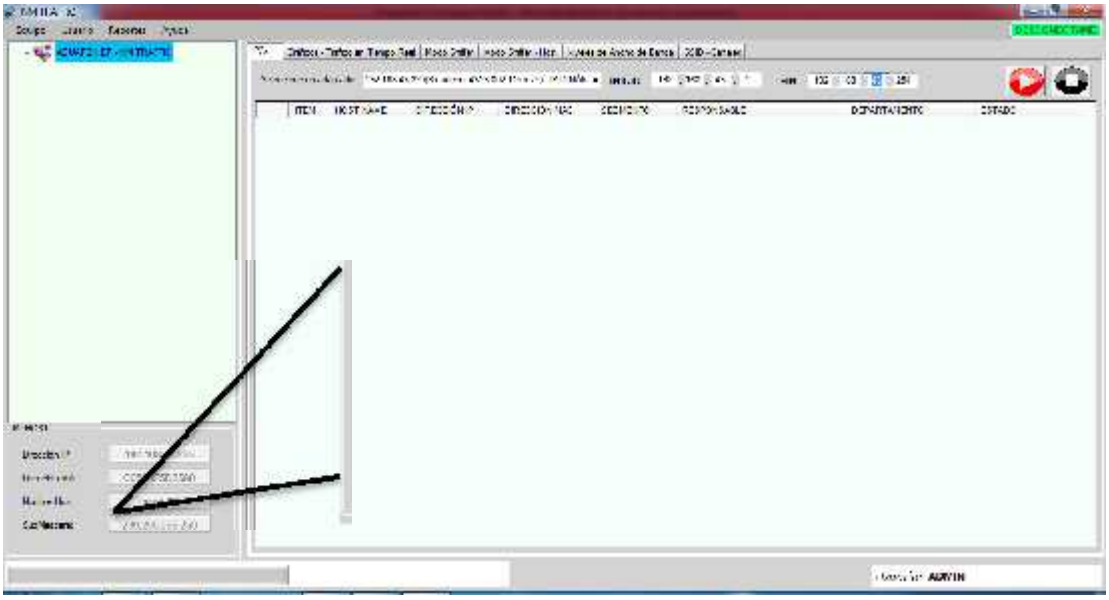


Gráfico 21: Datos del Equipo

En esta sección se pudo observar que los datos del equipo como dirección IP dirección MAC y demás son los que se obtuvo de manera automática en el momento que se ejecutó la aplicación, estos datos son obtenidos del equipo local y de la red a la cual esté conectado por medio inalámbrico y por cable.

Escaneo de Equipos

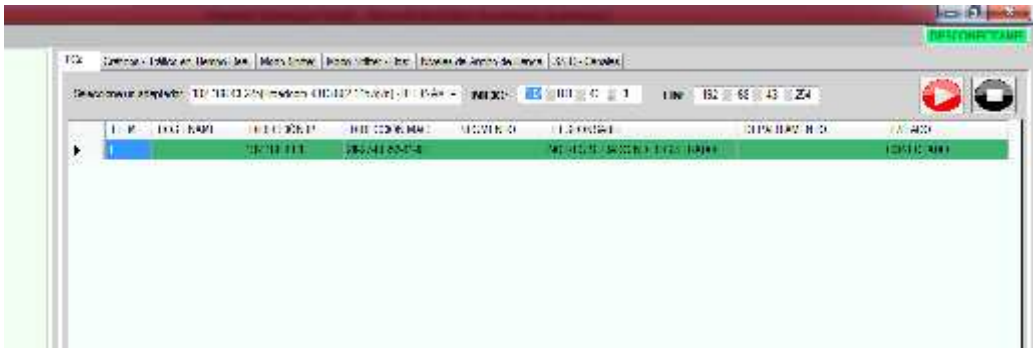


Gráfico 22: Escaneo de Equipos

Se pudo observar que esta funcionalidad se llevó a cabo de manera correcta, el escaneo de equipos se lo realizó mediante la selección de un adaptador de red la cual brindó un rango de IPs por defecto que fueron utilizados. Luego de estos pasos se dio clic en el botón play para iniciar el escaneo y de manera automática se listaron los equipos detectados.

Tráfico de Red

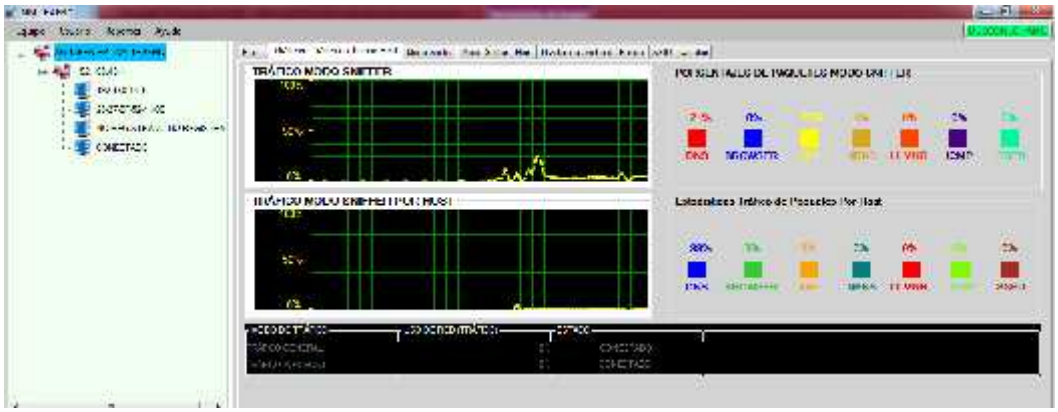


Gráfico 23: Tráfico de red forma gráfica

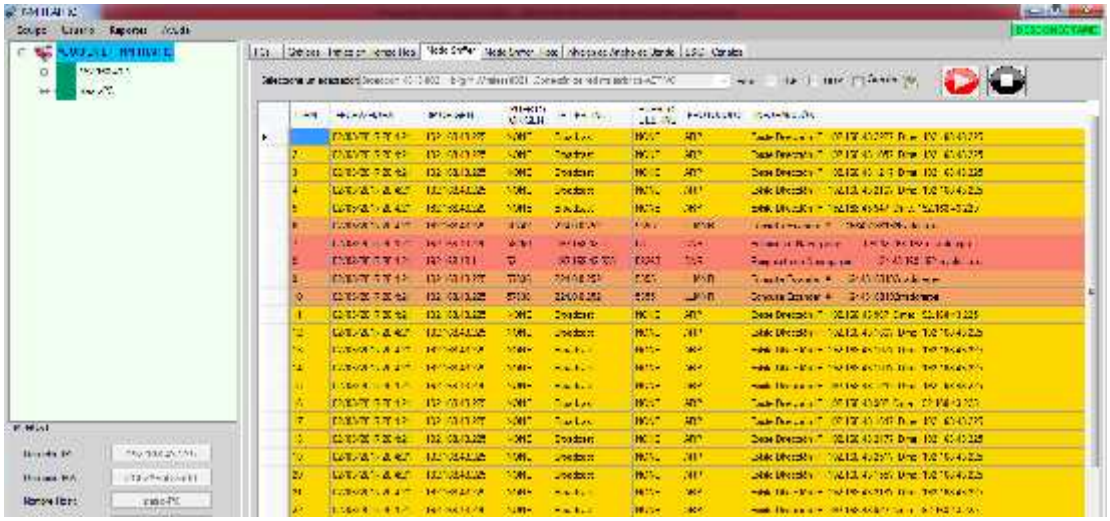


Gráfico 24: Tráfico de Red

En esta interfaz se pudo comprobar que el escaneo del tráfico de la red se lo realizó de forma correcta, este proceso se llevó a cabo de la siguiente manera, se seleccionó un adaptador de red la cual estaba conectada a la red y a internet. Luego de este paso se dio clic en el botón play quien llevó a esta operación ponerse en marcha y de

manera automática se listaban los paquetes de información y también de forma gráfica de acuerdo a los datos obtenidos de los paquetes de la lista.

Trafico Por Host

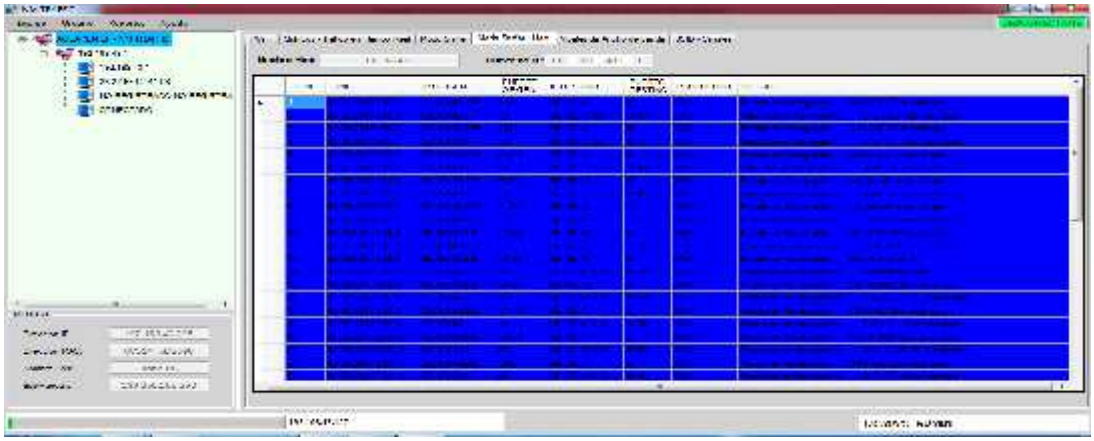


Gráfico 25: Tráfico por host

En este punto se pudo observar que el escaneo de tráfico mediante un host seleccionado se llevó a cabo de forma satisfactoria. Este proceso se lo realizó mediante los siguientes pasos, mientras se ejecutaba el proceso de tráfico de red se seleccionó un equipo cualquiera que estaba conectada a la misma red de listado de equipos detectados, y de manera automática se empezó a listar el tráfico.

Ancho de Banda de Internet

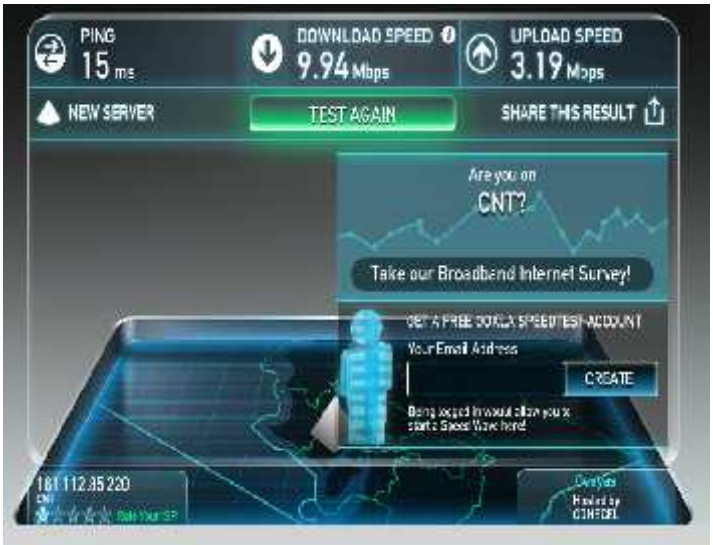


Gráfico 26: Niveles de Ancho de Banda

En esta funcionalidad se corroboró que los datos de niveles de ancho de banda que se obtuvieron de una URL de test de velocidad de internet fueron realizados correctamente. Este proceso se realizó mediante al hacer clic en el botón refrescar la cual posee una función de solicitud de test de ancho de banda y de manera automática presenta los niveles de subida y descarga en megas.

Escaneo de Redes WIFI

Gráfico 27: Escaneo de Redes WIFI listado

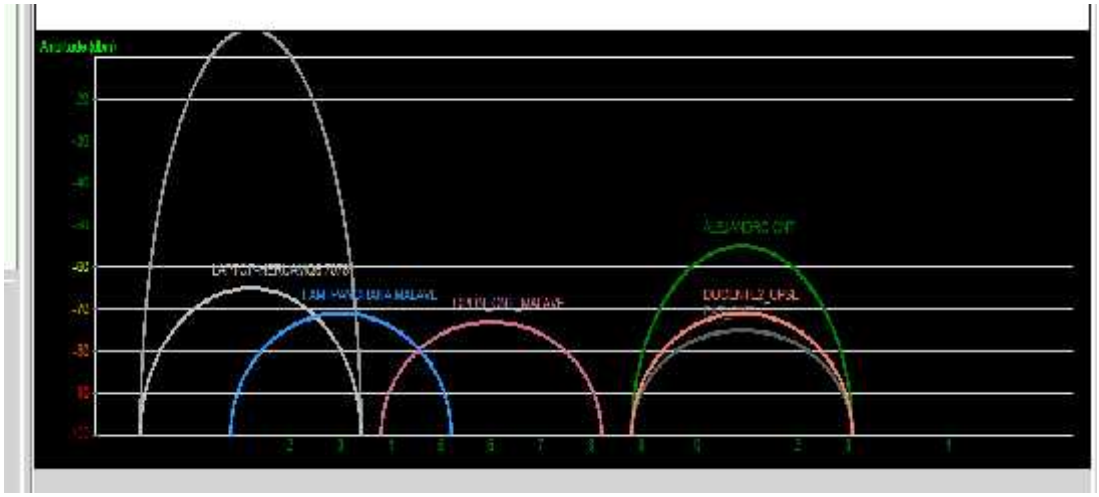


Gráfico 28: Escaneo de Redes WIFI

Se pudo comprobar que el escaneo de Puntos de Acceso o Redes Inalámbricas WIFI, se realizó satisfactoriamente y se lo llevó a cabo de la siguiente manera, se seleccionó un adaptador WIFI y al hacer clic en el botón de escaneo automáticamente se listaron todas las redes WIFI cercanas, también de forma gráfica se pudo presentar.

Reportes

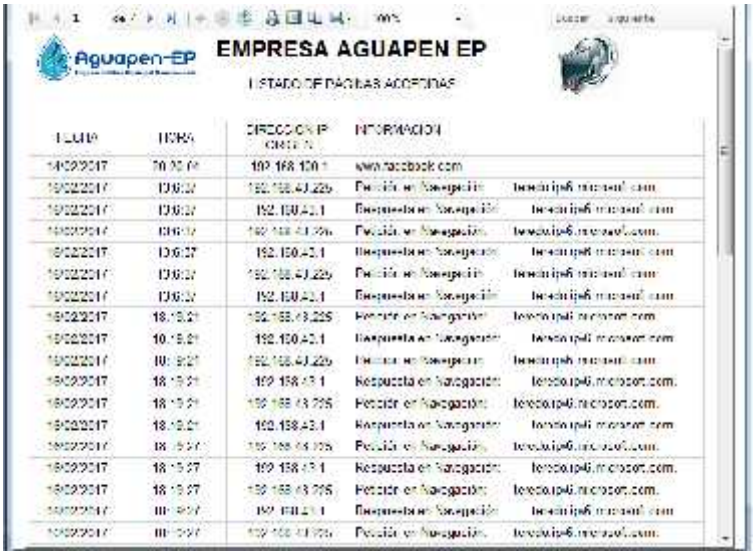


Gráfico 29: Reportes

En este punto los reportes son de mucha utilidad para el administrador, en este módulo se comprobó que los documentos generados fueron los adecuados y correctos para el administrador. Este proceso se llevó a cabo mediante la selección del tipo de información la cual se requiere visualizar, y al hacer clic en generar se pudo observar de forma automática un archivo de texto con los datos en forma de lista o de manera estadística.

CONCLUSIONES

Al implementar la herramienta propuesta lograra un monitoreo de tráfico de red en tiempo real, sondeo de canales WIFI y control de direcciones IP de cada PC con su respectiva información del usuario encargado.

La información que proporciona el aplicativo, ayudará a tomar decisiones y a evaluar servicios de la red, ancho de banda y uso del internet.

Mayor performance y respuesta en los procesos internos que ejecuta la organización, debido a que la red estará más disponible al tener un mejor control y restricciones dentro de ella.

El uso de herramientas para el monitoreo de redes es una aplicación fundamental del encargado de TI institucional, apoyándolo a encontrar problemas y optimizando los tiempo de atención por el soporte a esta índole.

RECOMENDACIONES

Dejar establecido como política de TI que cada cierto tiempo se realice un análisis de tráfico de la red local, monitoreos y mantenimientos de los equipos de comunicación para obtener un buen enlace y evitar que se generen problemas de interferencias, colapsos, pérdidas de información o mala conexión.

Hacer que la herramienta en cuestión en una segunda versión pueda ser accedida remotamente a través de una interfaz web para que el administrador pueda realizar sus monitoreos desde cualquier lugar que se encuentre.

Usar el proyecto como base para experimentar en el uso de nuevas librerías que agiliten el monitoreo de paquetes y protocolos de comunicación en interfaces multiplataforma.

BIBLIOGRAFÍAS

[1] M. Casado Tebar. (2016, Noviembre) ESCUELA POLITÉCNICA DEL EJÉRCITO [Online]. 1, 1. Disponible en: http://docplayer.es/703135-Escuela-politecnica-del-ejercito.html#show_full_text

[2] M. Medina. (2016, Noviembre). Simulador de Protocolos de Comunicaciones. DSpace en ESPOL [Online]. 5(2), 3-10. Disponible en: https://www.dspace.espol.edu.ec/bitstream/123456789/8148/1/Tesis-Simulador_Protocolos_Comunicaciones.pdf

[3] R. Zeas Martínez. (2016, Noviembre). Análisis Y Captura de Paquetes de Datos en una Red mediante la Herramienta Wireshark [Online]. 5(2), 8-24. Disponible en: http://190.11.245.244/bitstream/47000/168/1/UISRAEL-EC-SIS-378.242-404.pdf

[4] E. Barahona Delgado. (2016, Noviembre). DSpace en ESPOL: Analizador de trafico de red. DSpace en ESPOL [Online]. 5(2), 9-14. Disponible en: www.dspace.espol.edu.ec/bitstream/123456789/20042/1/Tesis%20Barahona-Gellibert.docx

[5] L. Lerones Fernández. (2016, Noviembre). Desarrollo de un analizador de red (SNIFFER) [Online]. 1(1), 9. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/454/1/38443tfc.pdf

[6] P. Jiménez Almagro (2016, Noviembre). Tesis Pablo Jiménez Danny Pucha - Repositorio Digital-UPS [Online]. 2(5), 27. Disponible en: http://dspace.ups.edu.ec/bitstream/123456789/10173/1/UPS%20-%20ST001813.pdf

[7] R. Redondo Núñez. (2016, Noviembre). Control de tráfico y administración de ancho de banda en linux con tcng [Online]. 2(1), 3-5. Disponible en: http://docplayer.es/12733097-Control-de-trafico-y-administracion-de-ancho-de-banda-en-linux-con-tcng.html

[8] Microsoft. (2016, Noviembre). Introducción a. NET Framework [Online]. 1, 1 Disponible en: https://msdn.microsoft.com/es-es/library/hh425099(v=vs.110).aspx

[9] A. Cobo. (2016, Diciembre). PHP y MySQL: Tecnología para el desarrollo de aplicaciones web [Online]. 12(4), 210-211. Disponible en: https://books.google.com.ec/books?id=zMK3GOMOpQ4C&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

[10] eSandra. (2016, Noviembre). Curso de MySQL (I): Introducción a las Bases de Datos Relacionales [Online]. 1, 1. Disponible en: http://www.esandra.com/mysql-i-introduccion-a-las-bases-de-datos-relacionales/

[11] L. Nina Limachi. (2016, Julio). Sniffers. Revista de Información, Tecnología y Sociedad – Sniffers [Online]. 1, 36-37. Disponible en: http://www.revistasbolivianas.org.bo/pdf/rits/n8/n8a16.pdf

[12] B. E. Bonilla Tumbaco. (2017, Enero). Diseño e implementación de una auditoría de seguridad a la información a los datos sensibles de un centro de educación superior [Online]. 2(2), 21-25. Disponible en: http://repositorio.upse.edu.ec/bitstream/46000/3709/1/UPSE-TIN-2015-0029.pdf

[13] J. WIESEL. (2016, Mayo). Cómo Instalar y Usar Nmap [Online]. 1, 2-3.Disponible en: http://codehero.co/como-instalar-y-usar-nmap/

[14] H. Castro. (2016, Mayo). tutorial analizador de protocolos “wireshark” - Universidad de los Andes [Online]. 1, 1. Disponible en: https://sistemasacademico.uniandes.edu.co/~isis3204/dokuwiki/lib/exe/fetch.php?media=tutoriales:tutorial_wireshark_rev_1.pdf

[15] Fiscalía General del Estado. (2017, Enero). Los delitos informáticos van desde el fraude hasta el espionaje [Online]. 1, 1. Disponible en: http://www.fiscalia.gob.ec/index.php/sala-de-prensa/3630-los-delitos-inform%C3%A1ticos-van-desde-el-fraude-hasta-el-espionaje.html

GLOSARIO

802.11: Tipo de estándar IEEE que define el uso de capas física y de enlace de datos del modelo OSI.

Browser: Browser o navegador web es un programa que permite ver la información que contiene una página web

Conmutador: Es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa de enlace de datos del modelo OSI.

Cuellos de botella: Cuando la capacidad de procesamiento de un dispositivo es mayor que la capacidad del bus al que se encuentra conectado el dispositivo.

Desktop: Computadora de escritorio u ordenador de mesa, es una computadora personal que es diseñada para ser usada en una ubicación estable.

Enrutador: Es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red) del modelo OSI.

Ethernet: Ethernet es un estándar de redes de computadoras de área local con acceso al medio.

Frame: También conocido como trama o paquete de datos usados en el nivel de enlace de datos del modelo OSI.

Java: Es un lenguaje de programación orientado a objetos, desarrollado por Sun Microsystems.

Multicast: Es el envío de la información en una red a múltiples destinos simultáneamente.

NetBIOS: Network Basic Input/Output System, es una especificación de interfaz para acceso a servicios de red, es decir, una capa de software desarrollado para enlazar un sistema operativo de red con hardware específico.

Netbook: Es una categoría de ordenador portátil de bajo costo y generalmente reducidas dimensiones, lo cual aporta una mayor movilidad y autonomía.

NetFlow: Es un Protocolo de red desarrollado por Cisco Systems para la recopilación de información de tráfico IP.

OSI: El modelo de interconexión de sistemas abiertos, también llamado es el modelo de red descriptivo creado por la Organización Internacional para la Estandarización. (ISO)

Paquete de datos: Un paquete de datos es una unidad fundamental de transporte de información en todas las redes de computadoras modernas.

Protocolos: Un protocolo es una regla que controla la comunicación en su forma más simple, un protocolo puede ser definido como las reglas que dominan la sintaxis, semántica y sincronización de la comunicación.

Sniffer: Significa analizador de paquetes, es un programa de captura de las tramas de una red de computadoras.

Software Libre: Es la denominación del software que respeta la libertad de los usuarios sobre su producto adquirido y, por tanto, una vez obtenido puede ser usado, copiado, estudiado, modificado y redistribuido libremente

Software: Comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas.

Subnetting: Es una colección de direcciones IP que permiten definir el número de redes y de host que se desean utilizar en una subred determinada

Tabla de enrutamiento: Es un documento electrónico que almacena las rutas a los diferentes nodos en una red informática.

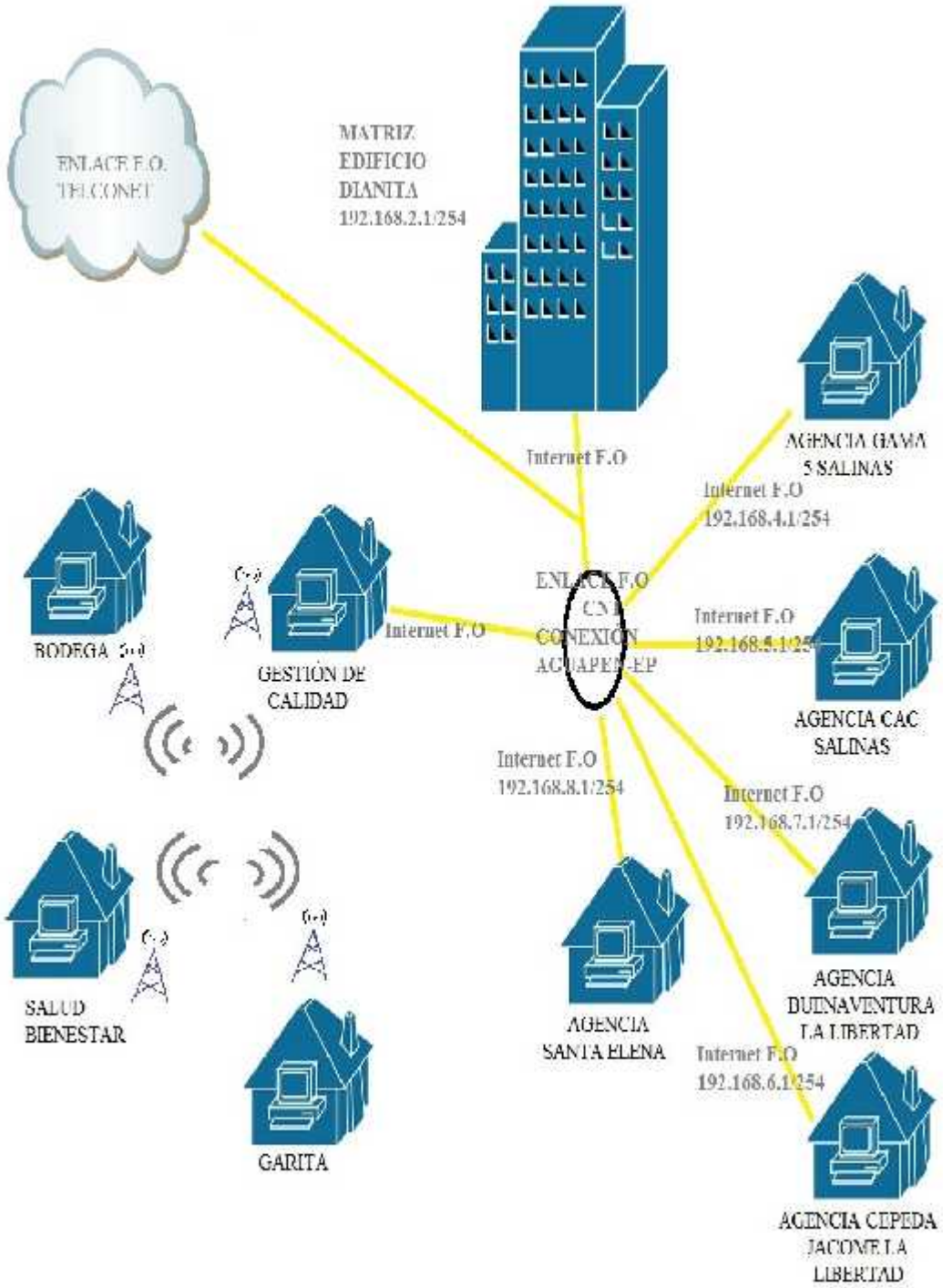
Topología Bus: Se caracteriza por tener un único canal de comunicaciones denominado bus, troncal o backbone al cual se conectan los diferentes dispositivos.

Trama: Es una unidad de envío de datos en el nivel de enlace de datos.

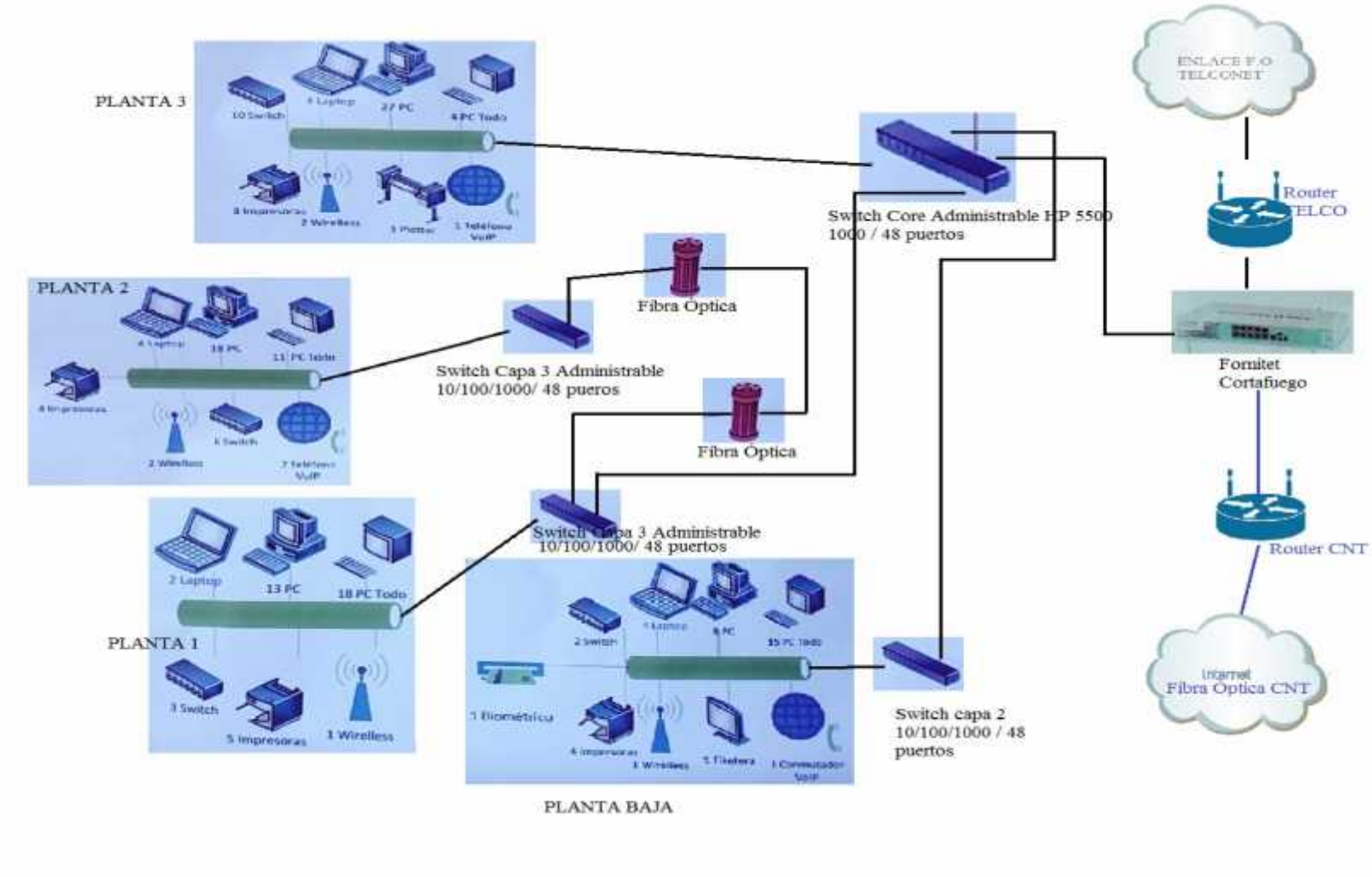
Virus: Programa informático que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario.

ANEXOS

ARQUITECTURA GENERAL DE LA RED DE LA EMPRESA AGUAPEN-EP



MATRIZ AGUAPEN-EP



UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA FACULTAD DE SISTEMAS Y TELECOMINCACIONES ESCUELA DE INFORMÁTICA

Encuesta

Buenos Tardes, para cumplir con los requerimientos propuestos, solicitamos de forma amable a ustedes que conforman parte del departamento de tecnología nos proporcionen información real, agradeciéndole de antemano por la atención brindada a la encuesta.

1. **¿Cuánto tiempo se demora en carga o descargar un archivo debido a la lentitud del servicio de internet de acuerdo a su conexión cableado o inalámbrico?**

( ) 0-15 minutos ( ) 16-30 minutos ( ) 31-54 minutos ( ) 46-60 minutos ( ) Más de 1 hora

2. **¿Con que frecuencia usted debe reiniciar el dispositivo WIFI debido a no tener acceso a la red?**

( ) Siempre ( ) Casi Siempre ( ) Algunas Veces ( ) Muy Pocas Veces ( ) Nunca

3. **¿Cuantas veces usted debe reiniciar su equipo de trabajo debido a que las aplicaciones son lentas y a veces tardan mucho tiempo en responder ya que el tráfico en la red es muy lento?**

( ) Siempre ( ) Casi Siempre ( ) Algunas Veces ( ) Muy Pocas Veces ( ) Nunca

4. **¿Cuantas veces le ha pasado que su dispositivo detecta el Access Point pero no se puede conectar a la red inalámbrica?**

( ) Todos los días ( ) frecuentemente ( ) De vez en cuando ( ) Rara vez ( ) Nunca

5. **¿Con que frecuencia usted debe configurar el canal de la red inalámbrica WIFI debido a las interferencias o solapamiento de otras redes inalámbricas?**

( ) Siempre ( ) Casi Siempre ( ) Algunas Veces ( ) Muy Pocas Veces ( ) Nunca

6. **¿Conoces algunas de las herramientas de monitoreo de tráfico de red que se listan a continuación?**
   - Dumpper
   - IpScan
   - NMAP
   - WireShark

- IP Traffic Monitor

Otros_____

7. ¿Estaría de acuerdo que en su área de trabajo se implemente un software para el análisis de tráfico de la red?

Si [ ] No [ ]

Si la respuesta es Si explicar el por qué.

¿Por qué?

_____
_____

8. ¿Con que frecuencia se debería realizar un monitoreo de trafico de red?

( ) Nunca
( ) Solo cuando se presente un problema en la red local
( ) Parcialmente
( ) Continuamente
( ) Todos los días

9. ¿Usted cree que con la ayuda de un analizador de tráfico de red le ayudaría a minimizar y solucionar fallas que existan dentro de la red? ¿Por qué?

_____
_____

10. ¿Estaría de acuerdo que en el aplicativo se implemente una opción para medir la tasa de transferencia relacionada con el ancho de banda que se está utilizando? ¿Por qué?

_____
_____