EVALUACIÓN DE DIVERSAS HERRAMIENTAS TECNOLÓGICAS PARA EL ANÁLISIS DE TRÁFICO DE LA RED DE DATOS EN LA CARRERA DE TECNOLOGÍA DE LA INFORMACIÓN

EVALUATION OF VARIOUS TECHNOLOGICAL TOOLS FOR THE ANALYSIS OF DATA NETWORK TRAFFIC IN THE INFORMATION TECHNOLOGY CAREER

Iván Jair Chóez Quimis [1*]

[1] Maestrando el Programa de Maestría de Tecnologías de la Información y la Comunicación. Ingeniero en Computación y Redes. Instituto de Posgrado. Universidad Estatal del Sur de Manabí. Ecuador. ORCID: https://orcid.org/0000-0002-9052-6385. Correo: choez-ivan7589@unesum.edu.ec

Karina Virginia Mero Suárez [2]

[2] Ingeniera en Sistemas, Magister en Informática Empresarial, Doctora en Tecnologías de la Información, Docente de la Carrera de Tecnologías de la Información y la Comunicación, Facultad Ciencias Técnicas, Universidad Estatal del Sur de Manabí. Jipijapa-Manabí. Ecuador. ORCID: https://orcid.org/0000-0002-7943-4981. Correo: karina.mero@unesum.edu.ec

*** Autor para correspondencia: choez-ivan7589@unesum.edu.ec**

Resumen

El propósito principal de la presente investigación fue realizar una evaluación de diversas herramientas tecnológicas para el análisis de tráfico de la red de datos en la Carrera de Tecnología de la Información de la Facultad de Ciencias Técnicas de la Universidad Estatal del Sur de Manabí. El análisis realizó con la finalidad de verificar errores en la red, y realizar el mejoramiento en la misma, teniendo en cuenta las características, ventajas y desventajas de los recursos que se necesitaron. La importancia de esta investigación radica en la utilización de las herramientas, siendo un analizador de paquete, que permitió identificar el tráfico malicioso, y de la misma manera comparar los distintos comportamientos que presenta la red. Se utilizaron métodos de investigación científica tales como, histórico-lógico, inducción-deducción, análisis-síntesis y la encuesta aplicada al personal administrativo del área de Sistema Informático. Llegando al resultado que la evaluación permitió conocer la herramienta adecuada para detectar, analizar y mapear el tráfico existente en la red. Se concluye que el uso de la herramienta permite cumplir con la demanda de los usuarios logrando obtener un mejor desempeño en cuanto a transferencia de datos e información, proporcionando las facilidades y recursos de la red.

Palabras clave: análisis; evaluación; herramientas; red; tecnología

Abstract

The main purpose of this research was to perform an evaluation of various technological tools for the analysis of data network traffic in the Information Technology Department of the Faculty of Technical Sciences of the Universidad Estatal del Sur de Manabí. The analysis was carried out with the purpose of verifying errors in the network, and to improve it, taking into account the characteristics, advantages and disadvantages of the resources that were needed. The importance of this research lies in the use of the tools, being a packet analyzer, which allowed to identify malicious traffic, and in the same way to compare the different behaviors presented by the network. Scientific research methods were used, such as historical-logical, induction-deduction, analysis-synthesis and the survey applied to the administrative personnel of the Computer System area. As a result, the evaluation allowed to know the adequate tool to detect, analyze and map the existing traffic in the network. It is concluded that the use of the tool allows to meet the demand of the users achieving a better performance in terms of data and information transfer, providing the facilities and resources of the network.

Keywords: *analysis; evaluation; tools; network; technology*

Fecha de recibido: 02/05/2023
Fecha de aceptado: 02/07/2023
Fecha de publicado: 04/07/2023

Introducción

El impacto que ha tenido el Internet y las nuevas tecnologías a nivel mundial en las personas, la sociedad, ha generado cambios fundamentales en todo aspecto, económico, social, político, en la comunicación, en la industria y muchos más. Las innovaciones tecnológicas y comunicacionales más conocidas como (TIC), acceden a aquella información haciendo que las personas interactúen entre sí, realizando cambios que mediante las tecnologías se desarrollan.

En relación con las redes inalámbricas, se puede decir que ofrecen gran flexibilidad en el despliegue, la misma que permite libertad de movimiento en la infraestructura, conectar cierta cantidad de dispositivos con cableados y otros simplemente inalámbricos, siempre y cuando teniendo en cuenta la topología a implementar, y el propósito para que se está creando una red. Cada día aumenta la creación de dispositivos que conforman el grupo llamado internet de las cosas (IoT). Estos dispositivos, sensores y aparatos tecnológicos son utilizados por el ser humano en el sector doméstico, en la industria, en los negocios y en todos los sectores de la sociedad.

Es por esta razón que en la evolución de las tecnologías es muy importante el análisis de tráfico de la red, debido a que las redes suelen ser víctima de hackeo, por ende, es evidente la utilización de herramientas tecnológicas las mismas que deben ser analizadas para escoger la adecuada e implementarla ya sea en una empresa u organización.

El análisis de tráfico de red se lo realiza con la finalidad de analizar y capturar paquetes de datos en la red de la Carrera de Tecnología de la Información y la Comunicación realizando el mejoramiento en la misma. Para esto es importante investigar y analizar cada una de las herramientas tecnológicas, enfocando sus características, ventajas y desventajas, y sobre todo saber los recursos que necesita para el funcionamiento.

A nivel mundial se han incrementado redes con fines distintos, creando una infraestructura tanto física como tecnológica, y de esta manera manipulando gran cantidad de información de mucha importancia para obtener así un funcionamiento eficaz. Cabe recalcar, que, toda información que circula en una red a nivel mundial está expuesta a infinidad de veces que esta sea vulnerada de cualquier manera y para fines maliciosos, es por esto que, es necesario realizar periódicamente un análisis en la red para verificar las falencias que está presentando y a la vez corregir cada una de ellas.

En la actualidad, es necesario realizar monitoreo y análisis de tráfico en la red, de manera que se va inspeccionando las actividades realizadas con anterioridad o en tiempo real siempre y cuando varié la herramienta tecnológica que se utilice para realizar este tipo de proceso en la red. En un monitoreo de la red se pueden realizar varios procesos, entre ellos se puede mencionar, la auditoria de las operaciones, el usuario que ejecuta una conexión, para luego examinar el tráfico que se genera en la red y aún más a los servicios corporativos que acceden dentro de la empresa.

Los ataques informáticos es uno de tantos inconvenientes que tienen las empresas u organizaciones día a día, de acuerdo a varios análisis e investigación se han desarrollado herramientas disponibles para hacer frente a estos ataques. Estas herramientas tecnológicas con idóneas para recopilar gran cantidad de datos para posteriormente analizarlos y dar solución al problema. Es de gran necesidad estar atentos de la seguridad de la información, debido a la gran cantidad de información que circula en la red de la empresa u organización, es por ello, que se requiere monitorear y analizar la mayoría de las actividades realizadas en tiempo actual, para evitar a posibles ataques o malfuncionamiento que suelen afectar el desempeño de la empresa.

La Carrera de Tecnología de la Información de la Universidad Estatal del Sur de Manabí (UNESUM) de Ecuador, ha evolucionado de cierta manera que la interacción de los estudiantes con el sistema o aula virtual es de alta concurrencia, a través de este recurso informático se reciben y envían documentos, pruebas de diagnósticos, por lo que los estudiantes hacen uso de la red, y es importante el enfoque que tiene esta investigación, debido al alto tráfico de la red y es por esta razón que emerge el objetivo general sobre la evaluación de las herramientas tecnológicas para analizar el tráfico de la red, además de su objetivo específico que es evaluar el estado actual de la red y posterior a esos análisis hacer su respectiva comparación para verificar que tan eficaz puede ser una de las herramientas a investigar.

Materiales y métodos

En el presente trabajo investigativo se utilizará la metodología inductiva, porque es una herramienta de investigación, la misma que nos permitirá receptar los mejores resultados especificando de manera general cada una de los fragmentos investigativos, mientras que, la metodología deductiva se la utilizará porque es una herramienta que nos ayuda a identificar cuáles serán los hechos ocurridos en tiempo real, como por ejemplo, el análisis de tráfico en la red, el registro de los paquetes de datos capturados.

Cabe recalcar que la metodología necesaria para el respectivo análisis de tráfico de red, es mediante las herramientas tecnológicas la misma que consiste en la captura de paquetes de datos, teniendo como objetivo principal el análisis de tráfico, por esta razón se la considera como una de las herramientas más eficaz para el

estudio de las comunicaciones y utilizada para la resolución de problemas en la red, la misma que se desarrolla mediante la metodología bibliográfica debido a la información investigada.

Método analítico. - se determina este método para llevar a cabo la presente investigación donde se analizará cada una de las características de las herramientas tecnológicas que permitan capturar paquetes de datos, proceso que lo hacen los llamados analizadores de tráfico de red.

Método explicativo. - este método se lo utiliza debido a la necesidad que presenta la investigación, la captura de paquetes se da mediante una herramienta tecnológica que su principal característica es mostrar los paquetes con información detallada, abriendo y guardando los paquetes capturados, para luego ser importados y exportados en diferentes formatos.

Conceptos relacionados con el tema objeto de estudio

Para la presente investigación es necesario analizar conceptos básicos para el análisis de tráfico de la red de datos, como son:

Seguridad informática: La seguridad informática, es la disciplina que se encarga de llevar a cabo las soluciones técnicas de protección de la información. En otras palabras, la seguridad informática es aquella que protege todo el sistema informático, asegurando la privacidad de cada una de la información que se manipula (Figueroa Suárez et al., 2018).

Ataque informático en la red: Un ataque informático es una acción perjudicial para los sistemas (ordenadores, redes informáticas y otros dispositivos electrónicos) de las empresas o de los particulares. Estos sistemas son vulnerables ante ataques informáticos. Por ello, es importante que conozcas que tipos de ataques informáticos existen y como enfrentarnos a ellos. (Hernández, 2022)

Detección de intrusos: (Alvernia Acevedo, 2018) afirma que "Es el proceso en el cual existe una constante vigilancia sobre redes de computadoras y los sistemas para garantizar que no hallan violaciones, por consiguiente, hay una búsqueda de información para establecer un informe de los eventos para realizar un posterior análisis que permita encontrar señales de la existencia de intrusiones y generar respuestas apropiadas".

Monitoreo de red: El monitoreo de la red es un proceso sistemático y continuo que busca detectar o descubrir algunas deficiencias en la red y asegurar, así, un rendimiento óptimo. La falla más habitual, por ejemplo, incide en la velocidad de transmisión de datos. Esto influye a múltiples factores como la sobre carga de los servidores, enrutadores, *swicths* defectuosos, o ciertas anomalías heterogéneas, es por ello que se lo conoce como un método que busca problemas y a la vez son solucionado mediante herramientas tecnológicas de red (Pereira, 2022).

Análisis de paquetes de datos: Según (Ríos & Fermín, 2019) afirman que "El análisis del tráfico de red se basa habitualmente en la utilización de sondas con interfaz Ethernet conectadas al bus. Dichas sondas, con su interfaz Ethernet funcionando en modo promiscuo, capturan el tráfico a analizar y constituyen la plataforma en la que se ejecutaran, de forma continua, aplicaciones propietarias o de dominio público, con las que se podrá determinar el tipo de información que circula por la red y el impacto que pudiera llegar a tener sobre la misma".

Análisis de tráfico: El análisis del tráfico infiere información a partir las características observables de los datos que circulan por la red. El análisis de tráfico está muy relacionado con el análisis de paquetes y se suelen

usar de forma conjunta. En el análisis de paquetes se estudia la información contenida en los paquetes que circulan por la red y a partir de eso trata de inferir información. (Merino, 2019)

Tráfico de red: Es un componente importante considerado para la medición del tráfico, control, y simulación en una red, en otras palabras, se puede decir que es cierta cantidad de datos que se mueven a través de una red en un momento estipulado. En donde los datos de red se encapsulan en paquetes, los mismos, que proporcionan en la red.
(Marcillo, 2023)

Tipos de análisis de tráfico: Generalmente cuando se lleva a cabo un análisis de tráfico de red, existen dos enfoques diferentes, los cuales se lo nombra a continuación: análisis de paquete y análisis de flujo de tráfico de red. Ambos cumplen una función que permite recopilar, analizar y presentar la información del tráfico de red.

Análisis de paquete o Captura de paquetes: Normalmente un analizador de paquetes es referido como un protocolo de análisis, que describe y realiza el proceso de captura e interpretación de los datos que se están recorriendo en la red. El análisis de paquete se lo realiza mediante un programa ejecutado en un dispositivo perteneciente a la red que tiene como función capturar, el dispositivo recibe todas las tramas de la capa de enlace de datos que lleguen hasta el adaptador de red.

Algunos dispositivos de red poseen la capacidad necesaria de realizar la inspección del tráfico entrante en sus puertos, mediante las configuraciones de un puerto espejo, lo que permite replicar todo el tráfico proveniente de un puerto del cual se requiera inspeccionar su tráfico.
Un analizar de paquetes permite:

- Entender las características de la red
- Determinar quién o qué está utilizando el ancho de banda disponible
- Identificar picos en la red en periodos de tiempo
- Distinguir las actividades maliciosas en la red. (Chacón Ramones & Moreno baute, 2021)

Análisis de flujo de tráfico

Se utilizan para el análisis de flujo los dispositivos que pertenecen a la red para poder generar un flujo del tráfico, el mismo que contiene información sobre los paquetes, es lo contrario del análisis de tráfico de paquetes, más bien se evalúan ciertas características en común que pudieran poseer los paquetes, la información será almacenada y así posteriormente enviada a la plataforma el cual permitirá su análisis y visualización con base a las características definida por el administrador de red. Un flujo consiste en cantidad de paquetes que son recibidos en una interfaz para su proceso de análisis.

Esquema básico como funciona un análisis de flujo de tráfico (Chacón Ramones & Moreno baute, 2021):

- **Exportador**: Encargado de recopilar la información y data del flujo y así mismo enviada al receptor
- **Colector**: Recibe toda la información del exportador y lo almacena para el respectivo procesamiento, dicha información es enviada al analizador.
- **Analizador**: Es el analizador que lleva a cabo todo el proceso de filtrado y análisis de todos los datos obtenidos del colector. Otras de las funciones que realiza es la visualización en forma gráfica de los datos recopilados.

Herramientas tecnológicas

En la investigación realizada por (Ocampo et al., 2017) mencionan que "Existen algunas herramientas que son capaces de coordinar ataques de DoS entre múltiples maquinas afectadas, de forma que el hacker solo debe infectar unos cuantos ordenadores de usuarios finales y lanzar el ataque desde ahí. Y lo más curioso es que no es necesario estar conectado a internet para realizar el ataque".

Herramientas para el análisis de tráfico de red

Su funcionamiento permite capturar los paquetes para poder realizar un análisis posterior, lo que permitirá se presente de una manera textual o gráficamente, dependiendo de las capacidades de las herramientas: Wireshark, SmartSniff, Kismet, TCPDump etc.

- Wireshark: Monitoriza el tráfico y captura los paquetes de datos que circulan en la red.
- SmartSniff: Permite mostrar el contenido de los paquetes que circulan por una red WIFI.
- Kismet: Es una herramienta de tráfico de red, su función es capturar los paquetes de red que circulan en la interfaz de la red de nuestro ordenador.
- TCPDump: Es un analizador en línea de comandos cuya utilidad es analizar el tráfico que circula por la red (Saavedra Ortiz & Simbaña García, 2018)**.**
- BruteShark: es una de las utilidades más potentes que vamos a recomendarte en este artículo. Estas son algunas de sus prestaciones: reconstrucción de sesiones TCP, Mapas de red, extracción de hashes para claves que hayan sido cifradas, cuenta con una variante para línea de comando y otra con interfaz gráfica.
- OmniPeek: es una opción profesional que te permite analizar redes de grandes dimensiones. Sin duda, es una buena opción si lo que buscas es una herramienta completa que lidie con las tareas más pesadas.
- Capsa: es otro actor muy a considerar en el mundo del analizador de tráfico de red. Cuenta con una versión para Windows únicamente, aunque en tres variantes: aplicación gratuita, versión estándar, herramienta empresarial (Otero, 2022).

Análisis de requerimientos generales para analizar el tráfico de red.

- Evaluaciones sobre los servicios y tráfico de red.
- Análisis de equipos y software.
- Determinar la herramienta adecuada para analizar el tráfico de red.
- Capacidad para las herramientas tecnológicas analizadoras de red.
- Instalar el analizador de tráfico de red y realizar los respectivos estudios.

Captura de paquetes de datos

Los paquetes se capturan como datos binarios, sin modificaciones. Puede leer la información de paquetes sin conexión con un analizador de paquetes como Wireshark o Tcpdump. Si necesita capturar rápidamente paquetes destinados al motor de enrutamiento o que se originan en el motor de enrutamiento y analizarlos en línea. (González, 2023)

Producto software

El producto de software, como resultado del proceso de desarrollo de software, se define como "el conjunto de programas de cómputo, procedimientos y posiblemente la documentación y datos asociados" (ISO, 2008). El gestor del proyecto es responsable que durante la ejecución del proyecto se generen todos los entregables, tanto internos como externos del proyecto. Sin embargo, desde la etapa de concepción del proyecto, el gestor se enfrenta al problema de hacer estimaciones con muy poca información para determinar tanto costos como tiempo de entrega. (García Mireles, 2018)

Estándares de calidad de software

Los estándares de calidad de software están directamente ligados a la competitividad en el mercado, al regular la creación de productos y servicios con base en las exigencias de los usuarios. Las deficiencias en los productos informáticos están ligadas al incumplimiento en las normas de calidad. A largo plazo, los errores pueden impactar significativamente en la economía y reputación de las marcas (Tamushi, 2022).

ISO/IEC 2501n – División de Modelo de Calidad: Las normas de este apartado presentan modelos de calidad detallados incluyendo características para calidad interna, externa y en uso del producto software. Actualmente esta división se encuentra formada por:

- *ISO/IEC 25010 – System and software quality models:* describe el modelo de calidad para el producto software y para la calidad en uso. Esta norma presenta las características y subcaracterísticas de calidad frente a las cuales evaluar el producto software.
- *ISO/IEC 25012 – Data Quality model:* define un modelo general para la calidad de los datos, aplicable a aquellos datos que se encuentran almacenados de manera estructurada y forman parte de un Sistema de Información. (Mendoza Huillca, 2018)

La calidad del producto software a evaluar debe cumplir con los requisitos para satisfacer a los usuarios, aportando beneficios como la funcionabilidad, rendimiento, seguridad, mantenibilidad, entre otros. Además, este modelo de calidad también está compuesto por ciertas características como: adecuación funcional, eficiencia de desempeño, compatibilidad, usabilidad, fiabilidad, seguridad, portabilidad.

ISO/IEC 2503n – División de requisitos de calidad.

Los estándares que forman parte de esta división ayudan a especificar los requisitos de calidad. Estos requisitos pueden ser usados en el proceso de especificación de requisitos de calidad para un producto software que va a ser desarrollado o como entrada para un proceso de evaluación. (Gómez, 2017)

- *ISO/IEC 25030 – Quality requirements:* provee de un conjunto de recomendaciones para realizar la especificación de los requisitos de calidad del producto software (Hernández De Leon, 2021)

Esta norma de calidad tiene como objetivo mejorar cada uno de los requisitos en la Calidad de Software, con ello nos proporciona requisitos y recomendaciones, que se usaran para definiciones y análisis de cada uno de ellos. Los requisitos de calidad del producto de software son necesarios para: especificación – planificación – desarrollo – evaluación.

ISO/IEC 2504n – División de evaluación de la calidad.

Estos estándares proporcionan requisitos, recomendaciones y guías para la evaluación de un producto software, tanto si la llevan a cabo evaluadores, como clientes o desarrolladores. (López, 2018) afirma que "Esta norma de calidad proporciona una descripción del proceso de evaluación de la calidad de los productos

de software y establece los requisitos para la aplicación de este proceso. Dicho proceso de evaluación consta de un total de cinco actividades".

1. Establecer los requisitos de la evaluación
2. Especificar la evaluación
3. Diseñar la evaluación
4. Ejecutar la evaluación
5. Concluir la evaluación

Por lo tanto, se puede observar en las tablas 1 y 2 las herramientas tecnológicas con las respectivas definiciones, características, ventajas, desventajas, costos y sistemas operativos.

Tabla 1 Herramientas de análisis de tráfico de red.

Herramientas	Ventajas	Desventajas	Características
Wireshark	• Consta de soporte solucionando errores que la comunidad detecta y lo captura para realizar el análisis. • Permite visualizar detalladamente los paquetes capturados. • Permite analizar la red gracias a sus comandos ayuda a filtrar detalladamente y asi acercarse a la causa raíz del problema.	• Difícil de descifrar la información que transita en la red. • Presenta un error con este mensaje "OUT of Memory" al mostrar una captura hecha con anterioridad.	• Captura de paquetes en vivo desde una interfaz de red. • Muestra los paquetes con información detallada de los mismos. • Abre y guarda paquetes capturados. • Importa y exporta paquetes en diferentes formatos.
SmartSniff	• Aportan con ideas, comunica errores. • Interactúan para ayudar a mejorar constantemente el código de un programa.	• Algunos sistemas los paquetes de salida UDP e ICMP no se capturan.	• Ayuda organizar la información de los paquetes. • Permite depurar, capturar, interpretar. • almacena los paquetes que viajan por la red para analizarlos y darle solución a los problemas de la red.
TCPDump	• Resuelve networking cuestiones. Por lo tanto en los paquetes se pueden guardar y analizar los archivos.	• No soporta una red con mucho tráfico. • No registra el paquete completo. • No mantiene los estados de la conexión.	• Lee, captura y almacena toda la información de la red. • Filtra todo el tráfico para ver solamente lo que es de nuestra importancia. • Depura cada una de las aplicaciones que usan en tiempo real en la red para comunicarse.
Kismet	• Analizador de tráfico en Linux para redes inalámbricas. • Se divide en un Stumbler y en Sniffer, el mismo que también cuenta con opciones de configuración de GPS.	• Requiere de un manejo avanzado de Linux con la finalidad de detectar todos los errores presentes en el momento de la instalación.	• Registra todos los paquetes analizados y guardar en un formato de archivo compatible con Tcpdump / Wireshark. • Determina el nivel de cifrado inalámbrico utilizado en un punto de acceso determinado. • Proporciona soporte para saltar de canal para encontrar todas las redes posibles.
ErPa	• Comprueba la validez del tamaño máximo de la captura.	• Tiene como límite 10.000 paquetes para capturar.	• Filtra, captura y realiza diagramas estadísticos de los protocolos básicos

	• Los datos se pueden visualizar en pantalla o grabarla en un fichero para posterior análisis.	• No posee garantía de proveedor por ser un analizador de código libre.	como FTP, SSH, Telnet, HTTP, POP3, SMTP.

Tabla 2: Analizadores de tráfico de red existentes en el mercado.

Herramienta	Descripción	Sistema Operativo	Costo
Wireshark	Analizador de protocolos de red más importante del mundo. Le permite capturar y navegar interactivamente el tráfico que se ejecuta en una red informática.	BSD, Linux, Mac, Windows	Gratis
Fiddler	Es un proxy de depuración web que registra todo el tráfico HTTP (S) entre su computadora e Internet. Fiddler le permite inspeccionar todo el tráfico HTTP (S), establecer puntos de interrupción y "violín" con datos entrantes o salientes.	Windows	Gratis
TCPdump	Analizador de paquetes común que se ejecuta bajo la línea de comando. Permite al usuario interceptar y mostrar TCP / IP y otros paquetes que se transmiten o reciben a través de una red a la que está conectada la computadora.	BSD, Linux, Mac, Windows	Gratis
Netcat	Utilidad de red destacada que lee y escribe datos a través de conexiones de red, utilizando el protocolo TCP / IP. Está diseñado para ser una herramienta confiable "back-end" que puede ser utilizada directa o fácilmente por otros programas y scripts.	Linux, Mac, Windows	Gratis
Kismet	Sistema de detección de intrusiones, más exclusivo para redes inalámbricas 802.11. Este programa funciona con cualquier tarjeta inalámbrica que soporte el modo de monitorización, y puede rastrear tráfico 802.11b, 802.11a, 802.11g y 802.11n.	Windows; Linux, FreeBSD, NetBSD, OpenBSD, y Mac OS X	Gratis
Microsoft Network Monitor	Analizador de paquetes. Permite capturar, ver y analizar datos de red y descifrar protocolos de red. Se puede utilizar para solucionar problemas de red y aplicaciones en la red.	Windows	Gratis
NetworkMiner	Herramienta de análisis forense de red (NFAT) para Windows. NetworkMiner se puede usar como una herramienta pasiva de captura de paquetes y sniffer de red para detectar sistemas operativos, sesiones, nombres de host, puertos abiertos, etc.	Linux, Mac, Windows	Freemium -Gratis
Packetyzer	Proporciona una interfaz de usuario de Windows para la biblioteca Ethereal de captura y disección de paquetes. Ethereal es utilizado por profesionales de la red en todo el mundo para la resolución de problemas, análisis, desarrollo de software y protocolos y educación.	Windows	Gratis
HTTP Debugger	Analizador y analizador de HTTP profesional para desarrolladores	Windows	Comercial
Ethereal	Utilizado por profesionales de redes de todo el mundo para la resolución de problemas, análisis, desarrollo de software y protocolos y educación. Tiene todas las características estándar que esperaría en un analizador de protocolos	Linux, Windows	Gratis
TCPflow	Captura datos transmitidos como parte de conexiones TCP (flujos) y almacena los datos de una manera conveniente para el análisis o depuración de protocolos.	Linux, Mac, Windows	Gratis

LanDetective	Monitorea el uso de Internet. La interceptación y el registro de los datos transferidos a través de protocolos de red de alto nivel	Windows	Comercial
Packet Peeper	Analizador de protocolos de red gratuito (sniffer de paquetes) para Mac OS X. Ensamblaje de flujo TCP. Privilegio de separación. Sesiones de captura simultánea. Filtros, que pueden definirse en cualquier momento.	Mac	Gratis
Debookee	Analizador de tráfico de red más simple y potente para macOS. Intercepción de tráfico de red Debookee puede interceptar y monitorear el tráfico de cualquier dispositivo en la misma subred, gracias a un ataque Man-in-the-middle	Mac	Comercial

En la tabla 3, se puede observar la comparación del número de paquetes capturados en el lapso de 15 minutos, a través de la evaluación de cinco herramientas tecnológicas que analizan el tráfico de la red. En donde la herramienta Wireshark se destaca con el mayor número de paquetes capturados, mientras que el analizador Windump obtiene 8201 paquetes capturados, tcpdump se lo considera en un nivel bueno para ser elegido como un analizador de paquetes de puerto ethernet a otro puerto, mientras que Kismet y ErPa son herramientas analizadoras, pero con su desventaja que se limitan a la captura de paquetes de datos.

Tabla 3: Comparativa de paquetes capturados con cinco herramientas analizadoras de tráfico de red.

Wireshark	**ErPa**	**Kismet**	**Tcpdump**	**Windump**
Paquetes Capturados	Paquetes Capturados	Paquetes Capturados	Paquetes Capturados	Paquetes Capturados
24737	4832	1800	6015	8201

Resultados y discusión

En el presente trabajo de investigación se realizó la técnica de la encuesta, la misma que fue realizada en el departamento de Sistemas Informáticos de la Universidad Estatal del Sur de Manabí, dirigida a cada uno del personal encargado que da un total de 10 personas, esta técnica se la realizó con el fin de tener conocimiento sobre la existencia y funcionamiento de los analizadores de tráfico de la red de la Carrera de Tecnología de la Información y la Comunicación.

Pregunta 1. ¿Conoce usted que es un Software analizador de tráfico de red?

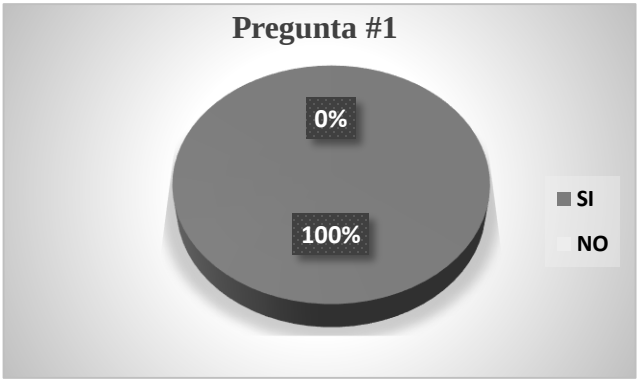

Figura 1: Conocimientos sobre qué es un Software analizador de tráfico de red.

Tabla 4. Conocimientos sobre que es un Software analizador de tráfico de red.

Alternativas	Frecuencia	Porcentaje
SÍ	14	100,00%
NO	0	0,00%
Total	**14**	100,00%

Análisis e interpretación: en la encuesta realizada al personal encargado del área de sistemas informático, da como resultado un 100%, confirmado que si conocen sobre un analizador de tráfico de red.

Pregunta 2. ¿Cuáles de las siguientes herramientas de analizador de tráfico de red usted conoce?

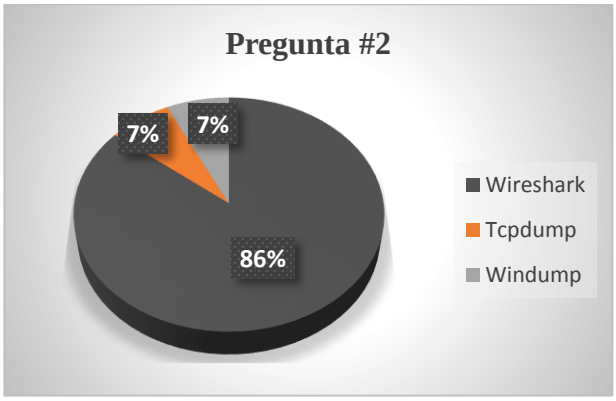

Figura 2: Herramientas de analizador de tráfico de red más conocidas.

Tabla 5: Herramientas de analizador de tráfico de red más conocidas.

Alternativas	Frecuencia	Porcentaje
Wireshark	12	85,71%
Tcpdump	1	7,14%
Windump	1	7,14%
Total	14	100,00%

Análisis e interpretación: se obtuvo como resultado que el 80% de los encuestados conocen el analizador de tráfico de red Wireshark, mientras que el 1% el software Tcpdump, y el 1% el Windump, considerando que el analizador más reconocido es el Wireshark debido a sus magníficas características.

Pregunta 3. ¿Alguna vez ha trabajado con algún analizador de tráfico de red?

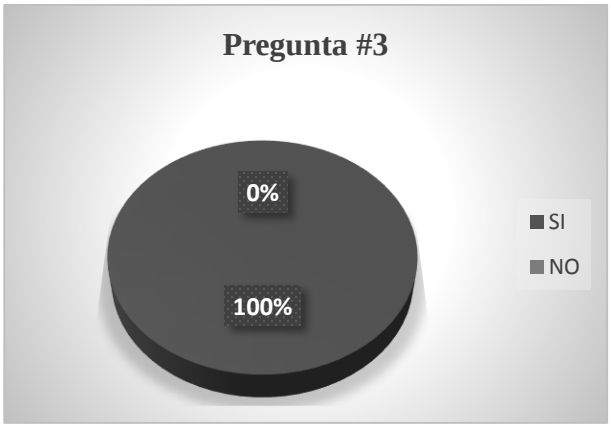

Figura 3: Frecuencia del uso del analizador de tráfico de red.

Tabla6: Frecuencia del uso del analizador de tráfico de red.

Alternativas	Frecuencia	Porcentaje
SÍ	14	100,00%
NO	0	0,00%
Total	14	100,00%

Análisis e interpretación: según en la encuesta se obtiene como resultado el 100% que si han trabajado con analizadores de trafico de red, debido a que la red implementada pertenece a una institución pública por ende necesita un analizador.

Pregunta 4. ¿Existe alguna herramienta analizadora de tráfico en la red de la Carrera de Tecnología de la Información y Comunicación?

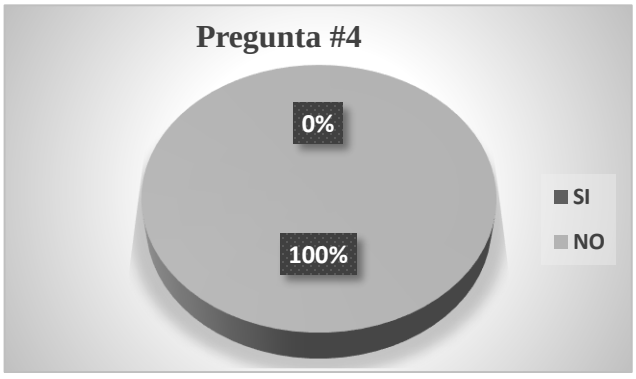

Figura 4: Herramienta analizadora de tráfico de la red en la Carrera de Tecnología de Información y la Comunicación.

Tabla 7: Herramienta analizadora de tráfico de la red en la Carrera de Tecnología de Información y la Comunicación.

Alternativas	Frecuencia	Porcentaje
SÍ	0	0,00%
NO	14	100,00%
Total	14	100,00%

Análisis e interpretación: mediante la encuesta el 100% indica que no tiene una herramienta analizadora de tráfico de red, debido a que la institución consta de equipos tecnológicos Mikrotik, incluyendo un Software llamado Winbox el mismo que permite manejar, configurar toda la red.

Pregunta 5. ¿Cómo cree usted que será el rendimiento de la red con un software analizador de tráfico de red en la Carrerea de Tecnología de la Información y Comunicación?

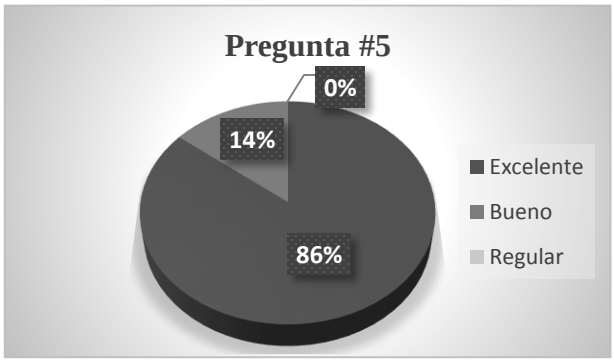

Figura 5: Rendimiento de la red con un analizador de tráfico de red.

Tabla 8: Rendimiento de la red con un analizador de tráfico de red.

Alternativas	Frecuencia	Porcentaje
Excelente	12	85,71%
Bueno	2	14,29%
Regular	0	0,00%
Total	14	100,00%

Análisis e interpretación: En esta última pregunta de la encuesta se obtuvo el 80% en la alternativa Excelente, mientras que el 20% considera que sería Bueno, sin embargo, esta herramienta tecnológica ayuda a verificar procesos, como la estadística de ancho de banda, los usuarios que se ingresen a la red, direcciones que estos ocupan, y además evita que aplicaciones inactivas utilicen un ancho de banda valioso.

Conclusiones

Se realizó una evaluación del estado actual de la red de la Carrera de Tecnología de la Información y la Comunicación, constatando que la red no presentó falencias. Se investigó cada una de las características de las herramientas tecnológicas para analizar el tráfico de red, por lo que se considera que existe una variedad de software analizadores de tráfico de red que son utilizados a nivel mundial, de acuerdo al sistema operativo compatible.

Finalmente, se monitoreó la red con una de las herramientas tecnológicas evaluadas y minuciosamente se analizó la funcionalidad de los procesos de la herramienta analizadora de tráfico de red iniciando con la identificación de toda la información que se transmite, y así se logra una visualización de los paquetes capturados, dando un resultado positivo considerando que este software analizador de trafico de red podría instalarse y ser capaz de detectar alguna actividad inusual en la red.

Referencias

Alvernia Acevedo, S. (2018). Wireshark: como herramienta de apoyo para el análisis de tráfico malicioso en una red de área local. Ocaña: Universidad Francisco de Paula Santander.

Chacón Ramones, L. O., & Moreno baute, R. A. (2021). Implementación de un sistema de análisis de tráfico de red, mediante el protocolo SFLOW en la red interna de la torre mistral para la empresa SANFAR. Caracas: Universsidad Católica Andrés Bello.

Figueroa Suárez, J., Rodríguez Andrade, R., Bone Obando, C., y Saltos Gómez, J. (2018). La seguridad informática y la seguridad de la información. Polo de conocimiento, XIV(18), 145-155.

García Mireles, G. (2018). Conceptos Básicos de Gestión de Proyectos de Software.

Gómez, A. (22 de Enero de 2017). wordpress.com. https://interpolados.wordpress.com/2017/01/22/norma-isoiec-25000-requisitos-y-evaluacion-de-la-calidad-de-los-productos-de-software/

González, M. (2023). Uso de la captura de paquetes para analizar el tráfico de red. TechLibrary.

Hernández De Leon, J. (2021). Ensayo de Iso 2503n.

Hernández, P. (18 de Octubre de 2022). fundaciontelefonica.com. https://www.fundaciontelefonica.com/noticias/ciberseguridad-4-tipos-de-ataques-informaticos/

López, R. (2018). ISO / IEC 2504n - División de Evaluación de la Calidad.

Marcillo, L. (2023). theastrologypage.com. https://es.theastrologypage.com/network-traffic

Mendoza Huillca, J. (2018). ISO-IEC-2501n.

Merino, A. (2019). postech.com.mx. https://postech.com.mx/Postech/ES/analysis.php

Ocampo, C. A., Castro Bermúdez, Y. V., & Solarte Martínez, G. R. (2017). Sistema de detección de intrusos en redes corporativas. Scientia et Technica Año XXII, 22(1), 60-68.

Otero, E. (24 de Junio de 2022). profesionalreview.com. https://www.profesionalreview.com/2022/06/24/analizador-de-trafico-de-red/

Pereira, A. (10 de Marzo de 2022). electrodata.com.pe. https://www.electrodata.com.pe/que-es-el-monitoreo-de-red/

Ríos, R., & Fermín, J. (2019). Análisis de Tráfico de una red local Universitaria. Telématique, 8(2), 15-27.

Saavedra Ortiz, M., & Simbaña García, V. (2018). Análisis del tráfico de red en los laboratorios especializados del departamento del ciencias de la computación. Sangolquí: Universidad de las fuerzas armadas.

Tamushi, A. (2022). Importancia de los estándares de calidad de software.