



UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

OCTUBRE 2017 – MARZO 2018

PROYECTO DE INVESTIGACION DE GRADO O DE FIN DE CARRERA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

TEMA:

ANÁLISIS DE TRÁFICO DE LA RED DE DATOS Y SU INCIDENCIA EN EL
ACCESO AL CONTENIDO WEB DE LOS ESTUDIANTES DE LAS INSTITUCIONES
EDUCATIVAS DEL DISTRITO 12D01

EGRESADO:

CESAR EDUARDO ANGULO TAPIA

TUTOR:

ING. MARIA GONZALES VALERO, MSc. MIE

AÑO 2018

ÍNDICE

ÍNDICE	i
ÍNDICE DE FIGURAS	ii
ÍNDICE DE TABLA	iii
ÍNDICE DE GRAFICOS	v
INTRODUCCIÓN.....	1
CAPÍTULO I.- DEL PROBLEMA	3
1.1. Idea o tema de Investigación.....	3
1.2. Marco Contextual.....	3
1.2.1. Contexto Internacional.....	4
1.2.2. Contexto Nacional.....	5
1.2.3. Contexto Local.....	6
1.2.4. Contexto Institucional.....	7
1.3. Situación problemática.....	8
1.4. Planteamiento del problema.....	11
1.4.1. Problema general.....	11
1.4.2. Subproblemas o derivados.....	12
1.5. Delimitación de la investigación.....	12
1.6. Justificación.....	13
1.7. Objetivos de investigación.....	14
1.7.1. Objetivo general.....	14
1.7.2. Objetivos específicos.....	14
CAPÍTULO II.- MARCO TEÓRICO O REFERENCIAL	15
2.1. Marco teórico.....	15
2.1.1. Marco conceptual.....	15
2.1.2. Marco referencial sobre la problemática de investigación.....	23
2.1.2.1. Antecedentes investigativos.....	23
2.1.2.2. Categorías de análisis.....	25
2.1.3. Postura teórica.....	50
2.2. Hipótesis.....	52
2.2.1. Hipótesis general.....	52
2.2.2. Subhipótesis o derivadas.....	52
2.2.3. Variables.....	52

CAPÍTULO III.- RESULTADOS DE LA INVESTIGACIÓN.	53
3.1 Resultados obtenidos de la investigación.	53
3.1.1 Pruebas estadísticas aplicadas.	53
3.1.2 Análisis e interpretación de datos.	60
3.2 Conclusiones específicas y generales.	83
3.2.1 General.	83
3.2.2 Específicas.	83
3.3 Recomendaciones específicas y generales.	85
3.3.1 General.	85
3.3.2 Específicas.	85
CAPÍTULO IV.- PROPUESTA DE APLICACIÓN.	87
4.1 Propuesta de aplicación de resultados.	87
4.1.1 Alternativa obtenida.	87
4.1.2 Alcance de la alternativa.	87
4.1.3 Aspectos básicos de la alternativa.	93
4.1.3.1 Antecedentes.	93
4.1.3.2 Justificación.	95
4.2 Objetivos.	96
4.2.1 General.	96
4.2.2 Específicos.	96
4.3 Estructura general de la propuesta.	96
4.3.1 Título.	96
4.3.2 Componentes.	97
4.4 Resultados esperados de la alternativa.	99
BIBLIOGRAFÍA.	100
ANEXOS.	103

ÍNDICE DE FIGURAS

FIGURA 1. UBICACIÓN DE LAS DISPOSITIVOS DE MONITOREO EN LA RED.....	2
FIGURA 2. TOPOLOGÍA DE BUS.....	28
FIGURA 3. TOPOLOGÍA DE ANILLO.....	28
FIGURA 4. TOPOLOGÍA DE ESTRELLA.....	29
FIGURA 5. TOPOLOGÍA DE ESTRELLA EXTENDIDA.....	29
FIGURA 6. TOPOLOGÍA JERÁRQUICA.....	30
FIGURA 7. TOPOLOGÍA DE MALLA.....	30
FIGURA 8. DATAGRAMA IP.....	32
FIGURA 9. DIRECCIONAMIENTO IP.....	36
FIGURA 10. EJEMPLO DE LA ARQUITECTURA DE RED IP.....	37
FIGURA 11. FUNCIONAMIENTO DEL MODELO OSI.....	39
FIGURA 12. ENTREVISTA.....	107
FIGURA 13 ENCUESTA.....	107
FIGURA 14 ENCUESTA.....	108
FIGURA 15 ENCUESTA.....	108
FIGURA 16 ENTREVISTA.....	109

ÍNDICE DE TABLA

TABLA 1. DETALLE HIPÓTESIS	53
TABLA 2. DETALLE DE SUBHIPÓTESIS 1	55
TABLA 3. DETALLE DE SUBHIPÓTESIS 2.....	56
TABLA 4. DETALLE DE SUBHIPÓTESIS 3.....	58
TABLA 5. DETALLE DE LA PREGUNTA N°1.....	60
TABLA 6. DETALLE DE LA PREGUNTA N°2.....	62
TABLA 7. DETALLE DE LA PREGUNTA N°3.....	64
TABLA 8. DETALLE DE LA PREGUNTA N°4.....	66
TABLA 9. DETALLE DE LA PREGUNTA N°5.....	67
TABLA 10. DETALLE DE LA PREGUNTA N°6.....	68
TABLA 11. DETALLE DE LA PREGUNTA N°7.....	69
TABLA 12. DETALLE DE LA PREGUNTA N°8.....	70
TABLA 13. DETALLE DE LA PREGUNTA N°9.....	71
TABLA 14. DETALLE DE LA PREGUNTA N°10.....	72
TABLA 15. ENTREVISTA REALIZADA EN LA UNIDAD EDUCATIVA FRANCISCO HUERTA RENDÓN	74
TABLA 16. ENTREVISTA REALIZADA EN LA UNIDAD EDUCATIVA DE AGOSTO.....	76
TABLA 17. ENTREVISTA REALIZADA EN LA UNIDAD EDUCATIVA JUAN MONTALVO	78
TABLA 18. ENTREVISTA REALIZADA EN LA UNIDAD EDUCATIVA ADOLFO MARÍA ASTUDILLO.....	80
TABLA 19. ENTREVISTA REALIZADA EN LA UNIDAD EDUCATIVA 29 DE AGOSTO.....	82
TABLA 20. INFORMACIÓN DE LA UNIDAD EDUCATIVA 29 DE AGOSTO	88
TABLA 21. INFORMACIÓN DE LA UNIDAD EDUCATIVA ADOLFO MARÍA ASTUDILLO.....	89
TABLA 22. INFORMACIÓN DE LA UNIDAD EDUCATIVA JUAN MONTALVO ...	90
TABLA 23. INFORMACIÓN DE LA UNIDAD EDUCATIVA 10 DE AGOSTO	91
TABLA 24. INFORMACIÓN DE LA UNIDAD EDUCATIVA FRANCISCO HUERTA RENDÓN	92
TABLA 25. ANTECEDENTE N°1	93
TABLA 26. ANTECEDENTE N°2.....	94
TABLA 27. ANTECEDENTE N°3.....	94

ÍNDICE DE GRÁFICOS

GRAFICO 1.EXISTENCIA DE PROCEDIMIENTOS DE SEGURIDAD INFORMÁTICA EN LAS UNIDADES EDUCATIVAS	60
GRAFICO 2. RESPONSABLE DE LA SEGURIDAD INFORMÁTICA	62
GRAFICO 3. DEPARTAMENTO RESPONSABLE DE LA SEGURIDAD INFORMÁTICA.....	64
GRAFICO 4. CONSIDERA USTED QUE EL INTERNET ES LENTO	66
GRAFICO 5. PROBLEMAS AL CONECTARSE A LA RED DE DATOS	67
GRAFICO 6. USTED UTILIZA LA REDES DE DATOS	68
GRAFICO 7. CONOCE USTED ALGUN SISTEMA DE CONTROL DE TRÁFICO	69
GRAFICO 8. NECESIDAD DEL ALGUN CONTROL DE TRÁFICO	70
GRAFICO 9. SOFTWARE QUE UTILIZAN LAS UNIDADES EDUCATIVAS	71
GRAFICO 10. HERRAMIENTAS DE SEGURIDAD IMPLEMENTADAS EN LA UNIDAD EDUCATIVA.....	72

INTRODUCCIÓN.

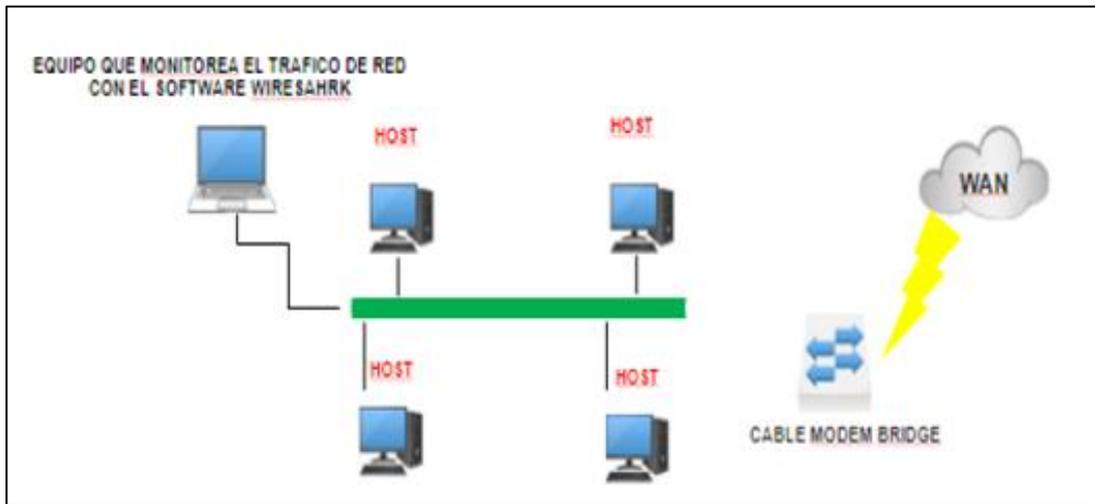
El siguiente proyecto de investigación tiene como intención el análisis de la información que transita a través de una red de datos para así poder tomar decisiones de como optimizar el desempeño en los procesos de la red que puedan estar presentando demoras en la transmisión y por ende podría causar un mal funcionamiento.

Se podrá realizar el análisis con la ayuda de las siguientes plataformas, una de ellas es un analizador del tráfico que hay en una red a nivel local (WIRESHARK) el cual proporcionara toda la información del tráfico que se genere a nivel de la red LAN, exponiendo en detalle cada una de las tramas IP que sean dudosas de tráfico no deseado en una red lo mismo que su contenido, para poder tomar medidas de bloqueos.

Otra plataforma que puede ayudar para analizar el tráfico de red es Advanced IP Scanner es una herramienta que nos permite tener a nuestro alcance la capacidad de poder controlar nuestra red LAN. El poder controlar la red nos facilita el acceso a las carpetas compartidas y servidores FTP para así garantizar el análisis de la red.

Asimismo se puede mencionar otra herramienta la cual es Capsa Free Network Analyzer esta permite el control y monitoreo de la red en tiempo real de los paquetes y así poder dar una solución algún problema que puedan surgir en la red.

Para entender un poco más acerca de esta topología del análisis que se va a realizar, se procederá a realizar un diagrama (Figura 1) muy general de cada una de las ubicaciones de las plataformas en la red donde se realizara la captura de los datos.



**FIGURA 1. UBICACIÓN DE LAS DISPOSITIVOS DE MONITOREO EN LA RED.
FUENTE: ELABORACIÓN PROPIA**

CAPÍTULO I.- DEL PROBLEMA

1.1. Idea o tema de Investigación.

Análisis de tráfico de la red de datos y su incidencia en el acceso al contenido web de los estudiantes de las Instituciones Educativas del Distrito 12D01.

1.2. Marco Contextual.

Para comprender cuando una Unidad Educativa necesita que se realice un análisis de tráfico en su recurso tecnológico es necesario conocer como los alumnos hacen uso de este recurso para poder determinar si se debe realizar dicho análisis.

Además se debe tener conocimientos sobre administración de redes para poder diagnosticar si el problema con la red se debe al buen o mal uso que le da el estudiante al recurso tecnológico de la Unidad Educativa.

Con el fin de contextualizar el problema y los objetivos de investigación se presenta a continuación los problemas de seguridad informática en la sociedad, y sobre todo en las unidades educativas a nivel internacional, nacional, local e institucional.

1.2.1. Contexto Internacional.

La implementación de nuevas tecnologías para cada necesidad que surge en nuestra vida y también la conexión permanente a internet sobre todo en instituciones educativas, acrecienta la importancia de profesionales y herramientas de ciberseguridad.

Un gran ejemplo que podemos narrar en España a través de un organismo como los es Instituto Nacional de Ciberseguridad (INCIBE) y la iniciativa de Internet Segura for Kids (*Internet Seguro para Niños*) fomentando tanto como en alumnos y padres los riesgos en Internet.

“Algunos de estos pueden ser: identidad digital, reputación, netiqueta (comportamiento en línea), gestión de la información, ciberacoso escolar, protección ante virus y fraudes, uso excesivo de las TIC y mediación parental” (La importancia de la ciberseguridad en los colegios., 2017).

Un informe de 2010 de la Kaiser Foundation en los EE.UU descubrió que los jóvenes de entre 8 y 18 años pasaban más de siete horas y media diarias utilizando alguna forma de media o dispositivo informático, incluyendo la TV, una consola de juegos, un ordenador o una tableta, y eso sin incluir el tiempo que los menores dedicaban a enviar y recibir mensajes de texto o a hablar por el teléfono móvil o a enviar WhatsApp. A parte del tiempo dedicado a la escuela o a dormir, esto se supone que casi cada momento que pasan los niños y jóvenes están utilizando alguno de estos sistemas. (Giant & Bernárdez, 2016)

En Latinoamérica el especialista de Awareness & Research de ESET Latinoamérica indica lo siguiente “Los maestros como los padres de familia deben instruir al estudiante sobre el uso responsable que se le debe de dar al recurso tecnológico tanto en la casa como en la institución, además la responsabilidad sobre las redes sociales ya que hoy en día son las plataformas habituales para el *cyberbullying* o ciberacoso; por tanto es tarea de los padres y docentes estar al tanto del comportamiento de los estudiantes para detectar a tiempo un posible caso y poder intervenir a tiempo”. (El Comercio , 2014)

Estos altos índices generan las posibilidades de acoso, acceso a contenidos no aptos para menores de edad, conducta poco segura, y riesgos generales en la salud o sociales, relacionadas con el uso excesivo a los recursos informáticos si la debida seguridad en las instituciones educativas.

1.2.2. Contexto Nacional.

El uso del internet en jóvenes ecuatorianos es cada día más desmedido por lo que se necesita de ciertas pautas al momento de hacer uso del mismo, debido a las amenazas que podemos encontrar en la red tales como:

- Cyberbullying (Acoso a través de la Red)
- Phishing (Solicitud ilegal de claves)
- Grooming (Sustitución de identidades)

Estas son algunas de las amenazas a las que están expuestos los estudiantes a la hora de hacer uso del internet, además al no tener control sobre el tiempo que estén en el internet podría ocasionar los siguientes inconvenientes:

- Estados de Somnolencia
- Alteraciones en su estado de ánimo
- Reducción de horas que dedica al estudio

Tanto los docentes como los padres de familia deberían conocer y entender las nuevas tecnologías para usarla de manera educativa y pedagógica a favor de nuestros jóvenes estudiantes de esta manera fomentar la creatividad y la innovación (Chacón, Vera, & Cabrera, 2015).

Por estas razones se deben tomar medidas en cuanto en el contenido web que los adolescentes y los jóvenes frecuentan, existiendo así programas que permiten tener un control adecuado de que paginas podemos visitar de esta manera estamos tomando medidas preventivas para poder neutralizar estas posibles amenazas.

1.2.3. Contexto Local.

A nivel de la Provincia de Los Ríos la implementación de nuevas tecnologías en las unidades educativas es algo que se viene dando más seguido ya que algunas instituciones cuentan con infraestructuras tecnológicas sofisticadas, pero el problema que se presenta al momento de hacer uso de estas, es que en muchas ocasiones el personal no se encuentra capacitado para el manejo de las mismas.

Otro de los inconvenientes que se presenta es el mal uso que le dan los estudiantes al internet ya que se dedican la mayor parte del tiempo a descargar música, videos, etc., que en ciertas ocasiones muchas de estas descargas suelen contener virus lo cual afectaría a las maquinas en las que se encuentren realizando estas actividades.

Esto genera lo que se conoce como ocio informático causando así que el alumno baje en su rendimiento académico, además de causar preocupación en los padres de familia, por todos estos problemas ya expuesto es que se propone un análisis del tráfico de red en las instituciones educativas pertenecientes al Distrito 12D01 para así mediante un informe poder exponer el uso que se le está dando a estas nuevas tecnologías, y además recomendar medidas de seguridad y de protocolos para poder darle solución a estos problemas.

1.2.4. Contexto Institucional.

En la actualidad dentro del Distrito 12D01 es notable el incremento del uso del internet debido a la implementación de los recursos tecnológicos que se han suscitado en las Instituciones Educativas esto resulta beneficioso para el alumno ya que por medio de estos recursos se sentirá motivado para poder realizar sus tareas e investigaciones. Pero esto va a depender del uso que le dé a este recurso.

Pero como ya se ha expuesto los peligros que han surgido debido a las nuevas tecnologías y plataformas que han surgido para la comunicación como lo son las redes sociales y además las plataformas de videos que muchas veces no son de contenido apto para menores; debido a toda esta problemática que se está dando dentro de los estudiantes que pertenecen al Distrito 12D01 se propone un análisis de tráfico para poder monitorear a la información que se accede en las instituciones educativas, y poder brindar un mejor control y fiabilidad al momento de acceder a internet.

Además mejorar el uso de ancho de banda para de esta manera poder hacer un mejor uso de este recurso tan importante para la educación, cabe recalcar que también se procederá a realizar recomendaciones una vez generado el informe para así fortalecer y concientizar a los estudiantes que sitios web son seguros de visitar.

1.3. Situación problemática.

En el nivel académico la tecnología se ha convertido en una pieza indispensable para cualquier área, siendo de utilidad en cada materia impartida en el aula de clases, debido a su gran utilidad al momento de realizar una investigación, debate e información con la que cuentan los estudiantes.

Uno de los problemas que se ha venido suscitando por el uso de páginas web dedicadas al ocio en las unidades educativas se ha convertido en un gran problema de inproductividad para el desempeño del alumno.

Además sin tomar en cuenta los peligros que genera en navegar por dichas páginas web que muchas veces contiene virus y amenazas informáticas al que son expuestos los recursos tecnológicos cuando el estudiante navega sin control por el internet.

Lamentablemente el uso incorrecto por parte de los estudiantes de esta gran herramienta, debido a este mal uso del recurso tecnológico también retrasan los procesos de investigación de los demás estudiantes al encontrarse ocupado el canal de datos en actividades que no corresponde a su aprendizaje. Debido al poco control que hay en las unidades educativas los estudiantes no hacen un uso correcto del recurso tecnológico, pues no existe un impedimento para el control sobre páginas web que tienen contenido para adultos o material que no es apto para menores.

Existen otros riesgos que los estudiantes hoy en día enfrentan tales como el acoso con elementos sexuales más conocido como “Child Grooming”, “Sexting” y el “Happy Slapping” donde lo más alarmante es que tanto el agresor como la víctima pueden ser menores de edad.

Al mismo tiempo la poca supervisión que existe en los hogares genera problemas como amenazas informáticas, la información que está disponible para poder compartir con desconocidos y su contenido web no apto para menores.

En la actualidad el control y hacer buen uso de internet es muy poco en las instituciones educativas y hogares, hoy en día encontramos diversos peligros en las redes de datos ya sean internas como las redes LAN (Red de Área Local) o externas como (Internet) cada vez se van expandiendo rápidamente sea por correos electrónicos o por cada descarga que se haga desde internet.

Aparte de estas amenazas tampoco se tiene control de la utilización de este recurso ni equidad en la distribución del canal por el cual se tiene acceso a internet esto sucede donde varios usuarios usan el recurso al mismo tiempo, ya que debido a la falta de control hay usuarios que absorben todo el canal en otras actividades no permitidas y a los usuarios que de verdad necesitan para algo importante les quedara muy reducido y tendrán una demora notable en sus procesos.

Además en las instituciones educativas y hogares se tiene muy poco control en cuanto al contenido web que acceden los menores pues en las instituciones la única supervisión que hay es un profesor quien no alcanza a estar pendiente de todos los estudiantes, y un padre de familia en los hogares, pero este control no puede ser constante, por lo contrario es más largo el tiempo que están sin supervisión y pueden tener más acceso ha contenido malicioso.

Debido a estos problemas se destaca la gran necesidad de optimizar, controlar y monitorear este importante recurso como son las redes de datos en instituciones educativas y hogares, utilizando herramientas que están disponibles en el mercado y son de fácil manejo, así podemos ofrecer un buen desempeño del recurso a cada uno de los usuarios que tienen acceso a la red.

1.4. Planteamiento del problema.

Es de conocimiento que los recursos tecnológicos han sido implementados en la mayoría de las instituciones educativas lo cual resulta beneficioso para el desarrollo de sus tareas pero al no hacer un buen uso de este recurso se puede convertir en una amenaza para los estudiantes.

Como consecuencia de la implementación de estos recursos tecnológicos y su utilización en las instituciones educativas hace que los estudiantes se encuentren en riesgo y amenazas por el bajo control de este recurso debido a que no todo el contenido web que se encuentra disponible es apto para menores de edad, lo que genera una mala utilización del recurso y no exista igualdad en la distribución del canal por el cual se tiene acceso al internet.

Por este motivo surge la necesidad de realizar un análisis de tráfico en la red las instituciones educativas del distrito 12D01 para poder tomar las medidas de protección adecuadas al momento que los estudiantes se encuentren navegando en internet.

1.4.1. Problema general.

¿Cómo el tráfico de la red de datos incide en el acceso al contenido web de los estudiantes de las instituciones educativas del distrito 12D01?

1.4.2. Subproblemas o derivados.

- ¿Cómo mejorar el nivel de rendimiento y el nivel de seguridad de la red de datos en las Unidades Educativas del Distrito 12D01?
- ¿De qué forma se podría garantizar que el contenido web al que accedan mediante la red de datos, sea apto para menores?
- ¿Qué pruebas se realizarán para ofrecer calidad de servicio en la red de datos de las Unidades Educativas del Distrito 12D01 a través de herramientas de software libre?

1.5. Delimitación de la investigación.

El siguiente proyecto de investigación será llevado a cabo durante los meses comprendidos ente Mayo y Julio del presente año, y específicamente en las Unidades Educativas pertenecientes al Distrito 12D01 comprendido por las siguientes cantones Babahoyo, Baba y Montalvo.

1.6. Justificación.

En este análisis de ingeniería de tráfico lo que se busca es optimizar el ancho de canal, supervisar y detectar los problemas de tráfico no deseado en la red y ejecutar acciones que ayuden a mejorar el ancho de banda, filtrado web y poder brindar así una mejor seguridad a la hora de navegar por internet.

Para poder brindar un mejor desarrollo tecnológico en las instituciones educativas, mejorar sus procesos y aportar con el desarrollo del proyecto se ha optado por hacer este análisis de tráfico para verificar y aprovechar la utilización de recursos tecnológicos y así mediante un completo análisis saber cómo los alumnos de las instituciones educativas están aprovechando dichos recursos asignados, además conocer que amenazas se encuentran en la red y poder tomar un correcto control de contenidos a nivel web y realizar una distribución adecuada de cada sala de las instituciones educativas.

Los más beneficiados serían las unidades educativas y los padres de familia ya que podrán tener un mejor control y un gran desempeño de este recurso que hasta ahora no se ha tenido en cuenta además con todo eso se puede tener gran atribución en la educación de los alumnos al contrario podría llegar a ser muy perjudicial en su desarrollo.

A nivel de ingeniería se va a ser el uso de un programa con el cual va a realizar el análisis de tráfico de red de datos el cual nos proporcionara los informes detallados de tráfico web, estadísticas de acceso a Internet, cantidades de ancho de banda utilizado y otras estadísticas que se adjuntarán.

Este proyecto obtendrá un gran impacto a nivel del distrito luego de realizar el análisis de los datos y los correctivos que se decidan tomar para las instituciones en las que se van a hacer las pruebas, ya que marcará un precedente en la optimización del recurso tecnológico.

1.7.Objetivos de investigación.

1.7.1. Objetivo general.

Analizar el tráfico de la red de datos y su incidencia en el acceso al contenido web de los estudiantes de las instituciones educativas del distrito 12D01

1.7.2. Objetivos específicos.

- Conocer el comportamiento del tráfico de internet y detectar las causas que generan retardo para verificar el comportamiento del tráfico de internet en las Unidades Educativas del Distrito 12D01.
- Verificar que aplicaciones pueden ser adicionadas a la red para mejorar procesos internos y optimizar la seguridad de la información.
- Ejecutar pruebas con la herramienta seleccionada de software libre.

CAPÍTULO II.- MARCO TEÓRICO O REFERENCIAL

2.1. Marco teórico.

2.1.1. Marco conceptual.

A continuación se plantearán todos los conceptos claves que serán muy importantes para la comprensión del tema.

ANCHO DE BANDA: El ancho de banda explicado de una manera fácil, se puede definir como el número de bits o cantidad de datos que se puede enviar de un punto a otro en una unidad de tiempo a través de un medio de conectividad. En algunos países empieza a tener características parecidas al espacio de almacenamiento siendo así que está disponible para casi todos los habitantes en gran cantidad y a un precio accesible. (Castaño Ribes & López Fernández, 2013)

ARP (*ADDRESS RESOLUTION PROTOCOL*) O PROTOCOLO DE RESOLUCIÓN DE DIRECCIONES: Es un protocolo utilizado para obtener la dirección física (dirección MAC) de un equipo a través de su dirección IP. Cuando un equipo quiere enviar datos a otro dentro de una red (por ejemplo, una red Ethernet) utilizando la arquitectura TCP/IP, el equipo emisor debe generar uno (o más) datagramas, y éstos deben ser pasados al nivel inferior (nivel de enlace) y encapsulados en una (o más) tramas Ethernet. En esta situación, la referencia al equipo destino suele ser su dirección IP, pero para poder generar las tramas Ethernet también es necesario conocer la dirección MAC. (Santos, 2014)

ARQUITECTURA TCP/IP: Una arquitectura es un conjunto de reglas que define la función que tiene la parte de los programas y del hardware de red que conforman una pila de capas. La arquitectura de red más usada hoy en día es la Arquitectura TCP/IP. (Carceller Cheza, Campos Saborido, & García Marcos, Arquitectura TCP/IP, 2013)

BANDA ANCHA: Al hablar de banda ancha muchas veces confundimos el término con ancho de banda, pero es un concepto muy distinto, la banda ancha es un conjunto de tecnologías que ofrece servicios convergentes es decir como voz, videos y datos a través de redes diferentes. En esta época moderna la banda ancha se ha convertido en una pieza fundamental para la competitividad entre países sobre todo en el sector económico. (Telecomunicaciones/TIC, 2013)

En términos técnicos, la “banda ancha” puede definirse por lo siguiente:

- Velocidades de transmisión mínimas (aunque existen diversas definiciones).
- Tipo de tecnología (por ejemplo, IMT-Avanzadas móviles o las llamadas tecnologías “4G”).
- Una serie de conceptos funcionales, entre los que se cuentan:
 - **Conexión permanente:** donde el servicio Internet está sujeto a actualizaciones instantáneas en tiempo real.
 - **Alta capacidad:** conexiones de baja latencia y alta capacidad que pueden transportar grandes cantidades de bits (información) por segundo (en lugar de la velocidad a la que viajan esos bits).

DHCP PROTOCOLO DE CONFIGURACIÓN DINÁMICA DE EQUIPOS

(DEL INGLÉS *DYNAMIC HOST CONFIGURATION PROTOCOL*): El

protocolo DHCP es el que envía la información necesaria para que pueda conectarse a una red del tipo TCP/IP, el modelo que usa es el de Cliente/Servidor, donde el servidor DHCP asigna a los clientes que solicitan direcciones de red, estableciendo los parámetros necesarios para su configuración automática y que acceden a la red TCP/IP. (Carceller Cheza, Campos Saborido, & García Marcos, Servicios en red, 2013)

DIVISIÓN DE SUBREDES: Son redes segmentadas de forma arbitraria por el administrador de la RED para suministrar una estructura de enrutamiento jerárquica, permite un mayor aprovechamiento de las redes, esta división de subredes permite que el administrador de la red brinde seguridad de bajo nivel a la LAN. (Carreño Fonseca, 2014)

DNS (*Domain Name System*) o Sistema de Nombres de Dominio: Es un sistema que hace legibles para los usuarios las direcciones IP. Para ello, asocia direcciones numéricas con direcciones alfanuméricas, como por ejemplo 173.194.34.16 con www.google.com. Este sistema es una base de datos jerárquica y distribuida que permite localizar equipos y servicios mediante nombres alfanuméricos fáciles de recordar. Sin DNS el usuario debería acceder a los recursos mediante el uso de las direcciones IP, lo que resultaría muy engorroso. Además, como estas pueden cambiar, sería muy complicado mantener una lista actualizada de direcciones. (Carceller Cheza, Campos Saborido, & García Marcos, DNS, 2013)

DOMINIO DE COLISIÓN: Un dominio de colisión es un segmento físico de una red de computadores donde es posible que los paquetes puedan "colisionar" (interferir) con otros. Estas colisiones se dan particularmente en el protocolo de red Ethernet. (Giraldo , 2012)

FIREWALL: El firewall es un software experto que se filtra entre las aplicaciones y el software de red para realizar un filtrado de paquetes a partir de unas reglas definidas por el administrador de la red, en el tráfico entrante la tarjeta de red recibe el paquete y lo identifica, luego antes de entregarlo a la aplicación que corresponde pasa por el firewall este decide si prosigue o no, en el tráfico saliente las aplicaciones procesan sus paquetes de datos pero pasa por el firewall antes de entregarlo al software de red para que sea enviado. (Roa Buendía, 2013)

FTP PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS O (FILE TRANSFER PROTOCOL): Es un protocolo que se encuentra en la capa de aplicación el cual facilita el uso compartido de ficheros entre sistemas. Además este protocolo permite a los usuarios guardar información en el servidor o descargarla independientemente del sistema operativo usado. (Carceller Cheza, Campos Saborido, & García Marcos, Servicios en red, 2013)

HACKING ÉTICO: El hacking ético, llamado también prueba de intrusión o “pen test” ayuda a comprobar si existen vulnerabilidades de seguridad en una organización, para luego a través de un informe, detallar aquellos fallos de seguridad que se encuentren, aminorar a la brevedad posible y así poder evitar fugas de información y ataques informáticos. (Guevara Soriano, s.f.)

HTTP PROTOCOLO DE TRANSFERENCIA DE HIPERTEXTO O (HYPERTEXT TRANSFER PROTOCOL): Es un protocolo que se encuentra en la capa de aplicación el cual permite la distribución y el compartir la información entre sistemas mediante páginas web. (Carceller Cheza, Campos Saborido, & García Marcos, Servicios en red, 2013)

PLATAFORMA UTM: Los dispositivos destacados como UTM ((Unified Threat Management, en inglés) o gestión unificada de amenazas, es una combinación de técnicas que ayudan a proteger las redes, cortafuegos, antivirus, antispam, filtro de contenido, detección y prevención de intrusos redes privadas virtuales y servidores proxy todo ello en un único aparato. (Escrivá Gascó, Romero Serrano, & Ramada, 2013)

PROTOCOLO ICMP (INTERNET CONTROL MESSAGE PROTOCOL) O PROTOCOLO DE MENSAJES DE CONTROL DE INTERNET: Este protocolo se utiliza para enviar notificaciones sobre datagramas con problemas. Los mensajes ICMP son generados normalmente en respuesta a errores producidos sobre datagramas IP o para propósitos de diagnóstico y enrutamiento. (Santos, 2014)

PROTOCOLO IP: El protocolo IP pertenece a la capa de internet del conjunto de protocolos TCP/IP. Su importancia se debe porque permite el desarrollo y transporte de datagramas de IP (paquete de datos), sin garantizar su entrega. El proceso que realiza es de manera independiente donde solo define su representación, ruta y envío. (CCM, 2017)

PROCOLO TELNET (*TERMINAL NETWORK*) O TERMINAL DE RED:

Es un protocolo cliente-servidor que permite la conexión a un equipo remoto a través de un terminal desde el cual se pueden ejecutar comandos y aplicaciones como si se ejecutasen de forma local. El protocolo Telnet envía los caracteres tecleados en el equipo local (cliente) al equipo remoto (servidor), el cual los interpreta como si se hubiesen tecleado en un terminal de comandos local. La salida producida en el equipo remoto se envía al equipo local donde se visualiza. Telnet utiliza el puerto 23. (Santos, 2014)

PROXY: Un proxy es un dispositivo intermediario que actúa de dos formas ya sea como un cliente o como servidor. Acepta peticiones del cliente como si fuera el servidor destino y se las reenvía al servidor real, que cree estar comunicándose directamente con el cliente. Después, cuando el servidor entrega la respuesta al proxy, este se encarga de hacérsela llegar al cliente. (Carceller Cheza, Campos Saborido, & García Marcos, Servicios en red, 2013)

RARP (REVERSE ADDRESS RESOLUTION PROTOCOL) O PROCOLO DE RESOLUCIÓN INVERSA DE DIRECCIONES: Se utiliza para que un dispositivo obtenga su dirección IP a partir de su dirección MAC. Este protocolo se utiliza cuando un dispositivo conectado a la red no tiene almacenada su configuración de red de forma que tiene que solicitarla. Debe haber un equipo que almacene las direcciones IP correspondientes y responda a los mensajes del protocolo RARP. Su funcionamiento es similar a ARP.

REDES PRIVADAS VIRTUALES (VPN): VPN es una nueva alternativa que permite implementar una extensión segura de la red local (LAN) sobre una red pública o no controlada como internet, realizando un proceso de encapsulación y de encriptación, de los paquetes de datos a diferentes sitios remotos con la utilización de infraestructuras públicas de transporte. Sus principales características son la integridad, esto garantiza que los datos enviados sean exactos, y confidencialidad, permite que lo transmitido solo sea interceptado por el emisor y destino. (Álvarez Delgado, Jorquera Cáceres, Sepúlveda Jorquera, & Zamora Esquivel, 2014)

SEGMENTACIÓN DE RED: Segmentar una red es dividirla en subredes para poder incrementar el número de computadores conectados a la red y así tener un mejor rendimiento, siempre y cuando exista una misma topología, el mismo protocolo de conocimiento, y el mismo entorno de trabajo. (Moncada Murillo, 2015)

SEGURIDAD INFORMÁTICA: La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización. (Costas Santos, 2014)

SMTP (SIMPLE MAIL TRANSFER PROTOCOL) O PROTOCOLO SIMPLE DE TRANSFERENCIA DE CORREO: Es un protocolo cliente-servidor que sirve para el envío de mensajes de correo electrónico de un usuario a otro o de un usuario a un servidor SMTP. El envío de correo entre un cliente y un servidor se lleva a cabo a través del puerto 25 de una conexión TCP.

TCP (*TRANSMISSION CONTROL PROTOCOL*) O PROTOCOLO DE CONTROL DE TRANSMISIÓN: Es un protocolo orientado a la conexión que proporciona confirmación de entrega de datos y gestiona el flujo de transmisión. A su vez, se encarga de la retransmisión de paquetes perdidos. (Carceller Cheza, Campos Saborido, & García Marcos, TCP y UDP, 2013)

UDP (*USER DATAGRAM PROTOCOL*) O PROTOCOLO DE DATAGRAMAS DE USUARIO: Es un protocolo mucho más simple que se centra en la entrega de paquetes para maximizar la velocidad de la comunicación cuando no se requiere el empleo de TCP. (Carceller Cheza, Campos Saborido, & García Marcos, TCP y UDP, 2013)

2.1.2. Marco referencial sobre la problemática de investigación.

2.1.2.1. Antecedentes investigativos.

Según (Solórzano Alcívar, 2017), realizó la investigación “ANÁLISIS DE TRÁFICO DE RED PARA UN CORRECTO DIMENSIONAMIENTO DE ENLACES FÍSICOS ENTRE LOS EDIFICIOS DEL GAD MUNICIPAL DEL CANTÓN JUNÍN”, En el caso de estudio se realizará un análisis de los servicios y tráfico de la red entre los edificios que componen el GAD Municipal del cantón Junín, y en base a los resultados obtenidos se determinará el tráfico de red existente, se realizará una propuesta de mejoramiento de infraestructura de red con dimensionamiento de enlaces en las áreas que componen el GAD Municipal del cantón Junín, acorde a los requerimientos de la red y al crecimiento de la misma en un futuro.

Según Oscar (Salazar Salazar, 2016), con el proyecto, “ANÁLISIS DE TRÁFICO PARA LA INFRAESTRUCTURA DE LA RED DE LA EMPRESA PUBLICA MUNICIPAL DE TRANSPORTE TERRESTRE, TRÁNSITO Y SEGURIDAD VIAL EPM PORTOVIAL, PARA OFRECER UN MODELO CON CALIDAD DE SERVICIOS (QoS)”, En el presente proyecto se realiza el análisis de tráfico de la infraestructura de la red de la Empresa Pública Municipal de Transporte Terrestre, Tránsito y Seguridad Vial EPM Portovial ofreciendo un modelo con calidad de servicio (QoS), cuyo objetivo es optimizar el uso de la red. La Calidad de Servicio (QoS) se traduce como la capacidad de una red para entregar un servicio específico a un tipo concreto de tráfico, el soporte de la QoS puede dar lugar a la reserva de un ancho de banda, a un tráfico con prioridades, a una prevención de la congestión.

También en la investigación de Antonio. (Cuadra Sánchez, 2017), con el tema “CONTRIBUCIÓN AL ANÁLISIS DEL TRÁFICO DE INTERNET”, En esta tesis se ha desarrollado una serie de técnicas avanzadas de análisis de tráfico que cubren nuevas necesidades en el ámbito de la monitorización de redes y servicios. Las técnicas tradicionales se basan en el mero análisis de los protocolos y su evolución en el tiempo, en lugar considerar los perfiles y las características del tráfico como se propone en esta tesis, lo que posibilita su aplicación a distintas disciplinas, como la detección de anomalías en la red, la supervisión de la calidad o la gestión de la seguridad. Se ha desarrollado una metodología novedosa para analizar el tráfico denominada “análisis del perfil de día típico”, que permite caracterizar el comportamiento del tráfico para los diferentes periodos del día.

En la investigación de John y Mildres (Perafán Ruiz & Caicedo Cuchimba, 2014), con el tema “ANÁLISIS DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA INSTITUCIÓN UNIVERSITARIA COLEGIO MAYOR DEL CAUCA.”, El contenido de este trabajo muestra la necesidad de la Institución Universitaria Colegio Mayor del Cauca, de llevar a cabo un análisis de riesgos de tipo informático basado en la metodología MAGERIT que es una metodología de análisis y gestión de riesgos de los sistemas de información elaborada por el consejo superior de administración electrónica, para minimizar los riesgos de la implantación y uso de las tecnologías de la información, enfocada a las administraciones públicas con el fin de clasificar adecuadamente los riesgos y de esta forma con los resultados obtenidos.

La siguiente investigación es de Luisa Fernanda (Sánchez Ojeda, 2016), con la propuesta “IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO PARA INSTITUCIONES FISCALES BENEFICIARIAS DEL PROYECTO DE DOTACIÓN DE CONECTIVIDAD”, Hoy en día debido al incremento en el uso de las redes en las diferentes empresas es indispensable mantener un control organizado y planificado para su escalabilidad y convergencia, para ello se requiere el uso de herramientas que permitan la administración eficiente de los recursos de la red. Con este fin se crearon los sistemas de gestión de red, que son herramientas que nos ayudan a supervisar la disponibilidad, capacidad, seguridad, etc., para garantizar el correcto desempeño de las redes y sistemas internos.

2.1.2.2. Categorías de análisis.

Para poder hacer un análisis de nuestras dos variables, comenzaremos a detallar cada una de ellas para poder comprender la necesidad de un análisis de tráfico de red en las instituciones educativas del Distrito 12D01.

Historia de las Red de datos

Debido al gran avance de la tecnología ha surgido la necesidad de recolectar, procesar y distribuir la información, por el paso del tiempo las formas de transmisión ha ido cambiando, comenzando así con cartas, redes telefónicas, radio y televisión, hasta estos tiempos donde existen las redes informáticas. En empresas o instituciones con muchas oficinas a veces en lugares distantes surgió la necesidad de compartir recursos, pues este proceso se demoraba cierto tiempo, cuando necesitaban hacerlo con un solo clic.

Por esta razón la importancia de las redes de datos ya que brinda a los usuarios oportunidades múltiples en materia de software y programas que permiten compartir recursos entre ellos esta es la necesidad de las redes de computadoras.

Según (Jordán, Galperin, & Peres, 2013) “En la actualidad, se observa una consolidación de trayectorias tecnológicas, asociada al continuo desarrollo de las redes de acceso de alta velocidad y la masificación de los dispositivos para acceder a los servicios provistos a través de ellas”.

Otra opinión acerca de este tema es de (K & Avila, 2015) que nos dicen que:

Las nuevas tecnologías, relacionadas con nuestro entorno, están agilizando, optimizando y perfeccionando algunas actividades que realizamos en nuestro día a día. La comunicación en la actualidad es algo que ha avanzado mucho, una comunicación que es mucho más rápida que antes, un ejemplo de comunicación actual, en concreto a través de Internet, en el caso de transmitir mensajes, imágenes, vídeos y todo tipo de documentos desde diferentes partes del mundo durante las 24 horas del día es algo que ha desplazado un poco el envío de documentos por medio del servicio postal convencional.

Mediante esta dos opiniones podemos decir que el desarrollo de la tecnología es de vital importancia sobre todo en el área de las redes ya que son las que nos permiten que exista la comunicación, el envío de información, y por ende se debe realizar un análisis de tráfico para poder examinar lo que consultan los estudiantes y así determinar posibles soluciones a tomarse en cuenta.

TRÁFICO DE RED O DATOS

El tráfico de red se refiere a la cantidad de datos que se mueven a través de una red en un momento determinado. Los datos de red están principalmente encapsulados en paquetes de red, que proporcionan la carga en la red. El tráfico de red es el componente principal para la medición del tráfico de red, el control del tráfico de red y la simulación.

La organización adecuada del tráfico de red ayuda a garantizar la calidad del servicio en una red determinada. El tráfico de red también se conoce como tráfico de datos. (Techopedia, s.f.)

El tráfico de red es uno de los componentes principales que ayuda a la medición y gestión del ancho de banda. Además, existen varias topologías de red que se pueden implementar en función de la cantidad de tráfico de red en el sistema.

TOPOLOGÍA DE RED

La topología de la red es la que define su estructura.

Existen dos tipos de topología:

- **Topología física:** describe cómo están dispuestos en la red los medios de transmisión.
- **Topología lógica:** define cómo acceden los ordenadores a la red.

En los casos de redes con varias topologías, diremos que se trata de una red mixta.

TOPOLOGÍA FÍSICA DE LA RED

Las topologías físicas más utilizadas son:

- **Topología de bus:** utiliza un único segmento de cable donde todos los equipos se conectan de forma directa (**Figura 2**)

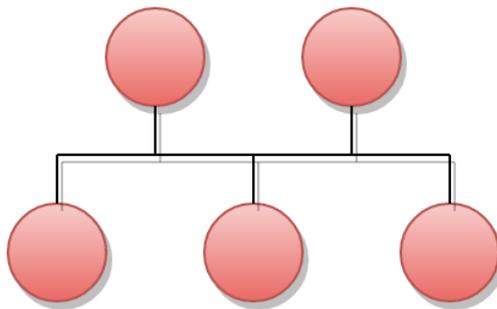


FIGURA 2. TOPOLOGÍA DE BUS
FUENTE: ELABORACIÓN PROPIA

- **Topología de anillo:** conecta cada equipo con el siguiente y el último con el primero, creando un anillo físico de cable (**Figura 3**).

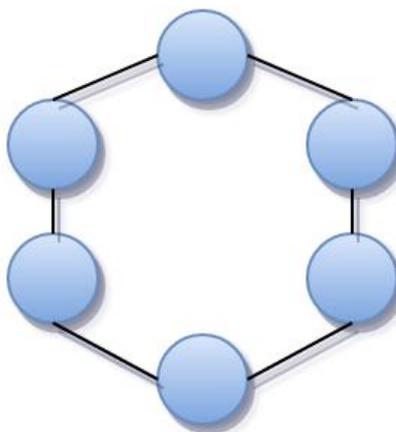


FIGURA 3. TOPOLOGÍA DE ANILLO
FUENTE: ELABORACIÓN PROPIA

- **Topología de estrella:** conecta los medios de transmisión de cada equipo a un único punto central de concentración. Este punto central suele ser un hub o un switch (**Figura 4**).

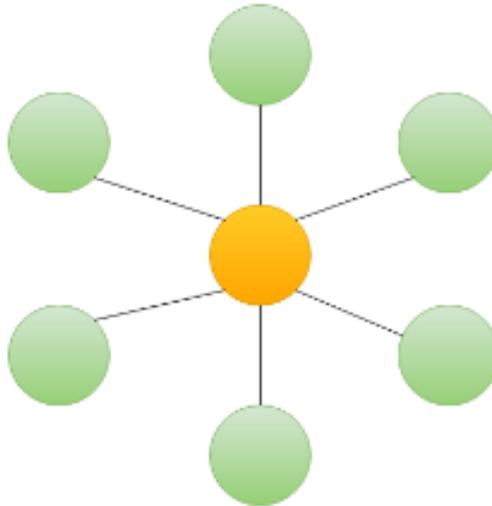


FIGURA 4. TOPOLOGÍA DE ESTRELLA
FUENTE: ELABORACIÓN PROPIA

- **Topología de estrella extendida:** consiste en la unión de varias redes con topologías de estrella. Todas las redes de estrella irán unidas, a su vez, a un punto central que reunirá las conexiones de todas ellas. Se utiliza para extender la longitud y dimensiones de la red (**Figura 5**).

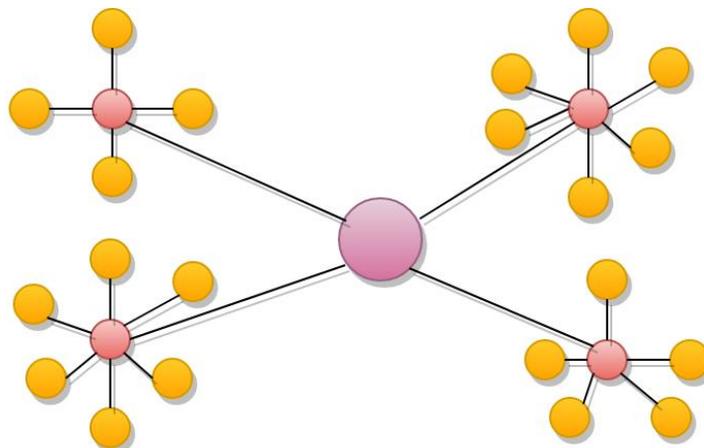


FIGURA 5. TOPOLOGÍA DE ESTRELLA EXTENDIDA
FUENTE: ELABORACIÓN PROPIA

- **Topología jerárquica:** es parecida a la de estrella extendida. Está formada por varias redes en forma de estrella conectadas entre sí y ordenadas de forma jerárquica. Normalmente el sistema se conecta a un computador que se encarga de controlar y gestionar el tráfico de la topología (**Figura 6**).

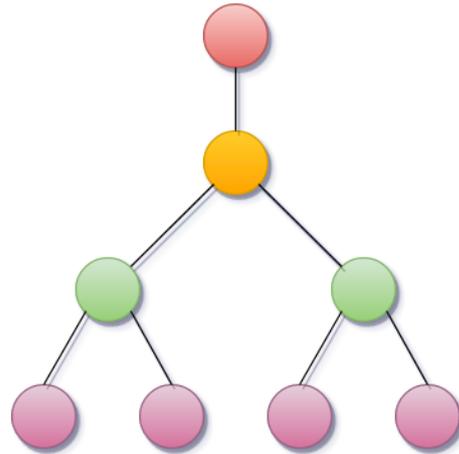


FIGURA 6. TOPOLOGÍA JERÁRQUICA
FUENTE: ELABORACIÓN PROPIA

- **Topología de malla:** aparece cuando cada nodo de la red está conectado a los demás nodos de la misma. De esta manera los paquetes de información disponen de multitud de caminos a seguir (**Figura 7**).

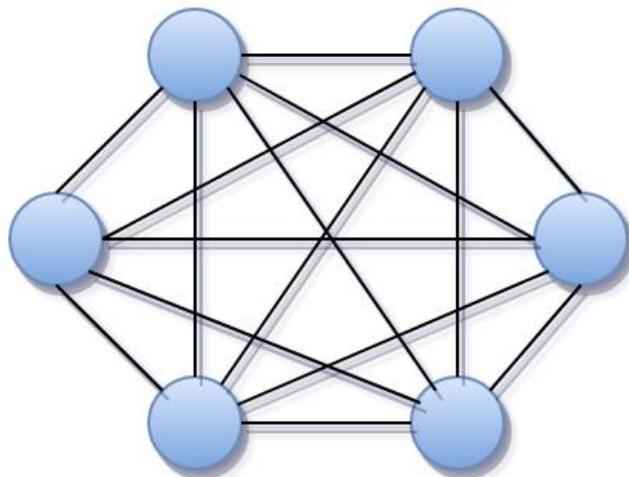


FIGURA 7. TOPOLOGÍA DE MALLA
FUENTE: ELABORACIÓN PROPIA

PROTOCOLO IP

El principal protocolo que utiliza la arquitectura TCP/IP en el nivel de red es el protocolo IP (Internet Protocol). IP es un protocolo del nivel de red no orientado a conexión, basado en datagramas y no fiable. (Santos, 2014)

- Se dice que un protocolo está basado en datagramas cuando la información que debe transmitir se divide en fragmentos. Por tanto, cada uno de los paquetes o fragmentos de información que transporta IP se le denomina datagrama. (Santos, 2014)
- IP es un protocolo no orientado a conexión, es decir, no se establece un camino previamente, con lo cual cada datagrama viaja de forma independiente pudiendo llegar al destino fuera de secuencia o duplicado. No se crean circuitos virtuales. (Santos, 2014)
- Y además es un protocolo no fiable, es decir, no ofrece comprobaciones ni seguimientos. IP intenta que la transmisión llegue a su destino lo mejor que puede pero sin ofrecer garantías. (Santos, 2014)

DATAGRAMA IP

La transmisión de los datos en el nivel de red utilizando el protocolo IP se realiza en unidades de información llamadas datagramas. Como es de suponer, un datagrama consta de dos partes, una cabecera y los datos.

La longitud de un datagrama es variable, pudiendo alcanzar un tamaño máximo de 65.535 bytes. A continuación se muestra la estructura de un datagrama IP (figura 8). Los números mostrados en la parte inferior de la figura son los tamaños de los campos de la cabecera expresados en bits.

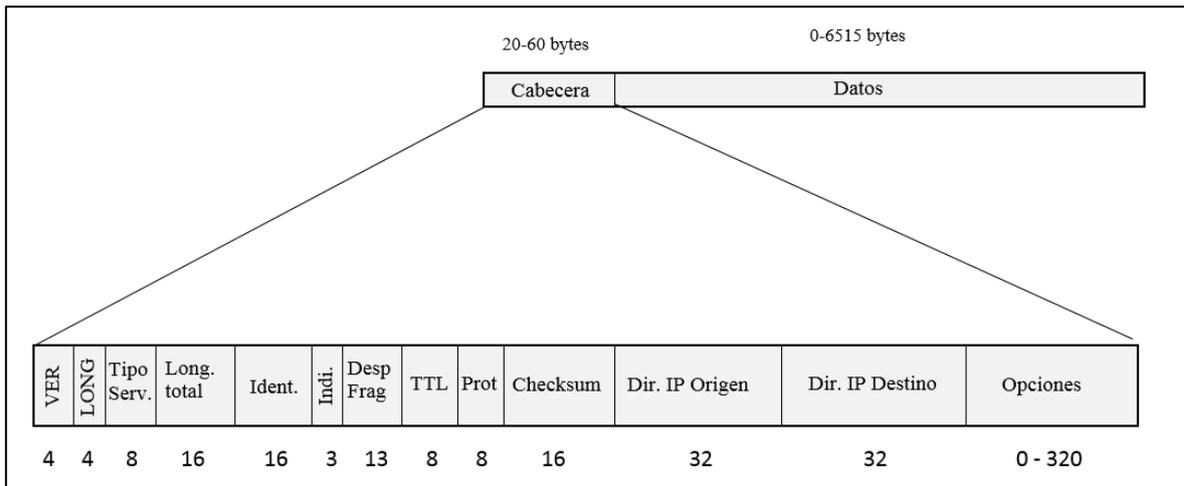


FIGURA 8. DATAGRAMA IP
FUENTE: ELABORACIÓN PROPIA

La descripción de cada uno de los campos es la siguiente:

- **Versión:** Se incluye la versión del protocolo IP. Actualmente la mayor parte de las redes utiliza la versión 4, por tanto este campo contiene el valor 4 en binario: 0100.
- **Longitud de la cabecera:** La cabecera de un datagrama IP no tiene un tamaño fijo. Su longitud puede estar entre 20 y 60 bytes. En este campo se define la longitud de la cabecera en un valor múltiplo de 4, es decir, el valor almacenado en este campo se multiplica por 4 para obtener el número total de bytes de la cabecera.

- **Tipo de servicio:** En la especificación original de IP este campo se utilizaba para incluir información sobre el nivel de retardo, fiabilidad y prestaciones, en función del tipo de servicio que se estuviera utilizando.

En la práctica este campo apenas ha sido utilizado, de forma que el IETF redefinió su uso como ECN (*Explicit Congestion Notification*), utilizado para enviar información sobre congestión de la red (RFC 3168).

- **Longitud total:** Almacena la longitud total del datagrama IP incluyendo la cabecera y los datos. Es un campo de 16 bits por lo que puede almacenar hasta una longitud de 65.535 bytes.
- **Identificación:** Este campo se utiliza cuando un datagrama original se fragmenta al pasar a una red diferente que trabaja con tamaños menores. A cada fragmento del datagrama original se le asigna un número de secuencia que es almacenado en este campo.
- **Indicadores:** Campo formado por tres bits, el primero es de uso reservado y debe ser 0. El segundo se utiliza para indicar si el datagrama está fragmentado, este bit estará activo para todos los datagramas resultantes de la fragmentación. El último bit indica si el datagrama es el último fragmento.
- **Desplazamiento del fragmento:** Este campo se utiliza para indicar el desplazamiento de los datos incluidos en el datagrama fragmentado respecto al datagrama original.

- **TTL (*Time To Live*) o Tiempo de vida:** Este campo es un número que indica el número de saltos que el datagrama puede realizar antes de ser descartado. Cuando se crea el datagrama se asigna a este campo un valor inicial (normalmente 127). Un salto se produce cuando el datagrama cambia de red, esto lo lleva a cabo un router. El router es el que decrementa el valor de este campo en una unidad. Si el valor del campo llega a cero, el datagrama se descarta. Este funcionamiento se utiliza para evitar que los datagramas permanezcan de forma indefinida en la red.
- **Protocolo:** Este campo es un identificador del protocolo de nivel superior utilizado. Los valores más comunes son: TCP, UDP o ICMP.
- **Cheksum o suma de comprobación:** Este campo se utiliza para la detección de errores en la cabecera. Para su cálculo no se tiene en cuenta los datos. Los errores de los datos deben ser detectados por los niveles superiores.
- **Dirección lógica de origen:** Este campo identifica el dispositivo de red del que parte el datagrama. El formato de la dirección lógica utilizado en IP se especifica en el siguiente apartado.
- **Dirección lógica de destino:** Este campo identifica el dispositivo de red al que va dirigido el datagrama. Opciones. Este campo se puede utilizar para enviar información adicional en la cabecera del datagrama aunque se utiliza con poca frecuencia.

DIRECCIONAMIENTO IP

En el protocolo IP, cada dispositivo debe tener asignada una dirección lógica conocida como dirección de red o dirección IP. La principal diferencia del direccionamiento lógico respecto al direccionamiento físico es que el primero es un direccionamiento jerárquico, donde una parte de la numeración se utiliza para identificar la red y otra parte para identificar el equipo dentro de la red.

La dirección IP está formada de 32 bits (4 bytes) y consta de tres campos de longitud variable dependiendo de la clase a la que pertenezca la dirección. Estos campos son la clase, el identificador de red y el identificador de estación.

Las clases se definieron en el protocolo IP para cubrir las necesidades de los diferentes tipos de organizaciones ya que cada tipo de clase permite un máximo de direcciones IP en cada red que pertenezca a dicha clase. Las clases que están definidas son:

- **Clase A:** En esta clase, el bit más significativo de la dirección IP vale 0. Se utilizan 7 bits para identificar la red y el resto de bits, es decir, 24, se utilizan para identificar un dispositivo dentro de la red.
- **Clase B:** En este caso, el valor de los dos primeros bits de la dirección es 10. Se utilizan 14 bits para identificar la red y 16 bits para identificar un dispositivo dentro de la red.

- **Clase C:** En este caso, el valor que se utiliza en los tres primeros bits para asignar la clase C es el 110. Se utilizan 21 bits para identificar la red y 8 bits para identificar un dispositivo dentro de la red.
- **Clase D:** Esta clase se identifica por contener en los cuatro primeros bits el valor 1110 y se utiliza para establecer direcciones de multienvío.
- **Clase E:** Identificada por sus primeros 4 bits tiene el valor 1111. Estas direcciones están reservadas inicialmente para usos futuros aunque en la práctica nunca se ha llegado a definir ningún uso para estas direcciones.

El resumen del direccionamiento se puede ver en la siguiente figura:

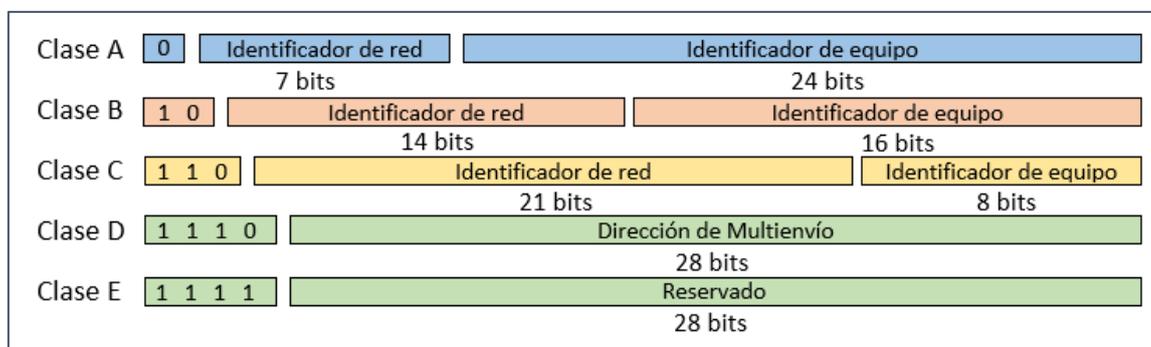


FIGURA 9. DIRECCIONAMIENTO IP
FUENTE: ELABORACIÓN PROPIA

ARQUITECTURA DE UNA RED IP

El direccionamiento lógico proporcionado por IP es el principal mecanismo para establecer los límites de una red. El rango de direcciones IP que una empresa u organización de cualquier tipo tiene asignado constituye la manera de identificar los equipos que pertenecen a la red interna. Un elemento fundamental en la arquitectura TCP/IP son los encaminadores o routers.

Estos dispositivos son capaces de transferir los datagramas IP de unas redes a otras dirigiéndolos a su destino final. Los routers están conectados, al menos, a dos redes lógicas diferentes, por tanto, se puede decir que los routers pertenecen a más de una red a la vez, y deben tener asignadas direcciones IP válidas en cada una de las redes a la que pertenezca.

El direccionamiento jerárquico que proporciona IP permite llevar a cabo un encaminamiento efectivo de los datagramas IP en los routers. En la siguiente figura se puede observar claramente la función de los mismos al unir redes con un rango de direcciones IP diferente permitiendo intercambiar tráfico entre ellas. Se ha utilizado para especificar los rangos de cada red direccionamiento CIDR.

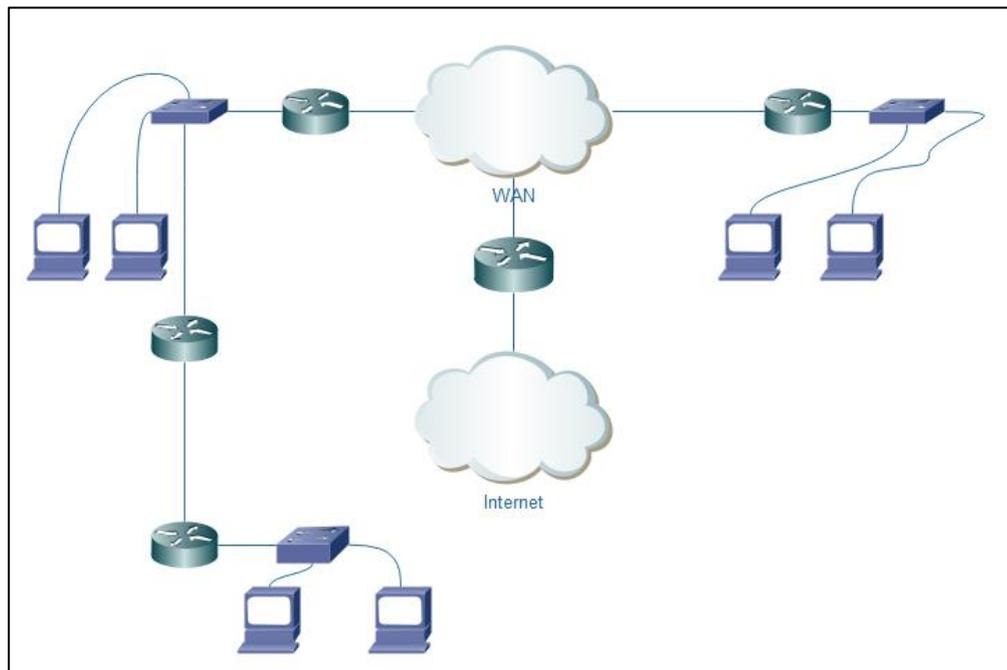


FIGURA 10. EJEMPLO DE LA ARQUITECTURA DE RED IP
FUENTE: ELABORACIÓN PROPIA

Desde el punto de vista de direccionamiento, el protocolo IP es capaz de llevar a cabo la entrega de datagramas a un destino que se encuentre en la misma red. Para comprobar que el host de destino está en la misma red que el host origen se utiliza la máscara, de forma que todos los bits de la máscara que estén a 1 deben coincidir en la dirección IP origen y destino para considerar que el destino está en la misma red. Sin embargo, si el host de destino no se encuentra en la misma red es necesario un dispositivo de interconexión como el router, que sea capaz de encaminar los datagramas a través de una determinada ruta que conducirá a la red donde se encuentra el host de destino.

MODELO OSI

OSI es un modelo basado en niveles para el diseño de sistemas de red. Este modelo además permite la interconexión de sistemas abiertos, o lo que es lo mismo, permite que dos sistemas diferentes se puedan comunicar independientemente de su arquitectura. Es importante resaltar que OSI es un modelo, no un protocolo.

Además, el modelo OSI no especifica los servicios ni los protocolos que forman parte de cada nivel.

Los niveles definidos en el modelo OSI son siete: físico, enlace, red, transporte, sesión, presentación, aplicación.

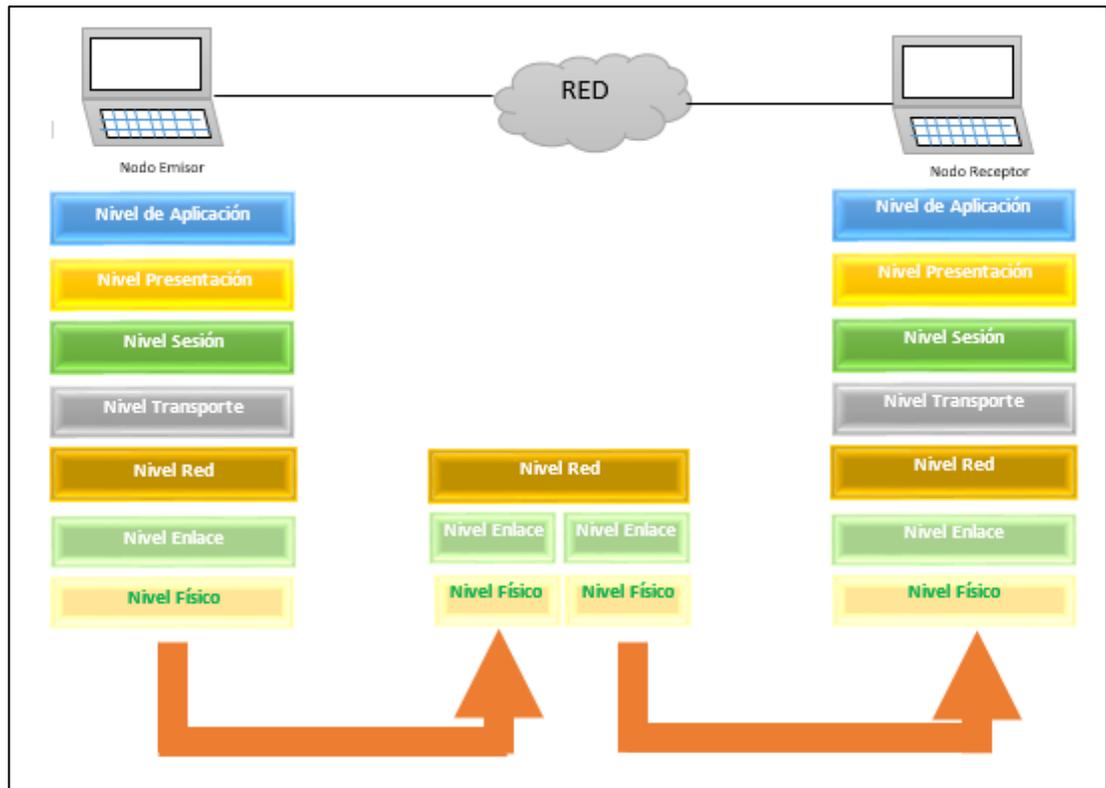


FIGURA 11. FUNCIONAMIENTO DEL MODELO OSI
FUENTE: ELABORACIÓN PROPIA

WIRESHARK

Wireshark es uno de los programas más usados por los administradores de red, una de sus funciones es analizar los paquetes de red y capturar estos paquetes para luego mostrarlos detalladamente como le sea posible. (Vásquez, 2013)

CARACTERÍSTICAS DE WIRESHARK

- Disponible para Linux y Windows
- Captura de paquetes en vivo desde una interfaz de red
- Muestra los paquetes con información detallada de los mismos
- Abre y guarda paquetes capturados

- Importar y exportar paquetes en diferentes formatos
- Filtrado de información de paquetes
- Resaltado de paquetes dependiendo el filtro
- Crear estadísticas

VENTAJAS

- Entre sus cualidades nos encontramos con una enorme versatilidad que le lleva a soportar más de 480 protocolos distintos, además de la posibilidad de trabajar tanto con datos capturados desde una red durante una sesión con paquetes previamente capturados que hayan sido almacenados en el disco duro.
- Wireshark soporta el formato estándar de archivos tcpdump, es capaz de reconstruir sesiones TCP, y está apoyado en una completa interfaz gráfica que facilita enormemente su uso.

DESVENTAJA

- Una de las desventajas es que en algún momento puede ser difícil de descifrar la información que transita en la red.

ADVANCED IP SCANNER

Advanced IP Scanner es una herramienta gratuita que te permitirá hacer exploraciones en una red de área local y recopilar información sobre los dispositivos conectados. Además de detectar a los equipos de la red, podrás acceder fácilmente a recursos como carpetas compartidas, servidores HTTP y servidores FTP. (Reyes, 2015)

CARACTERÍSTICAS

- Explora una red en cuestión de segundos.
- Detecta cualquier dispositivo de red.
- Explora puertos HTTP, HTTPS, FTP, RDP y carpetas compartidas.
- Permite conectar ordenadores ejecutando Radmin Server con un solo clic.
- Le permite apagar ordenadores de forma remota.
- Ejecutar comandos ping, tracert, telnet y SSH en el equipo seleccionado.
- Compatible con Wake-On-Lan.
- Lista de favoritos para una administración sencilla de la red.

VENTAJAS

- Control y acceso a recursos del equipo.
- Apagado y encendido remotos.
- Muestra información de los equipos conectados.
- Selección de rangos de IP's a analizar (ping).

DESVENTAJAS

- No permite tareas programadas.

CAPSA FREE

Capsa Free es un programa gratuito de analizador de red para monitoreo, solución de problemas y análisis de Ethernet. Brinda a los usuarios una gran experiencia para aprender a monitorear las actividades de la red, detectar problemas de red y mejorar la seguridad de la red. (Colasoft, s.f.)

CARACTERÍSTICAS PRINCIPALES

- Identificar y analizar más de 500 protocolos de red, así como las aplicaciones de red basadas en el análisis de protocolo.
- Captura de paquetes en tiempo real, así como la posibilidad de guardar los datos transmitidos a través de redes locales.
- Supervisar y guardar correo electrónico de Internet y mensajería instantánea de tráfico, ayudando a identificar a la seguridad y manejo de datos confidenciales.
- Diagnostica y localiza problemas de red en cuestión de segundos mediante la detección y localización de hosts sospechosos.

- Visualiza toda la red en una elipse que muestra las conexiones y el tráfico entre cada host.

VENTAJAS

- Supervisa, analiza y soluciona problemas de tráfico de redes cableadas e inalámbricas.
- Realiza captura de paquetes en tiempo real.
- Monitoreo de red.
- Análisis de protocolo avanzado.
- Decodificación de paquetes a profundidad.

ACCESIBILIDAD AL CONTENIDO WEB PARA TODAS LAS PERSONAS

Durante las últimas décadas se ha observado cómo ha ido evolucionando la tecnología en los diversos planteamientos ya sean educativos y sociales por lo que es necesario continuar trabajando para que exista una igualdad de oportunidades, ya sea en una institución pública o privada. Para lo cual se debe contar con dos aspectos los cuales son:

- Una institución que cuente con la diversidad de medios los cuales respondan a las necesidades de los que en ella estudian.
- Una institución donde los medios se encuentren disponibles para las necesidades de los receptores de la información.

Lo mismo pasa en el sector educativo las tecnologías de la información y comunicación se están convirtiendo en instrumentos básicos, reflejo de la sociedad en la que estamos viviendo por esta razón se debe tener acceso a la red como un requisito necesario para la inclusión social, situación que se vive en Ecuador de una manera paulatinamente.

Debido a la capacidad de acceder a los altos niveles de información que se encuentran en el internet de manera masiva e indiscriminada es posible generar problemas de gran calado social sobre todo en las instituciones educativas que no han tomado medidas para el buen uso del recurso tecnológico.

Entre los problemas de seguridad más graves se encuentran los delitos contra la libertad sexual, que van desde el mero acoso hasta el exhibicionismo o la provocación explícita:

- **Grooming (engatusar):** Es un término anglosajón que se refiere a los procedimientos (establecer lazos emocionales, obtener datos personales, enviar o solicitar imágenes de contenido erótico o pornográfico y chantaje posterior) que utilizan pederastas y pedófilos a la hora de ganarse la confianza del internauta menor de edad. (Gasteiz)
- **Cyberbullying (ciberacoso):** Se entiende por ciberacoso la persecución y hostigamiento, entre menores, en el entorno de una red de comunicaciones (Internet, teléfonos móviles u otras tecnologías telemáticas). Suele consistir en amenazas, humillaciones, chantaje, vejaciones o insultos de jóvenes a otros jóvenes. El anonimato, la falta de percepción del daño real causado y la frecuente adopción de roles imaginarios en la red convierten al ciberacoso en un grave problema. (Gasteiz)

- **Sexting (juego de palabras traducible por 'enviando sexo'):** El sexting consiste en el envío de contenidos de tipo sexual (principalmente fotografías y/o vídeos), producidos generalmente por el propio remitente, a otros menores por medio de teléfonos móviles. La presión de sus 'colegas', el deseo de ser reconocidos, la necesidad de que les presten atención, la inmadurez y otros motivos típicos de determinadas edades conforman las razones que descansan detrás de esta práctica. (Gasteiz)

FORMAS DE ACCESO AL CONTENIDO WEB

- **Búsqueda directa:** Es natural y saludable que los menores tengan curiosidad por saber y aprender. Internet ofrece mucha información y está siempre disponible, el riesgo está en que no siempre ofrece un contenido adecuado a la hora de dar respuesta a esa curiosidad. (Internet Segura ForKids, s.f.)
- **Búsqueda indirecta:** En ocasiones encuentran contenidos inapropiados de forma indirecta al buscar otros. También pueden acceder a comunidades virtuales buscando determinada información, pero una vez dentro reciben contenido de riesgo. (Internet Segura ForKids, s.f.)
- **Videojuegos y otros contenidos de ocio (cine, series y música online):** Los videojuegos pueden esconder gran cantidad de contenidos inapropiados para los menores, y a menudo se trata de contenido explícito: violencia, sexo, conductas y valores extremistas, etc. (Internet Segura ForKids, s.f.)

- **Mensajería y redes sociales:** A través de mensajería instantánea, correo electrónico, redes sociales son habituales los fraudes, escondidos detrás de promociones, cupones de descuento y comercio online, así como el intercambio de contenidos inapropiados entre menores (imágenes, vídeos, etc.). (Internet Segura ForKids, s.f.)
- **Publicidad:** En el entorno de las TIC la publicidad está siempre presente, y es independiente a la edad del consumidor. La mayor parte del contenido que encontramos en Internet es público y “gratuito”, lo que implica que el beneficio económico se consigue por otros medios. El más habitual es la publicidad, ya sea en forma de ventanas emergentes, banners, vídeos, redes sociales, blogs, etc. (Internet Segura ForKids, s.f.)

EL ACCESO A CONTENIDOS INAPROPIADOS INTERNET

En su concepción actual, es un sistema abierto a los usuarios en las dos direcciones. Por una parte, se benefician de los contenidos que encuentran durante su navegación y, por otra, pueden contribuir al enriquecimiento de la propia oferta de contenidos. La oferta de información y archivos compartidos en la Red es de tal magnitud que no es posible un control general sobre todos ellos, por lo que la vigilancia sobre el acceso a los mismos depende, en última instancia, de los deseos y la implicación de los propios usuarios. (Gasteiz)

Al navegar por Internet, el menor puede encontrarse, incluso sin buscarlo, con contenidos no adecuados para su edad, como páginas que ofrecen sexo explícito o páginas con contenidos violentos, lenguajes inadecuados o informaciones malintencionadas. (Gasteiz)

LOS PELIGROS DE LAS REDES SOCIALES

Las Redes Sociales son sistemas de interacción social consistentes en la facilitación, a través de un sistema informático, de un intercambio entre personas. Por su propia naturaleza son sistemas abiertos y muy dinámicos que invitan a la participación activa, a compartir contenidos y, en general, a la comunicación y el encuentro. (Gasteiz)

Estas redes son muy populares entre los menores porque les permiten crear una página personal, expresarse libremente y establecer vínculos con amigos. Las redes sociales pueden afectar a la seguridad de los menores porque ofrecen tantas opciones que dificultan el empleo de criterios de selección.

No se trata de satanizar las redes sociales, que son una herramienta de gran utilidad, sino de conocer en profundidad sus aportaciones, sus riesgos y la manera correcta de interactuar con ellas. (Gasteiz)

ADICCIÓN AL INTERNET

Se puede decir que las adicciones están ligados al tiempo y el consumo, pero (si podemos diagnosticar a tiempo podremos tomar medidas) si no disminuyen la situación se puede agravar al aumentar las experiencias con la adicción que se tenga. Entonces el uso del internet se vuelve un problema cuando se asocia a los siguientes factores: la novedad del tiempo, la edad en algunos casos, y la disponibilidad. Esto puede generar ansiedad en la primera fase del uso del internet, además sino se cuenta con el medio y los recursos para poder desenvolverse en el mundo virtual, lo que produce malestar en las personas que sufren esta adicción que se la denomina ciberadicción. (Echeburúa, 2016)

La ciberadicción consta de cinco adicciones las cuales son:

- Adicción computacional, asociada al uso de juegos en línea.
- Sobrecarga de información, que implica la navegación compulsiva por diferentes sitios.
- Compulsión en red, que hace referencia al gasto de dinero en compras.
- Adicción cibersexual, que incluye acceso a pornografía y relaciones sexuales facilitadas por internet.
- Adicción a las ciberrelaciones, dada a través del uso de las redes sociales.

CONSECUENCIAS DE LA ADICCIÓN A INTERNET

Existen varias consecuencias denotadas en el estudio de Adicción a Internet:

TRASTORNOS PSICOSOCIALES

En la Adicción a Internet se ha asociado a trastorno en el control de los impulsos, comportamientos obsesivos, disfuncionales e incluso enfermedades psiquiátricas como trastorno bipolar o depresivo, inestabilidad emocional con tendencia a evasión de la realidad, pobre tolerancia a la frustración, volubilidad e irritabilidad, egocentrismo, timidez, introversión, baja empatía, desvalimiento y baja autoestima, de igual forma, tendencia al aislamiento, predisposición al aburrimiento, búsqueda de sensaciones, preferencia por las actividades solitarias, autosuficiencia y reactividad emocional estos rasgos no son ajenos a la comorbilidad psiquiátrica predominante en estos pacientes, en los que se destacan los trastornos afectivos, como la depresión en primer orden y luego los problemas adictivos.

Se ha observado una reducción de la capacidad de expresión, principalmente en el lenguaje escrito, tendencia al aislamiento a la soledad y comportamientos antisociales.

Además de baja autoestima, por lo que muchos, escudados tras una máquina forman personalidades ficticias o actúan de tal manera que jamás la harían. Otro de los principales problemas encontrados son los contenidos inapropiados y el contacto con extraños.

TRASTORNOS ACADÉMICOS

Se define el rendimiento como la capacidad de responder satisfactoriamente frente a estímulos educativos, susceptible de ser interpretado según objetivos o propósitos educativos pre-establecidos. Este tipo de rendimiento académico puede ser entendido en relación con un grupo social que fija los niveles mínimos de aprobación ante un determinado grupo de conocimientos o aptitudes.

TRASTORNOS FAMILIARES

En la ciberadicción se ha visto un incremento en el fraccionamiento del sistema familiar, en donde el adolescente con sus características propias de su ciclo vital son más vulnerables de contribuir en ello. En estudios realizados en Ecuador se ha visto que la mayoría de adolescentes usan internet sin supervisión de sus padres, además estudiantes manifiestan que rara vez lo han recriminado sus padres por pasar mucho tiempo en el internet, Es decir existe poco interés de los padres acerca de usos, actitudes y practicas acerca de internet en sus hijos, haciendo de ellos presa fácil al involucramiento y posteriormente Adicción a Internet.

2.1.3. Postura teórica.

WIRESHARK: Es un programa de código abierto el cual ayuda al análisis de paquetes de datos en una red para encontrar problemas para desarrollar software y protocolos, y también como herramienta educativa. WireShark captura el tráfico de una red y analiza los paquetes. La visualización de esta información puede ser personalizada empleando filtros. Su nombre original era Ethereal, pero fue cambiado en 2006 a WireShark por cuestiones legales y fue desarrollada por Gerald Comb en 1998.

Se eligió WireShark sobre las demás herramientas análisis por las siguientes razones:

- Es un software gratuito.
- Es Multiplataforma.
- Es un analizador de muchos protocolos.
- Captura la información y la muestra de una manera dinámica al usuario.
- Permite guardar la captura de información para un análisis posterior.
- Además se puede solicitar los siguientes reportes:
 - Latencias promedios al igual que el Jitter
 - Flujo de paquetes por segundo
 - Cuantos hosts existen en la red (y cuáles son los que más información transmiten y/o reciben)
 - Cuáles son las aplicaciones más utilizadas (ejemplo HTTPs, DNS, RDP) y cuanto ancho de banda están consumiendo las mismas
 - Decodificación de telefonía IP para poder escuchar conversaciones o resolver problemas de calidad
 - Decodificar flujos de datos enviados mediante WIFI (siempre que tengamos las claves WPA o WEP correspondientes)
 - Ver estadísticas especiales como por ejemplo cuantos conflictos por IP duplicadas se han detectado, cuantas consultas DNS y los tiempos promedios de respuesta de las mismas, tamaño promedio de las tramas, entre otras.

2.2. Hipótesis.

2.2.1. Hipótesis general.

A través del análisis de tráfico se puede monitorear posibles amenazas que afecten a los estudiantes de las Unidades Educativas del Distrito 12D01.

2.2.2. Subhipótesis o derivadas.

- Conociendo el comportamiento del tráfico de red de las Unidades Educativas del Distrito 12D01 se podrá mejorar el nivel de rendimiento de la red de datos.
- Con la instalación de aplicaciones se podrá controlar las amenazas que se encuentran a la hora de navegar por internet y que el contenido web sea apto para menores.
- Ejecutando las pruebas con la herramienta de análisis de tráfico podemos determinar los riesgos que se corre al no tomar medidas de seguridad adecuadas para la red de datos.

2.2.3. Variables.

Variable Independiente: Análisis de Tráfico de la Red de Datos.

Variable Dependiente: Incidencia en el acceso al contenido web de los estudiantes de las Instituciones Educativas del Distrito 12D01.

CAPÍTULO III.- RESULTADOS DE LA INVESTIGACIÓN.

3.1 Resultados obtenidos de la investigación.

3.1.1 Pruebas estadísticas aplicadas.

- Prueba de Chi Cuadrado

HIPÓTESIS

H₀: A través del análisis de tráfico se puede monitorear posibles amenazas que afecten a los estudiantes de las Unidades Educativas del Distrito 12D01.

H₁: A través del análisis de tráfico no se podrá monitorear las amenazas que afecten a los estudiantes de las Unidades Educativas del Distrito 12D01.

Detalle	Pregunta 7	Pregunta 8	Total
Si	68	75	143
No	23	16	39
Total	91	91	182

TABLA 1. DETALLE HIPÓTESIS
FUENTE: ELABORACIÓN PROPIA

$$X^2_{calc} = \sum \frac{(f_o - f_e)^2}{f_e}$$
$$X^2_{calc} = \frac{(68 - 71.5)^2}{71.5} + \frac{(75 - 71.5)^2}{71.5} + \frac{(23 - 19.5)^2}{19.5} + \frac{(16 - 19.5)^2}{19.5}$$
$$X^2_{calc} = 0.171 + 0.171 + 0.628 + 0.628$$

$$X^2_{calc} = 1.598$$

Grados de Libertad

$$v = (\text{cantidad de filas} - 1) (\text{cantidad de columnas} - 1)$$

$$v = (2 - 1)(2 - 1)$$

$$v = 1(1) = 1$$

Nivel de significancia

$$1\% = 0.01$$

Regla de decisión

$$X^2_{calc} \leq \text{Valor crítico}$$

$$1.598 \leq 6.635$$

Decisión

Se puede aceptar la hipótesis nula y concluir que con el análisis de tráfico se detectara las amenazas existentes en las Unidades Educativas del Distrito 12D01.

SUBHIPÓTESIS N°1

H₀: Conociendo el comportamiento del tráfico de red de las Unidades Educativas del Distrito 12D01 se mejorará el nivel de rendimiento de la red de datos.

H1: Conociendo el comportamiento del tráfico de red de las Unidades Educativas del Distrito 12D01 no se podrá mejorar el nivel de rendimiento de la red de datos.

Detalle	Pregunta 4	Pregunta 5	Total
Si	72	67	139
No	19	24	43
Total	91	91	182

TABLA 2. DETALLE DE SUBHIPÓTESIS 1
FUENTE: ELABORACIÓN PROPIA

$$X^2_{calc} = \sum \frac{(f_o - f_e)^2}{f_e}$$

$$X^2_{calc} = \frac{(72 - 69.5)^2}{69.5} + \frac{(67 - 69.5)^2}{69.5} + \frac{(19 - 21.5)^2}{21.5} + \frac{(24 - 21.5)^2}{21.5}$$

$$X^2_{calc} = 0.089 + 0.089 + 0.290 + 0.290$$

$$X^2_{calc} = 0.758$$

Grados de Libertad

$$v = (\text{cantidad de filas} - 1) (\text{cantidad de columnas} - 1)$$

$$v = (2 - 1)(2 - 1)$$

$$v = 1(1) = 1$$

Nivel de significancia

$$1\% = 0.01$$

Regla de decisión

$$X^2_{calc} \leq \text{Valor crítico}$$

$$0.758 \leq 6.635$$

Decisión

Se puede aceptar la hipótesis nula y concluir que el nivel de rendimiento de la red de datos de las Unidades Educativas del Distrito 12D01 después del análisis de tráfico será óptimo y confiable.

SUBHIPÓTESIS N°2

H0: Con la instalación de aplicaciones se podrá controlar las amenazas que se encuentran a la hora de navegar por internet y que el contenido web sea apto para menores.

H1: Con la instalación de aplicaciones no se podrá controlar las amenazas que se encuentran a la hora de navegar por internet y que el contenido web sea apto para menores.

Detalle	Pregunta 9	Pregunta 10	Total
Si	75	66	141
No	16	25	41
Total	91	91	182

TABLA 3. DETALLE DE SUBHIPÓTESIS 2
FUENTE: ELABORACIÓN PROPIA

$$X^2_{calc} = \sum \frac{(f_o - f_e)^2}{f_e}$$

$$X^2_{calc} = \frac{(75 - 70.5)^2}{70.5} + \frac{(66 - 70.5)^2}{70.5} + \frac{(16 - 20.5)^2}{20.5} + \frac{(25 - 20.5)^2}{20.5}$$

$$X^2_{calc} = 0.287 + 0.287 + 0.987 + 0.987$$

$$X^2_{calc} = 2.548$$

Grados de Libertad

$$v = (\text{cantidad de filas} - 1) (\text{cantidad de columnas} - 1)$$

$$v = (2 - 1)(2 - 1)$$

$$v = 1(1) = 1$$

Nivel de significancia

$$1\% = 0.01$$

Regla de decisión

$$X^2_{calc} \leq \text{Valor crítico}$$

$$2.548 \leq 6.635$$

Decisión

A pesar de que algunas Instituciones Educativas pertenecientes al Distrito 12D01 cuentan con algunas herramientas y software de protección, la hipótesis nula es aceptable porque algunos docentes desconocen de estas herramientas para poder así supervisar a los alumnos a la hora que navegan en el internet.

SUBHIPÓTESIS N°3

H0: Ejecutando las pruebas con la herramienta de análisis de tráfico podemos determinar los riesgos que se corre al no tomar medidas de seguridad adecuadas para la red de datos.

H1: Ejecutando las pruebas con la herramienta de análisis de tráfico no se podrá determinar los riesgos que se corren al no tomar medidas de seguridad adecuadas para la red de datos.

Detalle	Pregunta 9	Pregunta 10	Total
Si	75	66	141
No	16	25	41
Total	91	91	182

TABLA 4. DETALLE DE SUBHIPÓTESIS 3
FUENTE: ELABORACIÓN PROPIA

$$X^2_{calc} = \sum \frac{(f_o - f_e)^2}{f_e}$$

$$X^2_{calc} = \frac{(75 - 70.5)^2}{70.5} + \frac{(66 - 70.5)^2}{70.5} + \frac{(16 - 20.5)^2}{20.5} + \frac{(25 - 20.5)^2}{20.5}$$

$$X^2_{calc} = 0.287 + 0.287 + 0.987 + 0.987$$

$$X^2_{calc} = 2.548$$

Grados de Libertad

$$v = (\text{cantidad de filas} - 1) (\text{cantidad de columnas} - 1)$$

$$v = (2 - 1)(2 - 1)$$

$$v = 1(1) = 1$$

Nivel de significancia

$$1\% = 0.01$$

Regla de decisión

$$X^2_{calc} \leq \text{Valor crítico}$$

$$2.548 \leq 6.635$$

Decisión

La hipótesis nula es aceptable porque una vez realizado el análisis de tráfico se procederá a la toma de decisiones para poder mejorar la red de datos en las Instituciones Educativas pertenecientes al Distrito 12D01.

3.1.2 Análisis e interpretación de datos.

1.- ¿Existen procedimientos de seguridad informática e instructivos establecidos en la unidad educativa?

Detalle	Frecuencia	Porcentaje
Si	48	53%
No	34	37%
Desconoce	9	10%

TABLA 5. DETALLE DE LA PREGUNTA N°1
FUENTE: ELABORACIÓN PROPIA

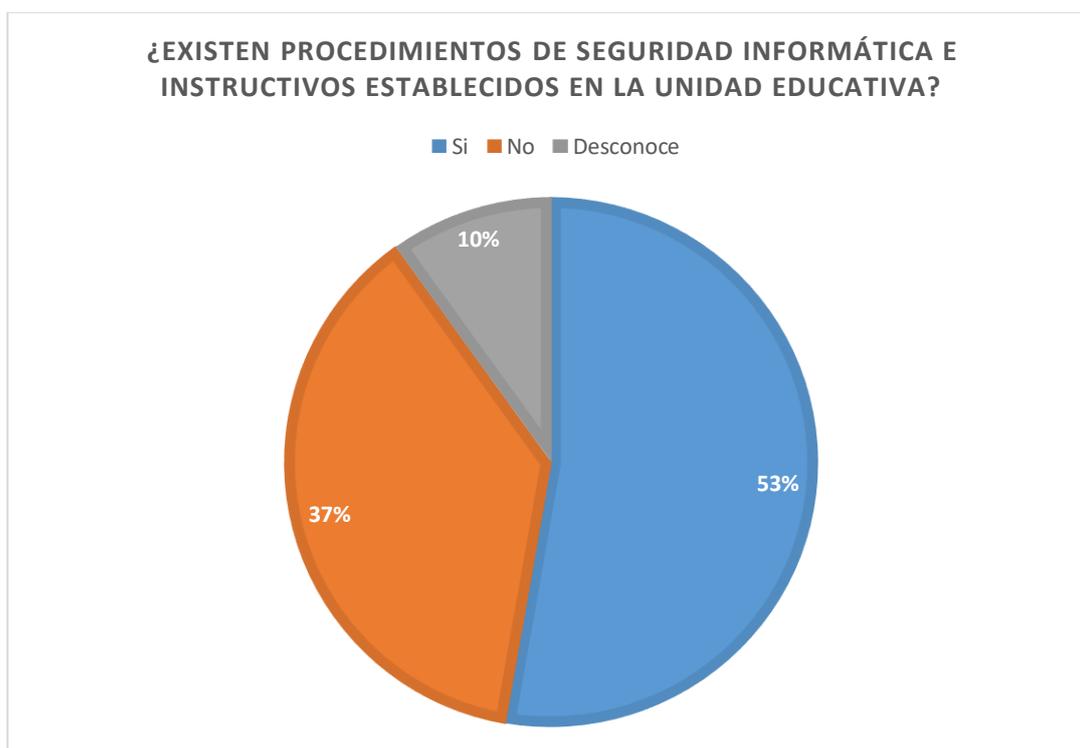


GRAFICO 1. EXISTENCIA DE PROCEDIMIENTOS DE SEGURIDAD INFORMÁTICA EN LAS UNIDADES EDUCATIVAS
FUENTE: ELABORACIÓN PROPIA

Análisis e Interpretación

El 53% de los docentes pertenecientes a las Unidades Educativa conocen que existen procedimientos e instructivos de seguridad en los establecimientos, el 37% no cuenta con estos parámetros y el 10% desconoce si existen algún tipo de procedimientos e instructivos de seguridad en las instituciones educativas.

A pesar de que algunos docentes conocen sobre estos procedimientos e instructivos de seguridad en algunos de los casos no se aplica al momento de sancionar algún alumno por hacer caso omiso a estos instructivos o procedimientos de seguridad.

2.- ¿Conoce si en la unidad educativa existe un responsable de la seguridad informática y la seguridad de la información?

Detalle	Frecuencia	Porcentaje
Si	73	80%
No	15	17%
Desconoce	3	3%

TABLA 6. DETALLE DE LA PREGUNTA N°2
FUENTE: ELABORACIÓN PROPIA

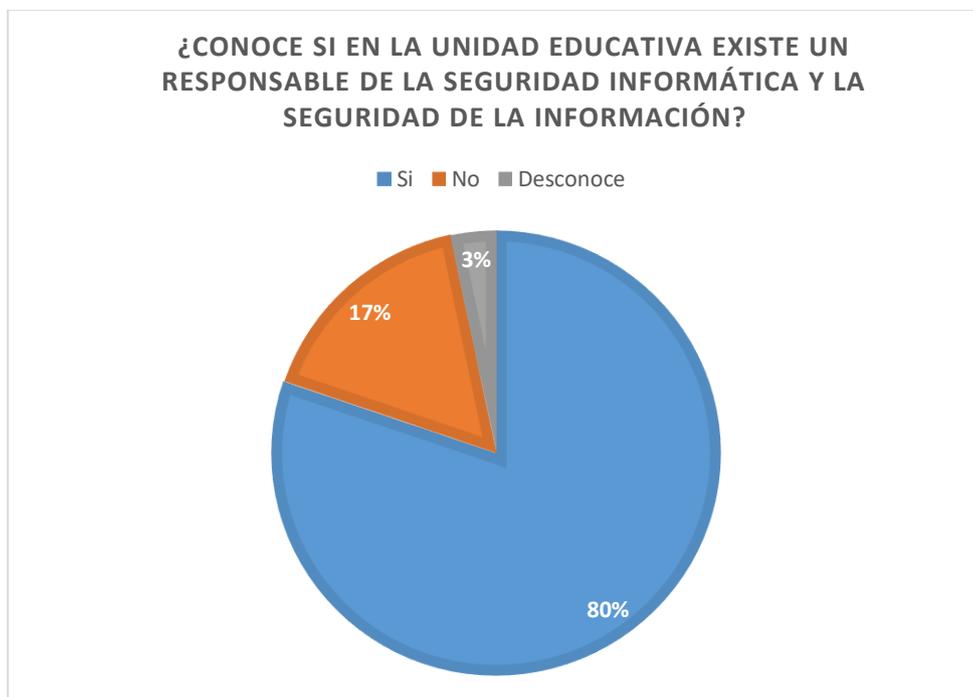


GRAFICO 2. RESPONSABLE DE LA SEGURIDAD INFORMÁTICA
FUENTE: ELABORACIÓN PROPIA

Análisis e Interpretación

El 80% de los docentes conoce que existe alguien encargado de la seguridad informática y seguridad de la información, mientras que el 17% no sabe si en su institución educativa existe alguien encargado de la seguridad informática, y el 3% desconoce si en su institución educativa hay alguien encargado de la seguridad informática y de la información.

Es bueno que la mayoría de los docentes conozca que exista alguien encargado de la seguridad informática y de la información, para poder sugerir que se tome más enserio el saber que están viendo los alumnos en las horas de consultar en una computadora.

3.- ¿Qué departamento considera que debe ser responsable de la seguridad informática y la información?

Detalle	Frecuencia	Porcentaje
Sistemas	85	93%
Administrativos	6	7%
Todas las áreas	0	0%
Otras	0	0%

TABLA 7. DETALLE DE LA PREGUNTA N°3
FUENTE: ELABORACIÓN PROPIA

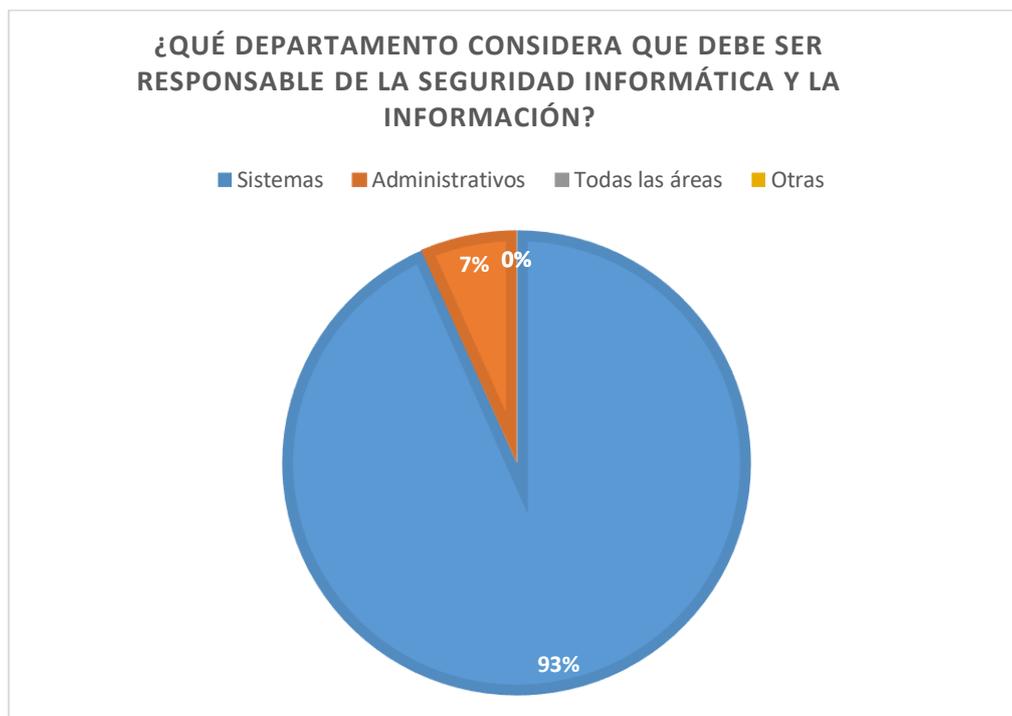


GRAFICO 3. DEPARTAMENTO RESPONSABLE DE LA SEGURIDAD INFORMÁTICA
FUENTE: ELABORACIÓN PROPIA

Análisis e Interpretación

De los profesores encuestados el 93% considera que la responsabilidad de la seguridad informática y de la información de estar sobre el departamento de sistemas, el otro 7% considera que la responsabilidad debe de estar en el departamento de administración.

En conclusión se puede decir que los docentes si conocen sobre quien o quienes debe de estar la responsabilidad de la seguridad informática y de la información.

4.- ¿Cree usted que el internet es lento por demasiados usuarios conectados?

Detalle	Frecuencia	Porcentaje
Si	72	79%
No	19	21%

TABLA 8. DETALLE DE LA PREGUNTA N°4
FUENTE: ELABORACIÓN PROPIA

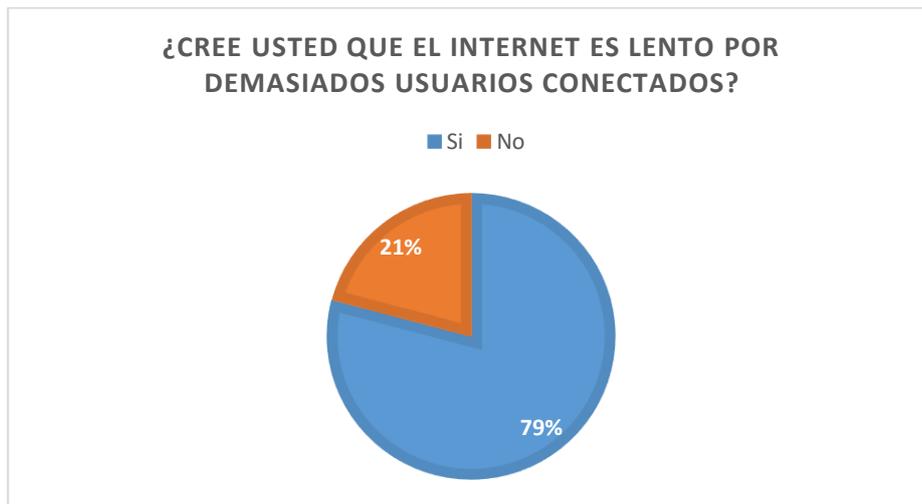


GRAFICO 4. CONSIDERA USTED QUE EL INTERNET ES LENTO
FUENTE: ELABORACIÓN PROPIA

Análisis e Interpretación

De los profesores encuestados y además hacen uso del internet de las unidades educativas el 79% cree que el internet es lento por la demanda de los usuarios conectados, y sobre todo que hacen mal uso del internet, el 21% creen que el internet es lento por otros motivos como el proveedor del mismo.

Uno de los motivos principales por lo que el internet es lento es debido al mal uso del mismo, ya que algunos alumnos no lo usan para sus investigaciones sino más bien para el ocio informático.

5.- ¿Usted ha tenido problemas al conectarse a las redes de datos?

Detalle	Frecuencia	Porcentaje
Si	67	74%
No	24	26%

TABLA 9. DETALLE DE LA PREGUNTA N°5
FUENTE: ELABORACIÓN PROPIA

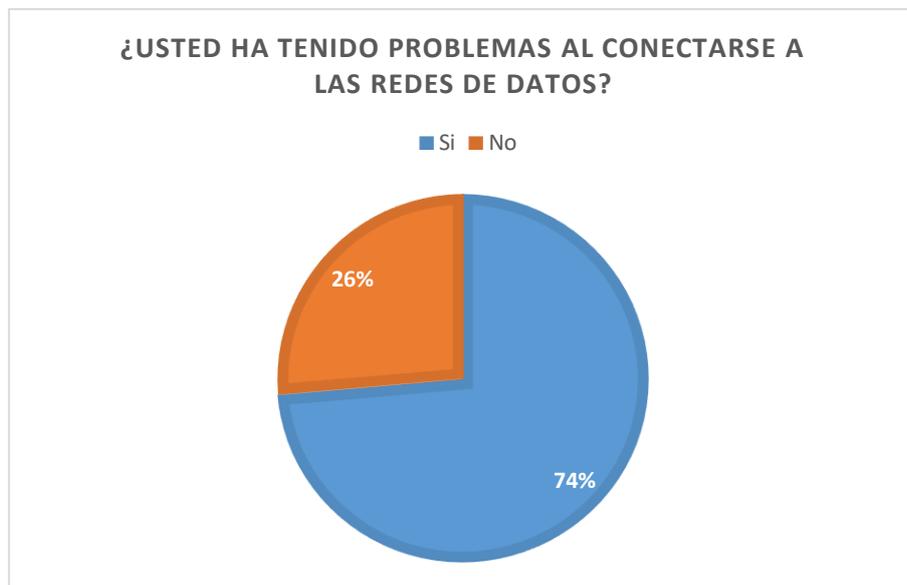


GRAFICO 5. PROBLEMAS AL CONECTARSE A LA RED DE DATOS
FUENTE: ELABORACIÓN PROPIA

Análisis e Interpretación

El 74% de los docentes encuestados ha tenido algún problema al momento de conectarse a la red de la institución educativa, mientras tanto el 26% no ha tenido ningún inconveniente.

Teniendo en cuenta que el 74% de los docentes ha tenido algún problema la conectarse al internet y al realizar el análisis de tráfico se podrá argumentar que esto se debe al mal uso del internet que le dan ciertos alumnos al momento de navegar en internet.

6.- ¿Para que usted utiliza las redes de datos?

Detalle	Frecuencia	Porcentaje
Trabajos investigativos	77	85%
Redes Sociales	0	0%
YouTube	11	12%
Entre otros	3	3%

TABLA 10. DETALLE DE LA PREGUNTA N°6
FUENTE: ELABORACIÓN PROPIA



GRAFICO 6. USTED UTILIZA LA REDES DE DATOS
FUENTE: ELABORACIÓN PROPIA

Análisis e Interpretación

El 85% de los docentes encuestados usan el internet para trabajos investigativos, el 12% para ver videos en YouTube, el 3% para otras tareas a realizar.

Los docentes hacen un buen uso del internet, mientras que los alumnos no lo hacen. Por este motivo se realizara el análisis de tráfico.

7.- ¿Conoce usted que es un sistema de control de tráfico en la redes de datos?

Detalle	Frecuencia	Porcentaje
Si	43	38%
No	48	62%

TABLA 11. DETALLE DE LA PREGUNTA N°7
FUENTE: ELABORACIÓN PROPIA

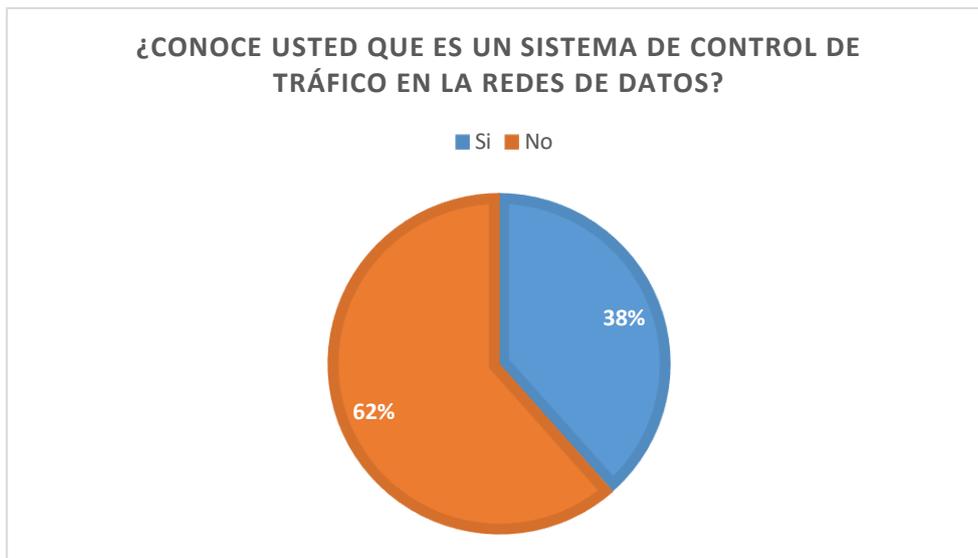


GRAFICO 7. CONOCE USTED ALGUN SISTEMA DE CONTROL DE TRÁFICO
FUENTE: ELABORACIÓN PROPIA

Análisis e Interpretación

El 38% de los docentes encuestados conoce lo que es un análisis de tráfico, caso contrario con el 62% de los docentes los cuales desconocen que es un análisis de tráfico. Aunque el porcentaje de los docentes que no conocen lo que es un análisis tráfico es bajo, no afecta en si se realizara el análisis de tráfico en las unidades educativas ya que las personas que no saben lo que es se les pueden explicar en qué consiste el análisis de tráfico.

8.- ¿Cree que es necesario aplicar algún control de seguridad informática para evitar el mal uso del internet en los alumnos?

Detalle	Frecuencia	Porcentaje
Si	75	90%
No	16	7%
Tal vez	0	3%

TABLA 12. DETALLE DE LA PREGUNTA N°8
FUENTE: ELABORACIÓN PROPIA



GRAFICO 8. NECESIDAD DEL ALGUN CONTROL DE TRÁFICO
FUENTE: ELABORACIÓN PROPIA

Análisis e Interpretación

El 90% de los docentes encuestados están de acuerdo en que se realice un análisis de tráfico en las unidades educativas, caso contrario con el 7% no están de acuerdo en realizar el análisis de tráfico, mientras el 3% piensa que tal vez deba realizarse.

Con el 90% de aceptación se procederá a realizar el análisis de tráfico en las unidades educativas pertenecientes al Distrito 12D01.

9.- ¿Qué software utiliza la unidad educativa para controlar software malicioso?

Detalle	Frecuencia	Porcentaje
Antivirus	25	21%
Anti-spam	5	4%
Antispyware	5	4%
Cortafuegos	80	69%
Otros	2	2%
Ninguno	0	0%

TABLA 13. DETALLE DE LA PREGUNTA N°9
FUENTE: ELABORACIÓN PROPIA

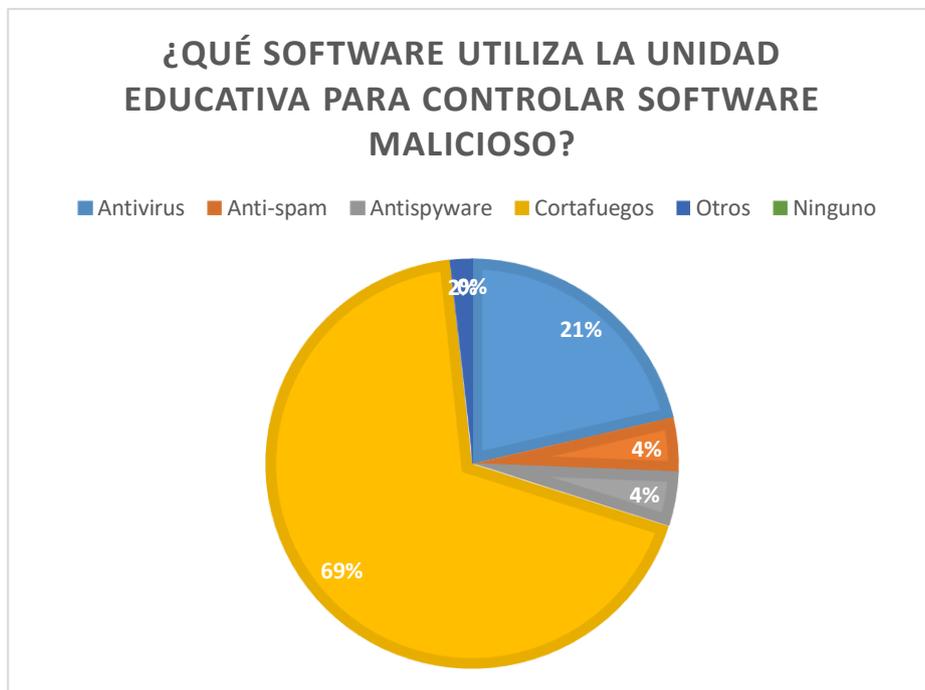


GRAFICO 9. SOFTWARE QUE UTILIZAN LAS UNIDADES EDUCATIVAS
FUENTE: ELABORACIÓN PROPIA

Análisis e Interpretación

El 21% de los docentes encuestados respondieron que las unidades educativas usan antivirus, el 4% anti-spam, el 4%, el 69% cortafuegos, y el 2% otras herramientas de seguridad.

10.- ¿Qué tipo de herramientas de seguridad tiene implementada la unidad educativa?

Detalle	Frecuencia	Porcentaje
Software	80	63%
Hardware	5	4%
Otras	7	5%
No posee	35	28%

TABLA 14. DETALLE DE LA PREGUNTA N°10
FUENTE: ELABORACIÓN PROPIA

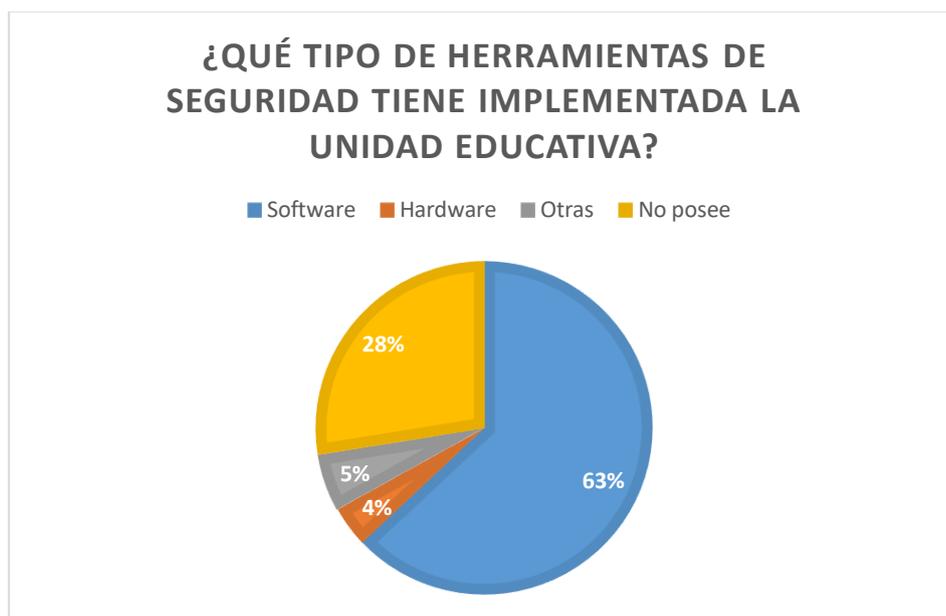


GRAFICO 10. HERRAMIENTAS DE SEGURIDAD IMPLEMENTADAS EN LA UNIDAD EDUCATIVA
FUENTE: ELABORACIÓN PROPIA

Análisis e Interpretación

El 63% de los docentes encuestados respondieron que las unidades educativas cuentan con software que en parte ayudan a proteger ciertos recursos de las mismas, otras cuentan con el 4% con hardware, y con el 5% otros; y 28% de ellas no poseen.

- Entrevistas

- Entrevista N°1

Nombre y Apellidos del entrevistado:	Lcda. Luisa Cárdenas
Cargo:	Rectora
Fecha de la entrevista:	05/03/2018
Lugar:	Unidad Educativa Francisco Huerta Rendón
<p>P: ¿Usted sabe si se cuenta con algún centro de soporte técnico sobre control de tráfico de las redes de datos?</p> <p>R: Primeramente Buenos días, la verdad es que en la Unidad Educativa no se cuenta con algún software o hardware que controle el tráfico de la red de datos.</p>	
<p>P: ¿Estaría usted acuerdo que exista un análisis de control de tráfico de las redes de datos para mejorar la conectividad?</p> <p>R: Sería bueno que se regule por lo menos cada tres meses el tráfico que circula por la red de datos de la Unidad Educativa.</p>	
<p>P: ¿Cree que internet es seguro? ¿Por qué?</p> <p>R: Depende del uso que se le dé, aunque en la actualidad existen bastantes medidas de seguridad para controlar el contenido al que acceden los jóvenes, de la misma manera existen formas para burlar estas medidas de seguridad.</p>	
<p>P: ¿Cree usted que el análisis de control de tráfico de las redes de datos ayude a mejorar el servicio que se presta?</p>	

R: Si, porque se tendría conocimiento a que están accediendo nuestros estudiantes y así mismo se podría implementar protocolos de seguridad para regular este problema.

P: **¿Cómo está su institución educativa con relación a estos asuntos de situaciones de violencia escolar, de bullying, de sexting y de grooming?**

R: Actualmente no conozco algún caso, pero he oído que si se da pero así mismo también he sido testigo de campañas en contra del bullying.

P: **¿Cuáles son los procedimientos y las estrategias definidas por la institución educativa para garantizar el deber de cuidado de todos sus estudiantes?**

R: Existen reglas que deben acatar al momento de ingresar algún laboratorio de la institución, de llegar a incumplir alguna se sanciona al estudiante.

**TABLA 15. ENTREVISTA REALIZADA EN LA UNIDAD EDUCATIVA FRANCISCO HUERTA RENDÓN
FUENTE: ELABORACIÓN PROPIA**

○ Entrevista N°2

Nombre y Apellidos del entrevistado:	Lcda. Janeth Silva
Cargo:	Rectora
Fecha de la entrevista:	06/03/2018
Lugar:	Unidad Educativa 10 de Agosto
<p>P: ¿Usted sabe si se cuenta con algún centro de soporte técnico sobre control de tráfico de las redes de datos?</p> <p>R: En estos momentos no se cuenta con algún soporte técnico en la Unidad Educativa</p>	
<p>P: ¿Estaría usted acuerdo que exista un análisis de control de tráfico de las redes de datos para mejorar la conectividad?</p> <p>R: Si, estaría de acuerdo.</p>	
<p>P: ¿Cree que internet es seguro? ¿Por qué?</p> <p>R: No, Es deber de los Padre de Familia y de los Profesores estar pendientes de que están haciendo nuestros hijos, estudiantes en una computadora.</p>	
<p>P: ¿Cree usted que el análisis de control de tráfico de las redes de datos ayude a mejorar el servicio que se presta?</p> <p>R: Tal vez, si se llegase a saber el resultado para poder seguir las recomendaciones que se den en este informe.</p>	
<p>P: ¿Cómo está su institución educativa con relación a estos asuntos de situaciones de violencia escolar, de bullying, de sexting y de grooming?</p>	

R: Como profesor he escuchado estos términos y es alarmante saber que muchos de nuestros jóvenes caen en estas situaciones, pero desconozco si alguno de mis estudiantes está siendo parte de estos nuevos problemas.

P: ¿Cuáles son los procedimientos y las estrategias definidas por la institución educativa para garantizar el deber de cuidado de todos sus estudiantes?

R: Se debe seguir las reglas que se dan a conocer el primer día de clases para poder hacer uso de algún equipo informático.

**TABLA 16. ENTREVISTA REALIZADA EN LA UNIDAD EDUCATIVA 10 DE AGOSTO
FUENTE: ELABORACIÓN PROPIA**

○ **Entrevista N°3**

Nombre y Apellidos del entrevistado:	Lcda. Irene Espinoza
Cargo:	Rectora
Fecha de la entrevista:	07/03/2018
Lugar:	Unidad Educativa Juan Montalvo
<p>P: ¿Usted sabe si se cuenta con algún centro de soporte técnico sobre control de tráfico de las redes de datos?</p> <p>R: Hasta el momento no se ha realizado nada parecido al control de tráfico de la red de datos de la Unidad Educativa.</p>	
<p>P: ¿Estaría usted acuerdo que exista un análisis de control de tráfico de las redes de datos para mejorar la conectividad?</p> <p>R: Por eso estaría de acuerdo en que se realice un control en el tráfico de la red de datos de la Unidad Educativa.</p>	
<p>P: ¿Cree que internet es seguro? ¿Por qué?</p> <p>R: Para mi parecer depende que uso se le dé, ya que si se lo uso para fines educativos es una herramienta muy buena, cosa contraria pasaría si se usa para fines como el ocio informático.</p>	
<p>P: ¿Cree usted que el análisis de control de tráfico de las redes de datos ayude a mejorar el servicio que se presta?</p> <p>R: La verdad me gustaría que se realice esto, pero no estoy seguro que se mejore la</p>	

situación actual de la red de datos de la Unidad Educativa.
<p>P: ¿Cómo está su institución educativa con relación a estos asuntos de situaciones de violencia escolar, de bullying, de sexting y de grooming?</p> <p>R: Se ha realizado campañas en contra del bullying, y además que tengan cuidado a la hora de conocer a alguien por medio de las redes sociales.</p>
<p>P: ¿Cuáles son los procedimientos y las estrategias definidas por la institución educativa para garantizar el deber de cuidado de todos sus estudiantes?</p> <p>R: Se tiene parámetros establecidos a la hora de hacer uso de una máquina.</p>

**TABLA 17. ENTREVISTA REALIZADA EN LA UNIDAD EDUCATIVA JUAN MONTALVO
FUENTE: ELABORACIÓN PROPIA**

○ Entrevista N°4

Nombre y Apellidos del entrevistado:	Ing. Silvia Goyes
Cargo:	Rectora
Fecha de la entrevista:	08/03/2018
Lugar:	Unidad Educativa Adolfo María Astudillo
<p>P: ¿Usted sabe si se cuenta con algún centro de soporte técnico sobre control de tráfico de las redes de datos?</p> <p>R: Se ha realizado soporte técnico pero a las maquinas, nunca a la red de datos.</p>	
<p>P: ¿Estaría usted acuerdo que exista un análisis de control de tráfico de las redes de datos para mejor la conectividad?</p> <p>R: Seria bueno para poder conocer el estado actual de la red de datos de la Unidad Educativa.</p>	
<p>P: ¿Cree que internet es seguro? ¿Por qué?</p> <p>R: En parte si, y en parte no. Si porque nos ayuda en nuestros deberes cotidianos. No porque cuando se usa de una manera inadecuada es perjudicial para la sociedad.</p>	
<p>P: ¿Cree usted que el análisis de control de tráfico de las redes de datos ayude a mejorar el servicio que se presta?</p> <p>R: Quizás dependiendo del resultado obtenido.</p>	
<p>P: ¿Cómo está su institución educativa con relación a estos asuntos de situaciones de violencia escolar, de bullying, de sexting y de grooming?</p>	

R: Se tiene conocimiento de algunos casos que se han dado en el Ecuador, por esta razón se hace hincapié en los estudiantes sobre estos casos.

P: **¿Cuáles son los procedimientos y las estrategias definidas por la institución educativa para garantizar el deber de cuidado de todos sus estudiantes?**

R: Existen medidas de seguridad para poder proteger de alguna manera los equipos de cómputo.

**TABLA 18. ENTREVISTA REALIZADA EN LA UNIDAD EDUCATIVA ADOLFO MARÍA ASTUDILLO
FUENTE: ELABORACIÓN PROPIA**

○ Entrevista N°5

Nombre y Apellidos del entrevistado:	Ing. Patricia Gómez
Cargo:	Rectora
Fecha de la entrevista:	09/03/2018
Lugar:	Unidad Educativa 29 de Agosto
<p>P: ¿Usted sabe si se cuenta con algún centro de soporte técnico sobre control de tráfico de las redes de datos?</p> <p>R: Desde que se terminó el contrato con el MINTEL (Ministerio de Telecomunicaciones y de la Sociedad de la Información), se desconoce el estado actual de la red de datos.</p> <p>P: ¿Estaría usted acuerdo que exista un análisis de control de tráfico de las redes de datos para mejorar la conectividad?</p> <p>R: Por este motivo sería beneficioso este análisis.</p>	
<p>P: ¿Cree que internet es seguro? ¿Por qué?</p> <p>R: En la actualidad con la aparición de las redes sociales ha dejado de tener un buen uso por parte de la sociedad y han decaído sus múltiples beneficios cuando lo usamos de una manera inteligente.</p>	
<p>P: ¿Cree usted que el análisis de control de tráfico de las redes de datos ayude a mejorar el servicio que se presta?</p> <p>R: Al conocer el estado actual de la red de datos se podrá mejorar para brindar un mejor servicio a los estudiantes.</p>	
<p>P: ¿Cómo está su institución educativa con relación a estos asuntos de situaciones</p>	

de violencia escolar, de bullying, de sexting y de grooming?

R: Se realizan campañas en contra del bullying, las otras dos no las conocía por ese nombre pero es alarmante saber que existe gente capaz de engañar a nuestros jóvenes para usarlos de una manera cruel.

P: ¿Cuáles son los procedimientos y las estrategias definidas por la institución educativa para garantizar el deber de cuidado de todos sus estudiantes?

R: Se da a conocer a los estudiantes sobre cómo deben usar los recursos informáticos que posee la institución.

**TABLA 19. ENTREVISTA REALIZADA EN LA UNIDAD EDUCATIVA 29 DE AGOSTO
FUENTE: ELABORACIÓN PROPIA**

3.2 Conclusiones específicas y generales

3.2.1 General.

- En las Unidades Educativas pertenecientes al Distrito 12D01 se detectaron anomalías en cuanto a la seguridad informática y la seguridad de la información como un retardo a la hora de hacer uso del internet, problemas de conexión y falta de personal capacitado para el control y administración de la red de datos, y un mal diseño de la red de datos todo esto aumenta la probabilidad de colisiones en la red.

3.2.2 Específicas.

- En algunas de las instituciones encuestadas se detectó la falta de personal capacitado para el control y administración de la red, pues se desconocía la topología de la red con la que se contaba. Esto se convierte en una debilidad importante si se desea mantener un óptimo desempeño, ya que si surge algún problema en la red, será difícil tomar acciones para impedir que se expanda por toda la red.
- Para las arquitecturas de redes existen diferentes formas de resolver asuntos de mucha importancia, una de ellas es la transferencia de datos de manera rápida y eficaz entre todos los dispositivos que se encuentren conectadas a la red. Muchas de estas herramientas se encuentran disponibles en el internet y de uso libre, además existen técnicas muy útiles que nos permitirán la búsqueda y solución de los problemas que se nos presenten en la red de datos.

- Teniendo en cuenta que se debe tener claras las herramientas con las que se puede contar, se vuelve de vital importancia un análisis y monitoreo de la red para esto se deben tener claros los conceptos básicos a la hora de realizar el análisis de tráfico de la red de datos. Con este conocimiento se puede controlar los paquetes de información dañinos que circulan por la red sin control y así poder tener un mejor provecho en la utilización del ancho de banda.

3.3 Recomendaciones específicas y generales

3.3.1 General.

- Debido a las anomalías expuestas anteriormente las colisiones son una parte inherente debido a su naturaleza contenciosa además esto puede aumentar la utilización del ancho de banda. La forma más recomendable para evitar estas colisiones y lograr una funcionalidad eficiente y eficaz es por medio de la segmentación, esto solo implicara determinar varios segmentos separados pero interconectados, además de un mejor manejo del ancho de banda.

3.3.2 Específicas.

- Considerando el desconocimiento por parte de algunos docentes en cuanto al entorno de la red de datos, se puede establecer grupos de trabajo que tengan dominios de colisión comunes, de acuerdo a la unidad educativa, de esta manera se podrá mejorar el tráfico de red específico para no afectar a ningún grupo de trabajo.
- Se puede recomendar una técnica conocida como Segmentación ya que su concepto es fácil de comprender, pero no es siempre fácil de implementar. La subdivisión de redes requiere un análisis apropiado de la red antes de ser implementada. Si no es implementada de manera correcta, se puede incrementar las cargas de tráfico en la red de datos.

- La opción que se menciona de Segmentar la red es una solución bastante viable, ya que permite mediante un análisis previo, determinar que equipos se puede situar en los dominios de colisión independientes y de esta forma disminuir significativamente el número de colisiones, sin la necesidad de adquirir nuevos equipos para mejorar la red de datos.

CAPÍTULO IV.- PROPUESTA DE APLICACIÓN.

4.1 Propuesta de aplicación de resultados.

4.1.1 Alternativa obtenida.

“Segmentación de la red de datos de las Unidades Educativas del Distrito 12D01 para disminuir el dominio de colisión en los dispositivos de la infraestructura de red”

4.1.2 Alcance de la alternativa.

Dentro del alcance del proyecto se encuentra el análisis de tráfico que se realizara en las Unidades Educativas pertenecientes al Distrito 12D01, mediante este análisis se podrá diagnosticar la red de datos, para poder comprobar los problemas expuestos mediante las encuestas realizadas a los docentes de las Unidades Educativas. Encuestas realizadas en cinco Establecimientos Educativos ubicados en el Distrito 12D01.

DATOS GENERALES DE LAS CINCO UNIDADES EDUCATIVAS DONDE SE REALIZARÁ EL ANÁLISIS DE TRÁFICO.

- **Unidad Educativa N°1**

Nombre de la institución:	Unidad Educativa 29 de Agosto
Código AMIE:	12H00217
Dirección de ubicación:	Cabecera Parroquial de Febres Cordero al margen izquierdo
Tipo de educación:	Educación Regular
Provincia:	Los Ríos
Cantón:	Babahoyo
Parroquia:	Febres Cordero (Las Juntas)
Nivel educativo que ofrece:	EGB y Bachillerato
Sostenimiento y recursos:	Fiscal
Régimen escolar:	Costa
Educación:	Hispana
Modalidad:	Presencial
Jornada:	Matutina y Vespertina
Tenencia del inmueble:	Propio
La forma de acceso:	Terrestre

TABLA 20. INFORMACIÓN DE LA UNIDAD EDUCATIVA 29 DE AGOSTO
FUENTE: ELABORACIÓN PROPIA

- **Unidad Educativa N°2**

Nombre de la institución:	UNIDAD EDUCATIVA ADOLFO MARÍA ASTUDILLO
Código AMIE:	12H00116
Dirección de ubicación:	ROLDÓS AVENIDA VEINTICINCO DE JUNIO BY PASS
Tipo de educación:	Educación Regular
Provincia:	LOS RIOS
Cantón:	BABAHOYO
Parroquia:	DR. CAMILO PONCE
Nivel educativo que ofrece:	Inicial, Educación Básica y Bachillerato
Sostenimiento y recursos:	Fiscal
Régimen escolar:	Costa
Educación:	Hispana
Modalidad:	Presencial
Jornada:	Matutina y Vespertina
Tenencia del inmueble:	Propio
La forma de acceso:	Terrestre

TABLA 21. INFORMACIÓN DE LA UNIDAD EDUCATIVA ADOLFO MARÍA ASTUDILLO
FUENTE: ELABORACIÓN PROPIA

- **Unidad Educativa N°3**

Nombre de la institución:	UNIDAD EDUCATIVA JUAN MONTALVO
Código AMIE:	12H00409
Tipo de educación:	Educación Regular
Provincia:	LOS RIOS
Cantón:	BABA
Parroquia:	BABA
Nivel educativo que ofrece:	Inicial, Educación Básica y Bachillerato
Sostenimiento y recursos:	Fiscal
Régimen escolar:	Costa
Educación:	Hispana
Modalidad:	Presencial
Jornada:	Matutina y Vespertina
Tenencia del inmueble:	Propio
La forma de acceso:	Terrestre

**TABLA 22. INFORMACIÓN DE LA UNIDAD EDUCATIVA JUAN MONTALVO
FUENTE: ELABORACIÓN PROPIA**

- **Unidad Educativa N°4**

Nombre de la institución:	UNIDAD EDUCATIVA 10 DE AGOSTO
Código AMIE:	12H00597
Dirección de ubicación:	10 DE AGOSTO JUAN XXIII
Tipo de educación:	Educación Regular
Provincia:	LOS RIOS
Cantón:	MONTALVO
Parroquia:	MONTALVO
Nivel educativo que ofrece:	EGB y Bachillerato
Sostenimiento y recursos:	Fiscal
Régimen escolar:	Costa
Educación:	Hispana
Modalidad:	Presencial
Jornada:	Matutina
Tenencia del inmueble:	Propio
La forma de acceso:	Terrestre

TABLA 23. INFORMACIÓN DE LA UNIDAD EDUCATIVA 10 DE AGOSTO
FUENTE: ELABORACIÓN PROPIA

- **Unidad Educativa N°5**

Nombre de la institución:	UNIDAD EDUCATIVA FRANCISCO HUERTA RENDON
Código AMIE:	12H00025
Dirección de ubicación:	AVENIDA CLEMENTE BAQUERIZO CALLE JUAN E VERDEZOTO
Tipo de educación:	Educación Regular
Provincia:	LOS RIOS
Cantón:	BABAHOYO
Parroquia:	CLEMENTE BAQUERIZO
Nivel educativo que ofrece:	Inicial, Educación Básica y Bachillerato
Sostenimiento y recursos:	Fiscal
Régimen escolar:	Costa
Educación:	Hispana
Modalidad:	Presencial
Jornada:	Matutina y Vespertina
Tenencia del inmueble:	Propio
La forma de acceso:	Terrestre

TABLA 24. INFORMACIÓN DE LA UNIDAD EDUCATIVA FRANCISCO HUERTA RENDÓN
FUENTE: ELABORACIÓN PROPIA

4.1.3 Aspectos básicos de la alternativa.

4.1.3.1 Antecedentes

En las Unidades Educativas del Distrito 12D01 no se encontró ningún antecedente sobre la propuesta, pero a nivel nacional se encontraron las siguientes soluciones para la problemática planteada, las cuales se detallan a continuación:

Título:	“ANÁLISIS DE LA RED DE COMUNICACIÓN DEL EDIFICIO DEL DISTRITO 7 DEL MINISTERIO DE EDUCACIÓN USANDO HERRAMIENTA DE SIMULACIÓN OPNET”.
Problema:	En el Edificio del Distrito 7 del Ministerio de Educación no cuenta con una buena comunicación entre sus áreas, las mediciones o pruebas reales en la red dentro del Edificio del Ministerio de Educación podría provocar la interrupción en las actividades que estén realizando, afectando al plan Educativo. Muchos de los usuarios de la red tienen problemas al poder enviar o recibir información dentro del distrito y hacia fuera de él, dado que no se puede realizar la verificación y análisis de la red físicamente por las interrupciones que se provocarían al parar las actividades de los equipos informáticos, así también los costos por la contratación de personal para el análisis serían muy costosos así también como la compra de equipos especiales para estos tipos de análisis. (Campoverde Jara, 2015)
Ubicación:	Machala
Solución:	Proponer un Rediseño para el Distrito 7 del Ministerio de Educación de la ciudad de Machala usando programa de simulación y modelado de redes de telecomunicaciones (OPNET).

TABLA 25. ANTECEDENTE N°1
FUENTE: ELABORACIÓN PROPIA

Título:	ESTUDIO DE TÉCNICAS Y HERRAMIENTAS PARA LA PREVENCIÓN Y DETECCIÓN DE INTRUSIONES A NIVEL DE APLICACIÓN EN LA RED DE DATOS DE LA UNACH
Problema:	A pesar de los mecanismos de seguridad implementados, se han registrado aunque no de manera concurrente, incidentes que atentan a la disponibilidad del sistema de nombres de dominio (DNS), esto han provocado: interrupción de las actividades normales de manera parcial o total del servidor DNS y lentitud de navegación hacia internet. (Yuquilema Heredia, 2016)
Ubicación:	Riobamba
Solución:	Implementación de un nIDPS basado en técnica de uso indebido para la red de servidores de la UNACH.

**TABLA 26. ANTECEDENTE N°2
FUENTE: ELABORACIÓN PROPIA**

Título:	SISTEMA DE GESTIÓN DE REDES PARA EL CONTROL Y DISTRIBUCIÓN DEL TRÁFICO EN LA RED LAN DE LA UNIDAD EDUCATIVA BAÑOS DEL CANTÓN BAÑOS.
Problema:	Las redes se saturan por la cantidad de terminales transmitiendo información, y la pérdida de datos es más probable si no se realiza un control de cada una de las áreas de trabajo, ya que de igual forma existen usuarios con privilegios tales como los departamentos administrativos que necesitan una conexión permanente a la red. Todas estas normas serían las políticas de acceso que se aplicarán sobre el sistema. (Sánchez Izurieta, 2014)
Ubicación:	Baños
Solución:	Sistema de Gestión de redes para el control y distribución del tráfico en la red LAN de la Unidad Educativa Baños del cantón Baños

**TABLA 27. ANTECEDENTE N°3
FUENTE: ELABORACIÓN PROPIA**

4.1.3.2 Justificación

Para que una red de datos funcione de la manera correcta y eficiente es necesario elaborar un análisis del tráfico que nos permitirá obtener la información que transita por la red para poder realizar el diagnóstico de la misma.

Para poder realizar el análisis de toda la información que utilizara una herramienta de software libre como lo es Wireshark, mediante este análisis se pretende optimizar el ancho de banda para la transmisión de datos y así poder generar una mejora en el uso de los servicios de red.

Si el diagnóstico de la red comprueba todos los problemas ya expuestos por los docentes encuestados, se propone la segmentación de la red de datos de cada establecimiento educativo; porque mediante esta técnica se disminuirá las colisiones provocadas por el retardo a una petición enviada por algún equipo informático que conforman la infraestructura de la red y se mejorará la comunicación institucional ya que se reducirá las probabilidades de caídas en la red cuando varios usuarios hagan uso de la red al mismo tiempo, los servicios de red como lo son la navegación web, descargas de archivos, transferencia de archivos, envío de correos, etc., serán óptimos y eficientes.

Con la elaboración de esta propuesta se busca generar un impacto positivo en el rendimiento de la red de datos en cada Unidad Educativa perteneciente al Distrito 12D01 a fin de que los servicios implementados en la misma sean rápidos, beneficiando a los alumnos, docentes y administrativos.

4.2 Objetivos.

4.2.1 General.

Aportar en la disminución del dominio de colisión en los dispositivos de la infraestructura de la red de datos mediante la técnica de segmentación de redes.

4.2.2 Específicos.

- Identificar grandes flujos de broadcast en la red de datos perteneciente a la Unidad Educativa.
- Rediseñar la red de datos empleando criterios de segmentación en las Unidades Educativas del Distrito 12D01.
- Determinar un mayor ancho de banda por usuario en la red de datos.

4.3 Estructura general de la propuesta.

4.3.1 Título.

“Segmentación de la red de datos de las Unidades Educativas del Distrito 12D01 para disminuir el dominio de colisión en los dispositivos de la infraestructura de red”

4.3.2 Componentes.

N°	Descripción	Inicio	Fin	Responsable
	Análisis de la red de datos de las Unidades Educativas del Distrito 12D01			
1	<ul style="list-style-type: none"> Determinar el tipo de red 	02/05/2018	16/05/2018	Cesar Angulo
2	<ul style="list-style-type: none"> Usuarios de la red 	02/05/2018	16/05/2018	Cesar Angulo
3	<ul style="list-style-type: none"> Diagrama físico de la red 	02/05/2018	16/05/2018	Cesar Angulo
	Análisis de tráfico de la red de datos en las Unidades Educativas del Distrito 12D01			Encargados de la Sala de Cómputo
4	<ul style="list-style-type: none"> Captura de las información de la red de datos usando la herramienta Wireshark 	17/05/2018	31/05/2018	Lcdo. Jonny Hidalgo Lcdo. José Torres Ing. Johana Sánchez Ing. María Hurtado Tnlgo. Limber Lucas
5	<ul style="list-style-type: none"> Análisis del protocolo ARP (ARP spoof) 	04/06/2018	08/06/2018	Cesar Angulo
6	<ul style="list-style-type: none"> Análisis del protocolo TCP (Port Flooding) 	11/06/2018	15/06/2018	Cesar Angulo
7	<ul style="list-style-type: none"> Análisis de Attacks DoS (Ataques de Denegación de Servicios) 	18/06/2018	22/06/2018	Cesar Angulo
8	<ul style="list-style-type: none"> Análisis de Malware (protocolo HTTP) 	25/06/2018	29/06/2018	Cesar Angulo

9	<ul style="list-style-type: none"> Ancho de banda consumido en el periodo de la muestra 	02/07/2018	06/07/2018	Cesar Angulo
10	<ul style="list-style-type: none"> Informe del análisis de tráfico en la red de datos del Distrito 12D01 	09/07/2018	10/07/2018	Cesar Angulo
	Segmentación de la red de datos en las Unidades Educativas del Distrito 12D01			
11	<ul style="list-style-type: none"> Dividir la red en Segmentos 	11/07/2018	18/07/2018	Cesar Angulo
12	<ul style="list-style-type: none"> Interconectar varios segmentos utilizando bridges o routers 	19/07/2018	26/07/2018	Cesar Angulo
13	<ul style="list-style-type: none"> Establecer Subredes en las Unidades Educativas 	27/07/2018	03/08/2018	Cesar Angulo
14	Entrega del informe sobre las actividades realizadas.	06/08/2018	07/08/2018	Cesar Angulo

4.4 Resultados esperados de la alternativa.

Mediante esta propuesta la cual es la segmentación de red, se podrá mejorar en un 75% la comunicación entre los equipos informáticos, y será más dinámica y segura, para así tener un balance entre las descargas de los paquetes de datos y una administración más efectiva.

Con la implementación del estudio de tráfico de datos en la red para el cual solo se necesita de 2 horas por sala de computo, se podrá determinar que aunque se tome un periodo de 4 a 8 horas para hacer la muestra, el comportamiento que se tendrá de la red va hacer el mismo que se tomara durante las primeras dos horas por lo que en las primeras dos horas se evidenciaran los posibles problemas que pueda tener toda la red.

Además de todos estos beneficios mencionados en el anterior párrafo, también mediante esta técnica se podrá disminuir las colisiones en la red de datos, mejorar la comunicación cliente/servidor, optimizar el ancho de banda para así tener una red de datos óptima y eficiente.

También se puede controlar los ataques de malware, implementando perímetros y medidas de seguridad pero esto no garantiza una seguridad absoluta de la información, sin embargo aplicando políticas de seguridad disminuirá las superficies de ataques, y el impacto del malware dentro de la red de datos del Distrito 12D01.

Instalando bloqueadores de páginas web emergentes (*pop-ups*), como *Website Bloker* o *Block Site* que son herramientas que ayudan a controlar el ingreso a páginas que no deben estar disponibles en las Unidades Educativas.

BIBLIOGRAFÍA

- Álvarez Delgado, D., Jorquera Cáceres, C., Sepúlveda Jorquera, G., & Zamora Esquivel, C. (28 de julio de 2014). <http://profesores.elo.utfsm.cl>. Obtenido de <http://profesores.elo.utfsm.cl/~agv/elo322/1s14/projects/reports/G20/Redes%20Privadas%20Virtuales%20%28VPN%29.pdf>
- Carceller Cheza, R., Campos Saborido, C., & García Marcos, C. (2013). *Servicios en red*. Macmillan Iberia, S.A. Recuperado el 30 de Enero de 2018
- Carceller Cheza, R., Campos Saborido, C., & García Marcos, C. J. (2013). *Servicios en red*. Macmillan Iberia, S.A. Recuperado el 30 de Enero de 2018
- Carceller Cheza, R., Campos Saborido, C., & García Marcos, C. J. (2013). *Servicios en red*. Macmillan Iberia, S.A. Recuperado el 30 de Enero de 2018
- Carceller Cheza, R., Campos Saborido, C., & García Marcos, C. J. (2013). *Servicios en red*. Macmillan Iberia, S.A.
- Castaño Ribes, R. J., & López Fernández, J. (2013). *Redes locales*. Macmillan Iberia, S.A. Recuperado el 23 de Enero de 2018
- CCM. (19 de Octubre de 2017). <http://es.ccm.net>. Recuperado el 20 de Enero de 2018, de <http://es.ccm.net/contents/274-el-protocolo-ip>
- Chacón, A., Vera, D., & Cabrera, A. (2015). Incidencia del uso del internet en los adolescentes de las instituciones de educación media. *Revista Ciencia UNEMI*, 57-66.
- Colasoft. (s.f.). *Colasoft*. Obtenido de <http://www.colasoft.com/capsa-free/>
- Colasoft. (s.f.). *Colasoft*. Obtenido de <http://www.colasoft.com/capsa-free/>
- Costas Santos, J. (2014). *Seguridad Informática*. Madrid, España: RA-MA, S.A. Recuperado el 19 de Enero de 2018
- Cuadra Sánchez, A. (26 de Junio de 2017). *Universidad Autonoma Madrid*. Obtenido de <https://repositorio.uam.es/handle/10486/679946>
- De Luis Gargallo, E. (2018). *La seguridad para los menores en Internet*. Barcelona: UOC. Recuperado el 22 de Marzo de 2018

- Echeburúa, E. (2016). *Abuso de Internet*. Difusora Larousse - Ediciones Pirámide.
Recuperado el 02 de Febrero de 2018
- Escrivá Gascó, G., Romero Serrano, R., & Ramada, D. (2013). *Seguridad informática*.
Madrid: Macmillan Iberia, S.A.
- Gasteiz, V. (s.f.). *Educación a los menores en el uso sin riesgos de Internet*. Madrid:
Ayuntamiento de Vitoria-Gasteiz.
- Giant, N., & Bernárdez, P. (2016). *Ciberseguridad para la i-generación : usos y riesgos de las redes sociales y sus aplicaciones*. Madrid , Narcea, España: S.A de ediciones .
Recuperado el 15 de 01 de 2018
- Gómez Vieites, Á. (2014). *Gestión de incidentes de seguridad informática*. Madrid: RA-
MA Editorial. Recuperado el 22 de Marzo de 2018
- Guevara Soriano, A. (s.f.). <https://revista.seguridad.unam.mx>. Recuperado el 19 de Enero de 2018, de <https://revista.seguridad.unam.mx/numero-12/hacking-%C3%A9ticos-mitos-y-realidades>
- Internet Segura ForKids. (s.f.). *Instituto Nacional de Ciberseguridad de España*. Obtenido de <https://www.is4k.es/necesitas-saber/contenido-inapropiado>
- Jordán, V., Galperin, H., & Peres, W. (Febrero de 2013). *Repositorio Cepal*. Obtenido de http://repositorio.cepal.org/bitstream/handle/11362/35399/S2013070_es.pdf?sequence=1&isAllowed=y
- K, A. K., & Avila, I. J. (Septiembre de 2015). *Conocimiento Digital*. Recuperado el 24 de Enero de 2018, de <https://grupo4herramientasinformatica.blogspot.com/2015/09/analisis-critico-de-la-tecnologia-en-la.html>
- Panda mediacenter*. (23 de 06 de 2017). Recuperado el 15 de 01 de 2018, de <https://www.pandasecurity.com/spain/mediacenter/noticias/ciberseguridad-en-los-colegios/>
- Perafán Ruiz, J. J., & Caicedo Cuchimba, M. (10 de Octubre de 2014). *Repositorio UNAD*. Recuperado el 23 de Enero de 2018, de <http://repository.unad.edu.co/bitstream/10596/2655/3/76327474.pdf>

- Reyes, L. A. (4 de Noviembre de 2015). *Prezi*. Obtenido de <https://prezi.com/lnkez7clz6ei/herramienta-des-escaneo-de-puertos/>
- Roa Buendía, J. F. (2013). *Seguridad Informática*. McGraw-Hill España.
- Salazar Salazar, O. (2016). *Pontificia Universidad Católica del Ecuador*. Obtenido de <http://repositorio.puce.edu.ec/bitstream/handle/22000/13171/Caso%20Estudio%20EPM%20Portovial.pdf?sequence=1&isAllowed=y>
- Sánchez Ojeda, L. F. (5 de Septiembre de 2016). *Repositorio Pontificia Universidad Católica del Ecuador*. Recuperado el 24 de Enero de 2018, de <http://repositorio.puce.edu.ec/bitstream/handle/22000/11144/Informe%20Caso%20de%20Estudio%20Unidad%20de%20%20%20%20%20%20%20Titulaci%C3%B3n.pdf?sequence=1>: <http://repositorio.puce.edu.ec/>
- Santos, M. (2014). *Sistemas telemáticos*. RA-MA Editorial. Recuperado el 31 de Enero de 2018
- Solórzano Alcívar, J. G. (16 de diciembre de 2017). <http://repositorio.puce.edu.ec>. Obtenido de <http://repositorio.puce.edu.ec/handle/22000/14127?show=full>
- Techopedia. (s.f.). *Techopedia*. Recuperado el 26 de Enero de 2018, de <https://www.techopedia.com/definition/29917/network-traffic>
- Telecomunicaciones/TIC, F. M. (14 de Mayo de 2013). <https://www.itu.int>. Obtenido de <https://www.itu.int/en/wtpf-13/Documents/backgrounder-wtpf-13-broadband-es.pdf>
- Vásquez, J. (11 de Junio de 2013). *manualwireshark*. Obtenido de <http://manualwireshark.blogspot.com/>

ANEXOS

ENCUESTA A LAS UNIDADES EDUCATIVAS

1.- ¿Existen procedimientos de seguridad informática e instructivos establecidos en la unidad educativa?

- Si ()
- No()
- Desconoce()

2.- ¿Conoce si en la unidad educativa existe un responsable de la seguridad informática y la seguridad de la información?

- Si ()
- No()
- Desconoce()

3.- ¿Qué departamento considera que debe ser responsable de la seguridad informática y la información?

- Sistemas()
- Administrativos()
- Todas las áreas()
- Otras

4.- ¿Cree usted que el internet es lento por demasiados usuarios conectados?

- Si ()
- No ()

5.- ¿Usted ha tenido problemas al conectarse a las redes de datos?

- Si ()
- No ()

6.- ¿Para que usted utiliza las redes de datos?

- Trabajos investigativos.
- Redes sociales.
- YouTube.
- Entre otros.

7.- ¿Conoce usted que es un sistema de control de tráfico en la redes de datos?

- Si
- No

8.- ¿Cree que es necesario aplicar algún control de seguridad informática para evitar el mal uso del internet en los alumnos?

- Si ()
- No()
- Tal vez()

9.- ¿Qué software utiliza la unidad educativa para controlar software malicioso?

- Antivirus()
- Anti-spam()
- Antispyware()
- Cortafuegos()
- Otros()
- Ninguno()

10.- ¿Qué tipo de herramientas de seguridad tiene implementada la unidad educativa?

- Software()
- Hardware()
- Otras()
- No posee()

**ENTREVISTA DIRIGIDA A LOS DIRECTORES
DE LAS UNIDADES EDUCATIVAS**

- a. **¿Usted sabe si se cuenta con algún centro de soporte técnico sobre control de tráfico de las redes de datos?**

- b. **¿Estaría usted acuerdo que exista un análisis de control de tráfico de las redes de datos para mejorar la conectividad?**

- c. **¿Cree que internet es seguro? ¿Por qué?**

- d. **¿Cree usted que el análisis de control de tráfico de las redes de datos ayude a mejorar el servicio que se presta?**

- e. **¿Cómo está su institución educativa con relación a estos asuntos de situaciones de violencia escolar, de bullying, de sexting y de grooming?**

- f. **¿Cuáles son los procedimientos y las estrategias definidas por la institución educativa para garantizar el deber de cuidado de todos sus estudiantes?**



FIGURA 12. ENTREVISTA
FUENTE: ELABORACIÓN PROPIA

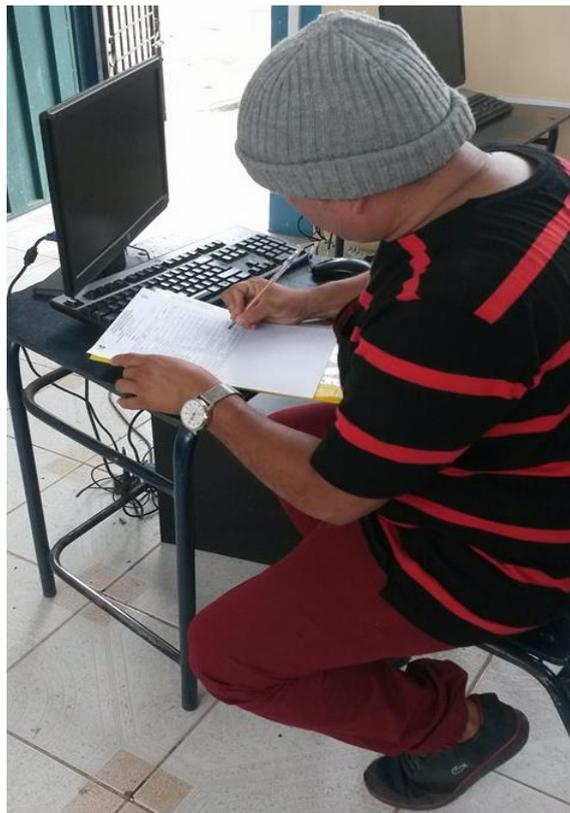


FIGURA 13 ENCUESTA
FUENTE: ELABORACIÓN PROPIA



FIGURA 14 ENCUESTA
FUENTE: ELABORACIÓN PROPIA



FIGURA 15 ENCUESTA
FUENTE: ELABORACIÓN PROPIA



FIGURA 16 ENTREVISTA
FUENTE: ELABORACIÓN PROPIA