

UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA:

INGENIERÍA DE SISTEMAS

Trabajo de titulación previo a la obtención del título:

INGENIERA E INGENIERO DE SISTEMAS

TEMA:

**ANÁLISIS DE LA INTERNETWORK DE LA INSTITUCIÓN EDUCATIVA
FISCAL “AMAZONAS” Y PROPUESTA DE REDISEÑO SIGUIENDO LA
METODOLOGÍA TOP-DOWN NETWORK DESIGN Y LOS CONTROLES
PERTINENTES DEL CIS BENCHMARK**

AUTORES:

ARIANA BELÉN SANTANA PÁEZ

RONNY ADRIÁN ZURITA MORALES

TUTOR:

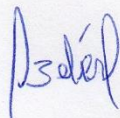
JOSÉ LUIS AGUAYO MORALES

Quito, enero 2021

CESIÓN DE DERECHOS DE AUTOR

Nosotros, SANTANA PÁEZ ARIANA BELÉN, con documento de identificación N° 1751290592, y ZURITA MORALES RONNY ADRIÁN, con documento de identificación N° 1722767496, manifestamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de grado titulado ANÁLISIS DE LA INTERNETWORK DE LA INSTITUCIÓN EDUCATIVA FISCAL “AMAZONAS” Y PROPUESTA DE REDISEÑO SIGUIENDO LA METODOLOGÍA TOP-DOWN NETWORK DESIGN Y LOS CONTROLES PERTINENTES DEL CIS BENCHMARK. Mismo que ha sido desarrollado para optar por el título de Ingeniera e Ingeniero de Sistemas, en la Universidad Politécnica Salesiana, quedando la universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en nuestra condición de autores nos reservamos los derechos morales de la obra antes citada. En concordancia, suscribimos este documento en el momento que hacemos la entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.



ARIANA BELÉN
SANTANA PÁEZ

CI: 1751290592



RONNY ADRIÁN
ZURITA MORALES

CI: 1722767496

Quito, enero del 2021

DECLARATORIA DE COAUTORÍA DEL TUTOR

Yo declaro que bajo mi dirección y asesoría fue desarrollado el Proyecto Técnico titulado ANÁLISIS DE LA INTERNETWORK DE LA INSTITUCIÓN EDUCATIVA FISCAL “AMAZONAS” Y PROPUESTA DE REDISEÑO SIGUIENDO LA METODOLOGÍA TOP-DOWN NETWORK DESIGN Y LOS CONTROLES PERTINENTES DEL CIS BENCHMARK realizado por Ariana Belén Santana Páez y Ronny Adrián Zurita Morales, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerado como trabajo final de titulación.

Quito, enero del 2021



JOSÉ LUIS AGUAYO MORALES

CI: 1709562597

DEDICATORIA

Mi trabajo de titulación lo dedico a mi amada madre Lucía de Lourdes Páez Pacheco quien gracias a su esfuerzo y perseveración logró brindarme una carrera universitaria, Mami gracias por ser esa fuente de inspiración y perseverancia hasta el final y ser junto con mi hermana los pilares fundamentales de mi vida.

A mi hermana Johana Pamela Santana Páez y su esposo Diego Arturo Paredes Carrillo quienes con sus palabras de aliento, motivación, consejos y cariño me ayudaron y guiaron a lo largo de la carrera para que siguiera adelante. Pame gracias por ser mi segunda mamá y mi amiga, protegiéndome de todo mal y luchando por mi hasta el final.

A mi hermano Oscar Paúl Santana Páez por enseñarme que todo tiene solución, que siempre hay que estar con una sonrisa en el rostro, aunque nuestro mundo se venga abajo y por escucharme cuando tenía algo que decirte.

A mi amado padre Manuel Mesias Santana Calderón por enseñarme a ser una persona fuerte y dedicada y que a pesar de la distancia sé que siempre estuviste cerca de mí, con palabras de aliento y llamadas, gracias papi.

A Aladino Cruz Sánchez por estar a mi lado, quererme tanto y enseñarme a amar las pequeñas cosas como los animalitos, la naturaleza, Aladino gracias por enseñarme a nadar y a construir mi primera cama.

A mi enamorado Ronny Adrián Zurita Morales por enseñarme otro punto de vista de la vida, eres la persona más generosa, comprensiva que he conocido en mi vida, gracias por guiarme y estar siempre a mi lado, eres mi motivación y que sea el primero de muchos logros juntos.

Ariana Belén Santana Páez

DEDICATORIA

Mi trabajo de titulación lo dedico a mi amado padre Carlos Manuel Zurita Quintana y a mi hermosa madre Hilda Magdalena Morales Córdova por todo el cariño, esfuerzo y sacrificio que hicieron para brindarme una carrera universitaria, gracias por los consejos y las palabras de aliento, a pesar de los momentos difíciles que hemos atravesado, lograron fomentar los valores y la motivación necesaria para cumplir esta meta, siendo unos padres abnegados y el pilar fundamental en mi vida.

A mi hermano Carlos Andrés Zurita Morales por cuidarme y demostrar el apoyo incondicional que se necesita como familia, demostrando el aprecio especial que tienes conmigo siempre siendo recto y honesto.

A mi hermano Luis Eduardo Zurita Morales que sin importar las diferencias siempre ha estado pendiente de mis logros, Lucho toda la vida has sido un amigo y confidente, haciendo que disfrute la vida con una sonrisa.

A mi enamorada Ariana Belén Santana Páez por ser la felicidad encajada en una sola persona, finalizar este proyecto es la esperanza que necesitamos en estos tiempos y el primero de muchos logros juntos.

Ronny Adrián Zurita Morales

AGRADECIMIENTO

Agradecemos a la Universidad Politécnica Salesiana por contribuir en nuestra formación profesional, así como a los docentes de la carrera de Ingeniería de Sistemas que impartieron sus conocimientos y experiencias.

A nuestro preciado amigo y mentor Ing. José Luis Aguayo Morales por orientarnos y motivarnos a seguir avanzando en la culminación de este proyecto de titulación y por todo el conocimiento transmitido en las horas de clase y durante la carrera, gracias por las tutorías en circunstancias que fueron difíciles para todos.

A la Institución Educativa Fiscal “Amazonas”, al Rector MSc. Alberto Allauca por brindarnos la posibilidad de realizar el proyecto de titulación, también al Lic. Manuel Mesías Santana Calderón por guiarnos en el levantamiento de información dentro de la institución y ser un querido padre y amigo.

ÍNDICE

Introducción	1
Antecedentes	1
Problema de estudio	2
Justificación	3
Grupo objetivo	4
Objetivo general.....	4
Objetivos específicos	4
Metodología.....	5
CAPÍTULO I	6
ESTADO ACTUAL DE LA RED	6
1.1 Descripción de la Institución	6
1.1.1 Datos Informativos	6
1.1.2 Estructura Organizacional	7
1.1.3 Visión	8
1.1.4 Misión	8
1.1.5 Contexto Institucional	8
1.1.6 Descripción de la Infraestructura actual de Red	10
1.1.7 Equipos físicos	10
1.1.8 Elementos de red	11
1.2 Vulnerabilidades	12
1.3 Requerimientos de la red por áreas.....	14
1.3.1 Requerimientos.....	14
1.3.2 Requerimientos de áreas administrativas, docentes y estudiantiles.....	15
CAPÍTULO II.....	16
METODOLOGÍA TOP-DOWN NETWORK DESIGN	16
2.1 Descripción de la metodología	16
2.1.1 Identificar las metas del negocio	17
2.1.2 Diseño lógico de la red	18
2.1.3 Diseño físico de la red	19
2.1.4 Optimizar, probar el diseño final de la red.....	21
2.2 Controles CIS	21
2.3 Nmap.....	27
2.4 Prtg network monitor	27
2.5 Riverbed modeler	28
2.6 Ipv4.....	28
CAPÍTULO III.....	29
DESARROLLO DE LA METODOLOGÍA TOP-DOWN.....	29

3.1	Identificar las metas del negocio	29
3.1.1	Análisis de las metas del negocio y restricciones	29
3.1.2	Análisis de los Objetivos Técnicos y sus Restricciones	30
3.1.3	Acceso a Internet	32
3.1.4	Caracterización de la Red Existente	37
3.2	Propuesta diseño lógico de la red	43
3.2.1	Topología de red.....	44
3.2.2	Modelo de Direccionamiento y Nombramiento.....	44
3.2.3	Desarrollo de estrategias de Seguridad de la Red	46
3.2.4	Desarrollo de estrategias de Gestión de la Red	50
3.3	Propuesta diseño físico de la red	50
3.3.1	Cableado estructurado para para Institución Educativa Fiscal “Amazonas” ..	51
3.3.2	Criterios de diseño del cableado estructurado.....	51
3.3.3	Equipos.....	63
3.4	Propuesta de rediseño para la Institución Educativa Fiscal “Amazonas”	63
3.4.1	Propuesta de Aplicaciones y servicios	63
3.4.2	Propuesta de diseño de Red Inalámbrica	64
3.4.3	Propuesta de Equipos	66
3.4.4	Propuesta de software.....	70
3.4.5	Simulación red Actual IEFA	73
3.4.6	Simulación red propuesta IEFA.....	74
3.4.7	Propuesta rediseño de topología de la internetwork de la IEFA	75
3.4.8	Configuración de Equipos propuestos para la red de la IEFA	76
CAPÍTULO IV		79
ANÁLISIS DE RESULTADOS		79
4.1	Resultados de simulación de la red actual de la IEFA	79
4.2	Resultados de simulación de la propuesta de rediseño para la Institución Educativa Fiscal “Amazonas”.....	80
4.3	Resultados de simulación por servicios	80
4.3.1	Servicio 1	80
4.3.2	Servicio 2	83
4.3.3	Servicio 3	85
4.3.4	Servicio 4	85
4.3.5	Servicio 5	87
4.3.6	Servicio 6	89
4.3.7	Análisis económico	92
4.3.8	Beneficio	95
CONCLUSIONES		96
RECOMENDACIONES		98

REFERENCIAS.....	99
------------------	----

ÍNDICE DE TABLAS

Tabla 1. Distribución de la Infraestructura de la IEFA.....	9
Tabla 2. Capacidad de ancho de banda requerido	34
Tabla 3. Tráfico recibido desde Base de Datos	81
Tabla 4. Tráfico enviado de Base de Datos	82
Tabla 5. Análisis de tráfico en Base de Datos	82
Tabla 6. Tráfico recibido en Email.....	83
Tabla 7. Tráfico enviado de Email	84
Tabla 8. Análisis de tráfico en Email	84
Tabla 9. Delay para Ethernet.....	85
Tabla 10. Tráfico recibido de FTP	86
Tabla 11. Tráfico enviado de FTP.....	86
Tabla 12. Análisis de tráfico en FTP	87
Tabla 13. Tráfico recibido de Http	88
Tabla 14. Tráfico enviado de Http.....	88
Tabla 15. Análisis de tráfico en Http.....	89
Tabla 16. Tráfico recibido de VOIP	90
Tabla 17. Tráfico enviado de VOIP	90
Tabla 18. Análisis de tráfico en VOIP.....	91

ÍNDICE DE FIGURAS

Figura 1. Foto aérea de la Institución realizada mediante dron	6
Figura 2. Organización jerárquica de la Institución Educativa Fiscal "Amazonas"	7
Figura 3. Visión de la IEFA	8
Figura 4. Misión de la IEFA.....	8
Figura 5. Contexto Institucional IEFA	9
Figura 6. Equipos de personal administrativo y docentes.....	11
Figura 7. Elementos físicos de la red de la IEFA	11
Figura 8. Monitoreo de los dispositivos de la IEFA utilizando Nmap.....	12
Figura 9. Vulnerabilidades del Router 881.....	13
Figura 10. Vulnerabilidad en dispositivos de red	13
Figura 11. Fases metodología Top - Down	17
Figura 12. Características de las Topologías de Red	19
Figura 13. Estándares de cableado estructurado ANSI/EIA/TIA	20
Figura 14. Categorías y uso de cable UTP	20
Figura 15. Controles CIS básicos, fundamentales y organizacionales.....	22
Figura 16. Monitoreo de aplicaciones utilizadas en la IEFA.....	31
Figura 17. Auditoría de aplicaciones y servicios utilizados en la IEFA	31
Figura 18. Capacidad de Simultaneidad	34
Figura 19. Principales códec para compresión de voz.....	35
Figura 20. Cabecera de protocolos para voz.....	36
Figura 21. Distribución de extensiones telefónicas	36
Figura 22. Topología de internetwork de la IEFA.....	38
Figura 23. Ubicación de Bloques de la IEFA	39
Figura 24. Cableado de Bloque 1	40
Figura 25. Cableado de Bloque 3	40
Figura 26. Cableado Bloque 4.....	41
Figura 27. Cableado de Bloque 6	41
Figura 28. Demanda de Internet obtenida por PRTG	42
Figura 29. Rendimiento de la red IEFA	42
Figura 30. Diseño lógico estado actual IEFA.....	43
Figura 31. Direccionamiento IPv4 para la IEFA	45
Figura 32. Propuesta diseño lógico IEFA.....	46
Figura 33. Plan de gestión para dispositivos de la IEFA	47
Figura 34. Parámetros diseño físico de la red.....	51
Figura 35. Diagrama esquemático de cableado estructurado.....	54

Figura 36. Propuesta de puntos de red para la IEFA	55
Figura 37. Cantidad de rack y switches	56
Figura 38. Simbología de voz-datos, bandejas y tuberías	56
Figura 39. Ubicación de puntos de red y canaletas en bloque Rectorado.	57
Figura 40. Ubicación de puntos de red y canaletas en bloque Inspección.	58
Figura 41. Ubicación de puntos de red, tuberías, canaletas y bandejas en Laboratorios.	59
Figura 42. Ubicación de puntos de red, tuberías, canaletas y bandejas en bloque 3.	59
Figura 43. Ubicación de puntos de red, tuberías, canaletas y bandejas en bloque 3.	60
Figura 44. Ubicación de puntos de red, recorrido de las bandejas y tuberías.	60
Figura 45. Ubicación de puntos de red, bandejas y canaletas.	61
Figura 46. Ubicación de puntos de red, bandejas y canaletas.	62
Figura 47. Ubicación de puntos de red, bandejas y canaletas.	62
Figura 48. Conectividad entre Bloques IEFA.....	63
Figura 49. Comparación de equipos Firewall.....	66
Figura 50. Comparación de equipos Router	67
Figura 51. Comparación de equipos Switch	68
Figura 52. Comparación de equipos ACCESS POINT	69
Figura 53. Comparación de Sistemas Operativos	71
Figura 54. Comparación de Antivirus	72
Figura 55. Comparación de herramientas de Monitoreo.....	72
Figura 56. Simulación Red Actual IEFA en Riverbed	73
Figura 57. Simulación propuesta de rediseño IEFA en Riverbed	74
Figura 58. Propuesta de Rediseño de red IEFA.....	75
Figura 59. Configuración AAA.....	76
Figura 60. Configuración ACL de la IEFA	77
Figura 61. Resultados Riverbed red actual IEFA	79
Figura 62. Resultados Riverbed red Propuesta IEFA	80
Figura 63. Proforma de dispositivos de red de la IEFA.....	92
Figura 64. Costo Software a utilizar en la IEFA	92
Figura 65. Costo cableado estructurado para la IEFA	93
Figura 66. Costo cuarto de Telecomunicaciones para la IEFA.....	94
Figura 67. Costo final de la propuesta para la IEFA.....	94
Figura 68. Costos de recuperación IEFA.....	95

RESUMEN

La red de datos de la Institución Educativa Fiscal “Amazonas” evidenciaba intermitencia en la conexión a Internet, que se podría: mejorar el sistema de cableado estructurado al igual que los enlaces a Internet, incrementar la seguridad a nivel de hardware y software, además se reubicarían los equipos de red para mejorar el servicio de red.

Utilizando la metodología Top – Down Network Design se plantea una propuesta de rediseño centrada en las necesidades de los usuarios realizando un diseño lógico y físico de la red que finaliza con pruebas de rendimiento de la internetwork. El esquema de red utilizado fue el jerárquico de tres capas (núcleo, distribución y acceso), en las que se aplicaron normas establecidas de cableado según la ANSI/TIA/EIA, se presupuestaron dispositivos de red y software licenciado obteniendo costos y beneficios para la IEFA. Los controles de seguridad del CIS Benchmark guiaron para proteger, resguardar la red de datos y dispositivos utilizados en la misma, brindando confidencialidad, integridad y disponibilidad.

A través del simulador Riverbed se compararon las redes del estado actual con la propuesta de rediseño, obteniendo estadísticas de tráfico para cada área de la institución, evidenciando un incremento de 63.3% en el rendimiento de la red.

ABSTRACT

The data network of the Institución Educativa Fiscal "Amazonas" presented intermittence in the Internet connection, which could: improve the structured cabling system as well as the Internet links, increase the security at the hardware and software level, in addition to they would relocate network equipment to improve network service.

Using the Top - Down Network Design methodology, a redesign proposal is proposed focused on the needs of the users, carrying out a logical and physical design of the network that ends with performance tests of the internetwork. The network scheme used was hierarchical with three layers (core, distribution and access), in which established cabling standards were applied according to ANSI / TIA / EIA, network devices and licensed software were budgeted, obtaining costs and benefits for the IEFA. The security controls of the CIS Benchmark guided to protect, safeguard the data network and devices used in it, providing confidentiality, integrity and availability.

Through the Riverbed simulator, the current state networks were compared with the redesign proposal, obtaining traffic statistics for each area of the institution, showing an increase of 63.3% in network performance.

INTRODUCCIÓN

El auge de la tecnología ha llegado a cada rincón del planeta, permitiendo al ser humano tener a la mano una serie de herramientas a disposición, estar comunicado constantemente con el mundo exterior e interactuar con otras personas. A estos avances se han sumado un sin número de instituciones educativas para brindar a estudiantes y autoridades los beneficios del Internet.

Antecedentes

La Institución Educativa Fiscal “Amazonas” (IEFA) busca automatizar y optimizar procesos, además permite a los usuarios de diferentes departamentos estar interconectados, acceder y compartir información que se genera de manera rápida, por lo tanto, se debe brindar una cobertura total de Internet en sus áreas.

Las técnicas utilizadas actualmente dentro de la institución carecen de automatización y seguridad lo que puede derivar en ataques hacia el centro educativo, crackers o personas mal intencionadas podrían acceder con facilidad a los recursos del colegio y realizar ataques como robo de credenciales, alteración de información, o sustracción de notas, las mismas que están catalogadas como activos.

Lo que conlleva que en base a los requerimientos planteados por parte del representante legal de la IEFA y los coordinadores de las diferentes áreas como son: Administrativa, Bachillerato General Unificado, Bachillerato Internacional, Comunes y Recreativas, desarrollar una propuesta de rediseño de la internetwork que mantenga todas las especificaciones conforme a cumplir los estándares basados en la metodología del Top-Down Network Design y los controles pertinentes del CIS Benchmark.

Problema de Estudio

La Institución Educativa Fiscal "Amazonas" es un establecimiento educativo que forma bachilleres de manera integral, tiene una comunidad de 3000 estudiantes, 115 docentes y 20 administrativos, por esta razón, se apoya en una red datos para su operación, manteniendo una organización definida, por lo cual requiere la disponibilidad de diferentes puntos de red, distribuidos entre área administrativa, salones de clase y laboratorios.

Se evidencia que no posee una red apropiada para sus necesidades, por algunas dificultades en la conexión a Internet, un sistema de cableado estructurado inadecuado, problemas con las impresoras de red, distribución de los equipos de red inalámbricos sin organización, gestión inadecuada de los enlaces a Internet y ausencia de seguridad a nivel de hardware y software.

El sistema de respaldo de calificaciones, los documentos generados por las áreas administrativas, las asistencias de alumnos y docentes de la institución se realizan manualmente. Esto genera varios inconvenientes a nivel de seguridad porque se encuentran afectadas la confiabilidad y disponibilidad de la información, en consecuencia, se generan errores al subir respaldos de los datos debido a que en el momento que ocurra algún fallo de cualquier índole, ya sea natural o provocado por el hombre, la información se perdería porque se encuentra almacenada en discos duros y no en una nube.

Justificación

De acuerdo con el análisis realizado a la estructura de red, los requerimientos de la Institución Educativa Fiscal “Amazonas” (IEFA) y el plan de crecimiento que tiene, se necesita diseñar una red de datos con el fin de adecuar y soportar todos los recursos tecnológicos, proporcionando una red segura con disponibilidad, estabilidad en la conexión, transmisión de datos, permitiendo así desarrollar los procesos internos y la ejecución del plan educativo con fiabilidad.

Con la propuesta de rediseño de la red de datos se logrará la ubicación correcta de los equipos, el cableado y etiquetas que facilitarán la resolución de problemas de conexión, mantenimiento de los equipos y mejor almacenamiento de datos evitando respaldos manuales con lo que se aliviará costos y tiempos de mantenimiento permitiendo encontrar la falla sin necesidad de revisar toda la red de la IEFA.

Los docentes se conectan a la red filtrándolos por medio de su dirección MAC (Media Access Control) para evitar el ingreso de estudiantes a los dispositivos de red. Cuando se presentan problemas en la Institución sobre conexión a Internet se retiran los cables de red y se los coloca en diferentes puertos hasta obtener otra conexión porque el cableado no se encuentra etiquetado de forma correcta, además si se requiere tener acceso a la red no se puede porque que los dispositivos de red se encuentran ubicados sin seguir un diseño estructurado.

Actualmente, no se ha auditado la red existente, consecuentemente, se utilizará un marco de trabajo internacional basado en el diseño Top-Down Network Design y el CIS Benchmark, para realizar la propuesta que mejorará el uso de recursos, beneficiando a las autoridades, docentes y estudiantes dentro de la IEFA.

Grupo Objetivo

El presente proyecto beneficia directamente a la Institución Educativa Fiscal “Amazonas”, incluyendo la comunidad estudiantil, docentes y área administrativa puesto que se realizará el rediseño de la red de datos, mejorando los pilares de seguridad como confidencialidad y disponibilidad de los datos, el almacenamiento de la información, la correcta implementación del cableado estructurado, redistribución adecuada de los equipos inalámbricos y cableados.

Objetivo General

Analizar la internetwork de la Institución Educativa Fiscal “Amazonas” y proponer un rediseño siguiendo la metodología Top-Down Network Design y los controles pertinentes del CIS Benchmark.

Objetivos específicos

Realizar el análisis del estado actual de la internetwork de la Institución Educativa Fiscal “Amazonas” para determinar amenazas y vulnerabilidades tanto en el diseño de red como en la seguridad.

Analizar los activos y procesos principales de la red de la IEFA para el rediseño lógico de la red.

Definir los componentes de hardware y software mediante un análisis costo beneficio para la propuesta de rediseño de la red de datos de la IEFA.

Proponer un rediseño de red sustentándose en la metodología Top-Down Network Design y los controles pertinentes del CIS Benchmark.

Evaluar el rediseño final de la red de datos sobre un software de simulación para realizar el análisis de resultados.

Metodología

El presente proyecto de titulación se basa en la metodología Top – Down para diseño de redes desarrollada por Priscilla Oppenheimer (Oppenheimer, Top Down Network Design, 2011), la cual conserva un enfoque caracterizado por dar prioridad a la capa siete o superiores a su vez que se explora las estructuras de grupos y divisiones para obtener información sobre a quién sirve la red y cuales aplicaciones serán ejecutadas para tener un proceso completo que asocie las necesidades del negocio junto con la tecnología disponible necesaria para garantizar el éxito de una organización (Hernández, 2011). La metodología consta de cuatro fases: Identificar las metas del negocio, diseño lógico de la red, diseño físico de la red y optimizar, probar el diseño final de la red.

En la primera fase se procedió a documentar la red, entrevistando al personal administrativo, docentes y estudiantil, con lo cual se recolectó la información sobre la institución.

En la segunda fase se asignó una topología de red, se diseñó el modelo de direccionamiento, las estrategias de seguridad y gestión de red las cuales se aplican junto con los controles del CIS Benchmark (CIS Controls, 2020).

En la tercera fase se accedieron a los planos de la institución para el rediseño del cableado estructurado, al mismo tiempo, se realizó el presupuesto de hardware y software para obtener los beneficios de la propuesta del rediseño.

En la cuarta fase se simuló la red actual y la propuesta de rediseño para obtener resultados estadísticos, que fueron analizados usando comparativas y sacando los porcentajes de rendimiento utilizando varianza y desviación estándar.

CAPÍTULO I

ESTADO ACTUAL DE LA RED

1.1 Descripción de la Institución

1.1.1 Datos Informativos

La Institución Educativa Fiscal “Amazonas” se encuentra ubicada en la provincia de Pichincha al sur de Quito sector la Villa Flora (Lauro Guerrero 1270e2E y Luis Iturralde) al momento consta de una edificación física aproximada de 2000 m². En la figura 1 se indica la ubicación geográfica de la IEFA (IEFA, 2020).



1.1.2 Estructura Organizacional

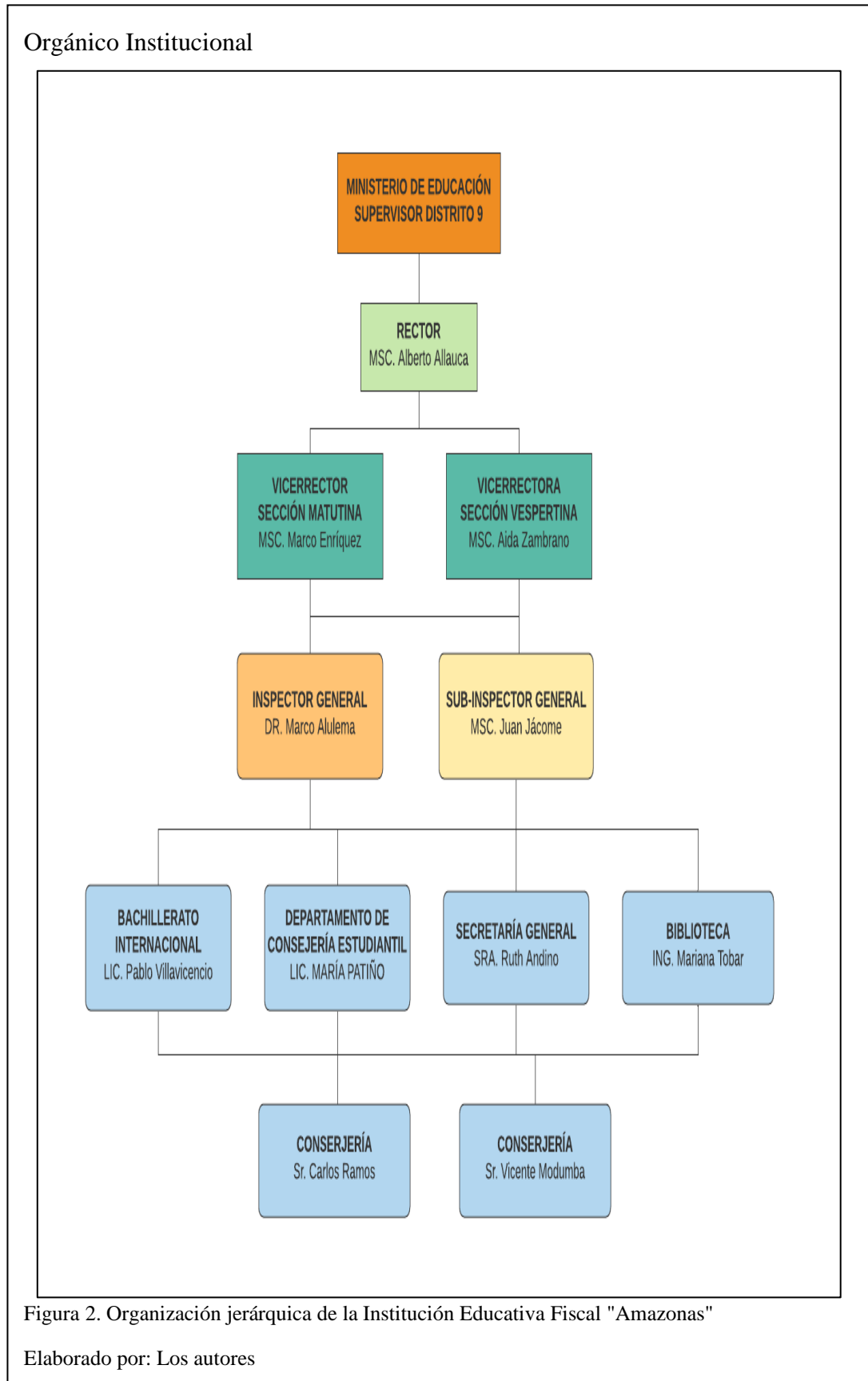


Figura 2. Organización jerárquica de la Institución Educativa Fiscal "Amazonas"

Elaborado por: Los autores

1.1.3 Visión

Enfoque de Educación de la IEFA

Para el año 2022, la Institución Educativa Fiscal “Amazonas” será líder en el Distrito Metropolitano de Quito, brindará una educación con enfoque internacional, centrada en el ser humano que garantizará su desarrollo holístico, en el marco del respeto a los derechos humanos, al medio ambiente sustentable y a la democracia, ofrecerá una educación incluyente y diversa, de calidad y calidez que promueva la iniciativa comunitaria; la mejora de competencias y capacidades para crear un mundo mejor y más pacífico, continuar sus estudios en instituciones de educación superior o integrarse al mundo del trabajo.

Figura 3. Visión de la IEFA

Fuente: Institución Educativa Fiscal “Amazonas”

1.1.4 Misión

Meta de la IEFA con sus estudiantes

La Institución Educativa Fiscal “Amazonas” es un establecimiento educativo que forma bachilleres de manera integral, sólidamente preparados y capacitados para continuar sus estudios en instituciones de Educación Superior o para integrarse al proceso productivo del país.

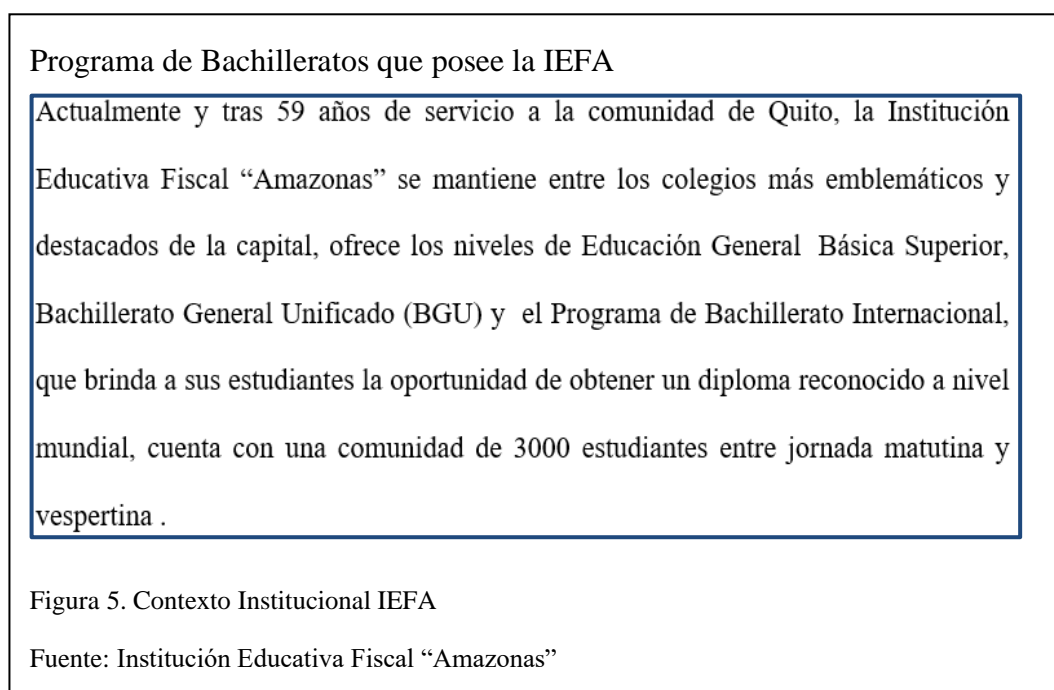
Figura 4. Misión de la IEFA

Fuente: Institución Educativa Fiscal “Amazonas”

1.1.5 Contexto Institucional

Los docentes de la institución han sido seleccionados por su perfil de investigación y preparación en docencia educativa los cuales son asignados por el Ministerio de Educación del Gobierno. Además, los alumnos son personas que deciden

ser proactivos, emprendedores y justos logrando ser agentes de cambio para el futuro del país (IEFA, 2020).



Distribución de la Infraestructura

La IEFA cuenta con una construcción de 10 bloques de dos y tres pisos respectivamente además de 3 áreas administrativas divididas en 2000 m².

Tabla 1. Distribución de la Infraestructura de la IEFA

Área de Bachillerato General Unificado	36 aulas	Aulas de clases
	1 laboratorio	Laboratorio de Computación
	2 laboratorios	Laboratorios de Física
	2 laboratorios	Laboratorios de Química
Área de Bachillerato Internacional	2 aulas	Aulas de clases
Áreas Administrativa	1 área	Rectorado
	2 áreas	Vicerrectorados
	1 área	Secretaría General
	1 área	Secretaría
	1 área	DECE
	1 área	Biblioteca
	1 área	Enfermería

	1 área	Inspección
Áreas Comunes	1 área	Auditorio
	1 área	Bar
	1 área	Baterías Sanitarias
	3 áreas	Sala de Profesores
	1 área	Sala de Profesores Bachillerato Internacional
Área Recreacional	1 área	Cancha de Básquet
	1 área	Cancha de Fútbol
	1 área	Granja
	1 área	Patio con juegos
Auxiliar de Servicios Generales	1 área	Garita conserje

Elaborado por: Los autores

1.1.6 Descripción de la Infraestructura actual de Red

La Institución Educativa Fiscal “Amazonas” posee acceso a Internet provisto por la Corporación Nacional de Comunicaciones, dispone de dispositivos de red como router y switch pero se encuentra limitada en el área administrativa por la cobertura inalámbrica que utiliza la red, no posee una administración completa de la red, el cableado no es el adecuado para proporcionar la utilización completa del ancho de banda que le otorga el Estado, también no poseen sistema de seguridad y respaldos de información.

1.1.7 Equipos físicos

En la figura 6 se detallan los equipos que pertenecen a la IEFA los cuales son facilitados por el Distrito 9.

Características de dispositivos

ÁREA	PC	SISTEMAS OPERATIVOS	SOFTWARE	RAM	DISCO DURO	CANTIDAD
Administrativos	PC	Windows 10	Office 2016 AVG	4	500 GB	5
Inspección	PC	Windows 7	Office 2013 AVG	2	250 GB	1
Subinspección	PC	Windows 8	Office 2013 AVG	4	250 GB	1
Secretaría General	PC	Windows 10	Office 2016 AVG	4	500 GB	1
DECE	PC	Windows 7	Office 2013 AVG	4	350 GB	3
Docentes	HP-240g	Windows 8	Office 2013 AVG	4	500 GB	48
	HP-240	Windows 7	Office 2013 AVG	4	350 GB	57
Bachillerato Internacional	PC	Windows 7	Office 2013 AVG	4	350 GB	1
Laboratorios Física-Química	PC	Windows 10	Office 2016 AVG	4	250 GB	2
Laboratorio de Computación	PC	Windows 7	Office 2013 AVG	4	250 GB	24
Biblioteca	PC	Windows Vista	Office 2013 AVG	2	80 GB	1
	PC	Ubuntu	Libre	2	80 GB	4

Figura 6. Equipos de personal administrativo y docentes

Elaborado por: Los autores

1.1.8 Elementos de red

En la figura 7 se detallan los diferentes equipos de red con los cuales la IEFA tiene acceso a Internet:

Dispositivos de red de la IEFA

EQUIPO	MARCA	MODELO	CANTIDAD
ROUTER	CISCO	881	2
ROUTER	TP-LINK	TL-WR740N	5
ROUTER	TP-LINK	WR941HP	1
ROUTER	D-LINK	DIR-600	2
ROUTER	D-LINK	AC750 DIR-809	1
ROUTER	HUAWEI	HG530	1
SWITCH	CISCO	Sg100-16	1
SWITCH	CISCO	Sg110d-05	1
SWITCH	TP-LINK	TL-SF1024D	3
SWITCH	TP-LINK	TL-SF1008D	3
SWITCH	TP-LINK	SF1016D	1
SWITCH	D-LINK	Des-1005	2

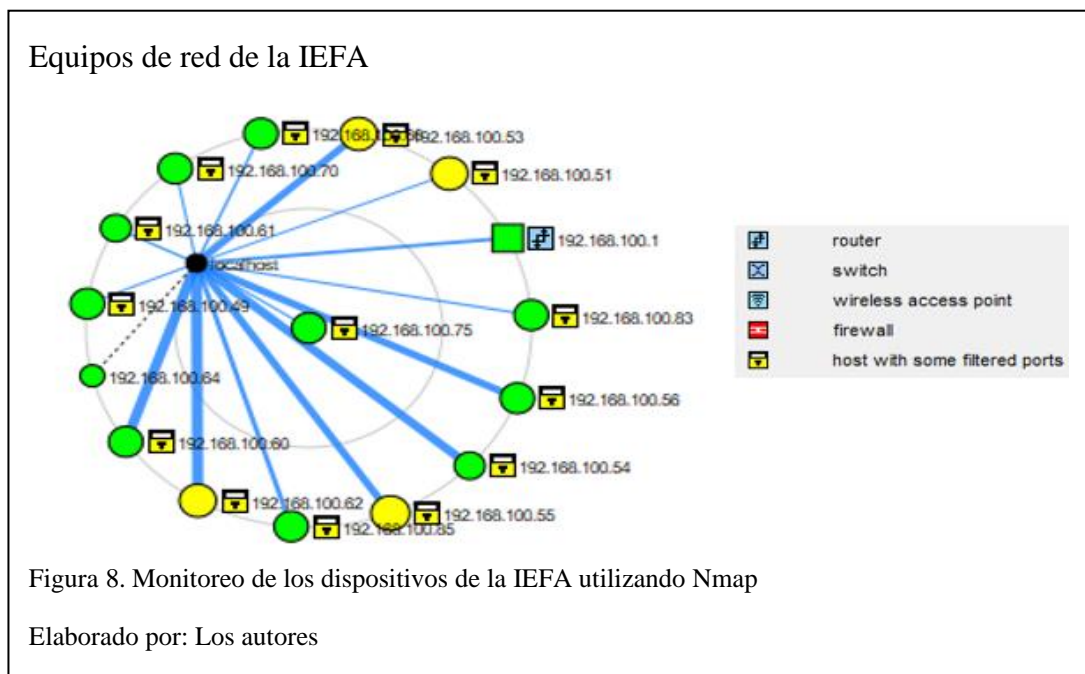
Figura 7. Elementos físicos de la red de la IEFA

Elaborado por: Los autores

1.2 Vulnerabilidades

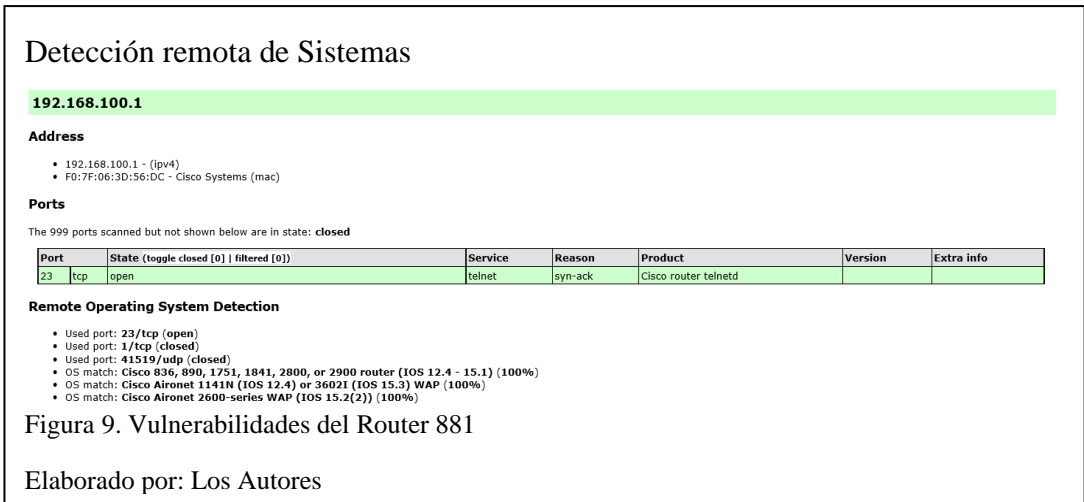
En la recolección de datos inicial se descubrió que no existen servidores, no hay políticas de seguridad, hay un router de frontera y estaciones de trabajo.

En la figura 8 se puede visualizar la topología de la red de datos según el monitoreo realizado por la herramienta Nmap, obteniendo que la internetwork de la IEFA cuenta únicamente con dispositivos Router y Host.

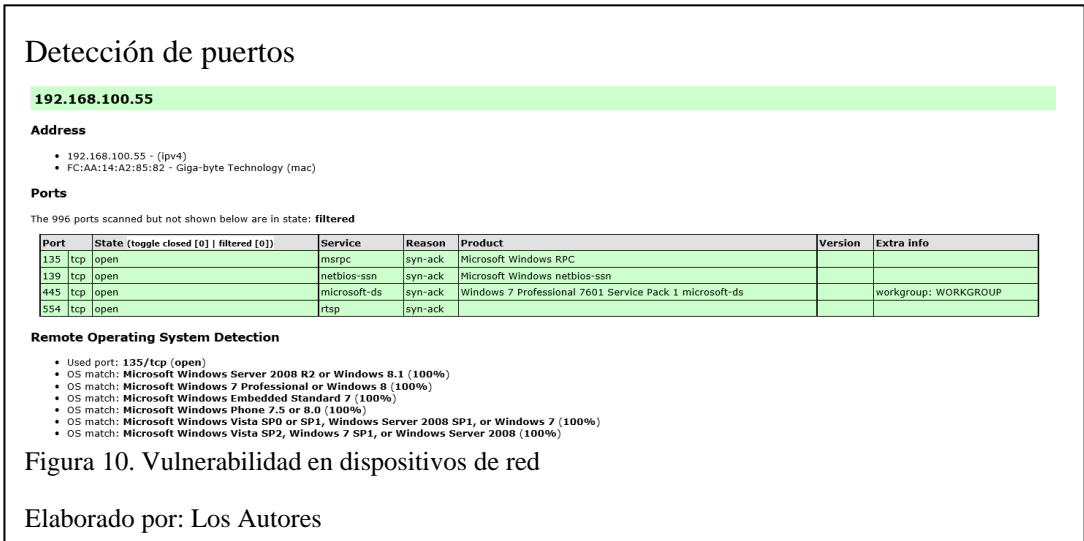


La institución no cuenta con un dispositivo de seguridad firewall, es una de las vulnerabilidades más evidentes, no existe un cortafuegos que separe la red externa de la interna y del mismo modo la red interna a la externa permitiendo todo tipo de transmisión de datos.

El equipo router 881 presenta vulnerabilidades en la seguridad de autenticación, al igual que permite conexiones mediante telnet hacia el equipo, evidencia puertos abiertos como el 23 en tcp.



En la figura 10 se observa que se encuentran abiertos los puertos tcp con lo que está permitiendo conexiones remotas a la red de la IEFA.



La falta de antivirus y licencias en el software que utiliza la institución provoca que se exponga a riesgos de seguridad que pueden afectar a las plataformas que usa la institución.

1.3 Requerimientos de la red por áreas

1.3.1 Requerimientos

Se recolectaron en base a una reunión con las autoridades de la Institución Educativa Fiscal “Amazonas”, en la cual expusieron las necesidades de las áreas administrativas y estudiantiles.

- Los requerimientos de administrativos, docentes y estudiantes se reafirmaron con una encuesta (Cordero & Marcillo, 2018).
- Los requerimientos de la red se clasifican a nivel de usuario, de tecnología y red.

1.3.1.1 Requerimientos a nivel de usuario

Determina las necesidades actuales y futuras de los usuarios, así como los límites que se plantean con respecto al dimensionamiento de la red, se debe realizar un análisis costo/beneficio para componentes de hardware y software con la finalidad de tomar decisiones.

La Institución Educativa Fiscal “Amazonas” tiene que permitir el acceso a los usuarios a diferentes servicios de la internetwork, la cual mantiene una conexión a Internet, compartiendo recursos lógicos y físicos dentro de las áreas.

1.3.1.2 Requerimientos a nivel de tecnología y red

La seguridad de la información que operan las áreas administrativas tiene que mantener estándares de control para evitar la pérdida de datos.

El ancho de banda utilizado debe procurar transferir la máxima cantidad de datos entre los diferentes puntos de la internetwork para determinar la calidad, la velocidad de la red y satisfacer las necesidades de la Institución Educativa Fiscal “Amazonas” (Guevara & Quizhpi, 2017).

1.3.2 Requerimientos de áreas administrativas, docentes y estudiantiles

1.3.2.1 Área administrativa

Por medio de conexiones guiadas y no guiadas necesitan acceso a correo electrónico, plataformas educativas, servicios de VOIP y video conferencia para realizar sus labores diarias.

1.3.2.2 Docentes

Los docentes de la institución requieren acceso por medios guiados y no guiados a correo electrónico, video conferencia, plataformas educativas y páginas de investigación, para poder comunicarse con los estudiantes y las áreas administrativas.

1.3.2.3 Estudiantes

Necesitan acceso a la red por medios guiados y no guiados para plataformas educativas, páginas de investigación, correo electrónico y videos para consultas.

CAPÍTULO II

METODOLOGÍA TOP-DOWN NETWORK DESIGN

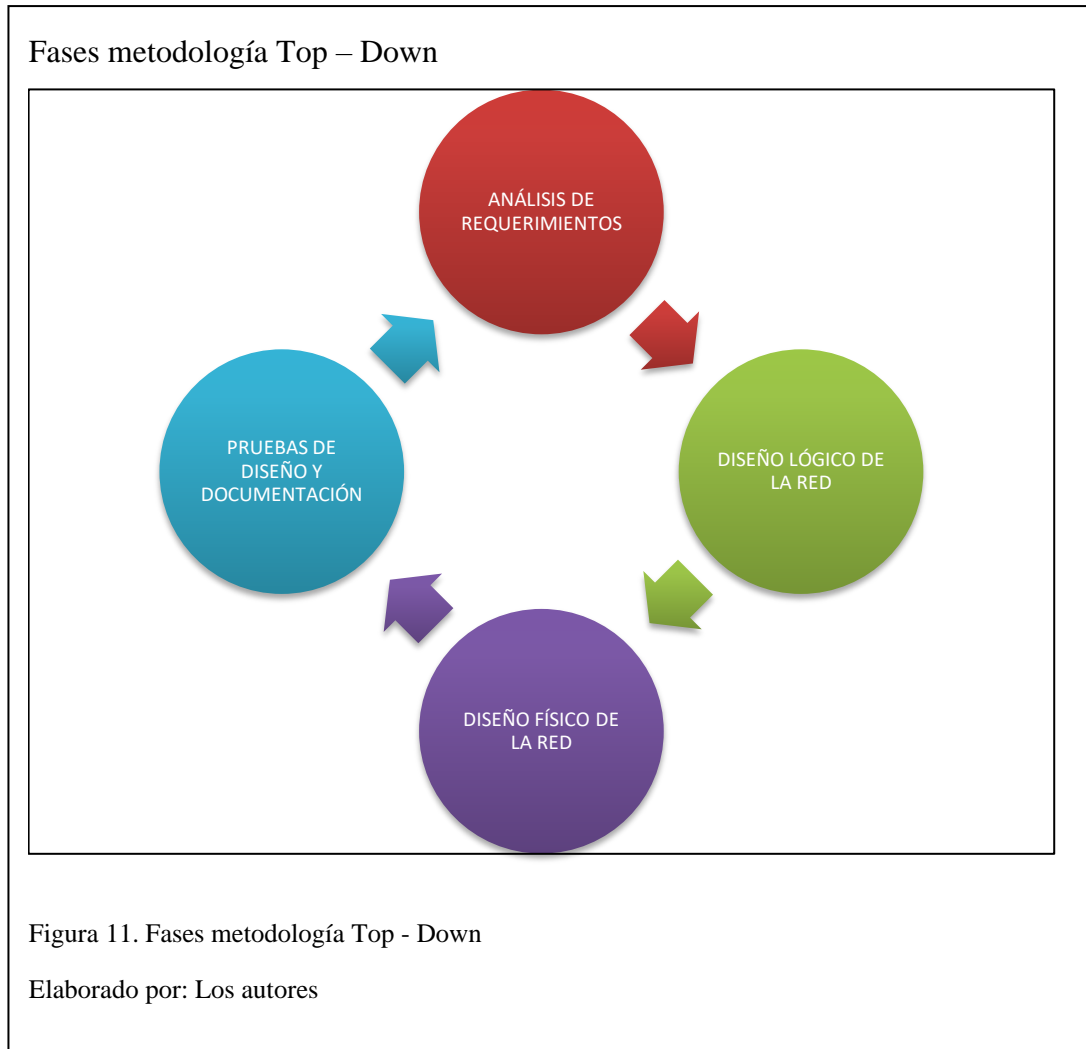
2.1 Descripción de la metodología

El diseño de redes basado en esta metodología comienza en las capas superiores del modelo de referencia OSI antes de moverse a las capas inferiores, alineándose a los objetivos y metas técnicas de las empresas, mientras se reconoce que el modelo lógico y el diseño físico puede adaptarse según la información que se recopila manteniendo la funcionalidad, disponibilidad, escalabilidad, seguridad y capacidad de gestión (Huerta, 2013).

Se utilizan procesos y herramientas que guían en la comprensión del flujo de tráfico, el comportamiento del protocolo y las tecnologías de interconexión de redes, manteniendo un orden desde las capas de aplicación, presentación, sesión y transporte para después trabajar en las capas inferiores (red, enlace de datos, física) debido a que en estas capas se analizan: la situación actual de la red, los requerimientos, las limitaciones y su estructura lógica que se debe tomar en cuenta al momento del desarrollo de la metodología (Oppenheimer, Top Down Network Design, 2011)

El proceso de diseño de red Top-Down incluye la exploración de estructuras organizativas y grupales para encontrar a las personas para quienes la red proporcionará servicios y de quienes el diseñador debe obtener información valiosa para que el diseño tenga éxito.

Según (Oppenheimer, Top Down Network Design, 2011) la metodología Top – Down consta de cuatro fases las cuales se encuentran definidas en la Figura 11.



2.1.1 Identificar las metas del negocio

Los objetivos comerciales y las restricciones de los clientes son el aspecto crítico en el diseño de la red, la información se la obtiene mediante consulta al personal que labora en la empresa y a los usuarios que la utilizan procurando que el alcance de las metas técnicas sirva para implementar o actualizar la red existente (Huerta, 2013).

Los objetivos técnicos de la institución son:

- Escalabilidad.
- Disponibilidad.
- Performance.
- Manejabilidad.

- Seguridad.

Cuando se examinan los objetivos técnicos se deben analizar y describir la infraestructura tanto a nivel lógico como nivel físico para comprender las áreas que se van a intervenir, por lo que se tiene un panorama que es utilizado para la planificación y posterior diseño de red (Oppenheimer, Top Down Network Design, 2011).

2.1.2 Diseño lógico de la red

En esta fase se diseña la topología de red, el modelo de direccionamiento, protocolos de switching y routing para los dispositivos de la internetwork, también se desarrollan estrategias de seguridad y de mantenimiento para la red para responder de manera eficiente cuando se tenga problemas en la red, en el diseño lógico se deben tener presente los siguientes procesos (Oppenheimer, Top-Down Network Design, 2011):

- Diseño de Modelo de Direccionamiento y Nombramiento.
- Selección de Protocolos de Switching y Routing.
- Desarrollo de estrategias de seguridad de la red.
- Desarrollo de estrategias de Gestión de la red.

Para implementar un diseño de topología de red se puede escoger según las características que se acoplen mejor al diseño de red, existen los siguientes tipos de topologías:

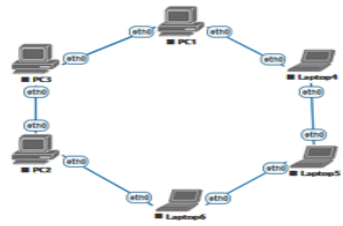

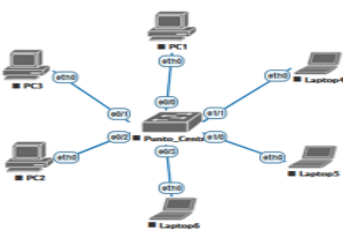
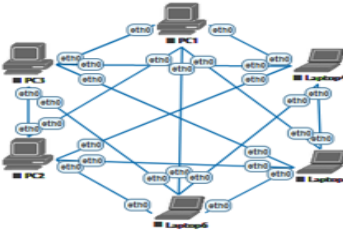
Definición de topologías		
Topología	Características	Gráfico
Anillo	Una topología de anillo conecta los dispositivos de red uno tras otro sobre el cable en un círculo físico.	
Bus	Los dispositivos se conectan en forma de serie uno a continuación de otro.	
Estrella	Todos los ordenadores se conectan a un nodo central que controla y realiza todas las funciones de red.	
Malla	Todos los dispositivos están interconectados entre sí.	

Figura 12. Características de las Topologías de Red

Fuente: (Martinez, 2007)

El direccionamiento lógico que se va implementar en la nueva red es IPv4, mientras se analizan y seleccionan los protocolos de conmutación junto al enrutamiento para que los dispositivos de la internetwork puedan converger (Oppenheimer, Top Down Network Design, 2011).

2.1.3 Diseño físico de la red

Para garantizar enlaces de extremo a extremo entre los usuarios de los sistemas de comunicación, la red de comunicación física subyacente generalmente se diseña de

forma independiente. Los diseños se optimizan minimizando la longitud de ruta promedio entre usuarios vinculados lógicamente (Kwon, 2013).

2.1.3.1 Normas para el cableado estructurado

Los estándares ANSI/EIA/TIA son:

Estándares para cableado estructurado

ANSI/TIA/EIA-568-A: “Estándar de Edificios Comerciales para Cableado de Telecomunicaciones”.

ANSI/TIA/EIA-568-B: “Este estándar especifica los requisitos de componentes y de transmisión según los medios”.

ANSI/TIA/EIA-569-A: “Normas de Recorridos y Espacios de Telecomunicaciones en Edificios Comerciales sobre cómo enrutar el cableado”.

ANSI/TIA/EIA-570-A: “Normas de Infraestructura Residencial de Telecomunicaciones”.

ANSI/TIA/EIA-606-A: “Normas de Administración de Infraestructura de Telecomunicaciones en Edificios Comerciales”.

ANSI/TIA/EIA-607: “Requerimientos para instalaciones de sistemas de puesta a tierra de Telecomunicaciones en Edificios Comerciales”.

ANSI/TIA/EIA-758: “Norma Cliente-Propietario de cableado de Planta Externa de Telecomunicaciones”.

Figura 13. Estándares de cableado estructurado ANSI/EIA/TIA

Fuente: (Cisco System, 2002)

2.1.3.2 Categorías para cableado estructurado

Cable UTP

Categoría	Uso	Ancho de banda
CAT 1	Voz solamente (cable telefónico)	-
CAT 2	Datos hasta 4 Mbps (Localtalk, Apple)	-
CAT 3	Datos hasta 10 Mbps (Ethernet 10Base-T)	16 MHz
CAT 4	Datos hasta 20 Mbps (Token Ring)	20 MHz
CAT 5	Datos hasta 100 Mbps (FastEthernet 100Base-T)	100 MHz
CAT 5e	Datos hasta 1000 Mbps (Gigabit Ethernet 1000Base-T)	100 MHz
CAT 6	Datos hasta 10 Gigabits (10GBase-T)	250 MHz

Figura 14. Categorías y uso de cable UTP

Fuente: (Cura, 2015)

2.1.4 Optimizar, probar el diseño final de la red

En la última fase, probar el diseño de la red es un proceso de diseño que cumple con los objetivos comerciales y técnicos, mientras que al probar el diseño se verifica que las soluciones que se han desarrollado proporcionan el rendimiento y QoS que el cliente espera (Oppenheimer, Top Down Network Design, 2011).

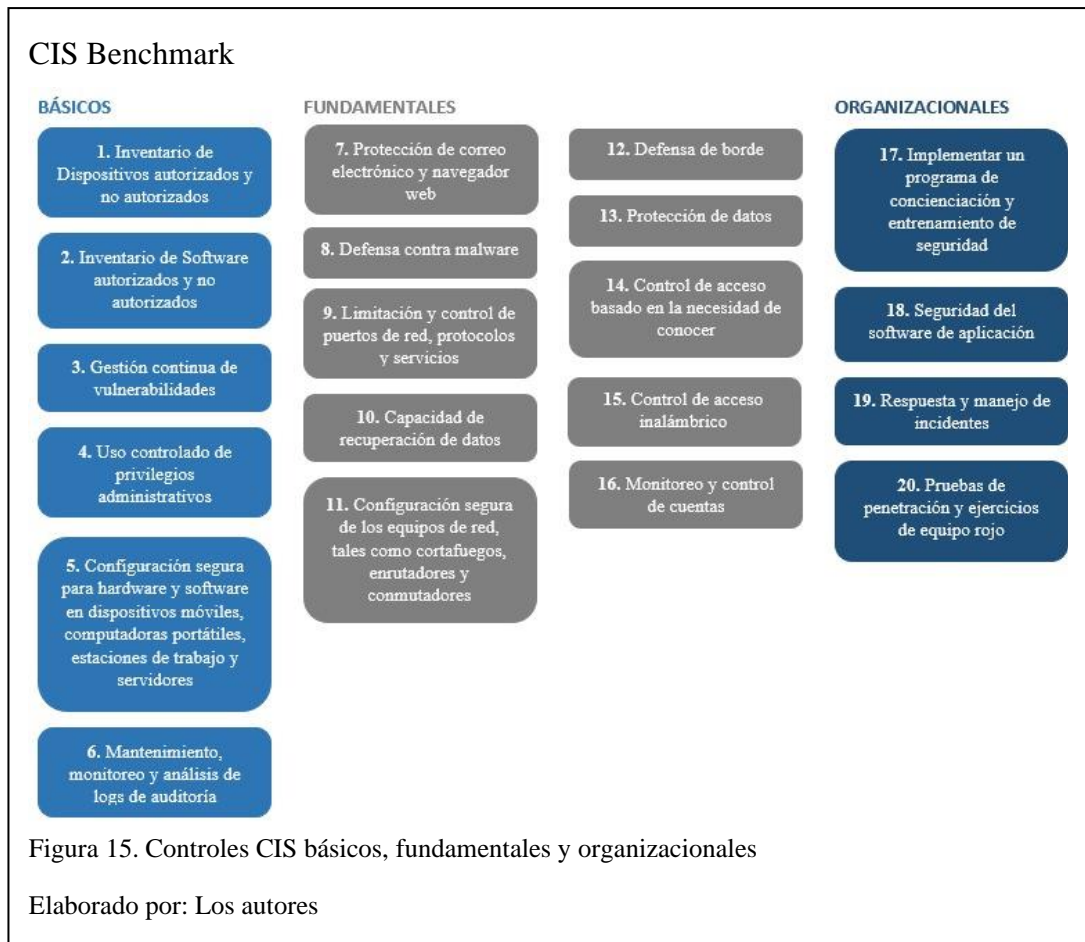
Para cumplir los objetivos de un cliente en cuanto a rendimiento, escalabilidad, disponibilidad y capacidad de administración de la red, se recomienda una variedad de técnicas de optimización. La optimización proporciona un alto ancho de banda, el bajo retardo y la fluctuación controlada que requieren muchos negocios críticos.

También es importante que un documento de diseño contenga un plan el cual debe recomendar procesos de administración y monitoreo de redes que pueden confirmar que la implementación cumple con los requisitos de rendimiento, disponibilidad, seguridad y capacidad de administración (Oppenheimer, Top Down Network Design, 2011).

2.2 Controles CIS

Según (CIS Controls, 2020) son prácticas de defensa que en conjunto sirven para mitigar los ataques más comunes contra sistemas y redes. Los desarrolladores de dichas prácticas provienen de diferentes sectores como son: educación, salud, gobierno entre otros.

Los controles CIS se desarrollaron con base en ataques reales y defensas efectivas lo cual asegura su efectividad al momento de detectar, prevenir, responder y mitigar el daño (CIS Controls, 2020).



CIS Control 1:

El primer control requiere que la organización conozca los dispositivos de su red “no se puede proteger lo que no se puede ver”. Por esta razón el primer control es catalogado como el más importante y los siguientes controles CIS se basarán en este.

Muchas de las organizaciones optan por productos integrales para mantener los inventarios de activos de TI, pero otra opción sería utilizar herramientas modestas para recopilar datos al barrer la red (CIS Controls, 2020).

CIS Control 2:

Después de implementar el primer control CIS y tener un buen manejo sobre la seguridad de los dispositivos que se encuentran ejecutando en la organización, el

siguiente paso es entender el tipo de software que se está ejecutando en esos dispositivos (CIS Controls, 2020).

El segundo control CIS se centra en la visibilidad del software en ejecución en el ambiente, se debe realizar el inventario del software en su totalidad, es decir autorizado y no autorizado para comprender de una mejor manera las vulnerabilidades y amenazas (CIS Controls, 2020).

En la actualidad la mayoría de organizaciones tienen a su disponibilidad muchas herramientas comerciales de inventario de activos y de software, ya sean gratis o pagadas (CIS Controls, 2020).

CIS Control 3:

El tercer control permite a la organización comprender y abordar las vulnerabilidades de los activos.

Para realizar el análisis de vulnerabilidades la organización se puede apoyar en las herramientas que se encuentran en Internet, las mismas que permiten la configuración de seguridad de los sistemas, lo más recomendable es que dichas herramientas midan las fallas de seguridad, las mapeen a vulnerabilidades y problemas categorizados (CIS Controls, 2020).

CIS Control 4:

El cuarto control se centra en la separación de deberes. Ayuda a minimizar el impacto de cualquier ataque que se haya realizado con éxito utilizando las credenciales del usuario comprometido para limitar la capacidad del atacante de ejecutar algún software malicioso, escalar privilegios o iniciar sesión en servidores críticos (CIS Controls, 2020).

CIS Control 5:

El quinto control abarca la configuración segura. Se establece una línea base de configuración para todos los dispositivos y el software de cada uno de ellos, posteriormente utilizarla para todas las implementaciones de sistemas nuevos que se realicen, de igual manera para auditar y monitorear las configuraciones de los sistemas actuales (CIS Controls, 2020).

CIS Control 6:

El sexto control comprende las respuestas a posibles incidentes y la detección de intrusos, así como al análisis de causa principal para problemas operativos.

La organización puede recopilar todos los registros de los sistemas críticos en base a su criterio y almacenarlos en una ubicación centralizada para que dichos registros puedan ser revisados diariamente o como se disponga (CIS Controls, 2020).

CIS Control 7:

El séptimo control explica la manera en que se pueden proteger los correos electrónicos y los navegadores web ante cualquier ataque que pueda llevarse a cabo sobre la organización (CIS Controls, 2020).

CIS Control 8:

El octavo control se centra en detectar, contener y prevenir ataques de virus y malware contra la organización. Dado que en la actualidad estos ataques son muy comunes y pueden causar mucho daño rápidamente (CIS Controls, 2020).

CIS Control 9:

El noveno control ayuda a la organización a comprender y asegurar los puertos abiertos y servicios que se encuentren en ejecución, ya que una de las principales vulnerabilidades son los crackers, generalmente realizan un barrido de puertos

buscando cuales se encuentran abiertos para empezar a tomar huellas digitales de estos servicios e identificar cualquier brecha en la red (CIS Controls, 2020).

CIS Control 10:

El décimo control se enfoca en realizar copias de seguridad de datos y respaldos de información, se prepara a la organización para recuperarse ante desastres o incidentes y del mismo modo minimizar el tiempo de inactividad necesario para que los sistemas vuelvan a estar en línea (CIS Controls, 2020).

CIS Control 11:

El décimo primer control se aplica a los dispositivos de red que son el elemento central de cualquier infraestructura de tecnología de la información (TI) y de la organización, puesto que los dispositivos de infraestructura de red poseen configuraciones predeterminadas orientadas a facilitar el despliegue y la facilidad de uso, no a la seguridad (CIS Controls, 2020).

CIS Control 12:

El décimo segundo control se enfoca en proteger y monitorear los puntos de entrada y salida de la red. Los atacantes examinan con cuidado las vulnerabilidades que se encuentran en los sistemas perimetrales para tener el acceso inicial a la red de la organización (CIS Controls, 2020).

CIS Control 13:

El décimo tercer control se enfoca en reducir el riesgo asociado con la fuga o violación de datos, se entienden como activos críticos a los datos que entran y salen de la organización, al no ser protegidos pueden ser interceptados por atacantes externos y causar anomalías (CIS Controls, 2020).

CIS Control 14:

El décimo cuarto control ayuda a la organización a limitar la capacidad de un atacante para acceder a los activos críticos, además la implementación de este control ayuda con el seguimiento de los cambios que se puedan dar en los datos confidenciales (CIS Controls, 2020).

CIS Control 15:

El décimo quinto control se enfoca en reducir los riesgos asociados con dispositivos de red inalámbrica, puntos de acceso y clientes inalámbricos. Las redes inalámbricas son susceptibles a riesgos debido a que su superficie de ataque es más amplio y fácil de alcanzar que las redes tradicionales (CIS Controls, 2020).

CIS Control 16:

El décimo sexto control se enfoca el asegurar las credenciales y mecanismos de autenticación. La importancia radica en proteger la organización ya sea de ex empleados o de usuarios malintencionados que tengan la posibilidad de ingresar la información importante (CIS Controls, 2020).

CIS Control 17:

El décimo séptimo control se enfoca en identificar los roles funcionales en la organización y las habilidades faltantes en la fuerza laboral para soportar la defensa de la empresa e incrementar la seguridad en la organización (CIS Controls, 2020).

CIS Control 18:

El décimo octavo control asegura las aplicaciones que se desarrollan al interior de la organización. El riesgo de las aplicaciones desarrolladas internamente se debe a

que son más vulnerables por a la falta de recursos para realizar las pruebas pertinentes antes de lanzar la aplicación (CIS Controls, 2020).

CIS Control 19:

El décimo noveno control se enfoca en las políticas y procesos, se centra en preparar a la organización para responder y contener un posible ataque siempre y cuando se implementen las políticas y procesos adecuados (CIS Controls, 2020).

CIS Control 20:

El vigésimo control se enfoca en identificar vulnerabilidades y debilidades de la organización antes que lo realice un atacante. Se puede realizar mediante múltiples técnicas, siguiendo la línea de proceso de pensamiento de un atacante (CIS Controls, 2020).

2.3 Nmap

Nmap es una herramienta Open Source empleada para realizar auditorías de seguridad, escaneo de redes y puertos, inventario de red, planificar actualizaciones y monitorear dispositivos o servicios de red. Escanea con gran facilidad redes grandes en intervalos de tiempo reducidos (NMAP, 2020).

2.4 Prtg network monitor

Paessler PRTG es un software de monitorización proactiva de red, que monitoriza continuamente dispositivos, sistemas y aplicaciones de tu infraestructura TI, proporcionando informes de estado y permitiendo generar alertas cuando se produce un error o los umbrales críticos (DANYSOFT, 2020). PRTG garantiza disponibilidad, rendimiento y correcto uso del ancho de banda en una red IT. La monitorización proactiva de la red permite al administrador una intervención rápida,

incluso remotamente si no se encuentra en el lugar en el que se produce el problema se pueden configurar varios puntos de presencia: todos los nodos vigilan a todos los sensores todo el tiempo, por lo que pueden comparar los tiempos de respuesta desde diferentes puntos de la red (LAN/WAN/VPN) (PAESSLER AG, 2020).

2.5 Riverbed modeler

Facilita un entorno virtual para modelar, analizar y predecir el rendimiento de las infraestructuras de TI, incluidas las aplicaciones, los servidores y las tecnologías de red. Está diseñado para complementar ejercicios de laboratorio específicos que enseñan conceptos fundamentales de redes. El software Riverbed Modeler Academic Edition está diseñado para cursos de redes de nivel introductorio y está dirigido solo con fines didácticos, incorpora herramientas para todas las fases de un estudio, incluido el diseño de modelos, simulación, recopilación y análisis de datos (RIVERBED TECHNOLOGY, 2020).

2.6 Ipv4

IPv4 es un protocolo sin conexión que se utiliza en redes de conmutación de paquetes. Opera con un modelo de entrega de mejor esfuerzo, ya que no garantiza la entrega, ni asegura la secuenciación adecuada ni evita la entrega duplicada. Estos aspectos, incluida la integridad de los datos, se tratan mediante un protocolo de transporte de capa superior, como el protocolo de control de transmisión (TCP) (ROSEN, 2014).

CAPÍTULO III

DESARROLLO DE LA METODOLOGÍA TOP-DOWN

3.1 Identificar las metas del negocio

3.1.1 Análisis de las metas del negocio y restricciones

La Institución Educativa Fiscal “Amazonas” propone una enseñanza que vaya de la mano evolutiva de la tecnología brindando información actual y veraz en las diferentes ramas de educación.

La IEFA actualmente necesita herramientas tecnológicas como Internet para complementar las actividades educativas dentro del plantel tanto para sus alumnos, docentes y personal administrativo. La necesidad se debe a la falta de conectividad a la red, la distribución errónea de cableado, la falta de políticas de seguridad en sus respaldos de información, para el inventario del software se utilizó el control 2 del CIS Benchmark (CIS Controls, 2020).

Las restricciones solicitadas por la IEFA se establecen mediante una revisión de los peligros y vulnerabilidades de la red, al depender de Internet para sus labores diarias; en la cual existen ventajas y desventajas según se utilice, dado que se tiene conectividad con el Distrito 9, con Bachillerato Internacional se debe mantener un acceso a recursos virtuales para estudiantes y accesos a plataformas de comunicación de VOIP para docentes de BI, mientras que docentes de Bachillerato General Unificado deben conectarse a medios educativos y recursos otorgados como Carmenta para subir notas de los estudiantes, por lo tanto, la velocidad de la internet debe ser distribuida para que toda la institución tenga conectividad.

3.1.2 Análisis de los Objetivos Técnicos y sus Restricciones

Mantener una administración sobre la segmentación de usuarios, definiendo y delimitando perfiles de acceso, aplicaciones y servicios que manejan, permite que se mantenga un control sobre el uso de ancho de banda. Esta segmentación se logra mediante el uso de VLAN (red virtual de área local) (Cisco System, 2020), sobre la internetwork, los usuarios consiguen mejor rendimiento en servicios y aplicaciones debido a la distribución de datos de la red.

Las autoridades de la Institución Educativa Fiscal “Amazonas” plantearon requerimientos sobre el ancho de banda que van a ser solventados con estrategias de seguridad “Cisco SCE (Cisco Service Control Engine) en el control del ancho de banda de usuario, este implica aplicar políticas y reglas por usuario, especificar su perfil y las aplicaciones más usadas” (Cisco System, 2020) y con el primer control de CIS (Center for Internet Security) con el cual se realiza un escaneo para verificar que se cuenta con el ancho de banda adecuado para verificar el historial de carga y la capacidad de la red (CIS Controls, 2020).

Se utiliza PRTG Network Monitor para obtener información de aplicaciones utilizadas en la red de la IEFA como se muestra en la Figura 16.

Resultados de sensores PRTG

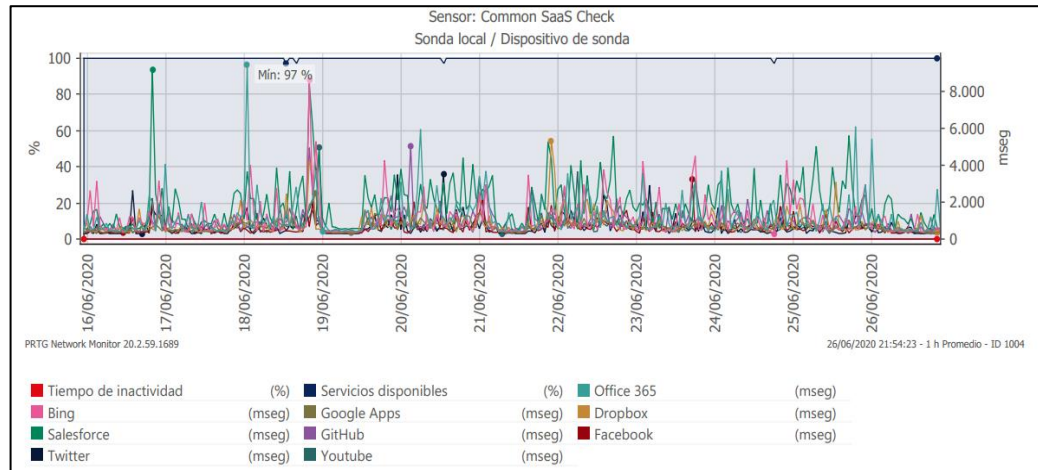


Figura 16. Monitoreo de aplicaciones utilizadas en la IEFA

Fuente: PRTG Network Monitor

Hay que tener en cuenta que el tiempo de monitoreo fue de 24 horas durante 10 días.

La auditoría de aplicaciones se muestra en la figura 17.

Aplicaciones y servicios de la IEFA

Tipo de Aplicaciones	Aplicaciones	Servicios
Navegadores Web	Bing	Cuenta con la ventaja de tener activado el filtro de contenido adulto por defecto lo cual es un beneficio al tratarse de una institución educativa.
Correo y almacenamiento en nube	Office 365	Se utiliza como correo institucional para los docentes y administrativos, es brindando por el Ministerio de Educación Distrito 9.
	Dropbox	Utilizado por los docentes para el almacenamiento de archivos.
Redes sociales	Twitter, Facebook	Herramientas interactivas y recreacionales.
Base de datos	Carmenta	Se utiliza para almacenamiento de notas, es brindando por el Ministerio de Educación Distrito 9.
Reproductor en línea	Youtube	Se utiliza como recurso de aprendizaje por parte de los docentes.
Groupware	Teams	Los docentes hacen uso de Teams para impartir clases virtuales.

Figura 17. Auditoría de aplicaciones y servicios utilizados en la IEFA

Elaborado por: Los autores

3.1.3 Acceso a Internet

La red de la IEFA según las recomendaciones de CIS controls, Cisco SCE y los requerimientos planteados, se procede a segmentar el ancho de banda manteniendo los siguientes criterios:

- Capacidad promedio para navegar en una página web.
- Capacidad de navegación para correo electrónico.
- Capacidad de comunicación mediante plataformas de VOIP.
- Capacidad de descarga de archivos.

3.1.3.1 Acceso a Página Web

Para realizar el cálculo de capacidad para navegar en una página web se utiliza el tamaño promedio que es 350 KB y un tiempo de carga que es igual a 10 segundos, teniendo en cuenta que en transmisión de datos 1Bytes/segundo es equivalente a 8bps. Las fórmulas utilizadas fueron obtenidas de (Shiguango & Lara, 2013).

$$\mathbf{CPW} = \frac{\mathbf{TpW}}{\mathbf{tpw}}$$
$$\mathbf{CPW} = \frac{350 \text{ Kilobytes}}{10 \text{ segundos}} * \frac{8 \text{ bits}}{1 \text{ Byte}}$$
$$\mathbf{CPW} = 280 \text{ Kbps}$$

Donde:

CPW: Capacidad necesaria para una página web.

Tpw: Tamaño promedio de una página web.

tpw: Tiempo que una página web demora en cargarse.

3.1.3.2 Acceso a correo electrónico

Para realizar el cálculo de capacidad necesaria para el correo electrónico se utiliza el tamaño promedio que es 1024 KB y un tiempo de carga que es igual a 10 segundos (Shiguango & Lara, 2013).

$$\begin{aligned} \mathbf{CCE} &= \frac{T_{ce}}{t_{ce}} \\ \mathbf{CCE} &= \frac{1024 \text{ Kilobytes}}{10 \text{ segundos}} * \frac{8 \text{ bits}}{1 \text{ Byte}} \\ \mathbf{CCE} &= 819.2 \text{ Kbps} \end{aligned}$$

Donde:

CCE: Capacidad necesaria para un correo electrónico.

Tce: Tamaño promedio de un correo electrónico.

tce: Tiempo que un correo electrónico demora en cargarse.

3.1.3.3 Descarga de archivos

Para realizar el cálculo de capacidad necesaria para correo electrónico se utiliza el tamaño promedio que es 10 MB y un tiempo de carga que es igual a 60 segundos (Shiguango & Lara, 2013).

$$\begin{aligned} \mathbf{CDA} &= \frac{T_{da}}{t_{da}} \\ \mathbf{CDA} &= \frac{10 \text{ MB}}{60 \text{ segundos}} * \frac{8 \text{ bits}}{1 \text{ Byte}} * \frac{1024 \text{ Kilobytes}}{1 \text{ MB}} \\ \mathbf{CDA} &= 1365.3 \text{ Kbps} \end{aligned}$$

Donde:

CDA: Capacidad necesaria para un correo electrónico.

Tda: Tamaño promedio de un correo electrónico.

tda: Tiempo que un correo electrónico demora en cargarse.

Para la segmentación del ancho de banda que requiere la IEFA se utilizarán las aplicaciones de página web, correo electrónico y las descargas de archivos con las cuales se realiza el cálculo para la capacidad de simultaneidad de las aplicaciones (Shiguango & Lara, 2013).

Porcentaje de simultaneidad			
Aplicación	Capacidad de la capa aplicación	Porcentaje de Simultaneidad	Capacidad de Simultaneidad
Página Web	280 Kbps	9%	25.2 Kbps
Correo Electrónico	819.2 Kbps	8%	65.54 Kbps
Descarga de archivos	1365.3 Kbps	6%	81.92 Kbps

Figura 18. Capacidad de Simultaneidad

Elaborado por: Los autores

La capacidad de un usuario para acceder a Internet se calcula mediante:

$$CU = CPW + CCE + CDA$$

$$CU = 25.2 \text{ Kbps} + 65.54 \text{ Kbps} + 81.92 \text{ Kbps}$$

$$CU = 172.66 \text{ Kbps}$$

Donde:

CU: Capacidad necesaria para que un usuario acceda a Internet.

En la tabla 2 se denota que la capacidad requerida para conexión de Internet es de 128113,72 Kbps o lo que son 128,11 Mbps, considerando un crecimiento futuro del 30% dentro de los próximos 5 años, se tendría un ancho de banda de 166.55 Mbps (Shiguango & Lara, 2013).

Tabla 2. Capacidad de ancho de banda requerido

Áreas IEFA	USUARIOS	Capacidad requerida (Kbps)
Rectorado	4	690,64

Vicerrectorados	8	1381,28
Biblioteca	20	3453,2
DECE	16	2762,56
Enfermería	4	690,64
Estudiantes	600	103596
Inspección	8	1381,28
Laboratorio de Computación	20	3453,2
Laboratorios de Física	6	1035,96
Laboratorios de Química	6	1035,96
Sala de Profesores	18	3107,88
Sala de Profesores Bachillerato Internacional	20	3453,2
Secretaría	4	690,64
Secretaría General	8	1381,28
TOTAL	742	128113,72

Elaborado por: Los autores

3.1.3.4 Telefonía IP

El cálculo de ancho de banda para transmitir VOIP tiene que utilizar la compresión de cabecera, la compresión de silencios y el códec (Shiguango & Lara, 2013).

Tiempo de encapsulación			
Codéc	Tasa Binaria	Tamaño PDU	Tiempo de Encapsulación
G.711	64 Kbps	160 Bytes	20ms
G.726	32 Kbps	80 Bytes	20ms
G.729	8 Kbps	20 Bytes	20ms
G.723.1	6,3 Kbps	24 Bytes	20ms
G.723.1	5,3 Kbps	20 Bytes	20ms

Figura 19. Principales códec para compresión de voz

Elaborado por: Los autores

La figura 20 muestra los tamaños de cabecera de los protocolos que intervienen en la transmisión de voz utilizando el códec G.729 (Shiguango & Lara, 2013).

Tamaño de voz

Protocolo	Tamaño
Payload	20 Bytes
Cabecera RTP	12 Bytes
Cabecera UDP	8 Bytes
Cabecera IP	20 Bytes
Tamaño Total	60 Bytes

Figura 20. Cabecera de protocolos para voz

Elaborado por: Los autores

En la figura 21 se indica el número de extensiones de VOIP por área y según el cargo.

Identificación de extensiones de voz

Área	Cargo	Número de extensión
Rectorado	Rector	101
	Vicerrector	102
	Vicerrectora	103
	Secretaria	104
Laboratorios	Laboratorio Química	201
	Laboratorio Física	202
Bachillerato Internacional	Sala de profesores BI	301
	Jefe de BI	302
Departamento de Consejería Estudiantil	Jefe DECE	401
Biblioteca	Bibliotecaria	501
Enfermería	Jefe de enfermería	601
Secretaría General	Secretaria General	701
Sala de profesores	Profesores	801
Inspección	Inspector	901
	Sub Inspector	902

Figura 21. Distribución de extensiones telefónicas

Elaborado por: Los autores

3.1.3.5 Base de datos

Para realizar el cálculo de capacidad necesaria para acceder a la base de datos del Distrito 9 desde la IEFA, se utiliza un tamaño de 120 KB y un tiempo de acceso de 5 segundos (Shiguango & Lara, 2013).

$$\mathbf{CASIS} = \frac{\mathbf{Tasis}}{\mathbf{tasis}}$$

$$\mathbf{CASIS} = \frac{120 \text{ Kbytes}}{5 \text{ segundos}} * \frac{8 \text{ bits}}{1 \text{ Byte}}$$

$$\mathbf{CASIS} = 192 \text{ Kbps}$$

Donde:

CASIS: Capacidad necesaria para acceder al sistema.

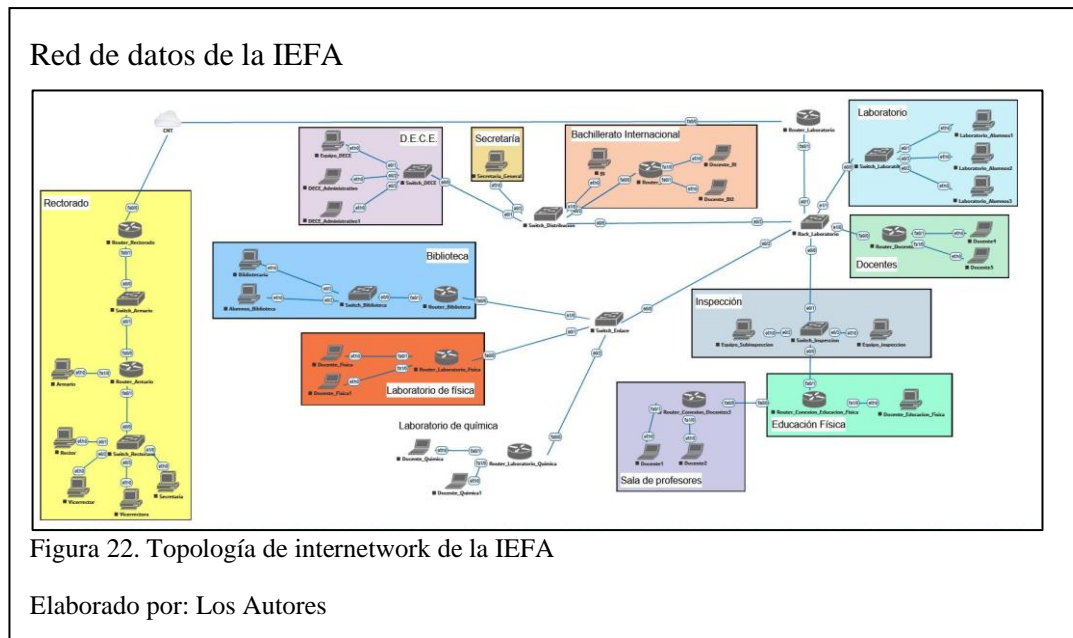
Tasis: Tamaño promedio de la información enviada hacia el sistema.

tasis: Tiempo promedio de respuesta del sistema.

3.1.4 Caracterización de la Red Existente

La Institución Educativa Fiscal “Amazonas” posee acceso a Internet provisto por la Cooperación Nacional de Telecomunicaciones (CNT), dispone de equipos de redes como: Router PON, switch, router inalámbrico, tarjetas de inalámbricas PCI computadoras y laptops. La institución educativa cuenta con una red cableada en las áreas administrativas, áreas de Bachillerato General Unificado, de Bachillerato Internacional y áreas comunales como se indica en la Figura 22, pero estas se encuentran limitadas por el cableado mal implementado, la falta de balanceo de carga en consumo de ancho de banda, lo cual se refleja en el manejo de una IP privada 192.168.100.0/24 en DHCP para toda la institución lo que provoca que no todos puedan acceder a Internet por el número de usuarios, en cuanto a cobertura inalámbrica

no poseen acceso todos los estudiantes, la ubicación de la infraestructura no permite hacer uso de los recursos a los que tiene acceso porque se presentan problemas al compartir recursos de hardware y software, esto radica en una ralentización en el proceso de aprendizaje por parte de los estudiantes y falta de acceso a recursos para docentes.



3.1.4.1 Caracterización del cableado y de los medios

Según (Oppenheimer, Top-Down Network Design, 2011) para intentar cumplir los objetivos de escalabilidad y disponibilidad para el diseño de red, es importante comprender el diseño del cableado y el cableado de la red existente, la IEFA dispone de un etiquetado de red sin estándar y conexiones cableadas desarrolladas según la necesidad de acceso a Internet, pero sin tomar en cuenta distancias de cableado LAN con lo que se pierde la calidad de servicio de la red.

La distribución del cableado es horizontal, vertical y entre bloques manejando una topología tipo estrella como se muestra en la Figura 23.

Diagrama de Bloques



Figura 23. Ubicación de Bloques de la IEFA

Elaborado por: Los autores

La Institución Educativa Fiscal Amazonas posee diez bloques distribuidos de la siguiente forma:

1. Rectorado.
2. Laboratorios.
3. DECE-Secretaría-Bachillerato Internacional-Biblioteca.
4. Laboratorio Computación.
5. Bachillerato BGU.
6. Inspección.
7. Bachillerato BGU.
8. Sala de Profesores.
9. Bachillerato BGU.
10. Auditorio.

Las áreas cinco, siete y nueve no disponen de cableado de red, por lo tanto, los estudiantes no poseen acceso a Internet.

Cableado área Rectorado

Rectorado			
Dispone de armario de telecomunicaciones			
Ubicación de salas de interconexión y demarcaciones a redes externas			
Cableado vertical			
	Fibra Óptica	Categoría 5e UTP	Categoría 6 UTP
Eje vertical 1	x	x	
Cableado Horizontal			
	Fibra Óptica	Categoría 5e UTP	Categoría 6 UTP
Primer Piso	x	x	
Cableado Área de Trabajo			
	Fibra Óptica	Categoría 5e UTP	Categoría 6 UTP
Primer Piso	x		x

Figura 24. Cableado de Bloque 1

Elaborado por: Los autores

Cableado áreas DECE-Secretaría-Bachillerato Internacional

DECE-Secretaría-Bachillerato Internacional			
Cableado vertical			
	Fibra Óptica	Categoría 5e UTP	Categoría 6 UTP
Eje vertical 1		x	
Eje vertical 2		x	
Cableado Horizontal			
	Fibra Óptica	Categoría 5e UTP	Categoría 6 UTP
Primer Piso		x	
Segundo Piso		x	
Cableado Área de Trabajo			
	Fibra Óptica	Categoría 5e UTP	Categoría 6 UTP
Primer Piso		x	x
Segundo Piso		x	x

Figura 25. Cableado de Bloque 3

Elaborado por: Los autores

Cableado áreas de Laboratorio de Computación

Laboratorio de Computación			
Dispone de armario de telecomunicaciones			
Ubicación de salas de interconexión y demarcaciones a redes externas			
Cableado vertical			
	Fibra Óptica	Categoría 5e UTP	Categoría 6 UTP
Eje vertical 1		x	
Eje vertical 2		x	
Eje vertical 3	x	x	
Cableado Horizontal			
	Fibra Óptica	Categoría 5e UTP	Categoría 6 UTP
Primer Piso		x	
Segundo Piso		x	
Tercer Piso		x	
Cableado Área de Trabajo			
	Fibra Óptica	Categoría 5e UTP	Categoría 6 UTP
Primer Piso		x	x
Segundo Piso		x	x
Tercer Piso		x	x

Figura 26. Cableado Bloque 4

Elaborado por: Los autores

Cableado área de Inspección

Inspección			
Cableado vertical			
	Fibra Óptica	Categoría 5e UTP	Categoría 6 UTP
Eje vertical 1			x
Cableado Horizontal			
	Fibra Óptica	Categoría 5e UTP	Categoría 6 UTP
Primer Piso			
Segundo Piso			x
Cableado Área de Trabajo			
	Fibra Óptica	Categoría 5e UTP	Categoría 6 UTP
Primer Piso			
Segundo Piso		x	x

Figura 27. Cableado de Bloque 6

Elaborado por: Los autores

3.1.4.2 Comprobación del estado de la Internetwork

En la red de la Institución Educativa Fiscal “Amazonas” existen horas de tráfico generado por jornadas las cuales son de 10:00 a 12:00 en jornada matutina y de 14:00 a 19:00 en jornada vespertina que corresponde a la mayor demanda de la red.

Horario de uso de Internet

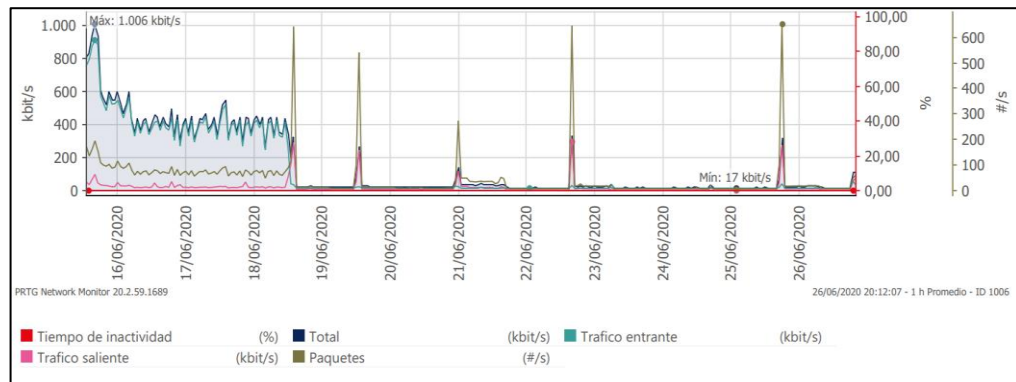


Figura 28. Demanda de Internet obtenida por PRTG

Fuente: PRTG Network Monitor

La salud de los dispositivos de red no es correcta por lo que se denota varias caídas en la navegación a Internet, con lo cual los equipos no encuentran la convergencia correcta para satisfacer las necesidades de la institución, además la falta de dominios de colisión junto con la inexistencia de VLANs producen que entre dispositivos se expulsan de los routers inalámbricos, así como los que se encuentran cableados. Al tratar de mantener IP estático no se procedió con el proceso de escalabilidad de la red, permitiendo que se vea afectada la disponibilidad y la confidencialidad de los usuarios. El rendimiento de la red se encuentra identificado en la figura 29.

Porcentaje de uso de la red de datos

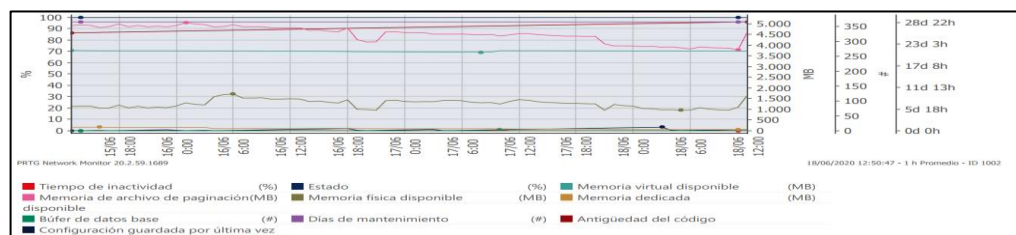
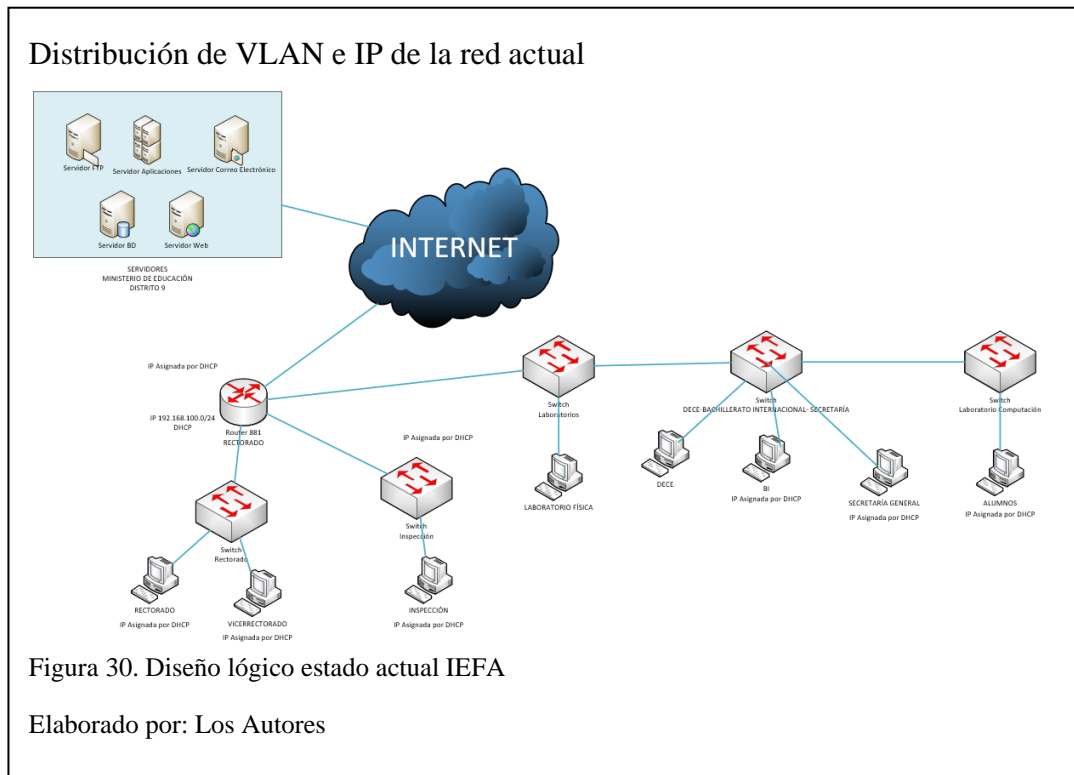


Figura 29. Rendimiento de la red IEFA

Fuente: PRTG Network Monitor

La figura 30 indica el estado actual del diseño lógico de la red de la IEFA.



3.2 Propuesta diseño lógico de la red

Esta fase se relaciona el diseño lógico de la red con los objetivos de la institución para tener escalabilidad y adaptabilidad (Huerta, 2013), por lo tanto, se analiza la distribución de los equipos, junto con estrategias de gestión y de seguridad para que la red evite problemas y fallas en la internetwork para tener un rendimiento estable en la red.

Esta fase se descompone en:

- Diseñar una Topología de red.
- Diseño de Modelo de Direccionamiento y Nombramiento.
- Desarrollo de estrategias de Seguridad de la Red.
- Desarrollo de estrategias de Gestión de la Red.

3.2.1 Topología de red

Para un diseño de topología de red se toman en cuenta los equipos a interconectar, las aplicaciones que se conectan, al igual que el tráfico que soporta la internetwork junto con la escalabilidad y la adaptabilidad (Huerta, 2013).

3.2.1.1 Selección de la topología de red

Para la red de la Institución Educativa Fiscal “Amazonas” se tiene acceso a Internet por dos conexiones, mediante fibra óptica provista por la Corporación Nacional de Telecomunicaciones en los bloques de rectorado y laboratorio, para el rediseño y después de realizar las mediciones de distancias entre bloques y siguiendo el modelo jerárquico de tres capas, se toma en consideración poner un armario en el bloque de Inspección como nodo central para dar conectividad a toda la institución.

3.2.2 Modelo de Direccionamiento y Nombramiento

La asignación de IP privadas para la internetwork de la Institución Educativa Fiscal “Amazonas” estará dividida en diez áreas que se dispondrán según las necesidades de cada departamento y tomando en cuenta un escalamiento de 30% a futuro, se mantendrá una red con un vlsn de la red 192.168.0.0/21 la cual se encuentra en el segmento de red que el ISP proporciona para acceder a Internet. Las VLANS configuradas se muestran en la figura 31.

VLAN y rango utilizable para la IEFA

VLAN	ÁREAS IEFA	Host Necesarios	Subred	Máscara de Subred	Máscara	Rango Utilizable	Broadcast
10	Administrativos	30	192.168.3.64	/27	255.255.255.224	192.168.3.65 - 192.168.3.94	192.168.3.95
15	Bachillerato Internacional	126	192.168.2.0	/25	255.255.255.128	192.168.2.1 - 192.168.2.126	192.168.2.127
20	Biblioteca	30	192.168.3.96	/27	255.255.255.224	192.168.3.97 - 192.168.3.126	192.168.3.127
25	Docentes	126	192.168.2.128	/25	255.255.255.128	192.168.2.129 - 192.168.2.254	192.168.2.255
30	Inspección	30	192.168.3.128	/27	255.255.255.224	192.168.3.129 - 192.168.3.158	192.168.3.159
35	Laboratorio Física/Química	30	192.168.3.160	/27	255.255.255.224	192.168.3.161 - 192.168.3.190	192.168.3.191
40	Laboratorio Computación	62	192.168.3.0	/26	255.255.255.192	192.168.3.1 - 192.168.3.62	192.168.3.63
45	Departamento de Consejería Estudiantil (DECE)	30	192.168.3.192	/27	255.255.255.224	192.168.3.193 - 192.168.3.222	192.168.3.223
50	Secretaría General	6	192.168.4.0	/29	255.255.255.248	192.168.4.1 - 192.168.4.6	192.168.4.7
55	Inalámbricas	510	192.168.0.0	/23	255.255.254.0	192.168.0.1 - 192.168.1.254	192.168.1.255
60	VOIP	30	192.168.3.224	/27	255.255.255.224	192.168.3.225 - 192.168.3.254	192.168.3.255

Figura 31. Direccionamiento IPv4 para la IEFA

Elaborado por: Los autores

3.2.2.1 Enrutamiento

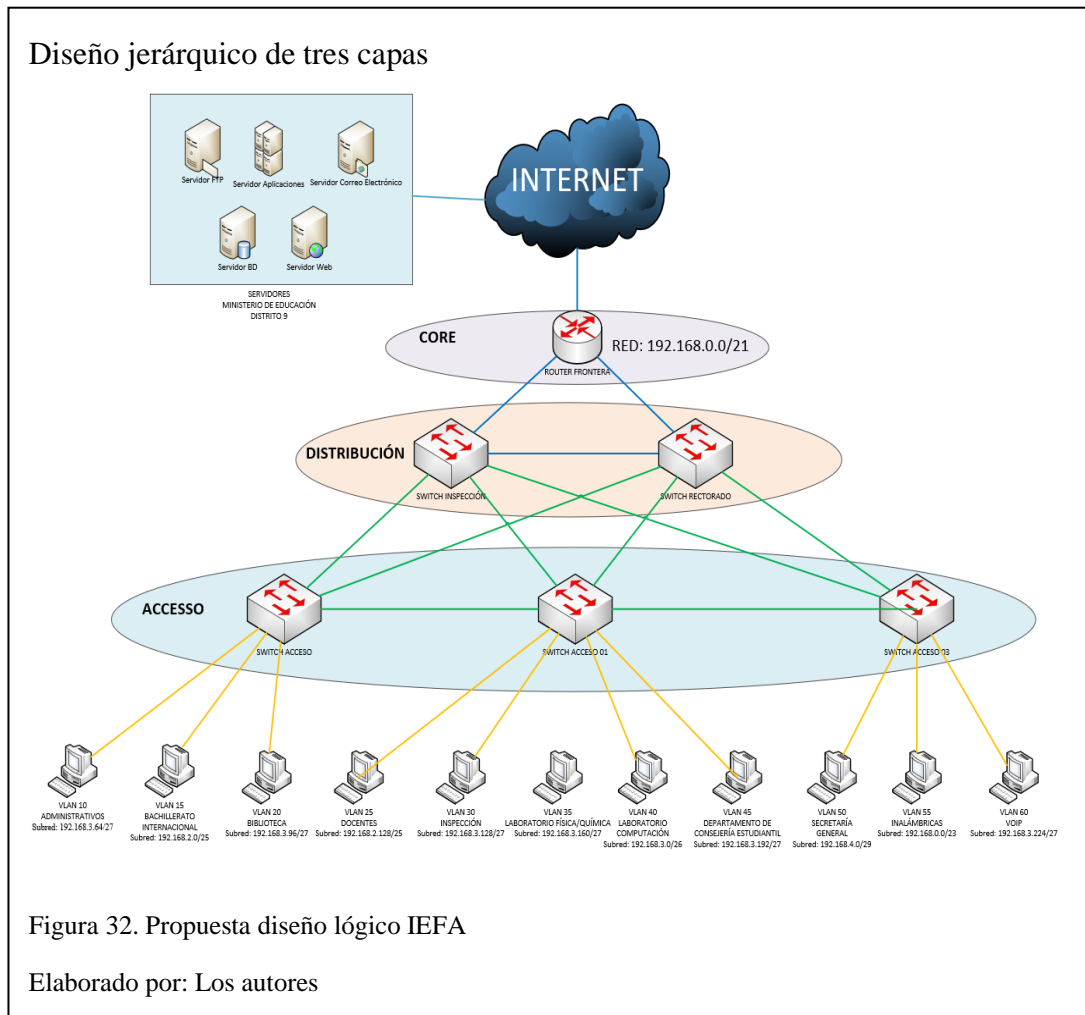
Es el proceso en el que los enrutadores aprenden sobre redes remotas, con lo cual se determina por donde enviar los paquetes de IP, para que eventualmente lleguen a su red destino escogiendo la mejor ruta para intercambiar datos entre las mismas (Community Cisco, 2020). Para el enrutamiento de la internetwork de la IEFA y la convergencia hacia redes externas se procede a utilizar OSPF.

3.2.2.2 Configuración

En la IEFA se utilizarán DHCP para las VLANS antes mencionadas, mientras que para los equipos en los que se va a enrutar se manejan IP dinámicas siguiendo el direccionamiento de las tablas 15 y 16 respectivamente.

Los dispositivos de la IEFA deben ser configurados de forma segura (CIS Controls, 2020), el control 5 se aplica al manejo de licencias para el software y antivirus.

En la figura 32 se indica la propuesta de diseño lógico para la red de la IEFA.



3.2.3 Desarrollo de estrategias de Seguridad de la Red

Se entiende como seguridad al conjunto de actividades o normas, las cuales al ser empleadas previenen y protegen a la organización de cualquier evento adverso suscitado por algún usuario mal intencionado o ante una intrusión no autorizada.

Activos de la IEFA

Activos	Riesgos	Requerimientos de seguridad
Firewall	<ul style="list-style-type: none"> - No se puede proteger contra los ataques cuyo tráfico no pase a través del firewall. - No pueden proteger a la red contra un ataque interno. - Son vulnerables a los ataques de ingeniería social y a virus. 	<ul style="list-style-type: none"> - Configurar correctamente los servicios y protocolos cuyo tráfico este permitido. - Se aplica la política restrictiva es decir se deniega todo el tráfico excepto el que está explícitamente permitido.
Router	<ul style="list-style-type: none"> - Robo de datos personales, información importante y/o credenciales. 	<ul style="list-style-type: none"> - Habilitar la configuración AAA. - Establecer contraseñas seguras, preferiblemente encriptadas. - Designar listas de control de acceso (ACL). - Habilitar la conexión (SSH) para cada inicio de sesión remota. - Limitar los dispositivos que se conecten al router mediante el filtrado MAC.
Switch	<ul style="list-style-type: none"> - Una persona externa sin autenticación puede acceder a información confidencial y provocar ataques de denegación de servicio. 	<ul style="list-style-type: none"> - Habilitar la configuración AAA. - Configurar los puertos del switch para que ingresen únicamente las tramas con direcciones MAC de origen específico. - Desactivar los puertos y servicios que no se utilicen.
ACCESS POINT	<ul style="list-style-type: none"> - Usuarios mal intencionados conectados a la red WIFI podrían realizar ataques de fuerza bruta o inyectar malware en servidores que carecen de seguridad adecuada. 	<ul style="list-style-type: none"> - Cambiar la contraseña de accesos a su panel de administración. - Cambiar la contraseña del WIFI con el cifrado WPA2.
Computadores	<ul style="list-style-type: none"> - Son susceptibles a ataques que violen la confidencialidad, integridad, disponibilidad y control de acceso del sistema o de datos personales. 	<ul style="list-style-type: none"> - Actualizar con regularidad el software con los últimos parches. - Activar el firewall. - Establecer usuarios por cada dispositivo con contraseñas seguras. - Instalar software de seguridad (antivirus).

Figura 33. Plan de gestión para dispositivos de la IEFA

Elaborado por: Los autores

3.2.3.1 Mecanismos de seguridad

3.2.3.1.1 Seguridad física

Los dispositivos reconocidos como activos de la institución (firewall, router y switch) se deberían mantener lo más alejados de los estudiantes y personal no autorizado, por tal motivo estarán colocados en la segunda planta del bloque 6 (inspección) bajo llave para cuyo ingreso se requiere una identificación, de tal manera que se puedan evitar accidentes como: incendios, inundaciones, interrupción de servicios, radiaciones y robo.

Hay que establecer el inventario de dispositivos autorizados y no autorizados (CIS Controls, 2020), apoyándose en el control 1, solo los dispositivos autorizados tienen acceso a la red, se registran los dispositivos mediante su dirección MAC debido

a que los docentes y administrativos cuentan con laptops personales suministrados por parte del Distrito.

Por otro lado, la seguridad también cubre los distintos métodos que se adquieran para proteger la información importante dentro de la IEFA, por este motivo la estrategia que se lleva a cabo es: realizar un respaldo de los datos sensibles del bloque 1 (rectorado), bloque 3 (secretaría, DECE y docentes de bachillerato internacional), bloque 6 (inspección) y bloque 8 (docentes) en la nube debido a su seguridad, también se puede implementar el uso de un disco duro individual para cada docente y/o administrativo el cual debe estar correctamente encriptado para evitar la fuga de datos.

Se debe tener una gestión continua de vulnerabilidades (CIS Controls, 2020), usando el control 3, con la información recopilada es prudente tomar medidas efectivas que contrarresten la deficiencia de la red y evitar que los sistemas informáticos se vean comprometidos.

3.2.3.1.2 Autenticación

Para ingresar a la red de la IEFA el usuario debe ingresar una contraseña la cual debe constar de mínimo 8 caracteres alfanuméricos y especiales.

Cada contraseña es individual dependiendo del bloque y de los usuarios, es decir, los estudiantes y docentes, así como los administrativos no compartirán una misma contraseña con el fin de evitar la sobre carga del ancho de banda y acceso de personas no autorizadas a los diferentes departamentos de la institución.

3.2.3.1.3 Autorización

Cada dispositivo que conforma la red cuenta con un perfil de Administrador, el cual tendrá los privilegios pertinentes para modificar la red según sus necesidades.

Únicamente los administradores de red tendrán acceso a los dispositivos mediante un usuario y una contraseña previamente configurada.

Los dispositivos (firewall, router y switch) se encuentran en el bloque 6 (inspección), las personas que pueden acceder a esta área son:

- Administrador de red.
- Inspector.
- Personal del departamento de inspección.

Cada dispositivo está configurado para que el administrador de red acceda al sistema operativo con privilegio de administrador y realice las adecuaciones necesarias.

Se debe tener en cuenta que dentro de la red puedan existir usuarios mal intencionados razón por la cual se establece el uso controlado de privilegios administrativos (CIS Controls, 2020) , para el control 4 se deben verificar continuamente que los usuarios con altos privilegios no utilicen dichas cuentas para navegar diariamente por la red ya que pueden ser susceptibles a ataques por parte de crackers.

3.2.3.1.4 Auditoría

Los datos que se deberían recopilar con mayor énfasis son los intentos de autenticación a la red, se utiliza el subcontrol 4.9 cuyo propósito es registrar y alertar los inicios de sesión fallidos a cuentas administrativas (CIS Controls, 2020), basado en el control 4, se puede programar mediante scripts en Shell.

3.2.4 Desarrollo de estrategias de Gestión de la Red

Las estrategias de gestión de la IEFA se basan en la operación y control de los activos que constituyen la red, de esta manera se puede asegurar el rendimiento, disponibilidad y escalabilidad de la red.

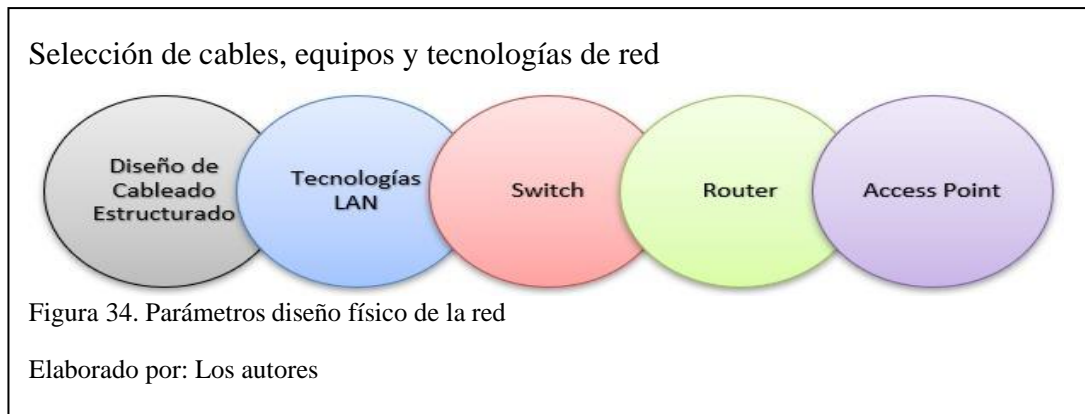
Se documentará toda la red, almacenando el histórico y configuración de cada dispositivo en soportes magnéticos u ópticos, debido a que en caso de presentar falla el administrador de red pueda hacer uso de estos y los equipos puedan ser restablecidos en el menor tiempo posible proporcionando la disponibilidad inmediata.

Se debe tener en cuenta que una de las estrategias primordiales debe ser la capacidad de recuperación de datos (CIS Controls, 2020) el cual corresponde al control 10, según denota el procedimiento se debe realizar una prueba periódicamente en el que se evaluará una muestra de las copias de la seguridad con la intención de restaurarlas, las restauraciones deben verificarse para garantizar que el sistema completo se encuentre intacto y funcional.

3.3 Propuesta diseño físico de la red

Es necesario la selección de equipos y tecnologías para lo cual se realiza una comparación entre los diferentes dispositivos de red que existen en el mercado manteniendo los parámetros de escalabilidad, seguridad, rendimiento y el factor económico para poder abarcar las necesidades de la Institución Educativa Fiscal “Amazonas” con respecto a la infraestructura de la internetwork.

Para el diseño físico se utiliza los siguientes parámetros:



3.3.1 Cableado estructurado para para Institución Educativa Fiscal “Amazonas”

Según las necesidades de la IEFA y su espacio físico se plantea el rediseño de cableado estructurado cambiando a UTP categoría 6 puesto que por su precio y versatilidad se acopla a las modificaciones que reciben las áreas de trabajo en los diferentes bloques. El mismo se utilizará para la conexión de los dispositivos de la internetwork por medios guiados y para las conexiones por medios no guiados se maneja una red de frecuencia 2.4 GHz para los docentes, alumnos e invitados que se conecten a la internetwork. El cableado de la Institución Educativa Fiscal “Amazonas” adquiere un rediseño cumpliendo las normas internacionales ANSI/TIA/EIA.

3.3.2 Criterios de diseño del cableado estructurado

3.3.2.1 Cableado horizontal

El cableado horizontal tiene que manejar varias aplicaciones como: comunicaciones de voz, comunicaciones de datos y redes de área local que utilizan los usuarios, a su vez la distribución horizontal se encuentra diseñada para facilitar el mantenimiento y reubicación de áreas de trabajo (Shiguango & Lara, 2013).

La topología del cableado será tipo estrella con un cable de salida para las áreas de trabajo y todos los cables de corrida horizontal deben terminar en paneles (Shiguango & Lara, 2013).

Las canalizaciones son las que vinculan la sala de equipos con los armarios de comunicaciones, se debe instalar escalerillas siguiendo la norma TIA-586C, además deberán llenarse desde un 40% hasta un 60% de su capacidad máxima para poder aumentar los cables según la necesidad de escalabilidad, Las escalerillas mantienen una distancia sobre el cielo falso de 30cm de la losa, para poder descender por la pared se utilizan canaletas decorativas.

3.3.2.2 Cableado vertical (Back-bone)

El rediseño del cableado para conectar las plantas de cada bloque es desde el punto que recibe la conexión a Internet mediante tubería, con esto se obtiene un beneficio en aseguramiento y protección de los cables mientras mantiene un diseño visualmente estético.

La topología del cableado será tipo estrella y se utilizarán cables UTP y cables de fibras ópticas 62.5/125 um (Shiguango & Lara, 2013).

3.3.2.3 Cuarto de telecomunicaciones

Se encuentra el armario principal MDF con los equipos y patch panel para recibir el cableado UTP categoría 6A, este cuarto se va encontrar ubicado en el Bloque de Inspección para transmitir el cableado horizontal y vertical para la institución.

Las consideraciones para cuartos de telecomunicaciones según la norma ANSI/EIA/TIA 569 son (Shiguango & Lara, 2013):

- Área mínima de 6 m².
- Aire acondicionado para mantener la temperatura de los equipos de red.
- Mínimo de un armario por piso.
- Acceso a personal autorizado.

Al diseñar el cuarto de telecomunicaciones se debe tener en cuenta:

- Conexión entre cuartos de telecomunicaciones.
- Puertas.
- Control de Temperatura.
- Protección contra fuego.
- Iluminación.
- Localización.
- Seguridad.

3.3.2.4 Distribución del rack

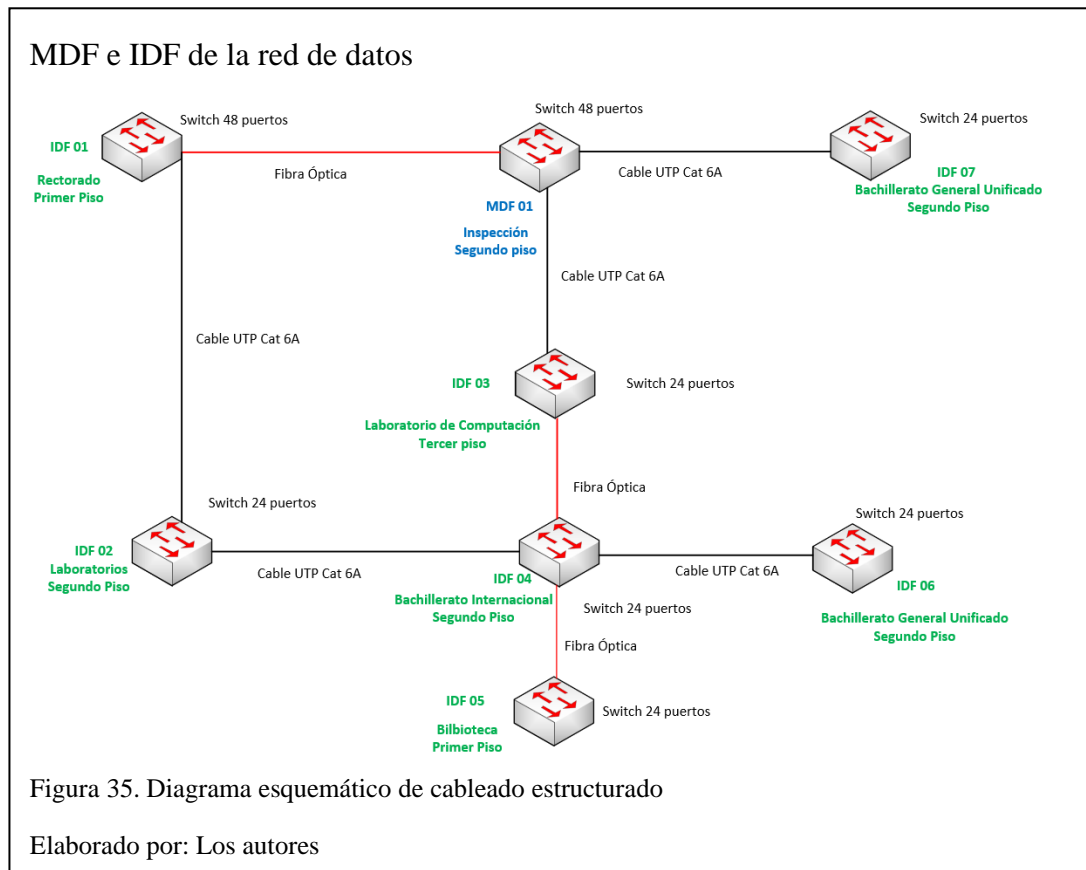
Para la propuesta de rediseño se recomienda utilizar rack de piso cerrados de 19” con lo que se manejará 1 MDF y 7 IDF que enlazan todos los bloques de la IEFA.

Cuarto de equipos

Se encuentra ubicado en el Bloque de Rectorado y cumple con los estándares ANSI/EIA/TIA 568-B y ANSI/TIA/EIA 569-A, además se utiliza las siguientes consideraciones (Shiguango & Lara, 2013):

- Área mínima de 12 m².
- Acceso solo al personal autorizado.
- Incorporar sistemas a tierra.
- Tiene que tener buena iluminación.
- Tomas eléctricas en circuitos separados.

En la figura 35 se muestra el diagrama esquemático de la red indicando los mdf e idf necesarios.



3.3.2.5 Áreas de trabajo

Se encuentran formadas por los elementos que el usuario utiliza para conectarse a los servicios de comunicaciones, se encuentra formado por los cables de usuarios, la toma de pared y los dispositivos (Shiguango & Lara, 2013).

Las consideraciones para las estaciones de trabajo son:

- Dos puntos de red para voz y datos.
- Cable UTP categoría 6A certificado con una distancia de 2,5 metros.
- Código de colores para los RJ45 es el T568B (Shiguango & Lara, 2013).

En la figura 36 se indica la cantidad de puntos de red actual que son 69 y la propuesta de la nueva distribución de puntos para cumplir con los requerimientos de la escalabilidad en un futuro, obteniendo un total de 217 puntos para la IEFA.

Propuesta de voz y datos

Áreas IEFA	Actual		Propuesta			Total
	Datos	Voz	Datos	Voz	Impresoras	
Rectorado	1	0	4	1	1	6
Vicerrectorados	3	0	8	2	1	11
Biblioteca	10	0	20	1	1	22
DECE	8	0	16	2	1	19
Enfermería	0	0	4	1	1	6
Inspección	4	0	8	2	1	11
Laboratorio de Computación	15	0	26	0	0	26
Laboratorios de Física	6	0	10	1	1	12
Laboratorios de Química	6	0	10	1	1	12
Sala de Profesores	4	0	30	1	1	32
Sala de Profesores Bachillerato Internacional	6	0	20	1	1	22
Secretaría	2	0	6	1	1	8
Bachillerato General Unificado	0	0	10	0	0	10
Secretaría General	0	0	8	1	1	10
TOTAL	69					217

Figura 36. Propuesta de puntos de red para la IEFA

Elaborado por: Los autores

3.3.2.6 Diseño red de datos

Pensando en la escalabilidad de la red se decidió colocar 8 rack con sus respectivos switches, patch panel y demás componentes. En la figura 37 se detalla: la unidad de rack cerrados, la cantidad de switches con sus puertos y los patch panel manteniendo en la infraestructura categoría de cableado 6A (Shiguango & Lara, 2013).

Asignación de rack para cada bloque

Bloque	Piso	Rack	Patch Panel	Equipo
Inspección	Piso 2	40U	48 puertos	1 Switch 48 puertos
Rectorado	Piso 1	20U	48 puertos	1 Switch 48 puertos
Laboratorios	Piso 2	12U	24 puertos	1 Switch 24 puertos
Bachillerato General Unificado	Piso 2	12U	48 puertos	2 Switch 48 puertos
Bachillerato Internacional	Piso 2	6U	24 puertos	1 Switch 24 puertos
Biblioteca	Piso 1	6U	24 puertos	1 Switch 24 puertos
Laboratorio de Computación	Piso 3	6U	24 puertos	1 Switch 24 puertos

Figura 37. Cantidad de rack y switches

Elaborado por: Los autores

La simbología a utilizar para el rediseño de la internetwork de la Institución Educativa Fiscal “Amazonas” es como se muestra en la figura 38.

Simbología








SIMBOLOGÍA	
SÍMBOLO	DESCRIPCIÓN
	Access Point
	Salida de Voz – Datos en pared
	Salida de Voz – Datos en el suelo
	Caja de revisión de pared 20X20
	Bandeja de piso 10X6
	Tubería EMT
	Caja de paso 20X20X9

Figura 38. Simbología de voz-datos, bandejas y tuberías

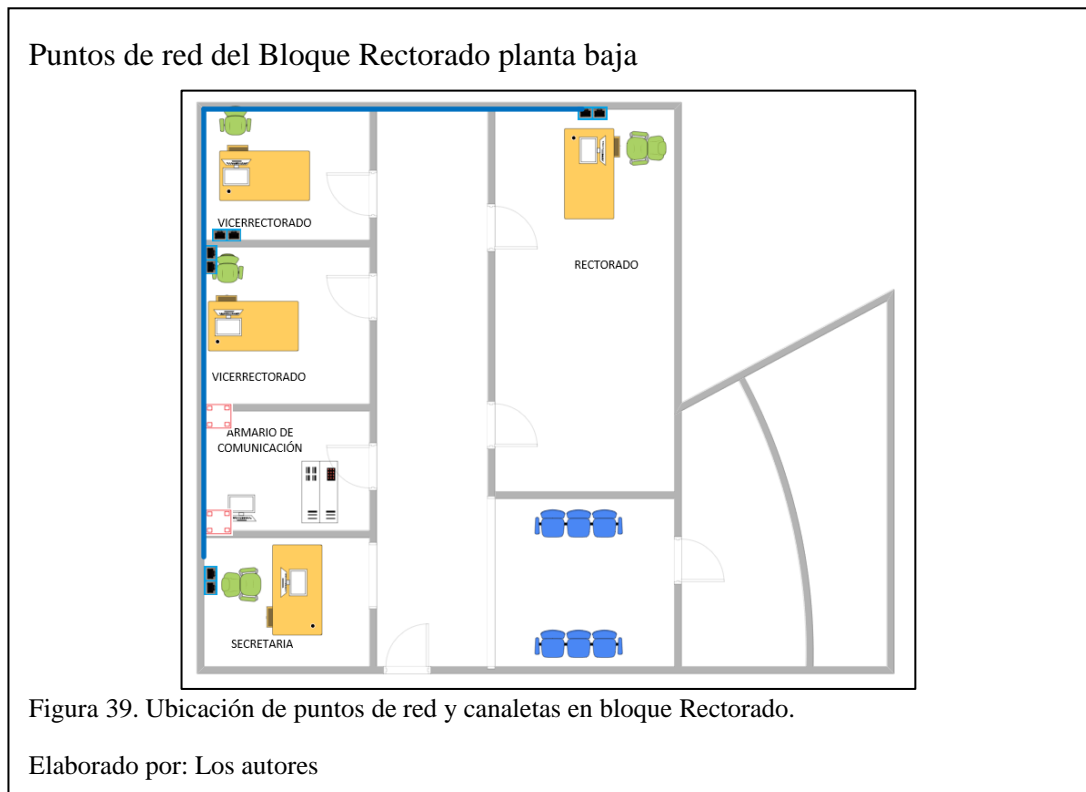
Elaborado por: Los autores

La propuesta mantiene que por cada usuario de la red se tengan dos puntos de red para lo cual se realiza los siguientes planos por áreas de trabajo.

3.3.2.7 Diseño de cableado estructurado Rectorado

En el rediseño se utiliza el rack que se encuentra en el armario de comunicaciones de Rectorado identificado como Bloque 1, repartiendo cables UTP a

través de bandeja de piso hacia los puntos de salida de voz - datos en la pared de cada área.



3.3.2.8 Diseño de cableado estructurado Inspección

En el bloque 6 se rediseña para instalar un cuarto de comunicaciones donde se instala el rack 2, el firewall, y desde esta área se repartirá el Internet al resto de la institución, esta área se encuentra ubicada en el segundo piso como se indica en la figura 40.

Puntos de red del Bloque Inspección Segundo Piso

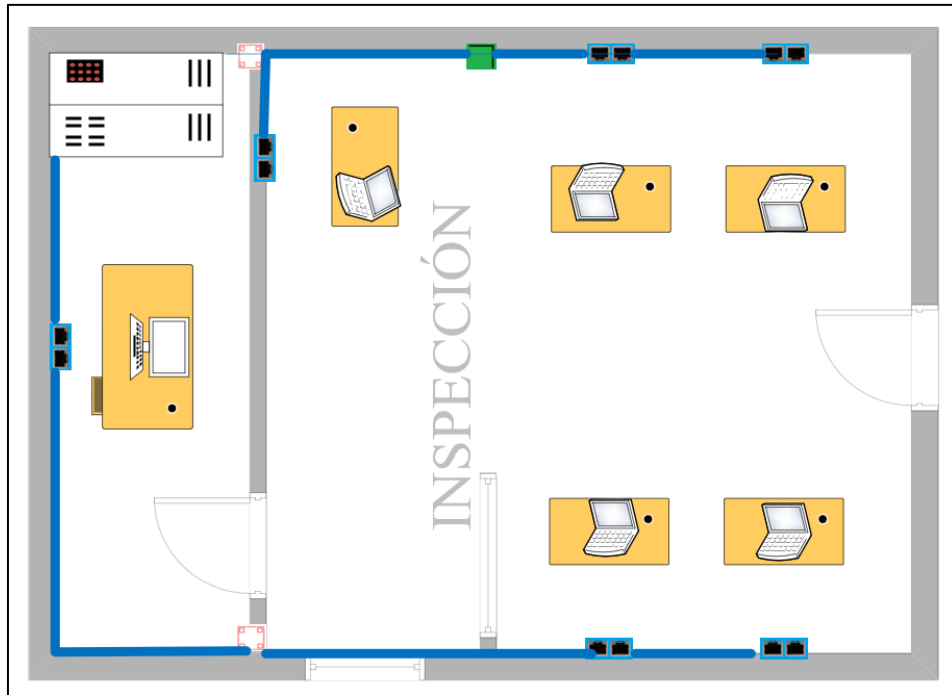


Figura 40. Ubicación de puntos de red y canaletas en bloque Inspección.

Elaborado por: Los autores

3.3.2.9 Diseño de cableado estructurado Laboratorios

El rediseño en el bloque de laboratorios empieza ubicando en cada laboratorio 2 puntos de red y un ACCESS POINT para el uso de docentes y estudiantes, como se necesitan pasar 2 cables UTP, se colocan en las canaletas, en la figura 41, se muestra la propuesta de diseño de cableado estructurado para los laboratorios de física y química que poseen similar estructura.

Puntos de red del Bloque Laboratorios Primer Piso

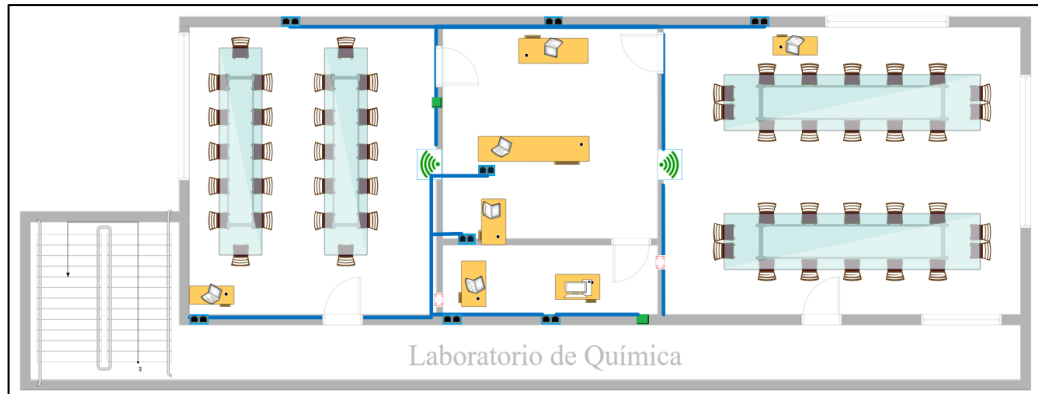


Figura 41. Ubicación de puntos de red, tuberías, canaletas y bandejas en Laboratorios.

Elaborado por: Los autores

3.3.2.10 Diseño de cableado estructurado Bachillerato Internacional, Biblioteca, DECE y Secretaría General

El rediseño en el bloque 3 ubicando en cada área puntos de red y ACCESS POINT para el personal administrativo y docentes en el segundo piso, mientras que en el primer piso donde se encuentra situada la biblioteca se aumentarán puntos de red para un futuro crecimiento.

Puntos de red del Bloque 3 Primer Piso

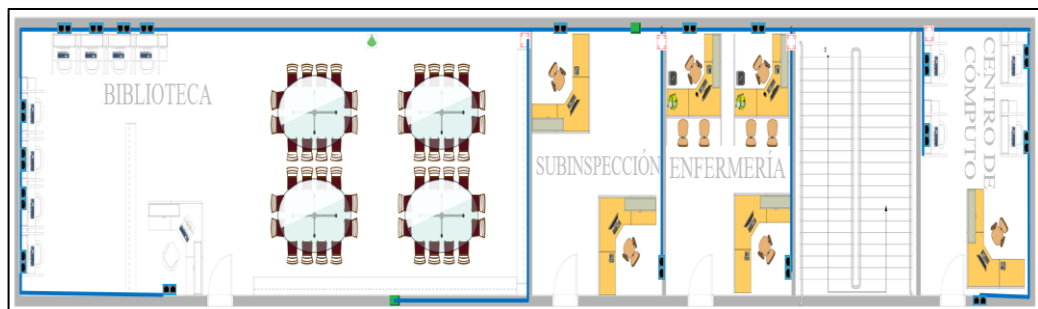


Figura 42. Ubicación de puntos de red, tuberías, canaletas y bandejas en bloque 3.

Elaborado por: Los autores

Puntos de red del Bloque 3 Segundo Piso

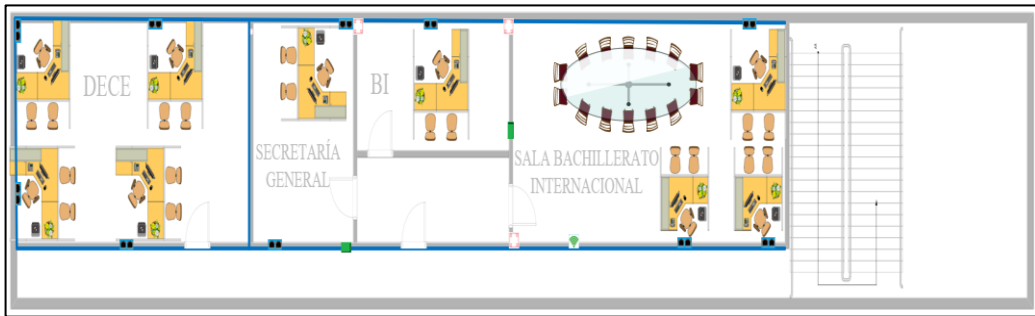


Figura 43. Ubicación de puntos de red, tuberías, canaletas y bandejas en bloque 3.

Elaborado por: Los autores

3.3.2.11 Diseño de cableado estructurado Laboratorios de computación

El rack de este laboratorio será reutilizado porque posee 3 switch de 24 puertos, para tener Internet en toda esta área se aumenta una cañería para mandar el cable UTP, también se puede dar redundancia a la red porque se reutilizan los cables UTP que unen el bloque 3 y 4.

Puntos de red del Laboratorio de computación Tercer Piso



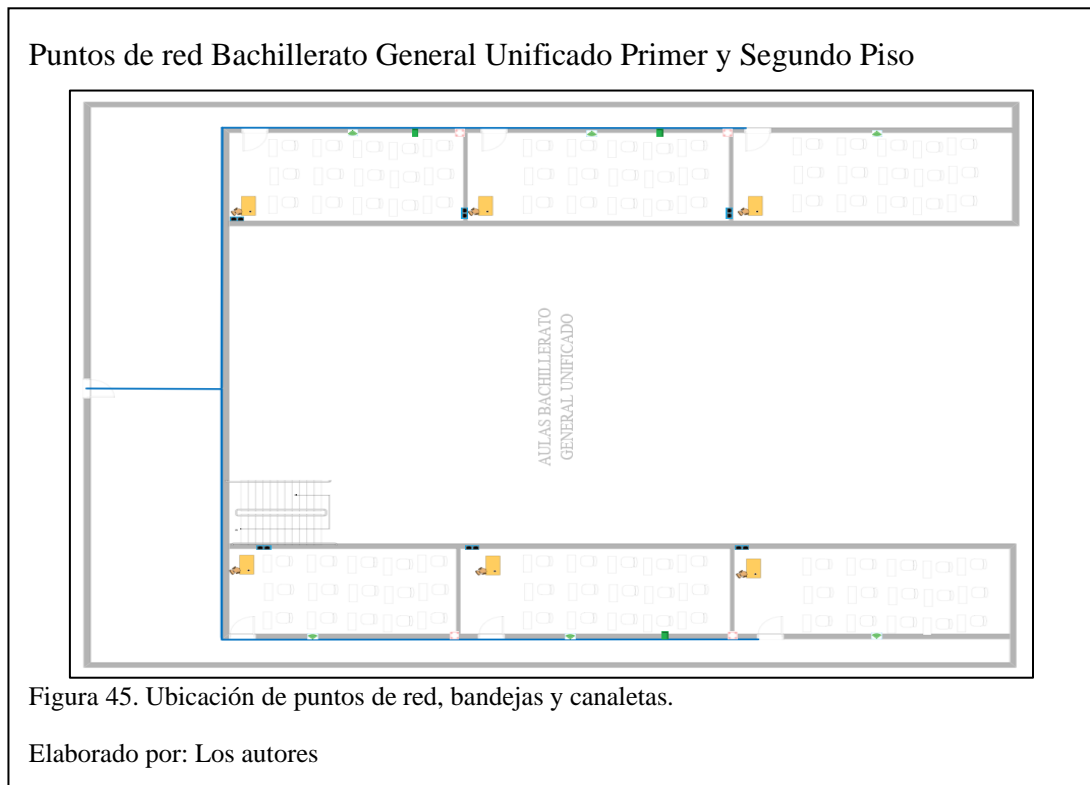
Figura 44. Ubicación de puntos de red, recorrido de las bandejas y tuberías.

Elaborado por: Los autores

3.3.2.12 Diseño de cableado estructurado Bachillerato general Unificado

El bloque 5 y 7 del BGU eran áreas sin Internet, con el rediseño y el uso de bandejas y tuberías se da un acceso por medios no guiados a cada aula mediante ACCESS POINT, además se propone utilizar medios guiados para puntos de voz y

datos para cada docente; el plano se puede usar para las aulas del primer y segundo piso.



3.3.2.13 Diseño de cableado estructurado Bachillerato general Unificado

El bloque 9 al igual que el bloque 5 y 7 accede a Internet mediante medios guiados para voz y datos para los docentes, mientras que por medios no guiados como ACCESS POINT acceden los estudiantes la similitud de la obra civil produce que los tres pisos tengan el mismo rediseño.

Puntos de red Bachillerato General Unificado primer, segundo y tercer piso

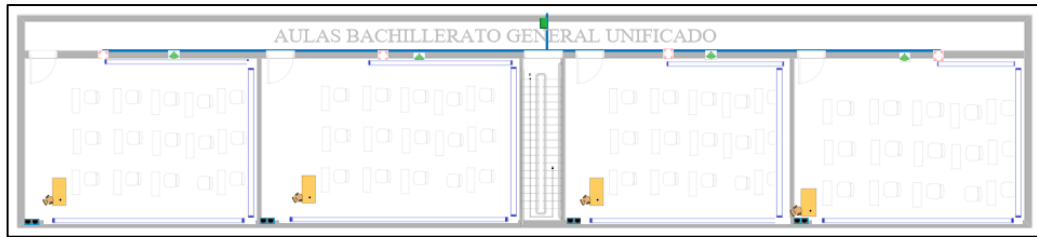


Figura 46. Ubicación de puntos de red, bandejas y canaletas.

Elaborado por: Los autores

3.3.2.14 Diseño de cableado estructurado Sala de profesores

El bloque 8 en el rediseño se coloca puntos de voz – datos y ACCESS POINT para obtener el acceso a internet que necesitan los docentes para investigación.

Puntos de red Sala Docentes



Figura 47. Ubicación de puntos de red, bandejas y canaletas.

Elaborado por: Los autores

3.3.2.15 Conectividad entre Bloques IEFA

El cableado se conecta entre los bloques de la institución respetando la distancia de 90 metros para evitar atenuaciones excesivas en la figura 48 se identifica la forma de conexión entre áreas de la IEFA.

Redundancia de red de datos

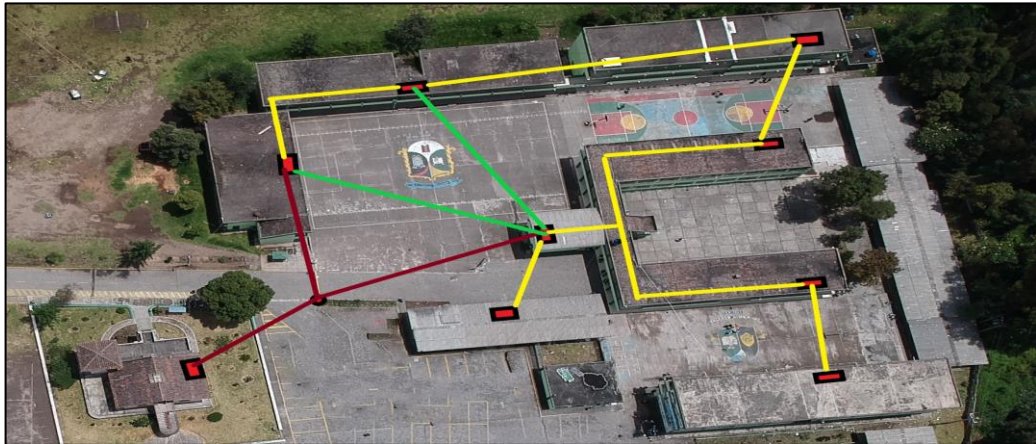


Figura 48. Conectividad entre Bloques IEFA

Elaborado por: Los autores

3.3.3 Equipos

Para la propuesta de rediseño de la IEFA se necesitan equipos que interconecten las áreas de la LAN, cumpliendo las necesidades de la institución que fueron determinadas en el diseño lógico además de los requerimientos técnicos.

3.4 Propuesta de rediseño para la Institución Educativa Fiscal “Amazonas”

3.4.1 Propuesta de Aplicaciones y servicios

En la tabla 3 se detallan las aplicaciones planificadas para la propuesta de rediseño de la IEFA.

Tabla 3. Aplicaciones planificadas

Tipo de aplicación	Aplicación	Comentarios
Web	Microsoft Edge	Se reemplazarán en todos los equipos el navegador Chrome por Microsoft Edge.
VOIP	Elastix	Serán reemplazadas todas las telefonías fijas.
Groupware	Zoom	Se utilizará de manera individual por cada

		administrativo, docente y estudiante.
Base de datos	Carmenta	Proporcionada por el Ministerio de Educación (Distrito 9)
E-Mail	Office 365	Proporcionada por el Ministerio de Educación (Distrito 9)
Groupware	Teams	Proporcionada por el Ministerio de Educación (Distrito 9)

Elaborado por: Los autores

En la tabla 4 se señalan los servicios de red planteados para la propuesta de rediseño de la IEFA.

Tabla 4. Servicios de red

Servicios	Comentarios
Seguridad	Firewall ASA 5510 para proteger la red interna de la IEFA contra amenazas.
QoS	Para tener disponibilidad de servicios ante algún problema de internet que pueda presentarse.
Monitoreo de Redes	PRTG.

Elaborado por: Los autores

3.4.2 Propuesta de diseño de Red Inalámbrica

Al diseñar una red Wireless se tiene en cuenta los factores como: número de usuarios, portal cautivo, frecuencias de operación, cobertura de dispositivos, aplicaciones en la red inalámbrica, nombre de la red (SSID) y seguridad de red.

3.4.2.1 Número de usuarios

La Institución Educativa Fiscal “Amazonas” tiene 1500 usuarios por jornada de clases.

3.4.2.2 Portal Cautivo

Es utilizado para mostrar un formulario e identificarse y mostrar las condiciones de uso que utiliza la red.

Los administradores de la IEFA darán permisos para que los usuarios se conecten mediante su correo y contraseña, que son proporcionados al empezar el periodo académico, el portal cautivo va a segmentar en 10 VLANS consideradas en el diseño de la red.

3.4.2.3 Cobertura de dispositivos

Mediante un estudio de Wireless Site Survey dentro de la Institución Educativa Fiscal “Amazonas”, se reconoce los lugares donde van a ser ubicados los Access-Point, brindando acceso a los usuarios a Internet.

3.4.2.4 Nombre o identificador de la red (SSID)

El SSID (Services Set Identifier) es un identificador único que se aplica al punto de acceso y al cliente inalámbrico, lo que les permite asociarse (COMMUNITY CISCO, 2020). A la red se pueden conectar de dos maneras:

- Cuando la difusión de broadcast en el SSID esté activa, haciendo que un host rastree las redes inalámbricas para enlistarlas y elegir a cuál conectarse.
- Cuando la difusión de broadcast esté desactivada, se debe ingresar manualmente el usuario y contraseña (Shiguango & Lara, 2013).

3.4.2.5 Seguridad

La seguridad para la IEFA será WPA2 que es el nivel de seguridad para los ACCESS POINT, la seguridad del portal cautivo y los dispositivos móviles (Shiguango & Lara, 2013).

3.4.3 Propuesta de Equipos

Se utilizan firewall, router, switch y ACCESS POINT para dar cobertura de Internet a todos los bloques según los requerimientos de la Institución Educativa Fiscal “Amazonas”, en base a los cuadrantes de Gartner descritos en el anexo 2, en las figuras 49, 50, 51 y 52 respectivamente se realiza la comparación de firewall, router, switch y ACCESS POINT según las especificaciones que tiene cada uno, para lograr la convergencia adecuada de la red.

Parámetros y marca de Firewall			
Parámetros \ Marca	CISCO ASA 5510	FORTIGATE 61E	PALO ALTO PA-220
Capacidad máxima de procesamiento	300 Mbps	250 Mbps	250Mbps
Capacidad máxima de procesamiento de VPN 3DES/AES	170 MBps	150 Mbps	150 Mbps
Cantidad máxima de sesiones	130000	70000	64000
Memoria Flash	256 MB	128	128
Interfaces virtuales (VLAN)	100	60	80
Seguridad en la capa de aplicaciones	Si	Si	Si
Funciones de firewall transparente de capa 2	Si	Si	Si
Costo	3495 USD	2399 USD	2900 USD

Figura 49. Comparación de equipos Firewall

Elaborado por: Los autores

Parámetros y marca de Router

Marca Parámetro	CISCO 881/K9	HUAWEI AR151-S2	MIKROTIK CCR1016-12S-1S+
Algoritmos de Encriptación	DES, 3DES, AES 128, AES 192, AES 256	DES, 3DES, AES 128, AES 192, AES 256	DES, 3DES, AES 128, AES 192, AES 256
Memoria Flash	128 MB	512 MB	1 GB
Número de Puertos	4-port 10/100 Ethernet switch	4 x FE LAN, 1 x FE WAN	4-port 10/100 Ethernet switch
Características de QoS	LLQ, WFQ, CBWFQ, CBTS, CBTP, PBR	LLQ, WFQ, CBWFQ, CBTS, CBTP, PBR	LLQ, WFQ, CBWFQ, CBTS, CBTP, PBR
Seguridad	DMVPN, Isec over IPv6, Isec stateful failover, SSL Firewall stateful failover, IPS.	Isec stateful failover, SSL Firewall stateful failover, IPS.	Isec stateful failover, SSL Firewall stateful failover, IPS.
Costo	0 USD porque posee el equipo la Institución	3000 USD	800 USD

Figura 50. Comparación de equipos Router

Elaborado por: Los autores

Parámetros y marca de Switch

Parámetro \ Marca	CISCO Switch CATALYST 3550-48	HUAWEI QUIDWAY S3600-28P-EI	JUNIPER EX3400-24T
Número de Puertos	48	24	48
Puertos	48 x 10/100 + 2 x GBIC.	24 x 10/100 + 4 x SFP.	48 x 10/100 + 2 x GBIC.
Seguridad	802.1x, SSH, SNMPv3, ACL, Port Security, MAC address notification, RADIUS/TACAC+ – Advanced QoS: L2-L4.	RADIUS, Secure Shell v.2 (SSH2), Extensible Authentication Protocol (EAP).	RADIUS, Secure Shell v.2 (SSH2), Port Security.
Características	Enrutamiento IP, capacidad de full dúplex, manejable.	Full-duplex, half-duplex.	Full-duplex, half-duplex.
MTBF	163000 horas.	479960 horas.	200000
QoS	QoS L2-L4 con CoS / DSCP, WRR, WRED, cola de prioridad estricta.	QoS L2-L4 con CoS / DSCP, WRR, WRED.	QoS L2-L4 con CoS / DSCP, WRR, WRED.
Costo	2300 USD	1400 USD	3300 USD

Figura 51. Comparación de equipos Switch

Elaborado por: Los autores

Parámetros y marca de equipos ACCESS POINT

Marca Parámetro	CISCO AIRONET AIR-AP4800-B-K9	HUAWEI AP5130DN	RUCKUS Q710
Características	Compatibilidad con Wi-Fi Multimedia (WMM), tecnología CleanAir, combinación de relación máxima (MRC), tecnología 4T4R MIMO, diversidad de desplazamiento cíclico (CSD).	Protocolo de puerta de enlace del Servicio de nombres de dominio de multidifusión (mDNS): admite el uso compartido de servicios AirPlay y AirPrint entre usuarios de diferentes VLAN.	Múltiples aplicaciones: desde cobertura y capacidad móvil hasta LTE privado y redes de host neutrales, Q710 cubre una amplia gama de casos de uso de CBRS.
Seguridad	WEP, WPA, WPA2-PSK, WPA2-802.1x, WPA, WPA2, WAPI, WIDS.	WEP, WPA, WPA2-PSK, WPA2-802.1x, WPA-WPA2, WAPI, WIDS.	WEP, WPA, WPA2-PSK, WPA2-802.1x, WPA, WPA2, WAPI, WIDS.
Múltiples SSID	Basada en vlan	Basada en vlan	Basada en vlan
Ahorro de energía	Si.	Si.	No
Número de clientes simultáneos	120	150	80
Costo	450	377	200

Figura 52. Comparación de equipos ACCESS POINT

Elaborado por: Los autores

3.4.4 Propuesta de software

Los equipos para personal administrativo, docentes y estudiantes son laptop y PC que fueron descritas en la figura 6, a las cuales según sus características de hardware y por requerimientos de la institución, para asegurar la integridad, confidencialidad y disponibilidad, se tiene que actualizar el sistema operativo y el antivirus. Según el análisis costo beneficio sobre sistemas operativos y antivirus que se muestran en las figuras 53 y 54, se tendría que instalar Windows 10 con todos sus componentes y con el antivirus Norton 360 se previenen vulnerabilidades.

Utilizar un antivirus con los registros activados y que son enviados a servidores de riesgo (CIS Controls, 2020), aplicando el control 6 se almacena la información disponible en caso de que se requiera un seguimiento además los antivirus proveen de protección contra malware para evitar ataques al sistema, dispositivo y datos (CIS Controls, 2020), utilizar el control 8 en una gestión centralizada de información que permite verificar si las defensas se encuentren activas y actualizadas.

Una configuración simple en el navegador puede dificultar la instalación de malware (CIS Controls, 2020), al aplicar el control 7 se reduce el spam en los correos debido a que se utiliza un proceso de autenticación, reporte y conformidad de mensajes basado en dominio (DMARC).

En las figuras 53, 54 y 55 se encuentran las ponderaciones detalladas para seleccionar el sistema operativo, el antivirus y la herramienta de monitoreo respectivamente.

Parámetros de Sistemas Operativos		
Sistema Parámetro	LINUX	WINDOWS
Modelo de licencia	Difícil de usar.	Apto para principiantes, manejo intuitivo por medio de interfaces gráficas de usuario.
Interfaz gráfica	Línea de comandos.	Interfaz gráfica de usuario.
Soporte	No todas las versiones cuentan con asistencia a largo plazo.	Asistencia a largo plazo garantizada.
Software	Existen muchas menos aplicaciones compatibles con Linux.	La mayor parte del software que sale al mercado es compatible con Windows.
Instalación	La mayor parte de los programas, controladores o paquetes se encuentran en repositorios fijos.	Los programas se instalan descargando archivos ejecutables desde Internet o mediante discos físicos.
Compatibilidad	Otros programas de terceros solo pueden ser instalados por un administrador.	Soporta un gran número de aplicaciones de terceros.
Actualización	Las actualizaciones son muy complejas.	Actualización de sistema sencilla y automatizada.

Figura 53. Comparación de Sistemas Operativos

Elaborado por: Los autores

Parámetros de Antivirus

Antivirus Parámetro	KASPERSKY TOTAL SECURITY	MCAFEE TOTAL PROTECTION	NORTON 360 WITH LIFELOCK ULTIMATE PLUS
Licencia 1 año	149.99 USD	99,99 USD	349.99 USD
Número de dispositivos	10	10	Ilimitado
Sistemas Operativos soportados	Windows, Mac®, Android, iOS.	Windows, Mac®, Android, iOS.	Windows, Mac®, Android, iOS.
Respaldo y restauración	Windows PC.	n/a	Windows PC.
Seguridad en línea	Dropbox 3 GB	n/a	500 GB
VPN segura	No	No	Si
Protección contra robo de identidad	No	Si	Si

Figura 54. Comparación de Antivirus

Elaborado por: Los autores

Parámetros de herramientas de monitoreo

Herramienta Parámetro	SOLARWINDS NETWORK	PRTG NETWORK MANAGER
Interfaz de usuario	GUI de Windows y GUI basada en web.	GUI de Windows y GUI basada en web.
Panel de control personalizable	si	si
Capacidad de expansión	si	si
Sondeo de hardware	Ventilador, fuente de alimentación y temperatura.	CPU y memoria, más a través del sensor según el soporte de hardware SNMP
Servicio al cliente	Soporte 24/7	- En línea. - Horas laborables
Coste	\$110/mes.	3200/única vez USD

Figura 55. Comparación de herramientas de Monitoreo

Elaborado por: Los autores

3.4.5 Simulación red Actual IEFA

Red actual IEFA

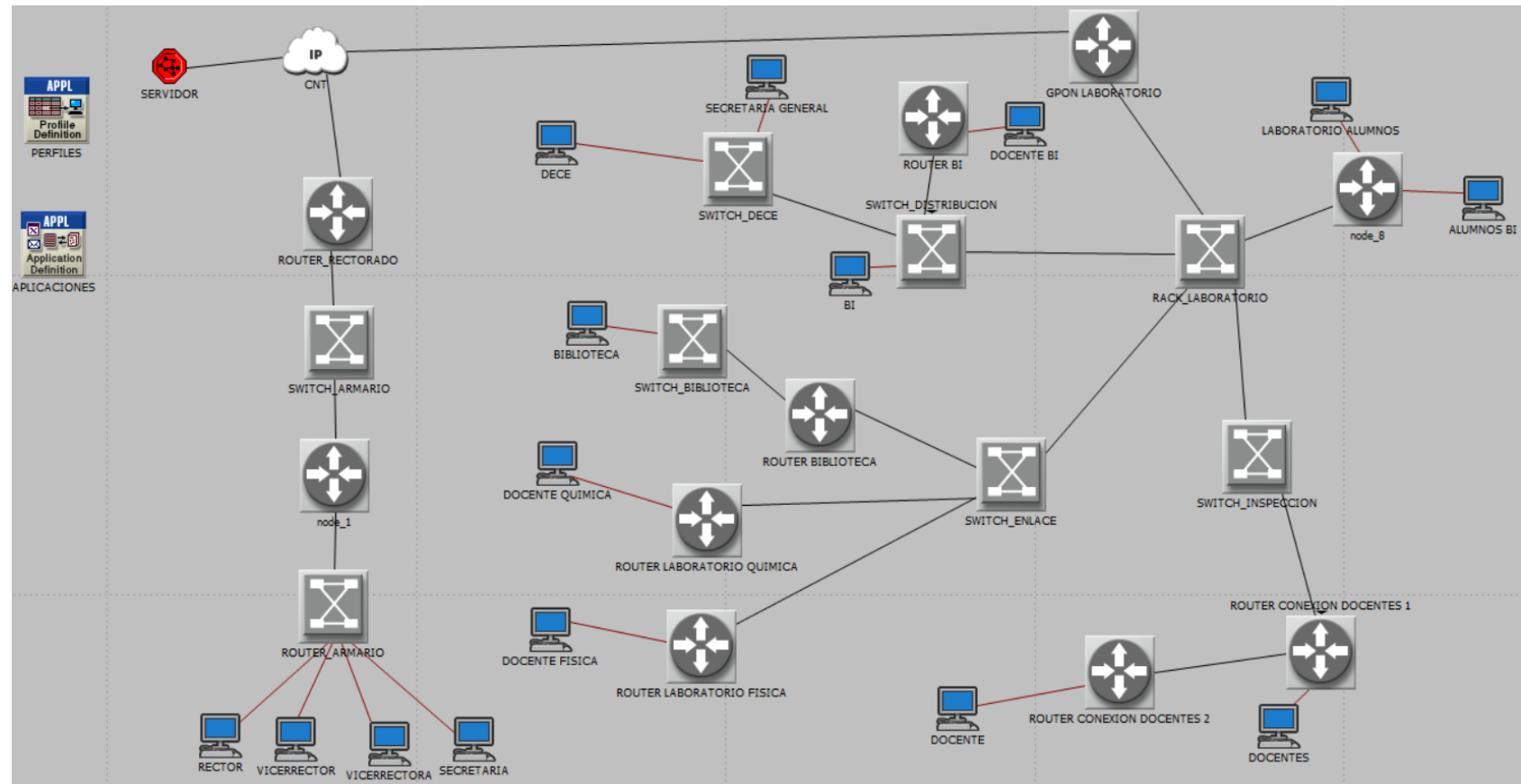
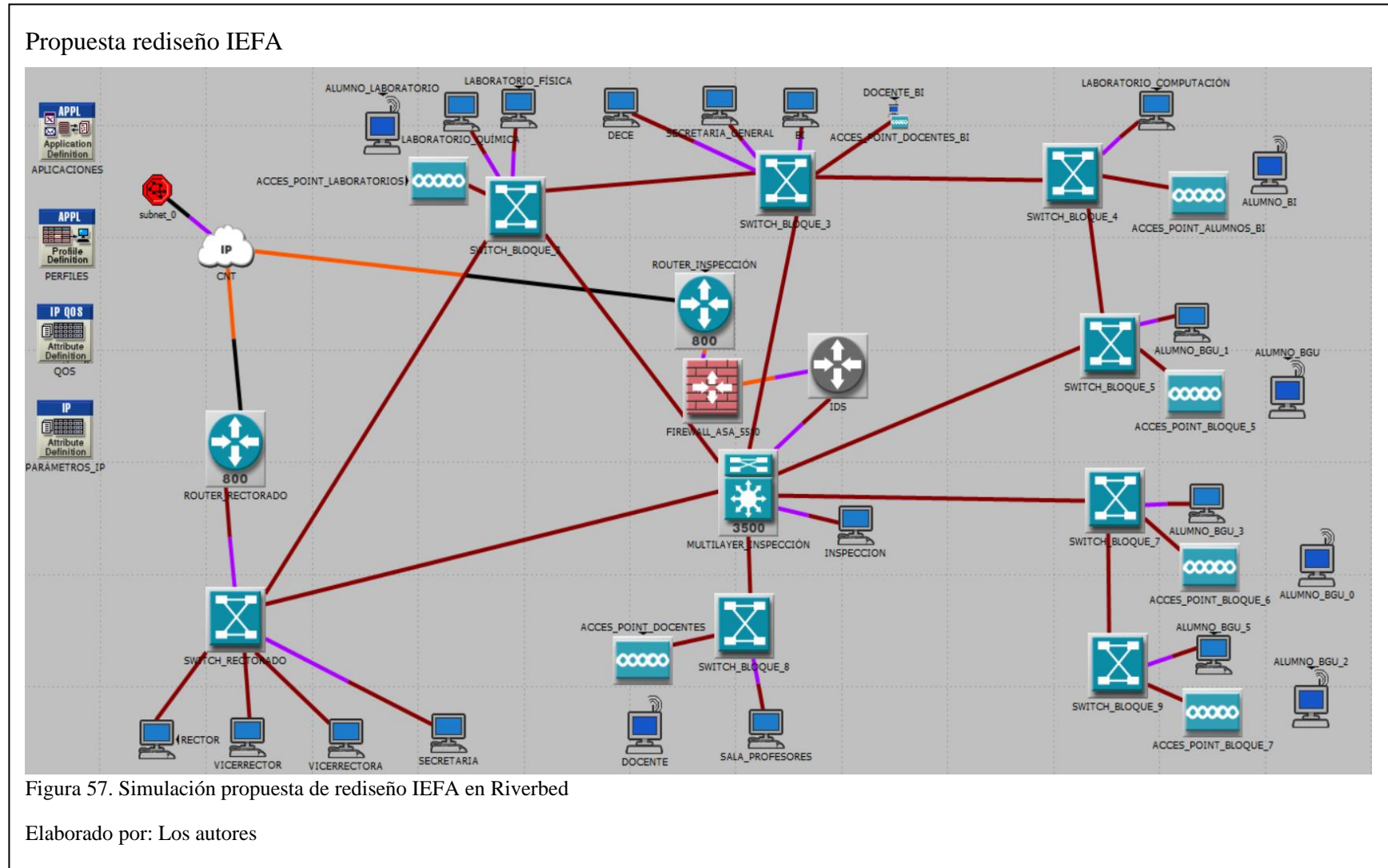


Figura 56. Simulación Red Actual IEFA en Riverbed

Elaborado por: Los autores

3.4.6 Simulación red propuesta IEFA



3.4.7 Propuesta rediseño de topología de la internetwork de la IEFA

Bloques en la Red de la IEFA

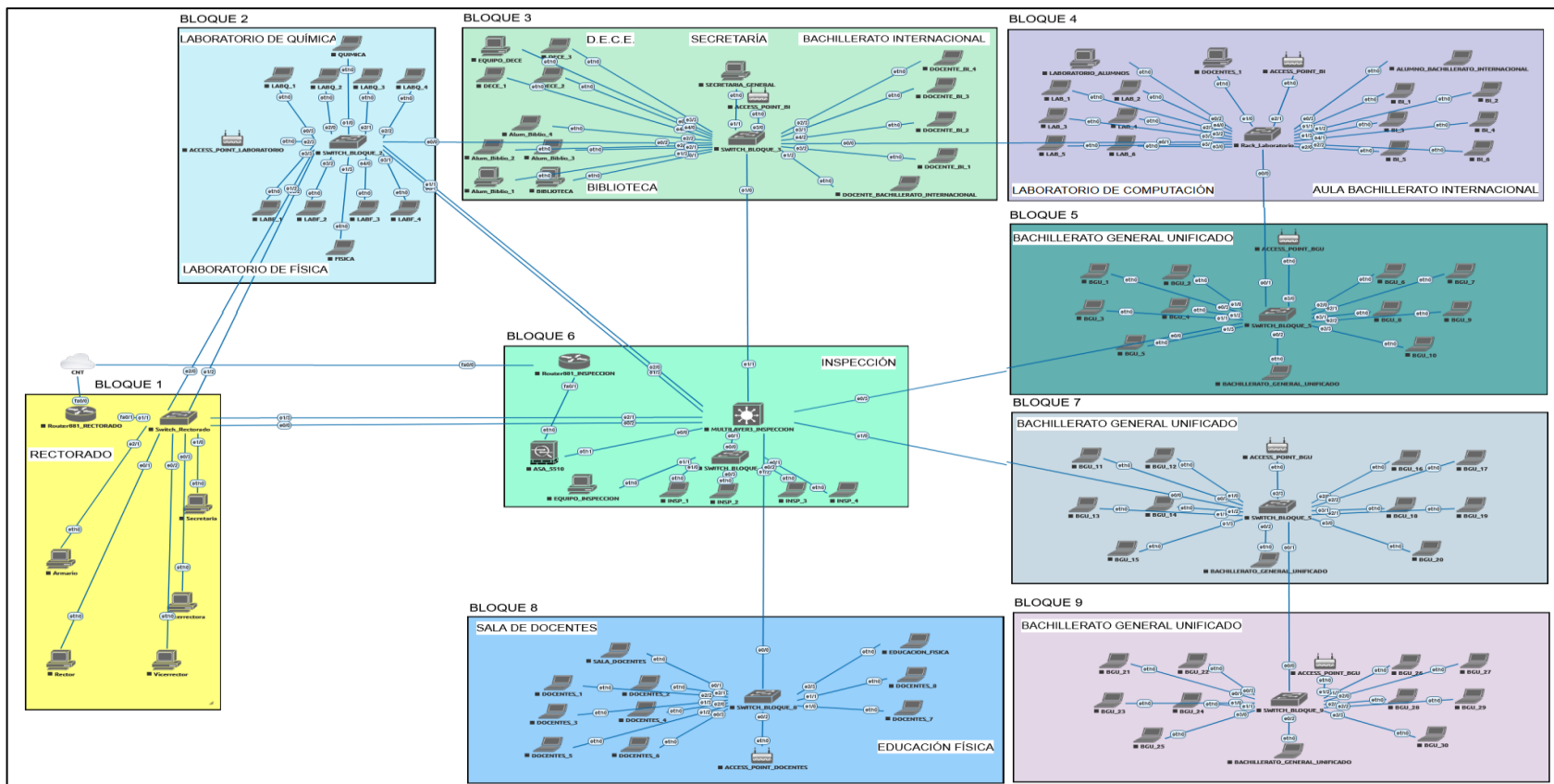


Figura 58. Propuesta de Rediseño de red IEFA

Elaborado por: Los autores

3.4.8 Configuración de Equipos propuestos para la red de la IEFA

Al implementar un IDS para corregir el flujo de información que intercambian redes en diferentes niveles (CIS Controls, 2020), se utiliza el control 12 para monitorear el tráfico en los bordes de red, para obtener una defensa perimetral.

Utilizando la configuración AAA se obtiene un control sobre el acceso a los dispositivos de red mediante una contraseña y un usuario que solo conoce el administrador de la red (CIS Controls, 2020), aplicando el control 4 en los dispositivos finales se deben implementar técnicas para que los usuarios utilicen contraseñas de al menos 8 caracteres, cuentas delicadas así el administrador de la red podrá recibir alertas de inicio de sesión fallidos, además el control 14 indica que al cifrar la información y las contraseñas no pueden acceder al texto plano original.

Seguridades de autenticación en equipos

Inicio sesión equipos	Configuración AAA
<pre>Router con0 is now available Press RETURN to get started. Institucion Educativa Fiscal Amazonas PROHIBIDO EL ACCESO NO AUTORIZADO Si no es usuario autorizado CIERRE SESION Todas las conexiones son monitoreadas User Access Verification Username: █</pre>	<pre>PROHIBIDO EL ACCESO NO AUTORIZADO Si no es usuario autorizado CIERRE SESION Todas las conexiones son monitoreadas^C banner motd ^CInstitucion Educativa Fiscal Amazonas ^C ! line con 0 password 7 06070B2C4540001C0316 login authentication SSH-LOGIN line aux 0 password 7 070E2541470710001113 line vty 0 4 login authentication SSH-LOGIN transport input telnet</pre>

Figura 59. Configuración AAA

Elaborado por: Los autores

El firewall se colocará en el límite entre la red de la IEFA e internet (CIS Controls, 2020), utilizando el control 11 se establece la configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores debido a que los usuarios mal intencionados suelen atacar a los dispositivos de infraestructura de red que se configuran de manera menos segura, se toman en cuenta una serie de pasos y

recomendaciones para obstruir brechas que se puedan encontrar mediante el uso de herramientas comerciales que ayudan a evaluar tales vulnerabilidades.

Para mantener control sobre puertos, protocolos y servicios se realiza un escaneo de puertos con una herramienta de monitoreo de la red (CIS Controls, 2020), aplicando el control 9 del CIS Benchmark.

El filtrado de tráfico se realiza mediante ACL que se ubican en los dispositivos de capa 2 y capa 3 para evitar acceso telnet a la red, evitando que los atacantes accedan a la internetwork de la IEFA.

IP y puertos permitidos

```
ip access-list extended Docentes_restriccion
deny tcp 192.168.8.0 0.0.0.254 69.0.0.0 0.255.255.255 eq www
deny tcp 192.168.8.128 0.0.0.63 69.0.0.0 0.255.255.255 eq 443
deny tcp 192.168.9.192 0.0.0.31 69.0.0.0 0.255.255.255 eq www
deny tcp 192.168.9.192 0.0.0.31 69.0.0.0 0.255.255.255 eq 443
deny tcp 192.168.9.160 0.0.0.95 69.0.0.0 0.255.255.255 eq www
deny tcp 192.168.9.160 0.0.0.95 69.0.0.0 0.255.255.255 eq 443
deny tcp 192.168.9.224 0.0.0.7 69.0.0.0 0.255.255.255 eq www
deny tcp 192.168.9.224 0.0.0.7 69.0.0.0 0.255.255.255 eq 443
permit ip any any
ip access-list extended Estudiantes_Restriccion
deny tcp 192.168.0.0 0.0.0.248 69.0.0.0 0.255.255.255 eq www
deny tcp 192.168.0.0 0.0.0.248 69.0.0.0 0.255.255.255 eq 443
permit ip any any
access-list 110 permit ip 192.168.0.0 0.0.0.248 any
access-list 110 permit ip any 192.168.9.192 0.0.0.31
access-list 120 permit ip 192.168.9.192 0.0.0.31 any
access-list 120 permit ip any 192.168.9.224 0.0.0.7
access-list 130 permit ip 192.168.9.224 0.0.0.7 any

ipv6 access-list Docentes_restriccion_ipv6
sequence 20 deny tcp any 2A03:2880:F12C:183::/64 eq www
permit ipv6 any any
ipv6 access-list Estudiantes_Restriccion_ipv6
sequence 20 deny tcp any 2A03:2880:F12C:183::/64 eq www
permit ipv6 any any
```

Figura 60. Configuración ACL de la IEFA

Elaborado por: Los autores

El acceso inalámbrico es una fuente de robo de información (CIS Controls, 2020), al aplicar el control 15 se encriptan las claves y se inhabilitan las capacidades de red, a su vez, al usar protocolos de autenticación y al crear redes inalámbricas separadas para personas confiables y no confiables se puede auditar la red ante un incidente.

Gestionar el ciclo de vida de las cuentas de sistema y aplicaciones con el fin de minimizar las oportunidades de los atacantes (CIS Controls, 2020), el control 16 evita que exploten las cuentas de usuarios permitidos que no se encuentran utilizadas, por

lo tanto, es conveniente usar cifrado o técnicas de hash combinadas con criptografía para todas las autorizaciones.

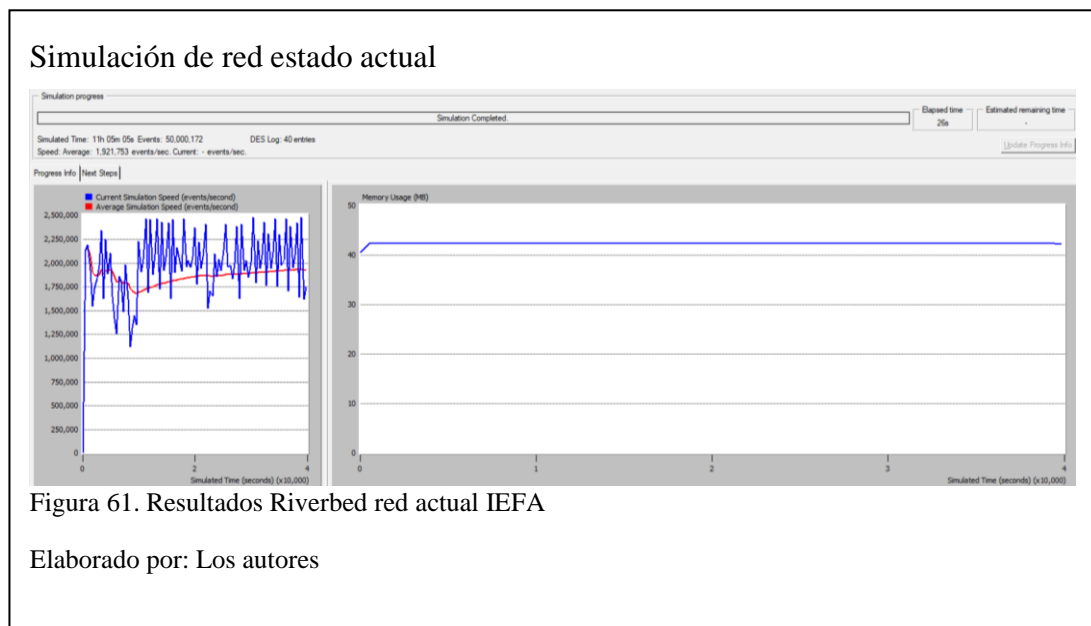
CAPÍTULO IV

ANÁLISIS DE RESULTADOS

Las simulaciones se realizan entre el estado actual de la red y la propuesta de rediseño utilizando el tráfico enviado y recibido, el cual se muestra en gráficas estadísticas utilizando AS IS y AVERAGE que son parte de las opciones para visualizar curvas estadísticas. Estas curvas son medidas en bytes/seg, los servicios que se utilizan para la comparación son: Base de Datos, Email, Ethernet, FTP, Http y VOIP.

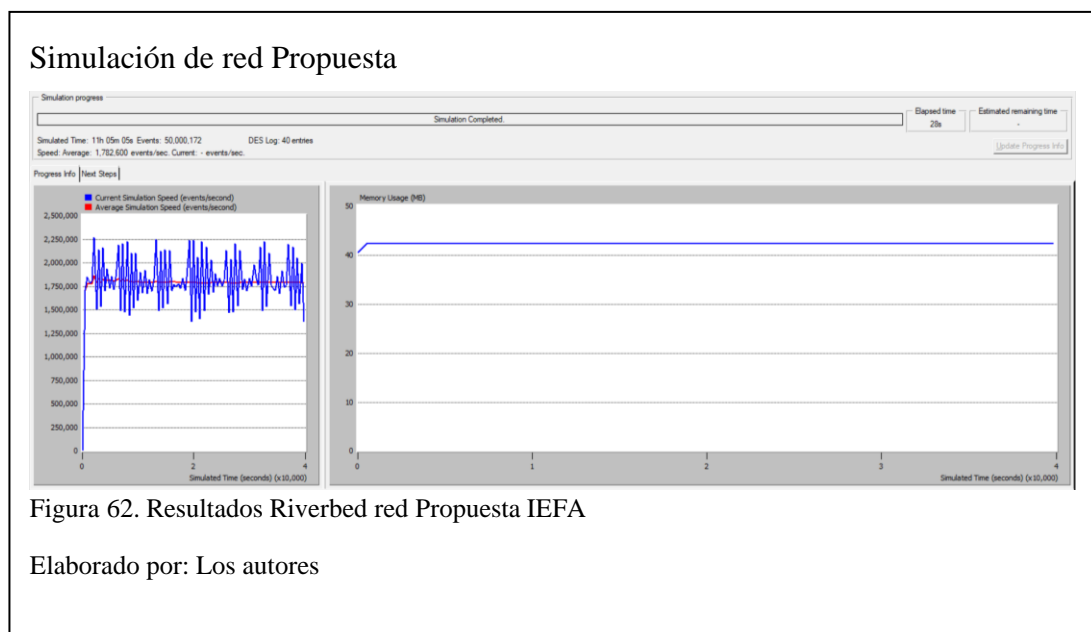
4.1 Resultados de simulación de la red actual de la IEFA

La simulación en Riverbed de la internetwork actual muestra una deficiente generación de tráfico de los servicios para la red, la simulación fue realizada para las 12 horas que se cumplen entre la jornada matutina y vespertina, por lo que se evidencia que se necesita un rediseño de red para la IEFA.



4.2 Resultados de simulación de la propuesta de rediseño para la Institución Educativa Fiscal “Amazonas”

La figura 62 muestra los valores pico que superan los 2000000 de eventos/segundo y una generación de tráfico constante en una simulación de 12 horas, lo que emula el uso de la internetwork para la jornada matutina y vespertina a la vez que mantiene un uso de memoria de 42 MB aproximadamente. Por lo que se demuestra que con la metodología Top-Down y los Controles CIS se ha mejorado el rendimiento de la red.



4.3 Resultados de simulación por servicios

4.3.1 Servicio 1

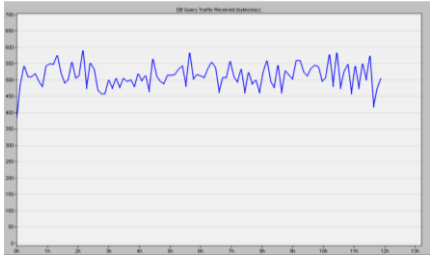
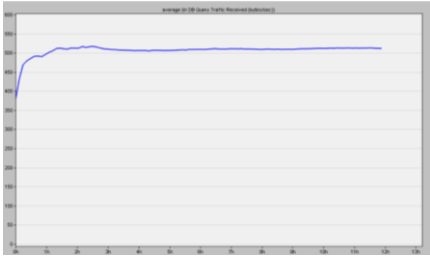
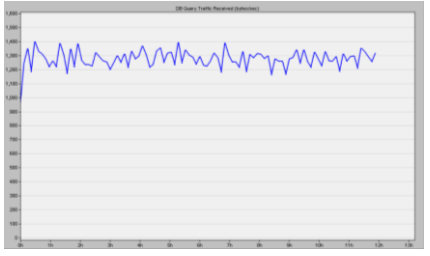
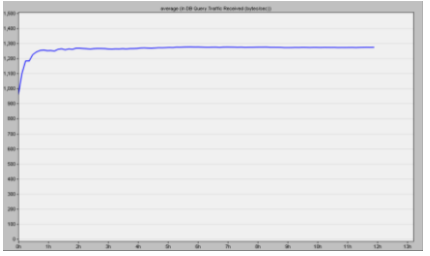
Base de datos (bytes/segundo)

Tráfico recibido

Para la comparación de tráfico se utilizan los métodos AS IS y AVERAGE que posee el simulador, para la base de datos se refleja en el estado actual, el poco consumo

de tráfico con un promedio de 500 bytes/segundo mientras que en el rediseño aumenta el promedio a 1250 bytes/segundo, con lo cual se accede a la información de forma eficaz.

Tabla 5. Tráfico recibido desde Base de Datos


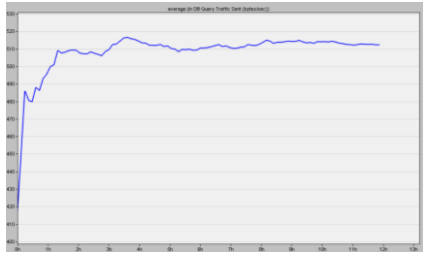

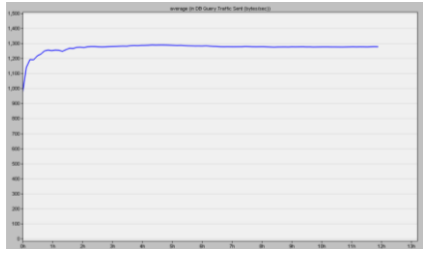
Simulación	AS IS	AVERAGE
Red Actual		
Red Propuesta		

Elaborado por: Los autores

Tráfico enviado

En la tabla 6 el tráfico enviado es mejor en la red propuesta porque mantiene un promedio de 1280 bytes/segundo, además, la red actual mantiene un promedio de 510 bytes/segundo generando poco consumo de datos afectando la calidad de la información.

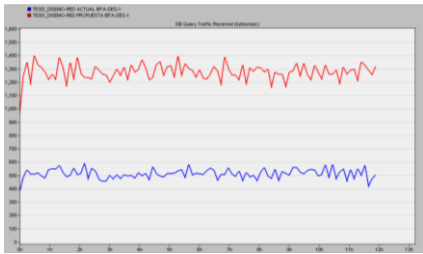

Tabla 6. Tráfico enviado de Base de Datos

Simulación	AS IS	AVERAGE
Red Actual		
Red Propuesta		

Elaborado por: Los autores

En la tabla 7 se observa que en el tráfico recibido y enviado de la red propuesta se obtiene $1275 \pm 8 \%$ bytes/seg, mientras que en la red actual se genera un tráfico de $500 \pm 16.3\%$ bytes/seg, por lo tanto, se evidencia que el tráfico ha mejorado en 65.2% con la propuesta de rediseño.

Tabla 7. Análisis de tráfico en Base de Datos

Servicio	Tráfico recibido	Tráfico enviado
Base de Datos		

Elaborado por: Los autores

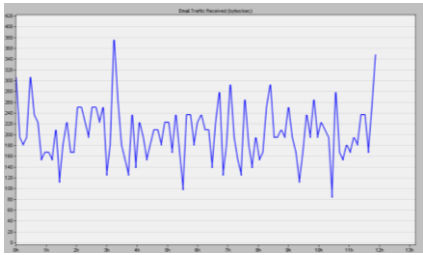
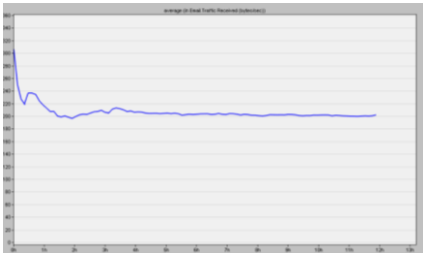

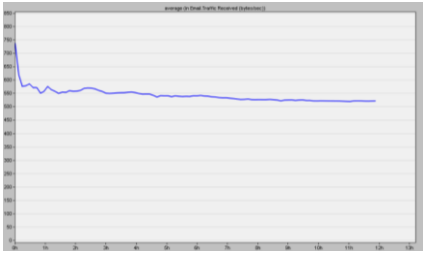
4.3.2 Servicio 2

Email (bytes/seg)

Tráfico recibido

En la tabla 8 en las imágenes comparativas se aprecia un mejor uso en la red propuesta para el servicio de Email descongestionando el tráfico de la red.

Tabla 8. Tráfico recibido en Email

Simulación	AS IS	AVERAGE
Red Actual		
Red Propuesta		

Elaborado por: Los autores

Tráfico enviado

En la comparativa de promedios de tráfico en la tabla 9 se refleja un consumo mayor de bytes para la red propuesta, pero generando el tráfico adecuado para su distribución, mientras que en el estado actual de la red se genera tráfico por cada 250 bytes/segundo.

Tabla 9. Tráfico enviado de Email

Simulación	AS IS	AVERAGE
Red Actual		
Red Propuesta		

Elaborado por: Los autores

En la tabla 10 se evidencia que el tráfico recibido en la red actual es $225 \pm 54.4\%$ bytes/seg, mientras que en la red propuesta es de $550 \pm 29.7\%$ bytes/seg, se observa con la propuesta de rediseño una mejora de 78.6% en el tráfico recibido.

El tráfico enviado de la red actual es $212.5 \pm 52.8\%$ bytes/seg, la propuesta de rediseño es de $475 \pm 34.4\%$ bytes/seg, por lo cual el tráfico incrementa en 72.7% con respecto a la red actual.

Tabla 10. Análisis de tráfico en Email

Servicio	Tráfico recibido	Tráfico enviado
Email		

Elaborado por: Los autores

4.3.3 Servicio 3

Ethernet (seg)

Los resultados obtenidos en la tabla 11 muestra un mejor comportamiento en el tráfico de carga para la red propuesta con un promedio 0.01ms, mientras que el tráfico de carga para la red actual es de 11ms lo cual da una diferencia en el Delay de 10.99 ms.

Tabla 11. Delay para Ethernet

Simulación	AS IS	AVERAGE
Red Actual		
Red Propuesta		

Elaborado por: Los autores

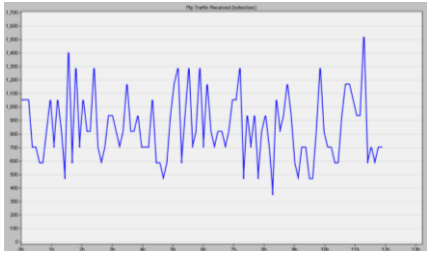
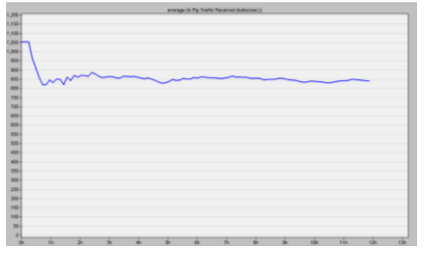
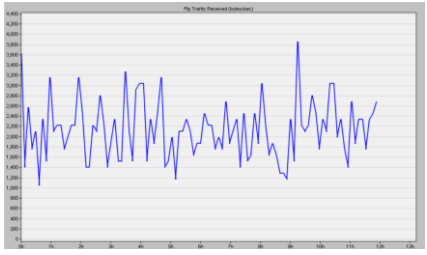
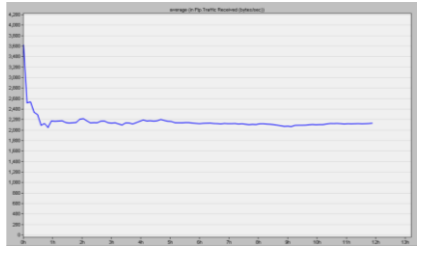
4.3.4 Servicio 4

FTP (bytes/seg)

Tráfico recibido

En la tabla 12 en el tráfico recibido para el estado actual de la red se denota un congestionamiento en la imagen AS IS, mientras que en la gráfica obtenida para la propuesta de rediseño se observa una mejora en el tráfico de la red, esto es debido a los protocolos utilizados para mejorar el rendimiento.

Tabla 12. Tráfico recibido de FTP

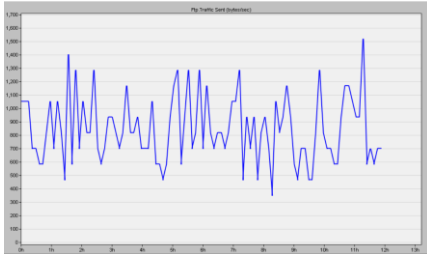
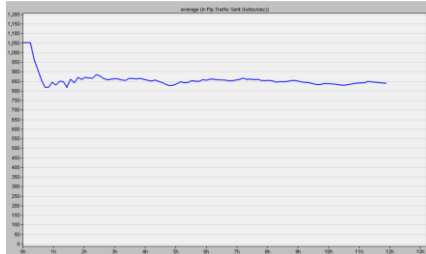
Simulación	AS IS	AVERAGE
Red Actual		
Red Propuesta		

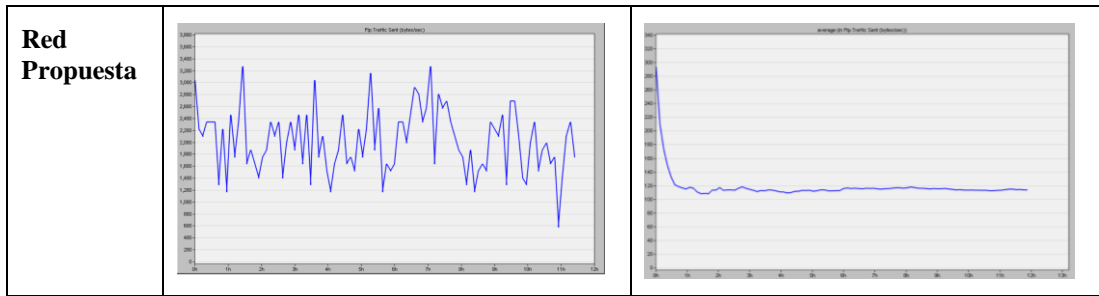
Elaborado por: Los autores

Tráfico enviado

En la comparación de escenarios de la simulación, utilizando el método AS IS y AVERAGE se comprueba que para el servicio FTP el tráfico mejora en la red propuesta debido a que se utiliza un manejo de VLANs que hace que los paquetes no se pierdan en la red.

Tabla 13. Tráfico enviado de FTP

Simulación	AS IS	AVERAGE
Red Actual		

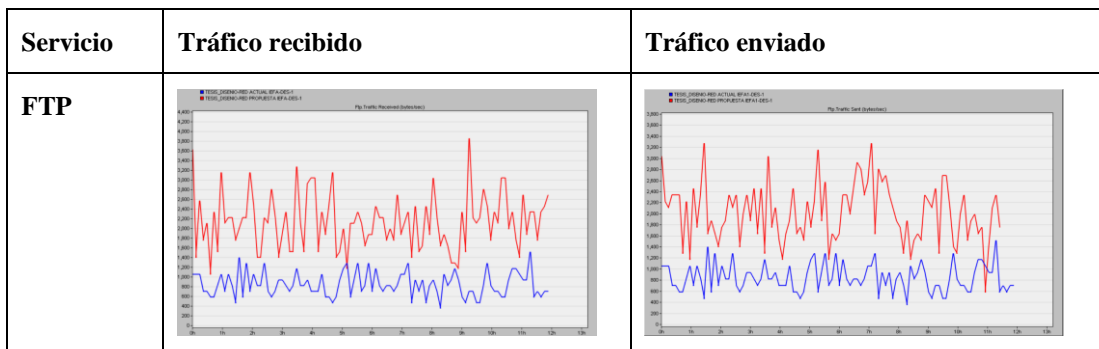


Elaborado por: Los autores

La tabla 14 denota que el tráfico recibido en la red actual es $900 \pm 45.4\%$ bytes/seg, mientras que en la red propuesta es de $2175 \pm 38.5\%$ bytes/seg, se observa con la propuesta de rediseño una mejora de 65.2% en el tráfico recibido.

El tráfico enviado de la red actual es $950 \pm 38.7\%$ bytes/seg, la propuesta de rediseño es de $2250 \pm 38.1\%$ bytes/seg, por lo cual el tráfico incrementa en 58.3% con respecto a la red actual.

Tabla 14. Análisis de tráfico en FTP



Elaborado por: Los autores

4.3.5 Servicio 5

HTTP (bytes/seg)

Tráfico recibido

Las pruebas correspondientes sobre el tráfico recibido en la red actual muestran un consumo de 32 bytes/seg afectando el rendimiento de la red, en la propuesta de rediseño el tráfico aumenta a 77 bytes/seg lo cual aumenta el envío de paquetes provocando un menor tiempo de uso de tráfico en la red.

Tabla 15. Tráfico recibido de Http

Simulación	AS IS	AVERAGE
Red Actual		
Red Propuesta		

Elaborado por: Los autores

Tráfico enviado

Las diferencias en las gráficas obtenidas en la simulación para el tráfico enviado indican que la propuesta de rediseño utiliza 6700 bytes/seg mientras que la red de estado actual maneja 2700 bytes/seg obteniendo una diferencia de 4000 bytes/seg en promedio.

Tabla 16. Tráfico enviado de Http

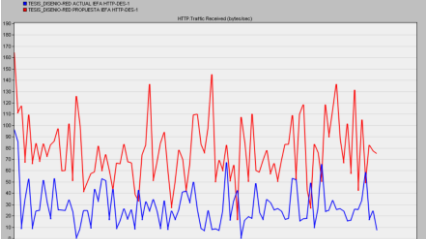

Simulación	AS IS	AVERAGE
Red Actual		
Red Propuesta		

Elaborado por: Los autores

En la tabla 17 se distingue que el tráfico recibido en la red propuesta es $2475 \pm 43.7\%$ bytes/seg, mientras que en la red actual es de $900 \pm 45.4\%$ bytes/seg, se observa con la propuesta de rediseño una mejora de 65.2% en el tráfico recibido.

El tráfico enviado de la red actual es $2675 \pm 13\%$ bytes/seg, en la propuesta de rediseño es de $6600 \pm 7.4\%$ bytes/seg, por lo cual el tráfico incrementa en 62.5% con respecto a la red actual.

Tabla 17. Análisis de tráfico en Http

Servicio	Tráfico recibido	Tráfico enviado
Http		

Elaborado por: Los autores


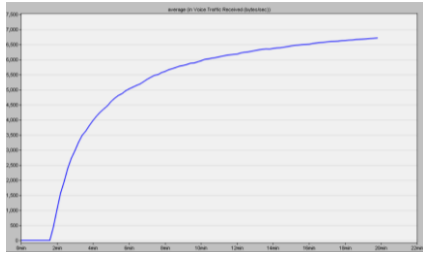
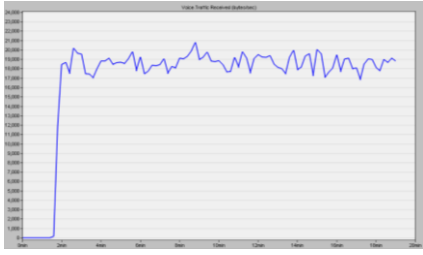
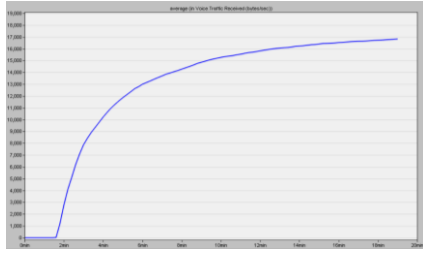
4.3.6 Servicio 6

VOIP (bytes/seg)

Tráfico recibido

El valor promedio más alto se obtiene en la red propuesta con 16500 bytes/seg lo cual hace que la calidad de servicio mejore, permitiendo el uso de plataformas de comunicación evitando caídas en la red.

Tabla 18. Tráfico recibido de VOIP

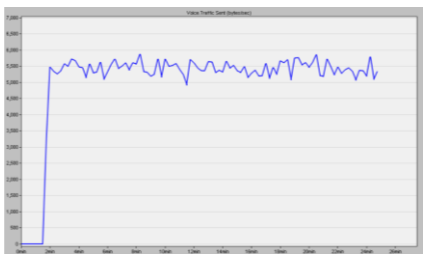
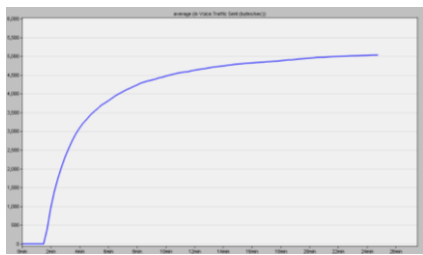

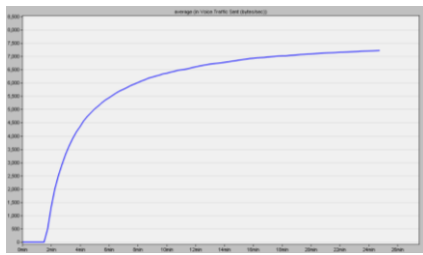
Simulación	AS IS	AVERAGE
Red Actual		
Red Propuesta		

Elaborado por: Los autores

Tráfico enviado

En la tabla 19 se aprecia que el tráfico enviado para el servicio de VOIP es mejor en la propuesta de rediseño que en el estado actual, debido a que en los métodos AVERAGE y AS IS se muestra un mejor rendimiento de la red.

Tabla 19. Tráfico enviado de VOIP

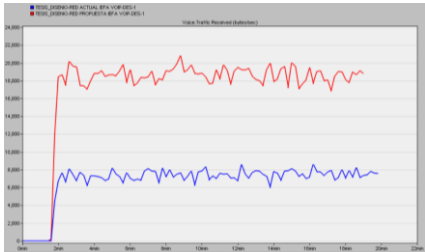
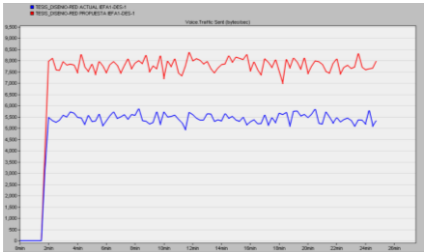
Simulación	AS IS	AVERAGE
Red Actual		
Red Propuesta		

Elaborado por: Los autores

La tabla 20 evidencia que el tráfico recibido en la red actual es $7000 \pm 11.7\%$ bytes/seg, mientras que en la red propuesta es de $19000 \pm 8.6\%$ bytes/seg, se observa con la propuesta de rediseño una mejora de 64.7% en el tráfico recibido.

El tráfico enviado de la red actual es $5500 \pm 7.4\%$ bytes/seg, la propuesta de rediseño es de $7625 \pm 7.6.7\%$ bytes/seg, por lo cual el tráfico incrementa en 28.6% con respecto a la red actual.

Tabla 20. Análisis de tráfico en VOIP

Servicios	Tráfico recibido	Tráfico enviado
VOIP		

Elaborado por: Los autores

4.3.7 Análisis económico

El costo total de la red es basado en dispositivos, software, cableado estructurado y cuarto de comunicaciones que son necesarios para la propuesta de rediseño, los costos referenciales se encuentran en las figuras 63, 64, 65 y 66, además el costo total se denota en la figura 67.

Descripción dispositivos			
DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO (USD)	PRECIO TOTAL (USD)
CISCO 881/K9	2	0*	0*
CISCO SWITCH CATALYST 3550-48	1	2300	2300
CISCO SWITCH 2960 -24PC-L	2	1900	3800
FIREWALL ASA 5510-BUN-K9	1	3495	3495
SWITCH TPLINK TL-SF1024D	5	0*	0*
HUAWEI AP5130DN	8	377	3016
TOTAL			12611

Nota: Los equipos con precio 0, son los que la IEFA dispone.

Figura 63. Proforma de dispositivos de red de la IEFA

Elaborado por: Los autores

Precio Software			
DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO (USD)	PRECIO TOTAL (USD)
NORTON 360	1	349.99	349.99
PRTG	1	3200	3200
OFFICE 365	150	25	3750
WINDOWS 10	150	150	22500
TOTAL			29799.99

Figura 64. Costo Software a utilizar en la IEFA

Elaborado por: Los autores

Descripción de cableado estructurado

DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO (USD)	PRECIO TOTAL (USD)
Rollo (305m) cable UTP cat. 6 Panduit	3	220	660
Patch Cord Cat 6	40	16	640
Face plate 4 puertos	113	2	226
Jack RJ-45 cat 6 (100u)	6	15	90
Cajas decorativas	44	1.50	66
Bandejas (20 cm)	1270	11.10	14097
Canaleta de piso (60x13 cm)	340	11.31	3845.4
Tubería emt (3m)	60	3	180
Caja de paso (20x20 cm)	30	11	330
Caja de revisión (30x30x10cm)	14	10	140
Certificación salidas Categoría 6	452	6	2712
TOTAL			22986.4

Figura 65. Costo cableado estructurado para la IEFA

Elaborado por: Los autores

Proforma de Cuarto de Telecomunicaciones

DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO (USD)	PRECIO TOTAL (USD)
Patch panel Cat 6A 48 puertos	1	50	50
Organizador de cables vertical	1	220	220
Rack de pared cerrado 25 ur	1	400	400
Bandeja estándar 2u 19"	8	15	120
Pdu Nexxt Multitoma Vertical De 12 Tomas 125v 15a	1	120	120
Mano de obra	1	30000	30000
Planos y documentación	1	5000	5000
TOTAL			35910

Figura 66. Costo cuarto de Telecomunicaciones para la IEFA

Elaborado por: Los autores

Presupuesto final

DESCRIPCIÓN	PRECIO TOTAL (USD)
Dispositivo	12611
Software	29799.99
Cableado estructurado	22186.4
Cuarto de telecomunicaciones	35910
TOTAL	100507.39

Figura 67. Costo final de la propuesta para la IEFA

Elaborado por: Los autores

4.3.8 Beneficio

La IEFA, al mantener la información respaldada siguiendo los planes de gestión propuestos evita, que al tener la pérdida de información por algún ataque informático tenga que gastar en los trabajos de recuperación, siendo su costo de \$ 300 por dispositivo, aproximadamente existen 150 dispositivos finales, el costo llegaría a \$45000, garantizando la confidencialidad de la información de la institución.

Al aplicar las estrategias de seguridad de la red y protección de datos (CIS Controls, 2020), el cual corresponde al control 13 se evita que la información de personal administrativo, docentes y estudiantes sea filtrada al público, así la institución no necesita incurrir en gastos de indemnización basados en los artículos 230, 231, 232 y 234 del código orgánico integral penal (ASAMBLEA NACIONAL, 2014) y la posible sanción del 17% de los ingresos totales de la institución .

La Institución Educativa Fiscal “Amazonas” al mejorar los servicios de red con la propuesta de rediseño, provee de acceso a material de educación virtual de forma eficiente con lo cual el colegio puede proponer una transición de bachillerato general unificado a bachillerato internacional haciendo que los alumnos posean un título avalado a nivel internacional, según los estudios realizados por (INEVAL, 2018) los alumnos de BI obtienen un 20% más de puntaje en la prueba para ingreso a la Universidad lo que les asegura acceder a becas en universidades estatales o internacionales.

Indemnizaciones y recuperación de la IEFA	
DESCRIPCIÓN	COSTO (USD)
Recuperación de Información	45000
Indemnizaciones por filtrado de datos personales	120000
TOTAL	165000

Figura 68. Costos de recuperación IEFA

Elaborado por: Los autores

CONCLUSIONES

Al realizar el análisis del estado actual de la internetwork se evidencia la inseguridad que existe en las redes de datos de la IEFA, se encontraron dispositivos activados con la configuración básica dirigidos a la funcionalidad de uso más no a la seguridad dejando en riesgo al tráfico e información que transite.

Al aplicar en conjunto las políticas de seguridad, estrategias de gestión de seguridad y controles del CIS Benchmark en las configuraciones de los dispositivos considerados como activos de la IEFA se resolvieron gran parte de las vulnerabilidades halladas en el análisis de estado actual.

El estudio de costos para la propuesta de rediseño es basado en hardware y software con un estimado de \$100507.39, logrando que la institución se beneficie de una transición de Bachillerato General Unificado a Bachillerato Internacional, mientras que al obtener la seguridad de la red mediante la propuesta de rediseño se evita que atacantes a la internetwork obtengan datos de personal administrativo, docentes y estudiantes, a su vez que pueden afectar a la información almacenada , así la IEFA descarta gastos de indemnización y recuperación por un costo de \$165000 aproximadamente como lo mandan las leyes vigentes.

Al rediseñar la estructura de la IEFA se procede a brindar cobertura de red a bloques de bachillerato general unificado y de bachillerato internacional, por lo cual la institución después del balanceo de carga adecuado de Internet, podrá trabajar para investigaciones de los docentes, además que los estudiantes tendrán acceso a información según los requerimientos de la institución.

Si bien el personal administrativo, docentes y estudiantes de la IEFA continua sus operaciones diarias durante el periodo escolar se han encontrado con ciertos contratiempos los cuales son: caída parcial o total de internet por bloques y periodos

largos de espera al realizar consultas los cuales pueden contrarrestar el tiempo de productividad, se aplicaron el 80% de los controles del CIS Benchmark los cuales resolverían los problemas hallados en la internetwork de la IEFA.

El análisis de los resultados obtenidos en la simulación para la propuesta de rediseño denota un 63.3% de incremento promedio en el rendimiento de la red, basado en el tráfico recibido y enviado entre los dispositivos de la internetwork, dado que la pérdida de paquetes no genera cuello de botella debido a la segmentación en VLANS de la red y con un protocolo de redundancia evitando que la institución tenga enlaces de red sin acceso a Internet.

Para el rediseño de red al mantener una topología tipo estrella extendida, la infraestructura de red se centraliza y se convierte en administrable, debido a la asignación de ACL, VLANS y el uso de un firewall, obteniendo una internetwork robusta que puede ser utilizada por personal administrativo, docentes y estudiantes de la institución.

RECOMENDACIONES

Se recomienda gestionar el ancho de banda con políticas de QoS para obtener un balanceo de carga adecuado para que los bloques de la institución y que sus diferentes departamentos obtengan el Internet que es necesario para su desempeño.

Es conveniente implementar un software de monitoreo para los usuarios de la institución, para garantizar los tiempos de solución en los dispositivos que muestren problemas.

Se recomienda actualizar el hardware y software de la institución debido a la antigüedad de la internetwork de la IEFA.

Es necesario emitir políticas de seguridad de la información en la IEFA que guíen el tratamiento de la información y de los procesos relacionados con ella.

REFERENCIAS

Artículos Académicos

Kwon, J. (09 de 10 de 2013). Physical network infrastructure design based on user communication patterns. *The European Physical Journal B*(427). doi:<https://doi.org/10.1140/epjb/e2013-31117-2>

Bibliografía

ASAMBLEA NACIONAL. (2014). *Código Orgánico Integral Penal*. Obtenido de https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/ECU/INT_CEDAW_ARL_ECU_18950_S.pdf

CIS Controls. (2020). *Center for Internet Security*. Obtenido de https://www.cert.gov.py/application/files/7415/3625/3112/CIS_Controls_Version_7_Spanish_Translation.pdf

Community Cisco. (2020). *Conceptos básicos de redes*. Obtenido de https://community.cisco.com/legacyfs/online/attachments/document/enrutamiento-conceptos_basicos.pdf

Oppenheimer, P. (2011). *Top Down Network Design*. Indianapolis: Cisco Press.

Sitios Web

AVFIREWALLS. (2020). *AVFIREWALLS security gateway*. Obtenido de <https://www.avfirewalls.com/FortiGate-61E.asp>

CCNA. (16 de 03 de 2018). *Port address translation*. Obtenido de <https://ccnaeducation.com/port-address-translation-pat/>

CISCO. (2019). *Cisco Aironet 4800 Access Points*. Obtenido de <https://www.cisco.com/c/en/us/products/wireless/aironet-4800-access-points/index.html#~:stickynav=1>

CISCO. (2020). *Network Switch Competitive Comparison Chart*. Obtenido de <https://www.cisco.com/c/en/us/products/switches/switching-competitive-comparison.html>

CISCO. (2020). *Ruckus Indoor APs*. Obtenido de https://support.ruckuswireless.com/product_families/2-ruckus-indoor-aps

CISCO PRESS. (2020). *Understanding and Configuring Multilayer Switching*. Obtenido de <https://www.ciscopress.com/articles/article.asp?p=700137>

Cisco System. (2002). *Estándares de cableado*. Obtenido de <https://sites.google.com/site/redesbasico150/introduccion-a-los-estandares-de-cableado/estandares-tia-eia>

Cisco System. (28 de 03 de 2020). *Cisco Service Control Engine*. Obtenido de https://www.cisco.com/c/en/us/td/docs/cable/serv_exch/serv_control/broadband_app/rel315/swcfg315/swcfg/Line_Interface.html

CISO PLATFORM. (2020). *Comparisons of Next Generation Firewall products*. Obtenido de <https://products.cisoplatform.com/security/comparisons/next->

generation-firewall-ngfw/cisco-asa-firewall-vs-fortinet-ngfw-vs-palo-alto-networks-ngfw

- COMMUNITY CISCO. (2020). *What is the definition of SSID*. Obtenido de <https://community.cisco.com/t5/wireless-mobility-documents/what-is-the-definition-of-ssid/ta-p/3129972>
- COMPARITECH. (2020). *Norton vs Kaspersky: Which is best?* Obtenido de <https://www.comparitech.com/antivirus/norton-vs-kaspersky/>
- Cura, S. (2015). *Tipos de cableado de ethernet*. Recuperado el 07 de 09 de 2020, de <https://sofiacuraarias.wordpress.com/2015/05/26/tipos-de-cableado-ethernet/>
- DANYSOFT. (2020). *Monitoriza infraestructura de TI con PRTG network monitor*. Obtenido de <https://www.danysoft.com/prtg/#funciones>
- EVE - NG. (2020). *Emulated Virtual Environment Next Generation*. Obtenido de <https://www.eve-ng.net>
- Hernández, E. (2011). *Metodología top - down*. Obtenido de <https://docplayer.es/1992087-Top-down-network-design-metodologia-de-diseno-top-down-analisis-de-metas-de-negocio-y-restricciones.html>
- IEFA. (2020). *Institución Educativa Fiscal Amazonas*. Obtenido de <https://iefamazonas.wixsite.com/iefa>
- INEVAL. (2018). *Estudio comparativo de los resultados de Ser Bachiller*. Obtenido de <http://evaluaciones.evaluacion.gob.ec/BI/estudio-comparativo-de-los-resultados-de-ser-bachiller-2017-para-los-estudiantes-de-bachillerato-internacional-vs-los-de-bachillerato-general-unificado-en-ciencias/>
- Martinez, E. (2007). *Topologías de red*. Obtenido de <http://eveliux.com/mx/curso/topolog.html>
- NMAP. (2020). *Nmap free security scanner*. Obtenido de <https://nmap.org/zenmap/>
- NORTON. (2019). *Get multiple layers of protection for your Cyber Safety*. Obtenido de <https://us.norton.com/products>
- NORTONLIFELOCK. (2020). *Comparison to other Security Software Vendors*. Obtenido de <https://www.nortonsecurityonline.com/norton-comparison.html>
- PAESSLER AG. (2020). *PRTG, todas las funciones al detalle*. Obtenido de https://www.es.paessler.com/prtg/features?gclid=Cj0KCQjwvvi5BRDkARIsAGD9vII41HK_jyw-6pG5yJwjY5ZEFJhVK1Ea0BnoGcB9Ep1S_xlcVS0sSIkaAriyEALw_wcB
- RIVERBED TECHNOLOGY. (2020). *Riverbed's Modeler Academic Community*. Obtenido de https://cms-api.riverbed.com/portal/community_home
- RSCOMPUTACIÓN. (19 de 12 de 2019). *Magic Quadrant for Endpoint Protection Platforms*. Obtenido de <https://rscomputacion.com/2019/12/19/gartner-nombra-a-microsoft-lider-en-el-cuadrante-magico-de-las-plataformas-de-proteccion-de-endpoint-2019/>
- SPICEWORK. (2020). *Palo Alto PA-220 vs Cisco 5506 w/Firepower*. Obtenido de <https://community.spiceworks.com/topic/1986186-palo-alto-pa-220-vs-cisco-5506-w-firepower>
- Unitel. (2020). *Normas sobre cableado estructurado*. Obtenido de <https://unitel-tc.com/normas-sobre-cableado-estructurado/>

Tesis

- Cordero, G., & Marcillo, X. (2018). *Propuesta de diseño del Data center y reestructuración de la red de datos de la Universidad Estatal de Bolívar (Tesis de pregrado)*. Universidad Politécnica Salesiana, Quito. Obtenido de <http://dspace.ups.edu.ec/handle/123456789/15100>
- Guevara, J., & Quizhpi, D. (2017). *Diseño de la Red de Campus de la empresa "Equipos y Suministros de Telecomunicaciones EQUYSUM" de la ciudad de Quito (Tesis de pregrado)*. Universidad Politécnica Salesiana, Quito. Obtenido de <http://dspace.ups.edu.ec/handle/123456789/14613>
- Lagla, C. (2019). *Propuesta de rediseño de red de datos de la empresa Cobrafacil Fabrasilisa S.A bajo metodología PPDIOO y diseño TOP-DOWN (Tesis de pregrado)*. Universidad Politécnica Salesiana, Quito. Obtenido de <http://dspace.ups.edu.ec/handle/123456789/16686>
- Ocampo, C. (2016). *Análisis y diseño de la red para la nueva unidad educativa del milenio Leopoldo Lucero para la empresa Azuldata (Tesis de pregrado)*. Universidad Politécnica Salesiana, Quito. Obtenido de <http://dspace.ups.edu.ec/handle/123456789/11615>
- Shiguango, M., & Lara, R. (2013). *Rediseño de la red de datos, aplicando normas y estándares internacionales de cableado estructurado, y equipamiento de red, para el Gobierno Autónomo Descentralizado Municipal de Archidona, Provincia de Napo (Tesis de pregrado)*. Obtenido de <http://www.dspace.uce.edu.ec/handle/25000/1717>