UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA:

INGENIERÍA DE SISTEMAS

Trabajo de titulación previo a la obtención del título de:

Ingeniera de Sistemas

TEMA:

REDISEÑO Y PROPUESTA DE IMPLEMENTACIÓN DE LA RED LÓGICA DE LOS LABORATORIOS DEL BLOQUE D Y DATA CENTER DE LA CARRERA DE INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN DE LA UNIVERSIDAD POLITÉCNICA SALESIANA SEDE QUITO CAMPUS SUR.

AUTOR:

SOFÍA ALEXANDRA DÍAZ BALDEÓN

TUTOR:

JORGE ENRIQUE LÓPEZ LOGACHO

Quito, agosto del 2020

CESIÓN DE DERECHOS DE AUTOR

Yo Díaz Baldeón Sofía Alexandra con documento de identificación N° 1722417290, manifiesto mi voluntad y cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autora del trabajo de titulación intitulado: "REDISEÑO Y PROPUESTA DE IMPLEMENTACIÓN DE LA RED LÓGICA DE LOS LABORATORIOS DEL BLOQUE D Y DATA CENTER DE LA CARRERA DE INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN DE LA UNIVERSIDAD POLITÉCNICA SALESIANA SEDE QUITO CAMPUS SUR", mismo que ha sido desarrollado para optar por el título de INGENIERA 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 mi condición de autora me reservo los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hago entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

DÍAZ BALDEÓN SOFÍA ALEXANDRA

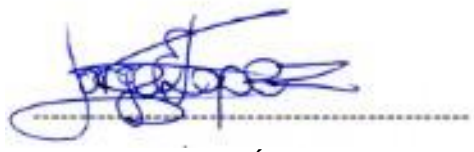
1722417290

Quito, agosto del 2020

DECLARATORIA DE COAUTORÍA DEL DOCENTE TUTOR

Yo declaro que bajo mi dirección y asesoría fue desarrollado el proyecto técnico, con el tema "REDISEÑO Y PROPUESTA DE IMPLEMENTACIÓN DE LA RED LÓGICA DE LOS LABORATORIOS DEL BLOQUE D Y DATA CENTER DE LA CARRERA DE INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN DE LA UNIVERSIDAD POLITÉCNICA SALESIANA SEDE QUITO CAMPUS SUR", realizado por Sofía Alexandra Díaz Baldeón, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerados como trabajo final de titulación.

Quito, agosto del 2020.



JORGE ENRIQUE LÓPEZ LOGACHO

CI: 1712082484

DEDICATORIA

Dedico este trabajo en primer lugar a Dios porque por su gracia y amor me ha bendecido y sin Él no lo habría alcanzado, a mis Padres y Hermano que han sido el pilar fundamental a lo largo de mi vida apoyándome en cada decisión y proyecto mostrándome el camino hacia mi superación personal, a mis Abuelitos quienes siempre me han brindado su apoyo incondicional.

Sofía Alexandra Díaz Baldeón

AGRADECIMIENTO

Agradezco a Dios por haberme bendecido y guiado para lograr una meta más en mi vida, a la Universidad Politécnica Salesiana y a cada uno de los Docentes que a lo largo de mi carrera estudiantil formaron sólidos conocimientos y han contribuido en mi formación académica, a mi tutor Ingeniero Jorge López por su profesionalismo, orientación y motivación para desarrollar y culminar con éxito mi proyecto de titulación.

Sofía Alexandra Díaz Baldeón

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ECUACIONES

RESUMEN

En el presente documento se pretende presentar la propuesta del rediseño de la red lógica del Data Center y bloque D de la Universidad Politécnica Salesiana sede Quito campus Sur, debido a que se ha notado un crecimiento exponencial en la misma, es por ello que por medio del uso de una metodología Top-Down se busca conocer las metas del negocio, falencias y virtudes dentro de la red y el modelo de la red.

Con la utilización de herramientas de monitoreo y simulación de datos se determina la situación actual de la red y generar así una propuesta acorde a los requerimientos, proponiendo y simulando las nuevas conexiones y las debidas configuraciones de protocolos en los diferentes dispositivos, con lo cual se desea garantizar una mejor administración de la red, y conseguir un mejor rendimiento tanto de los dispositivos como de las conexiones, conllevando así a brindar un mejor servicio hacia la comunidad universitaria.

En el capítulo 3 se encuentran tanto las configuraciones propuestas al igual que los resultados obtenidos de la simulación en cada escenario, y a través de la aplicación de ecuaciones de varianza y desviación media a los datos de throughput se concluye que la red presenta una mayor estabilidad en el escenario aplicado VLSM y direccionamiento dinámico.

ABSTRACT

This document aims to present the proposal for the redesign of the logical network of the Data Center and block D from Salesian Polytechnic University - Quito campus South, due to the fact that an exponential growth has been noted in it, which is why through the use of a methodology seeks to know the business goals, shortcomings and strengths within the network and the network model.

With the use of data monitoring and simulation tools, we want to understand the current situation of the network and thus generate a proposal according to the requirements, proposing and simulating the new connections and the proper protocols configurations in the different devices, with which it is desired to guarantee a better administration of the network, and to achieve a better performance of both the devices and the connections, thus leading to providing a better service to the university community.

Chapter 3 contains the proposed configurations and the results obtained from the simulation in each scenario, and through the application of variance equations and mean deviation to the throughput data, it is concluded that the network presents a greater stability with the application of VLSM and dynamic addressing.

CAPÍTULO I

INTRODUCCIÓN

1.1 ANTECEDENTES

En la Universidad Politécnica Salesiana Quito Campus Sur se encuentra el bloque D en donde se ubican tanto los laboratorios como también el DataCenter, incrementando así los servicios brindados a la comunidad universitaria; esto ha implicado que se incremente el número de usuarios conectados a la red y por lo tanto se ve la necesidad de que dichos servicios sean de alta calidad.

Las universidades, empresas y entidades gubernamentales cuentan con infraestructura de red que se han venido revisando, identificando así sus falencias tanto físicas como lógicas para así tomar las mejores decisiones y poder rediseñarlas. Ejemplo de esto lo constituye la Universidad Laica Eloy Alfaro¨ de Manabí (Aguaiza Tenelema, 2016), el Instituto Nacional de Estadísticas y Censos Matriz Central (Defaz Carrera & Gallegos Herrera, 2011), la empresa COBRAFACIL FABRASILISA S.A (Lagla Gallardo, 2019), la Institución *Educativa Túpac Amaru – Tumbes* (Lopez Quezada, 2018).

1.2 PLANTEAMIENTO DEL PROBLEMA

La Universidad Politécnica Salesiana Quito Campus Sur está conformada por diferentes bloques, equipados para satisfacer las necesidades de la comunidad universitaria, uno de ellos, el bloque D, provisto de laboratorios y que además alberga al Data Center, herramientas indispensables para la implementación de distintos servicios y clases prácticas al servicio de los estudiantes de las diferentes carreras, como son: Ingeniería de Sistemas, Electrónica, Civil, Mecánica y Ambiental el bloque se encuentra fuera de la red de la Universidad, sumándose a las razones por las cuales

ha existido un crecimiento de la red de datos a raíz de que han aumentado los servicios prestados por el Data Center desde su implementación, por lo cual se requiere un rediseño de la red lógica puesto que es necesario contar con diferentes configuraciones a nivel de conectividad de capa 2 y 3 para garantizar la confiabilidad e integridad de la información, y de igual manera garantizar un servicio ininterrumpido.

El proyecto contempla el análisis del estado inicial, el rediseño lógico, la respectiva simulación y la propuesta de la implementación en la red del bloque D.

1.3 OBJETIVOS

1.4 OBJETIVO GENERAL

Rediseñar y proponer la implementación de la red lógica de los laboratorios del bloque D y Data Center de la carrera de Ingeniería en Ciencias de la Computación de la Universidad Politécnica Salesiana, Sede Quito Campus Sur.

1.5 OBJETIVOS ESPECÍFICOS

- Analizar el estado inicial de la red del bloque D, recopilando información para determinar la red original.
- Analizar las falencias de la red permitiendo conocer la mejora a la red, integrando políticas de seguridad y QoS.
- Monitorear y analizar técnicamente la red rediseñada permitiendo comprobar que se han rectificado las falencias y que las configuraciones realizadas se encuentran en correcto funcionamiento.

1.6 METODOLOGÍA

La metodología aplicada es la de PPDIOO, la cual se basa en el ciclo de vida de redes PPDIOO (Preparación - Planificación - Diseño - Implementación - Operación -

Optimización), en cada una de ellas se adquiere diferentes datos, de igual manera dicha metodología permitirá conocer a fondo el objetivo de la red a rediseñar y optimizar.

Todas estas fases han sido aplicadas para conocer el estado de la red, sus falencias y así poder tomar las mejores decisiones respecto a la propuesta de rediseño, al igual que las configuraciones a realizar para que, al final se monitoree y se conozcan los resultados para saber si el rediseño propuesto ha sido exitoso.

1.7 ALCANCE

El trabajo a realizar es conocer el estado inicial de la red del bloque D y Data Center de la Universidad Politécnica Salesiana Quito campus Sur, con la finalidad de proponer el rediseño de la red brindando una solución frente a los requerimientos por parte de estudiantes y docentes colocando políticas de servicio, QoS, entre otras, consiguiendo en la red funcionalidad, adaptabilidad, flexibilidad y manejabilidad, conllevando a que los laboratorios y equipos de comunicación brinden los servicios de procesamiento y almacenamiento, para el desarrollo académico e investigativo de la comunidad universitaria.

Para la realización del rediseño de la red se deben conocer los servicios brindados, tipo de usuarios en la red y, como se dijo anteriormente, los requerimientos de los mismos, conllevando a la asignación de los recursos aumentando disponibilidad y calidad de servicio como también seguridad en la información, facilitando el procesamiento de aprendizaje y enseñanza.

Para la realización de lo antes mencionado se utiliza software de monitoreo, simulación, emulación y sniffers, herramientas que serán utilizadas desde el inicio del proyecto hasta su finalización permitiendo conocer el estado inicial de la red, realizar

las debidas configuraciones y ponerlas a prueba, con el objetivo de conocer si lo que se realizó permitió una mejora para la red.

Teniendo en cuenta que el objetivo del rediseño está enfocado a la LAN se puede tener en cuenta programas tales como Packet Tracer, CADE, Network Notepad, entre otras; en cuanto a emuladores y simuladores se tiene CNET Network Simulator, OPNET, GNS3, KivaNS entre otros.

1.8 JUSTIFICACIÓN

La red de datos del bloque D de la Universidad Politécnica Salesiana – Quito Campus Sur ha crecido desde el momento de su implementación, de igual forma, los servicios prestados por el Data Center han ido en aumento; con esto se ha dado paso a un mayor uso por parte de los docentes y estudiantes.

El servicio de virtualización permite que docentes y estudiantes puedan realizar sus investigaciones, proyectos de titulación, entre otros, dicha información debe ser resguardada ante cualquier intento de borrado o manipulación, ya que podría afectar en sobre manera la legitimidad al momento de presentar dichos trabajos. Los laboratorios no se encuentran con las debidas configuraciones de la red en cuanto a restricciones o accesos hacia la extranet, es por ello que existe un mayor riesgo en el manejo de la información.

Como se mencionó, actualmente la red brinda servicios a docentes y estudiantes, los paquetes de dichos servicios son tratados de igual manera en toda la red y conforme se ha dado el crecimiento de la red se produce congestión, por lo cual la entrega de paquetes se ralentiza, y en panoramas críticos, se pueden llegar a perder la información. Por lo tanto, con el incremento de volumen de tráfico, expansión de servicios, protocolos, multimedia entre otras se optó por aplicar QoS o calidad de

servicio, el cual permite reconocer los diferentes flujos de tráfico para así especificar el trato de cada uno y priorizar un tipo de tráfico sobre otro, con ello se llega a la coexistencia de diferentes servicios sin que el consumo de banda ancha se vea afectado.

La aplicación de políticas de seguridad permitirá que se controle la corrupción o borrado de información, al igual que el acceso a páginas no fiables permitiendo así prevenir la obtención de información con datos maliciosos o corruptos, finalmente para la disponibilidad de la información y servicios se realizará la configuración de diferentes protocolos como HSRP.

CAPÍTULO II

MARCO TEÓRICO

2.1 DEFINICIÓN DE REDES COMPUTACIONALES

Una red informática es "la infraestructura que posibilita que varios dispositivos intercambien datos entre sí, conectados para ello a algún medio físico que permita la transmisión de dichos datos" (Moreno Pérez & Santos González, 2014), de manera más simple se puede decir que es la conexión entre dos o más equipos mediante dispositivos alámbricos o inalámbricos, permitiendo su comunicación y compartiendo recursos, más los cuales no son controlados por computadoras centrales, por lo que se puede decir que las redes informáticas son autónomas. La comunicación se logra debido a la implementación de estándares, los cuales abarcan conectividad, transporte, protocolos, entre otros; permitiendo así la traducción de las acciones de los usuarios a comandos que puedan interpretar los equipos (Calderón Zetter, 2016).

El compartir recursos sin que exista impedimento geográfico es el objetivo principal de las redes informáticas, proporcionando disponibilidad de la información.

2.1.1 CLASIFICACIÓN

La clasificación de una red informática se puede realizar de diferentes maneras, tales como: tipo de conexión, alcance, relación funcional, etc.

2.1.1.1 Por su relación funcional

"El término relaciones entre redes se refiere a la forma en que una computadora utiliza los recursos de otra a través de la red" (Hallberg, 2006), por lo cual este tipo de redes se basan en realizar un intercambio de información a través de sus relaciones, existiendo así dos tipos:

- Red de punto a punto.
- Red cliente/servidor.

2.1.1.2 Por el alcance

- Red de área personal (PAN).
- Red de área metropolitana (MAN).
- Red de área amplia (WAN).
- Red de área local (LAN).

2.2 RED DE ÁREA LOCAL

Local Area Network por sus siglas en inglés, es una red a la cual los dispositivos se encuentran en un área geográfica limitada, llegando máximo a unos cientos de kilómetros de distancia, lo imprescindible de esta red es que los dispositivos conectados se encuentren dentro de una misma unidad organizativa; el ancho de banda dentro de esta red brinda una alta velocidad para el acceso a los servicios brindados (Olifer & Olifer, 2009).

2.3 MODELO JERÁRQUICO

El modelo de diseño jerárquico, propuesto por Cisco, incluye tres capas, permitiendo "implementar funciones específicas, simplificando tanto la implementación como la administración de la red" (Cisco, 2014). Dependiendo de las características y requerimientos de la red se utiliza dos o tres capas.

Ventajas del modelo jerárquico

- Escalabilidad

Al tener una jerarquía la red puede expandirse y crecer de acuerdo a los requerimientos del usuario, debido a que en cualquier capa se pueden agregar más nodos a la red y así conectar una mayor cantidad de dispositivos.

- Redundancia

  Se refiere a que tanto nodos como componentes de los mismos se encuentran replicados (Editorial Team GRITS, 2013) en la red, permitiendo así que se encuentre disponible en cualquier momento ante cualquier fallo.

- Rendimiento

  Dentro de la red se puede ver incrementado el flujo, siendo este más intenso, por ello en la red se puede incrementar un switch de alto rendimiento conllevando a mejorar la comunicación.

- Seguridad

  En cada capa se pueden emplear configuraciones o políticas de seguridad en cada dispositivo, como por ejemplo en switches, se pueden configurar el flujo de información de los puertos.

- Facilidad de administración

  La administración y mantenimiento de la red se vuelve más fácil debido a que la misma se encuentra segmentada, teniendo cada capa asignada sus tareas, esto conlleva a una supervisión adecuada.

2.3.1 CAPA DE ACCESO

Es la capa en donde se encuentran los dispositivos finales, es decir los dispositivos manejados por el usuario, y por los cuales se acceden a los servicios prestados, el objetivo de esta capa es el permitir que exista conexión entre los dispositivos y la red, y controlar que dispositivos acceden a la misma.

Los dispositivos que se encuentran en esta capa tienen una conectividad a 10/100/1000 Mbps, perteneciendo a ellos se encuentran los switch, puntos de acceso, teléfonos IP. Laptops, entre otros; el acceso de dichos dispositivos debe ser controlado para proteger la red de ataques maliciosos, pero garantizando el acceso a servicios autorizados.

2.3.2 CAPA DE DISTRIBUCIÓN

En la capa de distribución se hace posible la comunicación entre la capa de acceso y la capa central, proveyendo enrutamiento, filtrado, acceso a la WAN, y permitiendo o denegando el paso de paquetes hacia la capa central, utilizando políticas y realizando la configuración entre las LAN virtuales (VLAN).

De igual manera permite la escalabilidad, ya que reduce los gastos operativos, exigiendo menos cantidad de memoria, y permitiendo la agregación para múltiples switches de la capa de acceso (Cisco, 2014).

2.3.3 CAPA DE NÚCLEO O CENTRAL

Se llama capa núcleo debido a como su nombre lo dice es el núcleo de la red, en ella se realiza la comunicación con la capa de distribución, y de igual manera permite la conexión con el internet, es por ello que es indispensable que tenga una gran velocidad.

Se encarga de que el transporte de la información sea confiable y rápido, se debe tener en cuenta que los fallos en esta capa afectan a toda la red, por lo cual se debe configurar la tolerancia a fallos; para que en esta capa se maneje fiabilidad se debe considerar tecnologías de enlace de datos como FDDI, enlaces redundantes, entre otros, mientras que para la velocidad se debe tener en cuenta la latencia por lo cual la implementación de protocolos de enrutamiento en la capa de distribución debe ser analizada tomando en cuenta los tiempos de convergencia.

2.3.4 MODELO JERÁRQUICO CON NÚCLEO COLAPSADO

El modelo de núcleo colapsado es en el cual se combina la capa de distribución y la de núcleo en una sola, conllevando a que las funciones de cada una de ellas sean aplicadas en un solo dispositivo, siendo estos, equipos con mayor prestación.

Lo que se busca con este tipo de modelo es la reducción de costos y tener menos puntos de fallas sin perder las ventajas que brinda el modelo de tres capas. Según (Ariganello E. , 2016) el dispositivo de núcleo-distribución colapsado debe proporcionar lo siguiente:

- Rutas físicas y lógicas de alta velocidad de conexión a la red.
- Servir como punto de demarcación entre acceso, núcleo y de concentración de capa 2.
- Definir las políticas de acceso y de enrutamiento.
- Proveer calidad de servicio (QoS), virtualizacion de red etc.

Modelo jerárquico

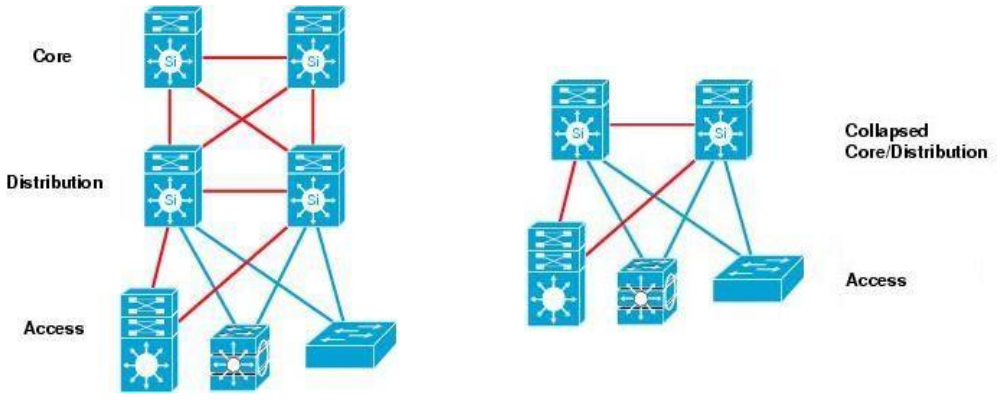


Figura 1 Modelo jerárquico de 3 capas y colapsado.

Fuente: (Sepúlveda, 2019).

2.4 QoS CALIDAD DE SERVICIO

La calidad de servicio es “el conjunto de parámetros que especifican las prestaciones que el usuario espera del servicio de interred extremo a extremo y a las facilidades opcionales que éste le proporciona” (Hernández Cueto & Vargas Galindo, 2018). QoS ayuda a medir ancho de banda, jitter, rendimiento, disponibilidad, entre otros; al medir tales criterios de la red se puede llegar a realizar una priorización de cierto tipo de tráfico sobre otro, permitiendo que el ancho de banda no se vea afectado y por tanto no exista una gran congestión en la red.

Actualmente el internet es una herramienta que se utiliza día a día, en la cual se realizan transacciones de información, sean educativas, personales o informativas, más el usuario requiere que toda esta información sea fiable y segura, pero en el envío de información, según Cisco, pueden ocurrir tres diferentes situaciones:

Delay o retraso

Se define retraso a la demora de llegada de un paquete a la terminal correspondiente; puede llegar a ocurrir debido a tráfico en la red o que el paquete tome una ruta más larga para evitar la congestión de la misma.

Fluctuación o jitter

Es la **“**Variación en el retraso**”** (Ariganello & Barrientos Sevilla, 2010), dependiendo de la posición en las colas, a lo largo del camino, se producen dichas variaciones afectando gravemente al flujo de audio y/o video, ya que se pueden producir cortes.

Pérdida

La pérdida se llega a dar en casos extremos, y sucede en el momento en que la red se encuentra congestionada, por lo que los paquetes se eliminan sin que sean entregados.

Para que estas situaciones no se den existen dos modelos de QoS basadas en redes IP según el IETF (Referencia: Internet Engineering Task Force), Integrated Service (Intserv) y Differentiated Service (Diffserv), dichos modelos tratan sobre el manejo preferencial al tráfico especificado.

2.5 SERVICIOS DIFERENCIADOS

Este modelo se basa en la clasificación de tráfico para después realizar el marcado de paquetes, llevando a cabo una buena escalabilidad y flexibilidad; "los servicios diferenciados generan un comportamiento diferente por salto en cada router o switch inspeccionando la cabecera de cada paquete para decidir cómo realizar el envío de ese paquete" (Ariganello & Barrientos Sevilla, 2010), es decir que se configuran políticas por sí mismo cada router o switch permitiendo a la vez tomar decisiones respecto a tipos de paquetes anteriormente enviados, en este modelo se encuentran dos tipos de routers, los de frontera en donde se realiza el marcado de tráfico y los internos los cuales se encargan de la congestión.

2.6 SERVICIOS INTEGRADOS

Este sistema trabaja con la metodología de reservar el ancho de banda adecuado para el envío de la información que requiera de una mayor prioridad, con la ayuda del protocolo RSVP (Resource Reservation Protocol), el cual se dirige por la red a través de cada router conociendo si la petición es soportada, hasta llegar al destino y dando a conocer el camino aceptado. (Ariganello & Barrientos Sevilla, 2010) Se definen dos servicios básicos en este sistema:

2.6.1 GARANTIZADO

Es un servicio encaminado a aplicaciones en tiempo real, garantizando que los datagramas lleguen a pesar del desbordamiento de cola y en el tiempo adecuado,

siempre que el flujo permanezca dentro de los parámetros de tráfico especificado (Shenker, Partridge, & Guerin, 1997).

2.6.2 DE CARGA CONTROLADA

Este servicio requiere de menores recursos, por lo cual se encuentra dirigido a aplicaciones que tienen un correcto funcionamiento en las actuales condiciones de internet más su rendimiento se degrada en situaciones de sobrecarga (Loor Fonseca & Pichoasamín Morales, 2001).

2.7 VLAN

La utilización de dispositivos de capa 2 en una red es llamada “red plana”, en ella existe un solo dominio de difusión y al aumentar dispositivos finales el desempeño de la red decrece debido a que los mensajes de broadcast inundan la red. La solución es el implemento de redes virtuales (VLAN), las cuales permiten que la red pueda ser segmentada, y que se creen grupos para cada tipo de usuario, permitiendo y denegando accesos, manejando así la seguridad en la red.

La comunicación entre las VLAN es indispensable si en la red se configura y maneja una gran cantidad de ellas, para ello se recurre al enrutamiento de switches multicapa o routers con conexiones físicas o lógicas hacia cada VLAN.

METODO ANTIGUO

Se lo realiza utilizando routers y switches, conectando cada interfaz física y configurando cada una de ellas en modo acceso y asignar estáticamente la VLAN a utilizar.

ROUTER-ON-STICK

De igual manera que en el método antiguo, se requiere routers y switches, más la configuración se lo realiza en el router, el cual se encarga del enrutamiento y del envío de paquetes por una misma interfaz física, al igual que la utilización de diferentes subinterfaces dedicadas a cada VLAN. En este modelo se define el modo en el que se va a utilizar la interfaz del router, siendo este configurado en modo troncal, debido a que existe flujo de información de diferentes de dispositivos que se encuentran en la misma VLAN, pero conectados a distintos switches (Cisco, 2017).

2.8 SVI (Interfaces virtuales)

En este método, se requiere switches multicapa, en los cuales se realiza toda la configuración, la cual es similar a la configuración de un switch de capa 2, en cada VLAN se configura una IP, y se coloca el comando para que el switch opere como un switch de capa 3.

2.9 VTP

La administración de VLAN en redes pequeñas puede ser fácilmente manejable si su configuración es manual, pero cuando se trata de redes más grandes y con proyección de escalabilidad se dificulta debido a que la configuración se debe realizar en cada switch. VTP, protocolo de enlace troncal, es un protocolo que permite configurar y administrar de mejor manera el dominio de las VLAN, debido a que se puede crear, borrar y renombrar las VLAN en un switch y este enviar dicho cambio a los demás switches de la red; este protocolo opera en tres modos distintos.

SERVIDOR

El switch que se configure en este modo es capaz de crear, renombrar y eliminar las VLAN, además de propagar la configuración realizada hacia los demás switches y los

sincronizan, esta comunicación se la realiza por los enlaces troncales. Dentro de una red solo puede existir un switch en este modo.

CLIENTE

En este modo, los switches no pueden realizar ninguna configuración a las VLAN, solo guardar la información que provenga del servidor, mientras que el dispositivo se encuentre activo. (Cisco, 2014)

TRANSPARENTE

En el modo transparente al igual que en el cliente, no puede realizar ningún cambio a las VLAN para que los demás switches actualicen, la configuración que se realice solo va a ser modificada localmente. El modo transparente no participa en el proceso de VTP, pero es capaz de reenviar los mensajes. cuando se realiza la configuración. (Ariganello & Barrientos Sevilla, 2010)

Utilizando VTP, cada switch anuncia las VLAN dependiendo de cada versión, de igual manera da a conocer los puertos troncales, dominio y contraseña; esta información solo se la pasa cuando los switches se encuentran en el mismo dominio. Los dominios permiten que los switches que utilizan la misma información sean agrupados. (Ariganello & Barrientos Sevilla, 2010)

2.10 STP

Spanning Tree Protocol, por sus siglas en inglés, es un protocolo que mantiene la red libre de bucles, a pesar de que se tenga trayectorias redundantes; este protocolo es configurado en capa 2, es decir que se ejecuta en bridges y switches. (Cisco, 2017)

STP detecta cualquier fallo en la red debido a que la explora constantemente y, a pesar de que la topología cambie, el protocolo realiza una reconfiguración de los puertos

evitando una pérdida total de la conectividad, todo esto se realiza mediante el uso del algoritmo de spanning tree (STA), dicho algoritmo designa un único switch como root bridge o puente raíz pero muchas veces la elección no es la más adecuada, por lo cual se debe realizar las configuraciones pertinentes para definir el root bridge que sea más conveniente y, a partir de ahí las funciones de los puertos son configurados, existiendo dos posibles tipos:

- **Puerto raíz-.** Proporciona la conectividad, y por el cual se alcanza al root bridge, conllevando a evaluar el coste de la ruta.
- **Puerto designado-.** Su funcionamiento es tal como un puerto normal, enviando tramas y BPDU.

Los puertos pueden encontrarse en diferentes estados, dependiendo del progreso en la red, son los siguientes:

- **Bloqueo-.** El puerto en este estado no es capaz de generar bucles en la red, se recibe las BPDU, pero no los envía.
- **Escucha-.** Se llega a este estado cuando el switch determina que puede ser seleccionado como puerto raíz o designado, si la ruta tiene un coste mayor, vuelve al estado de bloqueo.
- **Aprendizaje-.** Luego del período de escucha, el puerto empieza a enviar y recibir BPDU actualizando su tabla de direcciones MAC.
- **Envío-.** Este estado se logra después de cierto tiempo en Aprendizaje, aquí se envía y recibe tanto tramas como BPDU y de igual manera aprende y guarda las direcciones MAC.
- **Desactivado-.** El administrador de la red es quien configura este estado, o también se puede llegar si existe algún fallo en el sistema.

2.11 HSRP

Actualmente las organizaciones cuentan con un gran número de usuarios a los cuales ofrecen diferentes servicios, es por ello que no pueden permitir que exista inestabilidad en la red, conllevando a que la misma no se encuentre disponible, por esta razón la configuración de HSRP en la capa 3 permite la aplicación de redundancia tanto en dispositivos como enlaces, conllevando a que la información sea enviada por el dispositivo duplicado al existir alguna falla y así garantizar la estabilidad en la red.

Hot Stand-by Redundancy Protocol es un protocolo, configurado en capa 3, el cual permite asegurar la fiabilidad de la red, dando paso a la redundancia entre dos o más dispositivos; los routers que tienen redundancia, es decir, que pertenecen a un mismo grupo utilizan la misma IP y MAC virtual, teniendo cada dispositivo un estado, sea primario o standby.

En cada router se configura una prioridad y de allí se determina los estados de los routers, siendo así el que tiene mayor prioridad será el router primario y los otros serán standby. Entre estos routers existe el intercambio de paquetes tipo hello, esta comunicación ayuda a determinar cuándo se ha producido un fallo cambiando el estado de un router de standby a primario y encargándose de enviar el tráfico. (Huawei Technologies Co. Ltd, 2018)

CAPÍTULO III

ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED Y PROPUESTA DE REDISEÑO DE LA RED

3.1 DESCRIPCIÓN DEL ENTORNO

Mediante la utilización de la metodología PPDIOO en este capítulo se expone la situación actual de la red, sus elementos y la forma de ser administrada; para ello se han utilizado diferentes herramientas que han posibilitado obtener dicha información.

Dentro de la Universidad Politécnica Salesiana Quito Campus Sur se ubica el bloque D, el cual está equipado con laboratorios requeridos por la comunidad universitaria, de igual manera en este bloque se encuentra el Data Center, herramienta indispensable para la implementación de distintos servicios.

El edificio del bloque D se encuentra conformado por: una planta baja donde se encuentran 4 laboratorios y un piso donde está alojado el Data Center en conjunto con un laboratorio.

A continuación, se muestra las imágenes correspondientes a la planta baja y planta alta del bloque D.

Planta baja bloque D

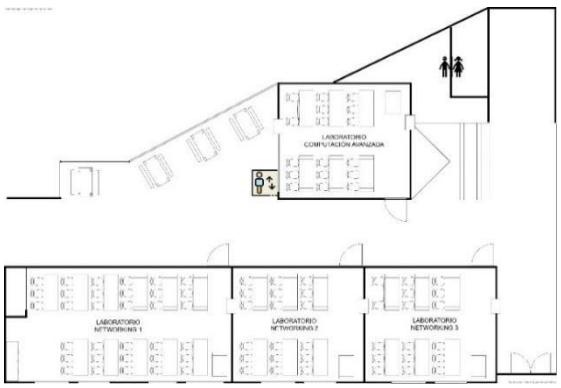


Figura 2 Plano planta baja bloque D.

Fuente: La autora..

Planta alta bloque D

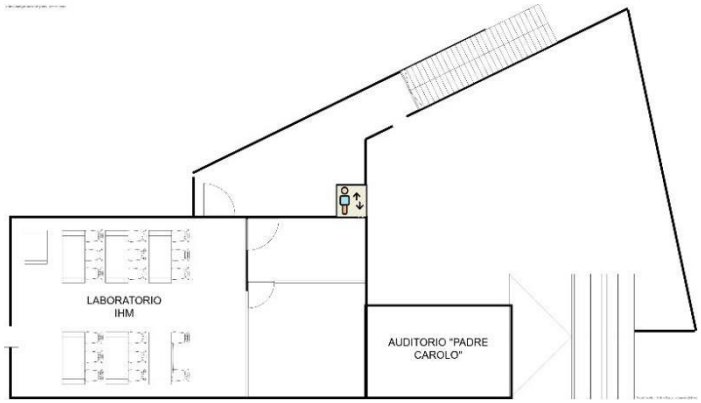


Figura 3 Plano planta alta bloque D.

Fuente: La autora..

Dentro del Data Center se encuentra en el Rack 1 cuatro switches, el primero es el switch de capa 3 administrable, Cisco Catalyst 9300 que consta de 48 puertos, el mismo se encuentra conectado con el Data Center ubicado en el bloque A, dicha conexión permite obtener ciertas políticas, las cuales han sido implementadas para toda la comunidad universitaria; de igual manera se conecta con el laboratorio de Sistemas Embebidos ubicado en el bloque C.

Siguiendo al Cisco Catalyst 9300 se encuentran conectados tres switches Cisco, dos de ellos son los switches Cisco SG550 de 24 puertos y de igual manera se encuentra el switch Cisco SG500 de 24 puertos.

Dentro del Rack 2 se encuentran 2 switches SAN HPE SN3000B de 24 puertos, los mismos que se encuentran conectados al clúster conformado por 3 servidores HP Apollo ProLiant XL230a y un servidor HP Apollo ProLiant XL250a, y el clúster se encuentra conectado a los dos servidores de almacenamiento, HPE 3PAR StoreServ 8200 y SAN HPE MSA 2050 obteniendo así un almacenamiento de 110TB.

La comunicación de los servidores es a través de fibra óptica y aplicando redundancia en cada dispositivo. En la tabla 1 se muestran los dispositivos activos dentro del Data Center.

Tabla 1 Dispositivos activos del Data Center

TIPO	MODELO	CANTIDAD
Storage HPE	3PAR Storage 8200	1
Storage HPE	MSA 2050 SAN Storage	1
Switch Cisco	Catalyst WS-C2960	3
Switch Cisco	Catalyst 2960-X	1
Switch Cisco	Catalyst 9300	3
Servidor HP Apollo	ProLiant XL230a Gen9	3
Servidor HP Apollo	ProLiant XL250a Gen9	1
Servidor HP Apollo	ProLiant XL190a Gen9	2
Switch SAN	HPE SN3000B 24/12 FC	2
Wireless Access Point	Cisco 802,11AC W2 AP	3

Fuente: La autora.

3.2 ANÁLISIS DE LA RED EXISTENTE

En la figura 4 se muestra la topología lógica que actualmente dispone el Data Center, donde se puede observar de igual manera que la red LAN trabaja de acuerdo al modelo jerárquico con núcleo colapsado, este modelo se ha implementado debido a razones presupuestarias y teniendo en cuenta el tamaño del espacio físico en el que se encuentra.

La red cuenta con diferentes dispositivos interconectados con redundancia, siendo la tasa de velocidad de transmisión entre servidores de 10Gbps a 16Gbps, mientras que la velocidad de los switches hacia los dispositivos es de 1Gbps. La conexión implementada entre bloques está realizada mediante fibra, en cuanto a la conexión horizontal está realizada por medio de cable UTP Cat 6a, y dentro del Data Center la conexión utilizada entre los racks de servidores y de comunicaciones está realizada con cable UTP Cat 7.

Topología lógica de la red

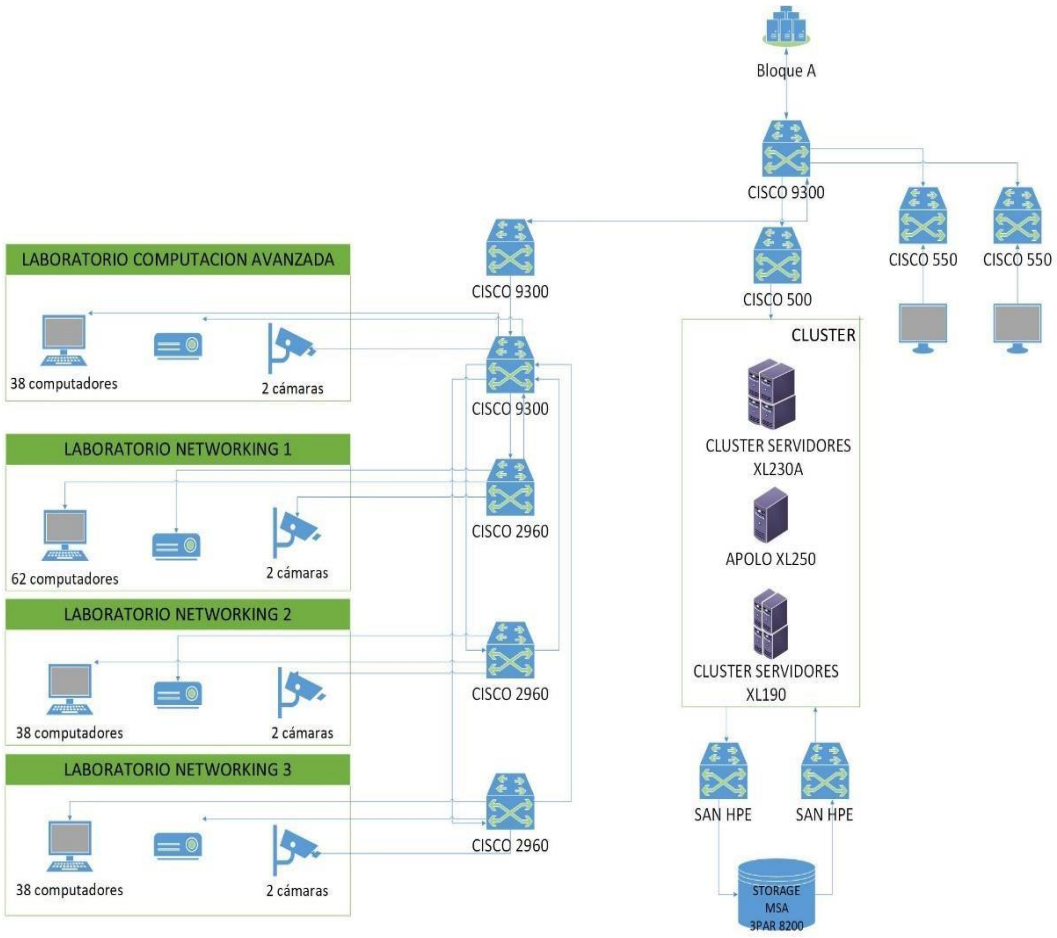


Figura 4 Topología Lógica.

Fuente: La autora.

3.2.1 SERVICIOS

3.2.1.1 Conectividad

El Data Center brinda el servicio de conectividad a todo el edificio del bloque D dicho servicio permite la comunicación entre los diferentes dispositivos y terminales simultáneamente.

La comunidad universitaria tiene la facilidad del ingreso a los servicios tanto presencial como remotamente, obteniendo seguridad de conexión, velocidad y libre

acceso a herramientas educativas al momento de requerir la utilización de los laboratorios y máquinas virtuales.

3.2.1.2 Virtualización

La virtualización es una tecnología que permite la abstracción de la realidad física de las máquinas en quese ejecuta el software (R. Gavilán, 2019). Es decir que permite la creación lógica de dispositivos o recursos sin que se pierda el potencial que poseen los mismos, siendo estos sistemas operativos, servidores, entre otros.

Este servicio es un activo importante dentro del Data Center, debido a que realiza un gran aporte al lograr la creación de máquinas virtuales conllevando a brindar a la comunidad universitaria el uso de las mismas para la realización de proyectos y tesis.

3.2.1.3 Seguridad

El servicio de seguridad brindado por el Data Center tiene como objetivo principal el salvaguardar la información, ya que es el activo más importante dentro de cualquier empresa. Por lo tanto, administradores y usuarios se rigen a políticas como el uso de contraseñas conllevando así a proporcionar confidencialidad en la información. Debido a la conexión existente entre el bloque A y el bloque D, la red del Data Center se encuentra allanada por políticas proporcionadas por el departamento de TI de la Universidad Politécnica Salesiana Campus Sur, el cual restringe el acceso a ciertas páginas de contenido dudoso o indebido.

3.2.1.4 Almacenamiento

El servicio de almacenamiento brindado por el Data Center proporciona una capacidad de 110TB el cual se encuentra conformado por tres sistemas; MSA el cual cuenta con

24 discos SSD, el 3PAR Master cuenta con 26 discos SSD y finalmente el 3PAR -UPS cuenta con 24 discos, siendo estos, 10 discos SSD y 14 discos FC.

Dicho servicio se encuentra administrado por la plataforma de virtualización VMware vSphere, y permite que el acceso a información fundamental para la comunidad universitaria como estudiantes y docentes sea sencillo, de igual manera permite alojar contenido de proyectos e investigaciones sin que sea importante el tamaño de los mismos.

3.2.2 DIRECCIONAMIENTO

El Data Center maneja dos segmentos de red, una maneja los servidores, máquinas virtuales, accesos remotos; la segunda red es la perteneciente al direccionamiento dentro de los laboratorios. Las direcciones que manejadas en cada red 172.17.42.0/24 y 172.17.44.0/24, respectivamente; la asignación de direcciones IP dentro de cada red son asignadas y administradas por el personal dentro del Data Center.

3.2.3 ANÁLISIS DEL TRÁFICO DE RED

El análisis del tráfico de red es un paso importante ya que es imprescindible conocer el completo estado en el que se encuentra la red del Data Center, conllevando así a conocer los servicios más utilizados y el flujo que estos generan tanto de entrada como de salida.

Para ello se ha utilizado herramientas de monitoreo tales como PRTG y Wireshark permitiendo así conocer tanto el uso de los recursos como también el tráfico dentro de la red. El monitoreo de la red utilizando PRTG fue realizado por un periodo de dos semanas, conociendo el tráfico en diferentes servidores y enlaces de la red, de igual manera, el monitoreo realizado con Wireshark tuvo una duración de tres días y con

dicho monitoreo se conoció los protocolos presentes dentro del Data Center, y sus ocurrencias, todo ello se detalla a continuación.

Tabla 2 Protocolos presentes dentro de la red

Protocolos	Ocurrencias	Porcentaje
UDP	1.985.080	2962,12%
LLMNR	1.491.652	2225,83%
MDNS	1.412.289	2107,41%
FIP	712.590	1063,32%
NBNS	554.620	827,60%
TCP	269.691	402,43%
ARP	108.870	162,45%
SSDP	68.967	102,91%
DHCPv6	55.108	82,23%
DHCP	15.009	22,40%
BROWSER	13.088	19,53%
HTTP	5.753	8,58%
DNS	5.482	8,18%
ICMPv6	3.304	4,93%
ICMP	46	0,07%
TOTAL	**6701549**	**100%**

Fuente: La autora.

PROTOCOLO TCP

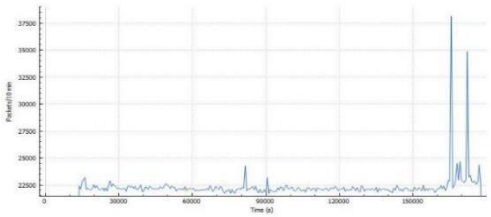


Figura 5 Monitoreo protocolo TCP.

Fuente: La autora.

PROTOCOLO DHCP

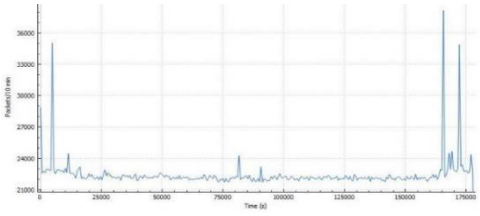


Figura 6 Monitoreo protocolo DHCP.

Fuente: La autora.

PROTOCOLO HTTP

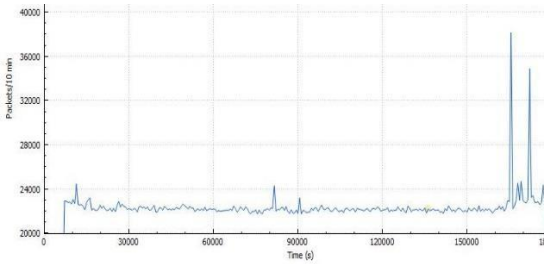


Figura 7 Monitoreo protocolo HTTP.

Fuente: La autora.

PROTOCOLO DNS

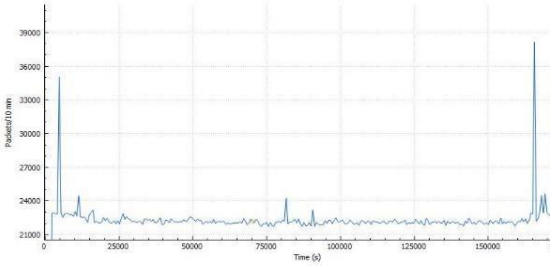


Figura 8 Monitoreo protocolo DNS.

Fuente: La autora.

PROTOCOLO UDP

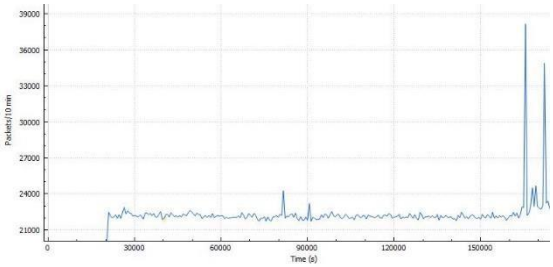


Figura 9 Monitoreo protocolo UDP.

Fuente: La autora.

Lo que se puede observar en el monitoreo de los protocolos con Wireshark es que existe una variación entre 2200 y 2500 paquetes enviados y recibidos cada 10 minutos; con un pico, conllevando así a tener un máximo de 3800 paquetes enviados y recibidos durante 10 min.

	Sensor	Promedio	Mínimo	Máximo
1.	(002) eth0 Traffic	25.734 kbit/s	33 kbit/s	1.252.801 kbit/s
2.	(1073741825) FC port 0/1 Traffic	21.869 kbit/s	12.621 kbit/s	690.815 kbit/s
3.	(1073741829) FC port 0/5 Traffic	13.225 kbit/s	6.443 kbit/s	224.259 kbit/s
4.	(1073741833) FC port 0/9 Traffic	9.578 kbit/s	495 kbit/s	681.387 kbit/s
5.	(002) HPE FlexFabric 10Gb 2-port 533FLR-T Adapter Traffic	8.018 kbit/s	1.478 kbit/s	83.701 kbit/s

Figura 10 Sensores de ancho de banda más usados.

Fuente: La autora.

Los resultados obtenidos del monitoreo de PRTG respecto a los enlaces permite conocer los 5 primeros de ellos que hacen mayor uso de ancho de banda, siendo el primero el enlace de ethernet, del cual se obtuvieron los siguientes resultados, mostrados en la figura 11 y figura 12.

Monitoreo enlace ethernet – 15 días

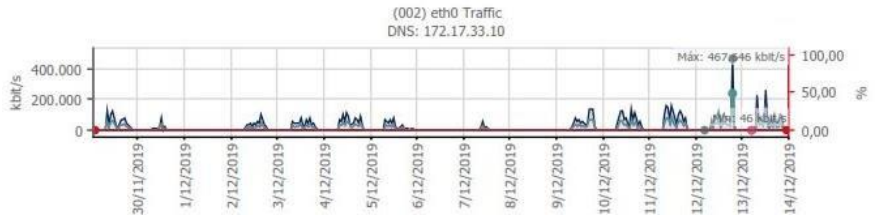


Figura 12 Monitoreo del enlace ethernet por 15 días.
Fuente: La autora.

Monitoreo enlace ethernet – 11 horas

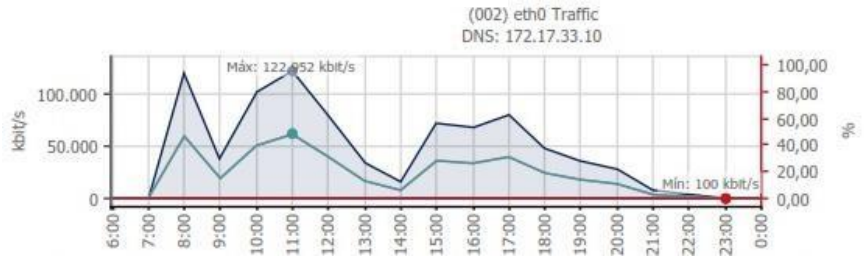


Figura 11 Monitoreo del enlace ethernet por 11 horas.
Fuente: La autora.

A partir de la información recolectada se ha realizado la simulación del entorno actual del Bloque D y Data Center en la herramienta Opnet, en ella se han colocado dispositivos con características similares a los que se encuentran dentro de la red para generar gráficas similares a la realidad.

La topología detallada en la figura 14 muestra la red en su estado inicial, en dicha topología se ha realizado las configuraciones actuales tanto de las direcciones IP como de igual manera distintos servicios, los cuales generan un tráfico similar al que se encuentra dentro de la red; con ello se pudo realizar la simulación de 3 horas para obtener datos que a futuro van hacer comparados con la propuesta de implementación del rediseño de la red.

En la figura 14 se puede apreciar el servicio BDD el cual ha sido implementado para simular el tráfico de la red y se puede observar que los paquetes enviados tienen un máximo de 42000 y un promedio de 22000 paquetes, valores similares a los obtenidos en la red real.

Servicio de base de datos

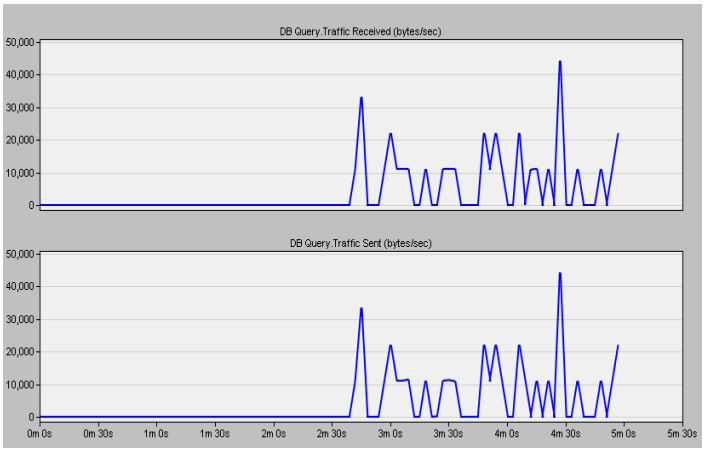


Figura 13 Servicio BDD.
Fuente: La autora.

Topología inicial de la red

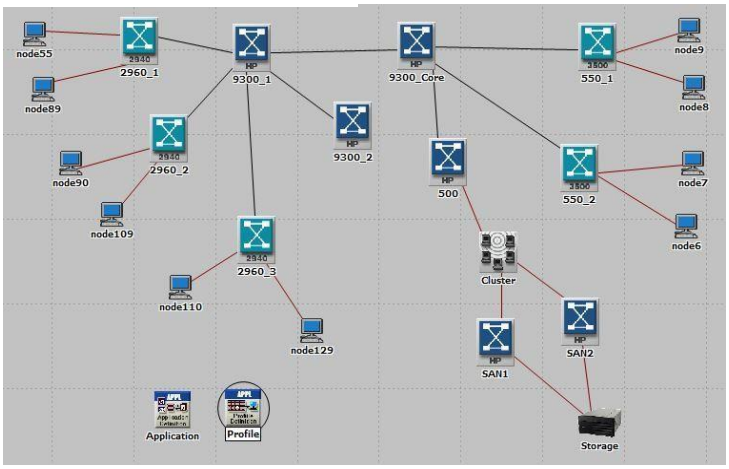


Figura 14 Topología inicial de la red.
Fuente: La autora.

3.3 PROPUESTA DE REDISEÑO DE LA RED

Después de haber analizado las características actuales de la infraestructura del bloque D de la Universidad Politécnica Salesiana se procede a proponer el rediseño de la red.

3.3.1 TOPOLOGÍA DE RED

Para el nuevo diseño de la red se ha tomado en cuenta la implementación de redundancia en los dispositivos sustanciales al igual que la aplicación de ciertos protocolos los cuales permiten aprovechar los enlaces redundantes, permitiendo así que la red sea más estable y no exista pérdida de información o datos ante algún fallo por parte de los dispositivos.

Por lo antes mencionado se plantea la propuesta de conexiones y topología de la red presentada en la figura 15; en ella se puede observar que el switch core Cisco Catalyst 9300 permanece de la topología inicial, más el cambio que se propone son las conexiones hacia los siguientes switch Cisco Catalyst 9300 y de igual manera entre ellos, siguiendo de los switches mencionados se realizan las conexiones desde los mismos hacia los switch Catalyst 2960 finalmente estos conectados a los dispositivos finales; por otra parte se encuentran las conexiones de los switches Cisco SG550 y SG500, este último switch se comunica con el clúster de servidores HPE Prolliant, el mismo conectado hacia el servidor de almacenamiento; las conexiones mencionadas se han propuesto con la finalidad de tener redundancia y poder así activarla e implementar los diferentes protocolos HSRP, STP, VTP, entre otros; permitiendo así garantizar el correcto funcionamiento de la red ante cualquier fallo presentado tanto en dispositivos como en nodos.

Topología propuesta

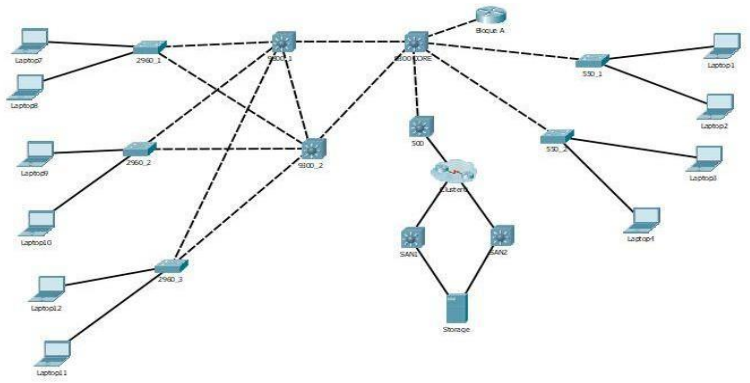


Figura 15 Topología propuesta.
Fuente: La autora.

3.3.2 DIRECCIONAMIENTO

Partiendo de la información sobre el tamaño de la red dentro del Data Center se han diferenciado cuatro subredes, las cuales se conectan con el objetivo de acceder a los servicios e información, dichas subredes actualmente se encuentran con el direccionamiento administrado por el personal del Data Center, siendo una práctica deficiente para la administración de las direcciones y un trabajo extra para el personal.

Para la propuesta de direccionamiento se toma en cuenta la capacidad de crecimiento de la red, es por ello que al conversar con los administradores del DataCenter se acordó realizar un incremento del 30% a la cantidad actual de dispositivos de cada subred permitiendo conocer el escalamiento de cada una de ellas, dicha información se puede encontrar en la tabla 3.

Tabla 3 Proyección de la cantidad de dispositivos en el siguiente año

Subred	Cantidad a futuro
Virtualización	2048
Inalámbrica	650
Laboratorios	309
Administración	100

Fuente: La autora.

Con las cantidades en conocimiento se ha propuesto dos diferentes escenarios, cada uno de ellos partiendo de la dirección de red 172.17.x.x, ya implementada en el Data Center, el primer escenario se refiere a la implementación del direccionamiento estático y por otro lado en el segundo escenario se propone el direccionamiento dinámico utilizando VLSM y DHCP, permitiendo así tener una mejor administración de las direcciones, una configuración más simple en los dispositivos y evitar el agotamiento de direcciones IP.

En los dos escenarios se configura el switch de core, Switch Cisco Catalyst 9300, con la IP 172.17.x.200, siendo este el gateway para los diferentes dispositivos. Se propone el último octeto como el .200 debido a que ante cualquier usuario malicioso que se conecte a la red, el gateway no sea tan vulnerable y no sea una IP fácil de conocer como al colocar una dirección habitual como lo sería 172.17.x.1 o 172.17.x.254.

VLSM

Partiendo de la red 172.17.x.x se ha aplicado el método VLSM para segmentar la red en las cuatro subredes antes mencionadas, con el fin de administrar de mejor manera las direcciones IP y permitir un mejor tráfico; en la tabla 4 se puede observar el resultado del método aplicado, conociendo la dirección de red y la submáscara de red de cada segmento.

Tabla 4 Direccionamiento de subredes aplicando VLSM

Red	Dirección de red	Prefijo	Submáscara de red	Dirección de broadcast
Virtualización	172.17.42.0	20	255.255.240.0	172.17.47.255
Inalámbrica	172.17.48.0	22	255.255.252.0	172.17.51.255
Laboratorios	172.17.52.0	23	255.255.254.0	172.17.53.255
Administración	172.17.54.0	25	255.255.255.128	172.17.54.128

Fuente: La autora.

En la figura 16 se evidencia el crecimiento de la red manejada por el Data Center con la adquisición e implementación de nuevos equipos y servicios; siendo el servicio de virtualización el más utilizado, en la figura 18 se observa el crecimiento en cuanto a la creación de máquinas virtuales a raíz de requerimientos por parte de estudiantes y docentes, siendo estas utilizadas en diferentes áreas, descritas en la figura 17.

Ámbitos de aplicación de máquinas virtuales

USO	N° MÁQUINAS	%
Coordinacion Académica	1	1%
Administración	17	10%
Titulación	31	18%
Respaldo	35	20%
Investigación	35	20%
Academia	54	31%

Figura 17 Ámbitos de aplicación de máquinas virtuales.

Fuente: (CPD, 2019).

Cantidad de equipos adquiridos

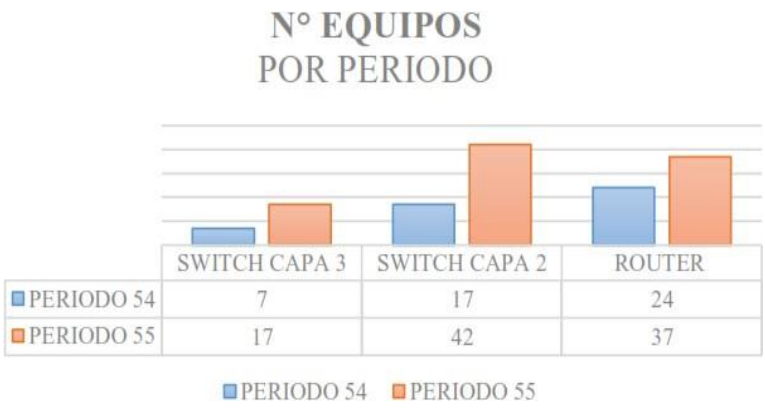


Figura 16 Equipos de networking adquiridos por período.

Fuente: (CPD, 2019).

Curva de crecimiento y proyección de máquinas virtuales

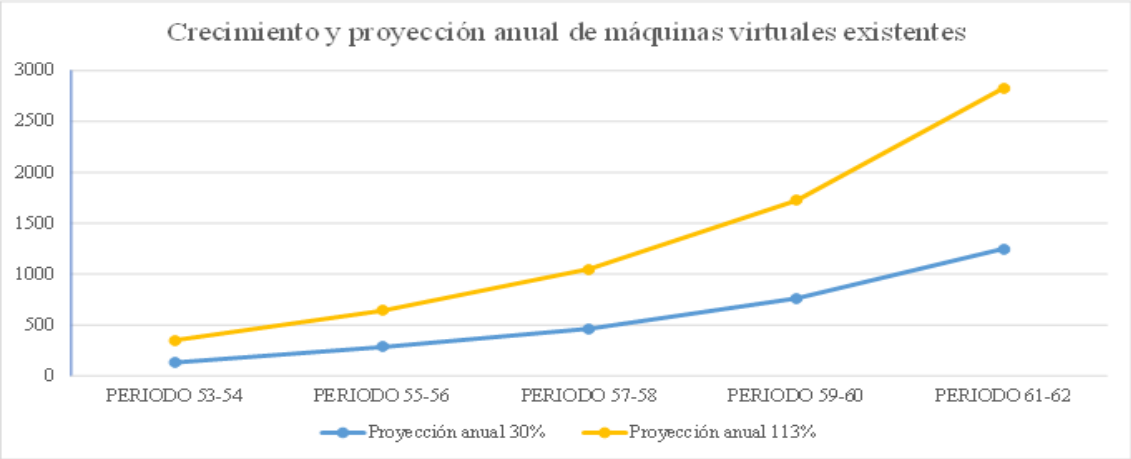


Figura 18 Crecimiento y proyección anual de máquinas virtuales existentes.

Información obtenida de (CPD, 2019).

Se ha tomado en cuenta que el porcentaje anual de crecimiento de la red es del 30%, con ello y la información obtenida se ha realizado la tabla 5 y la figura en donde se puede evidenciar que existe un porcentaje mayor respecto al requerimiento de máquinas virtuales, por lo cual se tiene las proyecciones anuales tanto del 30% como también del incremento mencionado anteriormente.

Tabla 5 Crecimiento y proyección anual de máquinas virtuales existentes

	Cantidad anual	Proyección anual 30%	Proyección anual 113%
PERIODO 53-54	102	133	218
PERIODO 55-56	218	283	358
PERIODO 57-58	358	465	586
PERIODO 59-60	586	762	962
PERIODO 61-62	962	1250	1577

Fuente: La autora.

Curva de crecimiento y proyección de máquinas virtuales

	CREADAS	ELIMINADAS	EXISTENTES
PERIODO 53	17	10	58
PERIODO 54	63	19	102
PERIODO 55	71	5	173
PERIODO 56			218

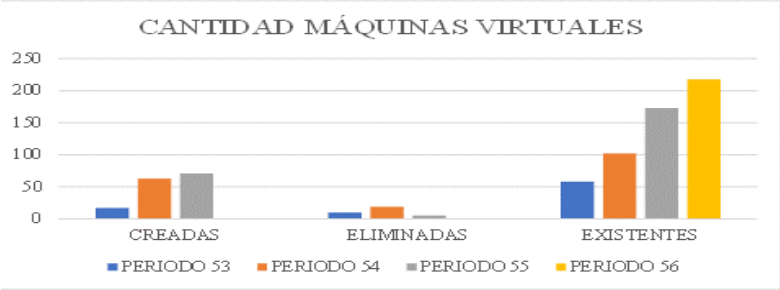


Figura 19 Cantidad de máquinas virtuales.

Información obtenida de (CPD, 2019).

Con la información obtenida se evidencia que el agotamiento de direcciones IP para las máquinas virtuales se presentará sin la aplicación de un correcto direccionamiento, por lo cual es indispensable el cambio de máscara de red.

3.3.3 VTP

Con la implementación de las VLAN se ve en la necesidad de implementar el protocolo VTP el cual permite una mejor administración de las VLAN, menor complejidad en el análisis de la red y puesto que la red es escalable dicho protocolo agiliza la configuración de las VLAN en dispositivos nuevos.

En el diseño propuesto el switch Core Catalyst 9300 se lo va a configurar en modo Server, el cual contiene una base de datos de todas las VLAN creadas, mientras que los demás switches van a estar en modo Client, es decir que van a recibir y utilizar las VLAN configuradas.

Además de conocer los modos VTP que se va a configurar en cada dispositivo, se debe tomar en cuenta que para el correcto funcionamiento de este protocolo todos los

dispositivos se deben encontrar en un mismo dominio, siendo configurados tres componentes con la misma información, estos son: dominio, contraseña y versión. Los siguientes datos informan sobre los datos a configurar en los dispositivos.

Dominio: ICC

Versión: 2

Contraseña: ICC_Networking

Configuración VTP en dispositivos

Configuración VTP - Servidor

```
9300_Core(config)#vtp mode Server
9300_Core(config)#vtp domain ICC
9300_Core(config)#vtp password ICC_Networking
9300_Core(config)#vtp version 2
9300_Core(config)#int ran g1/0/4-5
9300_Core(config-if-range)#switchport mode trunk
```

Figura 20 Configuración Cisco Catalyst 9300 Core-Servidor
Fuente: La autora.

Configuración VTP - Cliente

```
9300_1(config)#vtp version 2
9300_1(config)#vtp mode client
9300_1(config)#vtp domain ICC
9300_1(config)#vtp password ICC_Networking
9300_1(config)#interface f0/1
9300_1(config-if-range)#switchport trunk encapsulation dot1
9300_1(config-if-range)#switchport mode trunk
```

Figura 21 Configuración para los switches – Cliente
Fuente: La autora.

3.3.4 VLAN

La creación de las VLAN permite segmentar el tráfico de la red mediante la creación de redes lógicas independientes para así tener un mejor control y seguridad; y cabe recalcar que es de fácil aplicación.

Para la asignación de las VLAN se implementó la configuración con una separación de cinco respecto a los identificadores, dicha separación se propone teniendo en cuenta que dentro de la subred virtualización existen subgrupos referentes al ámbito de trabajo como se observa en la Figura 16, que a pesar de no es necesario la segmentación de las mismas puede en un futuro requerirse, al igual que en las demás subredes; respecto a la cantidad de separación, se han tomado los mayores valores mostrados en la misma figura.

Tabla 6 Propuesta de asignación de las VLAN

ID VLAN	NOMBRE
55	Virtualización
60	Inalámbrica
65	Laboratorios
70	Administración

Fuente: La autora.

Configuración de las VLAN

Configuración VLAN

```
9300_Core(config)#VLAN 55
9300_Core(config-VLAN)#name Virtualizacion
9300_Core(config-VLAN)#exi
9300_Core(config)#VLAN 60
9300_Core(config-VLAN)#name Inalambrica
9300_Core(config-VLAN)#exi
9300_Core(config)#VLAN 65
9300_Core(config-VLAN)#name Laboratorios
9300_Core(config-VLAN)#exi
9300_Core(config)#VLAN 70
9300_Core(config-VLAN)#name Administracion
9300_Core(config-VLAN)#exit
9300_Core(config)#int ran g1/0/4-5
9300_Core(config-if-range)#switchport mode trunk
```

Figura 22 Configuración de VLAN en Cisco Catalyst 9300 Core – Servidor
Fuente: La autora.

3.3.5 HSRP

Partiendo del diseño propuesto en la figura 15 se configura el protocolo HSRP en los switches de capa 3 Cisco Catalyst 9300 pertenecientes a la subred “Laboratorios”, mientras que en la subred de “Administración” se realiza la configuración en los switches SAN.

Dicho protocolo permite conocer el estado de los dispositivos y evita que la información se pierda mediante técnicas de redundancia, es decir que si en algún momento cualquiera de los dos switches falla la información seguirá siendo enrutada, llegando así a su destino.

Tabla 7 Propuesta para la configuración HSRP

Dispositivo	Dirección IP	IP Virtual	Prioridad
9300_1	172.17.52.5	172.17.52.7	110
9300_2	172.17.52.6	172.17.52.7	100
SAN1	172.17.54.5	172.17.54.7	110
SAN2	172.17.54.6	172.17.54.7	100

Fuente: La autora.

Subred de Laboratorios para configuración de HSRP

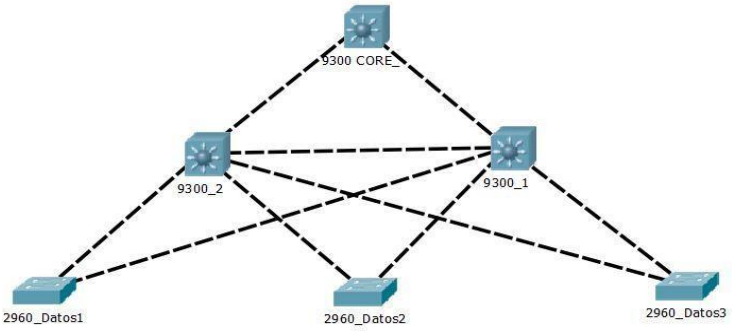


Figura 23 Dispositivos a configurar HSRP en la subred de Laboratorios.
Fuente: La autora.

Subred de Administración para configuración de HSRP

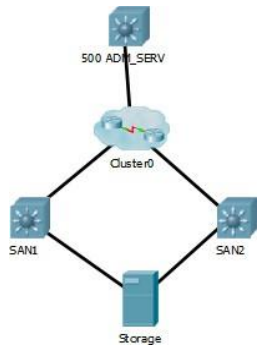


Figura 24 Dispositivos a configurar HSRP dentro de la subred de Administración.
Fuente: La autora.

A partir de la información observadas en las figuras 23, 24 y la tabla 7 se procede a realizar las configuraciones en los dispositivos anteriormente mencionados, el switch Catalyst 9300_1 se colocará como el switch activo, al igual que el SAN1, mientras que el switch 9300_2 y SAN2 serán los switch en standby.

Configuración HSRP en dispositivos

Configuración HSRP – Switch 9300_1

```
no switchport
ip address 172.17.52.5 255.255.254.0
duplex auto
speed auto
standby 1 ip 172.17.52.7
standby 1 priority 110
standby 1 preempt
standby 1 track FastEthernet0/1
standby 1 track FastEthernet0/2
standby 1 track FastEthernet0/3
```

Figura 25 Configuración HSRP - Switch 9300_1
Fuente: La autora.

Configuración HSRP – SAN1

```
no switchport
ip address 172.17.54.19 255.255.255.128
duplex auto
speed auto
standby 1 ip 172.17.54.25
standby 1 priority 110
standby 1 preempt
```

Figura 27 Configuración HSRP - Switch SAN1
Fuente: La autora.

Configuración HSRP – Switch 9300_2

```
no switchport
ip address 172.17.52.6 255.255.254.0
duplex auto
speed auto
standby 1 ip 172.17.52.7
standby 1 preempt
standby 1 track FastEthernet0/1
standby 1 track FastEthernet0/2
standby 1 track FastEthernet0/3
```

Figura 26 Configuración HSRP - Switch 9300_2
Fuente: La autora.

Configuración HSRP – SAN2

```
no switchport
ip address 172.17.54.20 255.255.255.128
duplex auto
speed auto
standby 1 ip 172.17.54.25
standby 1 preempt
standby 1 track FastEthernet0/1
```

Figura 28 Configuración HSRP - Switch SAN2
Fuente: La autora.

3.3.6 STP

En base a la figura 23 y la figura 29 se ha tomado en cuenta ciertos dispositivos de la red para realizar la configuración del protocolo STP; se ha determinado que el switch que se va a configurar como el Puente Raíz dentro de la subred laboratorios va a ser el switch Cisco Catalyst 9300, y debido a que es el mismo dispositivo para el Puente Raíz Secundario se ha configurado el segundo switch Cisco Catalyst 9300, en la Figura 29 se muestra la subred de Administración, que al igual que en la de Laboratorios, se cuenta con dos dispositivos iguales, por lo cual se va a realizar el mismo procedimiento, con esta configuración se logra que no exista pérdidas dentro de la red y el funcionamiento de los dispositivos no se vean afectados en el momento que exista algún fallo por cualquiera de estos dispositivos; con ello se evita que se generen colapsos por tormentas de broadcast, los cuales minoran el consumo innecesario de recursos dentro de la red. Los demás dispositivos serán configurados con una prioridad mayor que los anteriores dispositivos mencionados, con ello se busca que no exista competencia por establecer el Puente Raíz.

Subred Administración para configurar STP

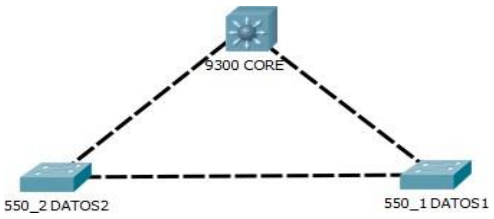


Figura 29 Dispositivos a configurar STP dentro de la subred Administración.

Fuente: La autora.

Estas configuraciones permiten que el manejo de la red sea más eficiente sin que existan cambios no controlados en la topología, detecta los fallos casi al instante evitando así que existan *loops* por lo cual no permite que la conectividad en los

dispositivos se pierda, y por último es un protocolo que beneficia a la escalabilidad de la red, permitiendo que se implementen enlaces redundantes, o se realicen cambios de equipos.

Configuración STP en dispositivos

Configuración STP – Switch 9300_1

```
9300_1(config)#no spanning-tree vlan 1
9300_1(config)#interface range g0/1-2
9300_1(config-if-range)#shutdown
9300_1(config)#interface range f0/6-24
9300_1(config-if-range)#shutdown
9300_1(config)#spanning-tree VLAN 65-75 priority 61440
9300_1(config)#interface range f0/1-5
9300_1(config-if-range)#spanning-tree guard root
9300_1(config-if-range)#exit
9300_1(config)#spanning-tree portfast default
```

Figura 30 Configuración STP - Switch 9300_1
Fuente: La autora.

Configuración opcional STP – Switch 9300_1

```
9300_1(config)#no spanning-tree vlan 1
9300_1(config)#interface range g0/1-2
9300_1(config-if-range)#shutdown
9300_1(config)#interface range f0/6-24
9300_1(config-if-range)#shutdown
9300_1(config)#spanning-tree vlan 65 root primary
9300_1(config)#spanning-tree vlan 70 root primary
9300_1(config)#interface range f0/1-5
9300_1(config-if-range)#spanning-tree guard root
9300_1(config-if-range)#exit
9300_1(config)#spanning-tree portfast default
```

Figura 31 Configuración STP alternativa - Switch 9300_1
Fuente: La autora.

La configuración realizada tiene como objetivo eliminar la VLAN 1, la cual es creada por defecto, se la elimina debido a que se encuentra creada la VLAN 70 para Administración; las siguientes líneas de configuración permiten convertir el switch 9300_1 en root, es por ello que el costo asignado a cada una de las VLAN ha sido el valor de 32768, también se propone dicha configuración para que en un futuro el

protocolo STP no necesite configuración si se ve la necesidad de incrementar el número de las VLAN; por último se coloca el último comando en los puertos troncales por reforzar la seguridad del Puente Raíz, evitando que otro switch tome este rol.

Se puede observar que existe una configuración opcional, con ello se quiere demostrar que la configuración STP va a ser exitosa, más se debe tomar en cuenta que en el momento que se configure las nuevas VLAN también se tiene que configurar el protocolo STP. En la figura 32 se observa que con la configuración realizada el switch core ha tomado la posición como Puente Raíz.

Resultado comando "show spanning-tree"

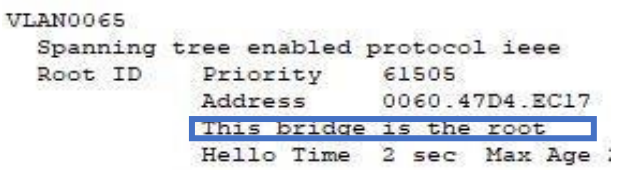


Figura 32 Resultado comando show spanning-tree.
Fuente: La autora.

Respecto a la configuración de los switches restantes, se ha realizado la debida configuración eliminando la VLAN 1 y colocando el costo de STP en 49152, con ello se asegura que el switch 9300_1 y 550_1 sean los designado como Puente Raíz.

Configuración STP

```
9300_2(config)#no spanning-tree vlan 1
9300_2 (config)#spanning-tree VLAN 65-79 priority 49152
9300_2(config)#interf rang fa0/4-5
```

Figura 33 Configuración STP - Switch 9300_2
Fuente: La autora.

Configuración alternativa STP

```
9300_2(config)#no spanning-tree vlan 1
9300_2(config)#spanning-tree VLAN 70 root secondary
9300_2(config)#spanning-tree VLAN 65 root secondary
```

Figura 34 Configuración alternativa - Switch 9300_2
Fuente: La autora.

3.3.7 QoS CALIDAD DE SERVICIO

El flujo de tráfico respecto a los diferentes protocolos que existen dentro de la red puede generar congestión en la misma, es por ello que con la debida configuración de calidad de servicio influye en la mejora de la red.

Para la configuración de QoS se han analizado las aplicaciones y servicios presentes en la red, protocolos y puertos comprendidos en cada uno de ellos.

A partir de los datos e información obtenida se ha decido proponer la implementación de servicios diferenciados por lo que se han realizado seis grupos en base a los servicios que proporcionan, conllevando a distribuir la cantidad de banda ancha de la red en diferentes porcentajes, dicha información se puede observar en la tabla 8.

Tabla 8 Puertos y protocolos utilizados en los servicios

Servicio	**%**	**Puertos**	**Protocolo**
VoIP	30	1720	H323
		5004	RTP
		5005	RTCP
		5060	SIP
Video	30	554	RTSP
		1935	RTMP
		1755	MMS
Virtualización		3389	
Web	10	80	HTTP
		443	HTTPS
		491	HTTP
		8080	HTTP
Correo	10	110	POP3
		995	POP3 SSL
		143	IMAP
		993	IMAP SSL
		25	SMTP
		587	SMTP SSL
Base de datos	10	3306	
		389	LDAP

		1433	
		1434	
		5432	
Tráfico protocolar	10	67	DHCP
		53	DNS
		5355	LLMNR
		22	SSH

Fuente: La autora.

Partiendo de la información clasificada se ha realizado la configuración de las ACL para tener un mejor control en el flujo de información, de igual manera en este apartado se ha decidido agregar la implementación de políticas de seguridad mediante la creación de la acl-Trash, denegando el paso de bittorrent; este procedimiento ha sido aplicado con el objetivo de tener una mayor seguridad y de igual manera permitir una fácil configuración de QoS.

Configuración ACL

Configuración de las ACL

```
9300_Core(config)#access-list 105 deny tcp any any range 6881 6999
9300_Core(config)#access-list 106 permit udp any 172.17.54.0 0.0.0.127 eq 1720
9300_Core(config)#access-list 106 permit udp any 172.17.54.0 0.0.0.127 range 5004 5005
9300_Core(config)#access-list 106 permit udp any 172.17.54.0 0.0.0.127 eq 5060
9300_Core(config)#access-list 106 permit tcp any 172.17.54.0 0.0.0.127 eq 5060
9300_Core(config)#access-list 107 permit tcp any any eq 554
9300_Core(config)#access-list 107 permit tcp any any eq 1935
9300_Core(config)#access-list 107 permit tcp any any eq 1755
9300_Core(config)#access-list 107 permit udp any any eq 1755
9300_Core(config)#access-list 107 permit tcp any any eq 3389
9300_Core(config)#access-list 108 permit tcp any any eq www
9300_Core(config)#access-list 108 permit tcp any any eq 443
9300_Core(config)#access-list 109 permit tcp any any eq 110
9300_Core(config)#access-list 109 permit tcp any any eq 995
9300_Core(config)#access-list 109 permit tcp any any eq 993
9300_Core(config)#access-list 109 permit tcp any any eq 143
9300_Core(config)#access-list 109 permit tcp any any eq 25
9300_Core(config)#access-list 109 permit tcp any any eq 587
9300_Core(config)#access-list 110 permit tcp any any eq 3306
9300_Core(config)#access-list 110 permit tcp any any eq 389
9300_Core(config)#access-list 110 permit udp any any eq 389
9300_Core(config)#access-list 110 permit tcp any any range 1433 1434
9300_Core(config)#access-list 110 permit tcp any any eq 5432
9300_Core(config)#access-list 111 permit tcp any any eq 67
9300_Core(config)#access-list 111 permit tcp any any eq 22
9300_Core(config)#access-list 111 permit tcp any any eq 5355
9300_Core(config)#access-list 111 permit tcp any any eq 53
9300_Core(config)#access-list 111 permit udp any any eq 53
```

Figura 35 Configuración ACL - Switch 9300_Core
Fuente: La autora.

Para la configuración de QoS como anteriormente se mencionó, se ha tomado en cuenta el ancho de banda con el que cuenta la red, y aplicarlo en las políticas de QoS. En el Data Center se cuenta con 1Gbps dentro de la red LAN, mientras que se tiene una salida de 100 Mbps lo que es igual a 100000Kbps, dicho valor es necesario en Kbps debido a la configuración admitida en los dispositivos, y de dicho valor se ha designado los siguientes porcentajes:

- 30% - VoIp.
- 30% - Streaming y Virtualización
- 10% - Servicios web
- 10% - Correo
- 10% - Transaccionalidad
- 10% - Tráfico protocolar

Configuración QoS

Configuración de QoS

```
9300_Core(config)#class-map acl-105
9300_Core(config-cmap)#description acl-105 Trash
9300_Core(config-cmap)#match access-group 105
9300_Core(config-cmap)#exit
9300_Core(config)#class-map acl-106
9300_Core(config-cmap)#description acl-106 VoIP
9300_Core(config-cmap)#match access-group 106
9300_Core(config-cmap)#exit
9300_Core(config)#class-map acl-107
9300_Core(config-cmap)#description acl-107 Stream_Virtualizacion
9300_Core(config-cmap)#match access-group 107
9300_Core(config-cmap)#exit
9300_Core(config)#class-map acl-108
9300_Core(config-cmap)#description acl-108 Web
9300_Core(config-cmap)#match access-group 108
9300_Core(config-cmap)#exit
9300_Core(config)#class-map acl-109
9300_Core(config-cmap)#description acl-109 Correo
9300_Core(config-cmap)#match access-group 109
9300_Core(config-cmap)#exit
9300_Core(config)#class-map acl-110
9300_Core(config-cmap)#description acl-110 Transaccionalidad
9300_Core(config-cmap)#match access-group 110
```

Figura 36 Configuración QoS - Switch 9300_Core (a)
Fuente: La autora.

Configuración de las ACL

```
9300_Core(config-cmap)#exit
9300_Core(config)#class-map acl-111
9300_Core(config-cmap)#description acl-111 TrafProtocolar
9300_Core(config-cmap)#match access-group 111
9300_Core(config-cmap)#exit
9300_Core(config)#policy-map TraficoRed
9300_Core(config-pmap)#class acl-106
9300_Core(config-pmap-c)#bandwidth 145164
9300_Core(config-pmap-c)#exit
9300_Core(config-pmap)#class acl-107
9300_Core(config-pmap-c)#bandwidth 145164
9300_Core(config-pmap-c)#exit
9300_Core(config-pmap)#class acl-108
9300_Core(config-pmap-c)#bandwidth 48388
9300_Core(config-pmap-c)#exit
9300_Core(config-pmap)#class acl-109
9300_Core(config-pmap-c)#bandwidth 48388
9300_Core(config-pmap-c)#exit
9300_Core(config-pmap)#class acl-110
9300_Core(config-pmap-c)#bandwidth 48388
9300_Core(config-pmap-c)#exit
9300_Core(config-pmap)#class acl-111
9300_Core(config-pmap-c)#bandwidth 48388
9300_Core(config-pmap-c)#exit
9300_Core(config)#policy-map Trash
9300_Core(config-pmap)#class acl-105
*9300_Core(config-pmap)#police cir 8000 conform-action transmit exceed-action drop
9300_Core(config-pmap)#exit
9300_Core(config)#interface gigabitEthernet1/0/6
9300_Core(config-if)#service-policy input Trash
9300_Core(config-if)#exit
9300_Core(config)#interface range gigabitEthernet1/0/1-5
9300_Core(config-if-range)#service-policy output TraficoRed
9300_Core(config-if-range)#exit
```

Figura 37 Configuración QoS - Switch 9300_Core (b)
Fuente: La autora.

*La configuración de la política no se la ha podido simular en packet tracer por las limitaciones de la herramienta, más en la página de (Cisco, 2020) se observa que dicha configuración es aplicable en el dispositivo exitosamente.

3.3.8 RESULTADOS

Desarrollando las actividades consideradas en cada etapa del proyecto se ha configurado en dos escenarios el direccionamiento y los distintos protocolos propuestos, los escenarios se encuentran diferenciados por el tipo de direccionamiento implementado, estático y dinámico. A continuación, se detallan las gráficas obtenidas de la simulación del estado inicial de, rediseño con direccionamiento estático y rediseño con direccionamiento dinámico; al igual que las respectivas comparaciones.

En la figura 38 se expone la topología propuesta simulada en la herramienta Opnet, permitiendo generar los resultados para su debido análisis.

La topología se encuentra conectada con enlaces de 40Gbps de los switches a los dispositivos finales, para la conexión entre switches se utilizaron enlaces de punto a punto OC192, los cuales trabajan a velocidades cerca de 1Gbps.

Topología simulada en Opnet

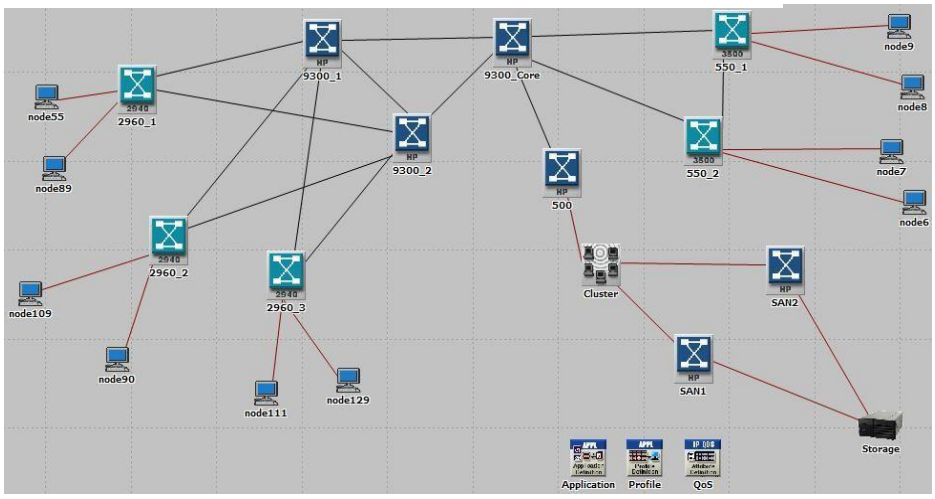


Figura 38 Topología simulada en la herramienta Opnet.
Fuente: La autora.

Gráficas resultantes de la situación inicial

En la figura 39 se observa el tráfico enviado y recibido del servicio de base de datos dentro de toda la red, teniendo un máximo de 45000 bytes/seg envío de 45000 bytes/seg, al igual que en la recepción

Tráfico del servicio de base de datos

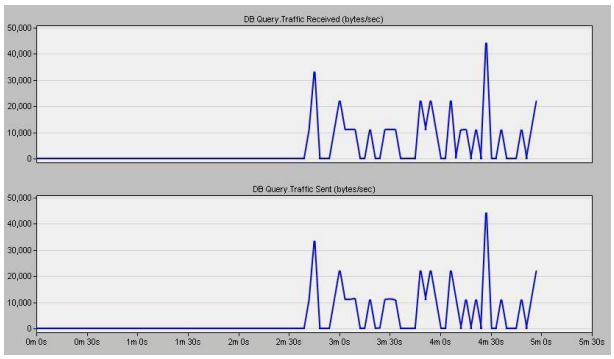


Figura 39 Tráfico enviado y recibido de servicio de BDD.
Fuente: La autora.

Los resultados obtenidos de un cliente de base de datos se pueden apreciar en la figura 40, teniendo en el tráfico enviado 23000 bytes/seg como pico máximo y un promedio de 11000 bytes/seg, en cuanto al tráfico recibido tiene 350 bytes/seg como punto máximo de consumo y un promedio de 180 bytes/seg.

Tráfico del cliente de base de datos

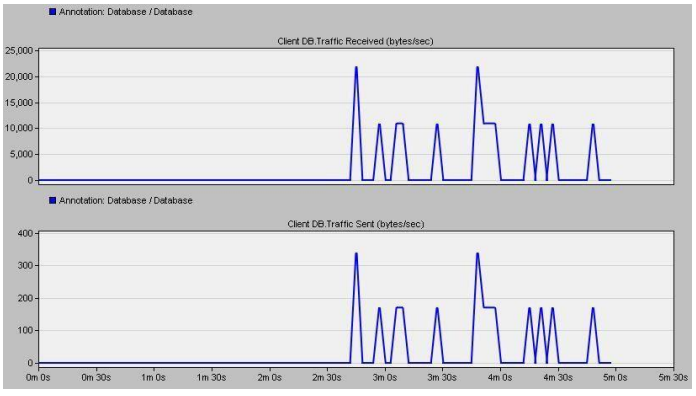


Figura 40 Tráfico enviado y recibido del cliente BDD.
Fuente: La autora.

La figura 41 representa el tráfico IP dentro del switch Cisco Catalyst 9300 el cual está configurado como el switch core, en dicha imagen se evidencia que el punto máximo

encontrado tanto en el tráfico de recepción como en el de envío es de 9 paquetes/seg, siendo este el único punto máximo en todo el tráfico ya que decrece a un promedio de 1.8 paquetes/seg.

Tráfico del protocolo IP

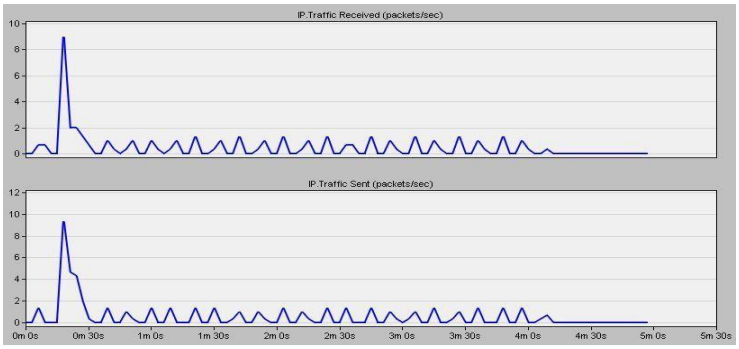


Figura 41 Tráfico enviado y recibido del protocolo IP.
Fuente: La autora.

En la figura 42 se observa el tráfico del servicio de videoconferencia, en el que se puede evidenciar que existe un retardo de variación de $1x10^{-18}$ seg, un tráfico de recepción y envío de datos de 8000000 bytes/seg como punto máximo y estabilizándose en dicho valor, por lo cual genera un consumo de ancho de banda constante.

Tráfico del servicio de videoconferencia

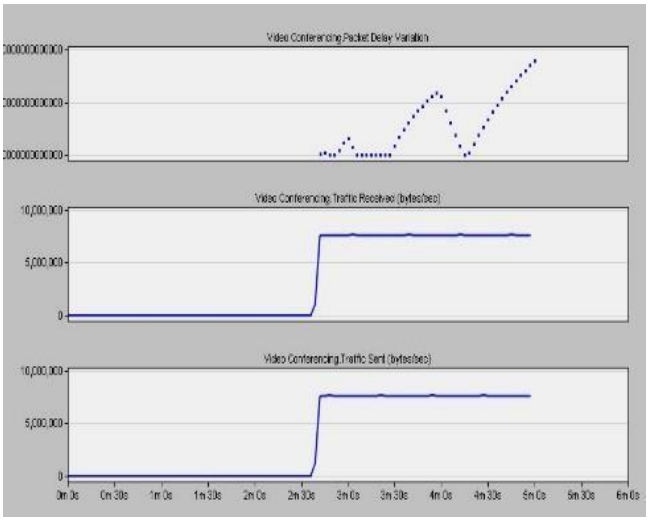


Figura 42 Tráfico del servicio de videoconferencia.
Fuente: La autora.

Cabe mencionar que la calidad del servicio tanto de audio como de voz no es garantizada, por lo cual pueden existir intermitencias y mala calidad de videoconferencias en el momento que exista saturación del canal, es por ello que va a presentarse siempre un retardo; al configurar QoS lo que se desea es proporcionar un menor retardo al momento de ofrecer dicho servicio.

Gráficas resultantes del rediseño propuesto

Como anteriormente se mencionó se ha realizado la simulación de dos escenarios, con la variación de la configuración del direccionamiento, más en los dos escenarios el tráfico generado está configurado con segmentación de redes mediante las VLAN al igual que la configuración de QoS en los enlaces, protocolo HSRP, entre otras.

En primer lugar, se va a realizar el respectivo análisis de los servicios en cada escenario y finalmente se realizará un análisis comparativo entre los mismos respecto al protocolo HSRP y la implementación de VLAN.

Tráfico del servicio de base de datos

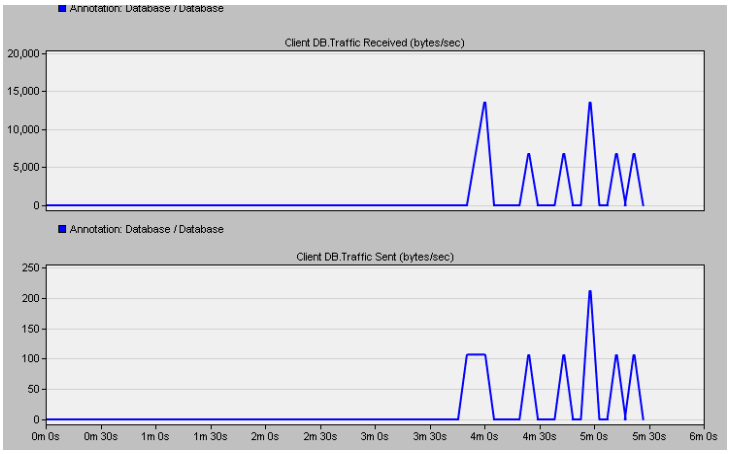


Figura 43 Tráfico enviado y recibido del cliente BDD.
Fuente: La autora.

La figura 43 muestra que el tráfico enviado por el cliente de base de datos alcanza en sus puntos máximos un valor de 14000 bytes/seg y un promedio de 5700 bytes/seg,

mientras que en el tráfico de envío se evidencia ciertos puntos máximos con un valor de 210 bytes/seg, y un promedio de 100 bytes/seg.

En la figura 44 se observa los datos obtenidos en la simulación de los escenarios estático y dinámico respecto al uso de VLAN, de lo cual se puede afirmar que el tráfico de envío y de recepción en el direccionamiento estático genera un pico máximo de 3200 bits/seg mientras que en el dinámico el mayor pico es de 490 bits/seg; si ampliamos el número de dispositivos a los que se encuentran en la red, los picos generados por el escenario del direccionamiento estático van a generar una mayor carga en la red que el dinámico.

Tráfico de los escenarios aplicados VLAN

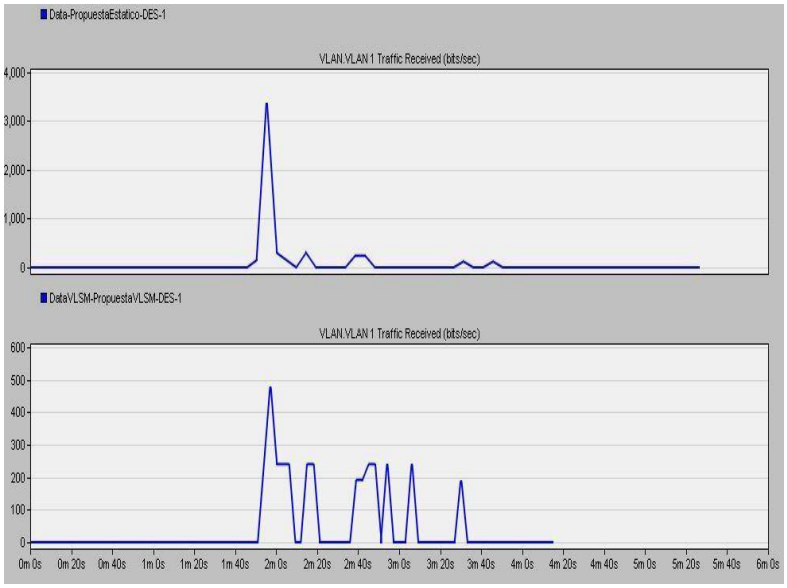


Figura 44 Escenario estático y dinámico aplicado VLAN.
Fuente: La autora.

En la figura 45 y figura 46 se puede evidenciar la información obtenida de la implementación del protocolo HSRP en los dos escenarios propuesto.

Evidenciando que el tráfico de recepción presenta valores continuos de 0 bits/seg, mientras que en el tráfico de envío en el escenario aplicado enrutamiento estático se encuentran picos de diferentes valores, siendo el valor máximo de 80 bits/seg,

seguidamente este valor desciende conllevando a obtener un promedio de 70 bits/seg; en el escenario aplicado enrutamiento dinámico se encuentra un pico de 85 bits/seg el cual posteriormente decrece para estabilizarse, tomando un valor constante de 45 bits/seg a lo largo del tiempo de simulación.

Resultado de tráfico HSRP en los escenarios propuestos

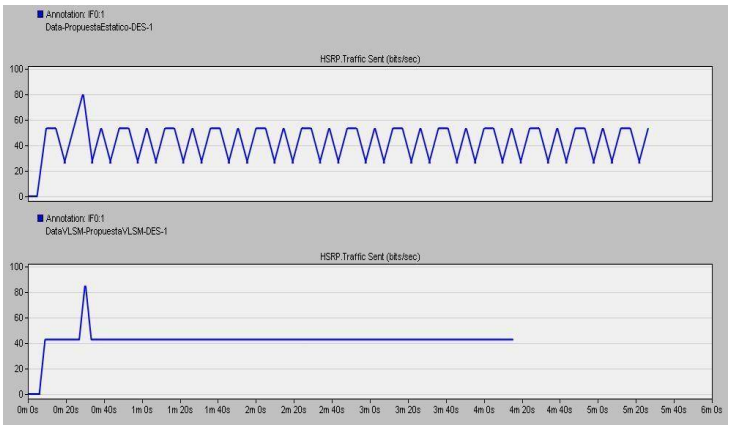


Figura 45 Tráfico enviado del protocolo HSRP en los escenarios estático y dinámico.
Fuente: La autora.

Resultado de tráfico HSRP en el escenario inicial

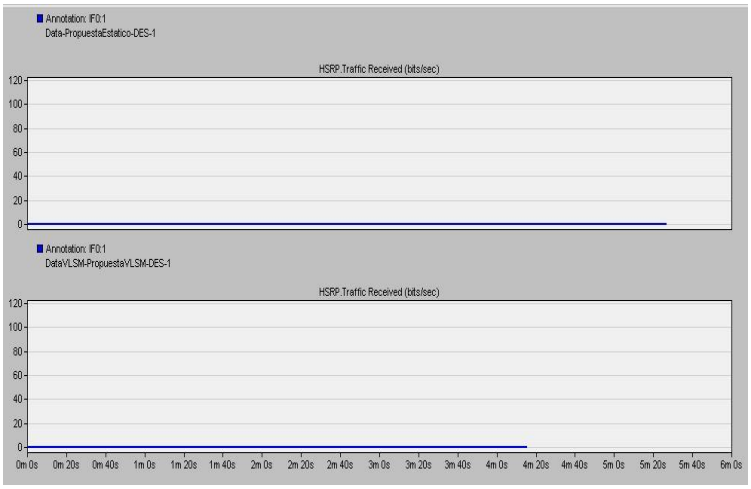


Figura 46 Tráfico recibido del protocolo HSRP en los escenarios estático y dinámico.
Fuente: La autora.

3.3.8.1 ANÁLISIS ESTADÍSTICO

Para realizar un análisis estadístico se ha partido de la obtención de valores de los tres escenarios respecto al throughput.

En la figura 47 se puede apreciar la comparativa de los valores obtenidos, siendo la línea roja el escenario inicial de la red, la verde el escenario con direccionamiento dinámico y finalmente la línea azul representa el escenario con direccionamiento estático. Se evidencia que el escenario que tiene los menores valores es el de direccionamiento dinámico y con los datos de la figura 33, se evidencia que 800 bits/seg y 0 bits/seg son los valores máximos y mínimos alcanzados respectivamente.

Gráfica comparativa de throughput

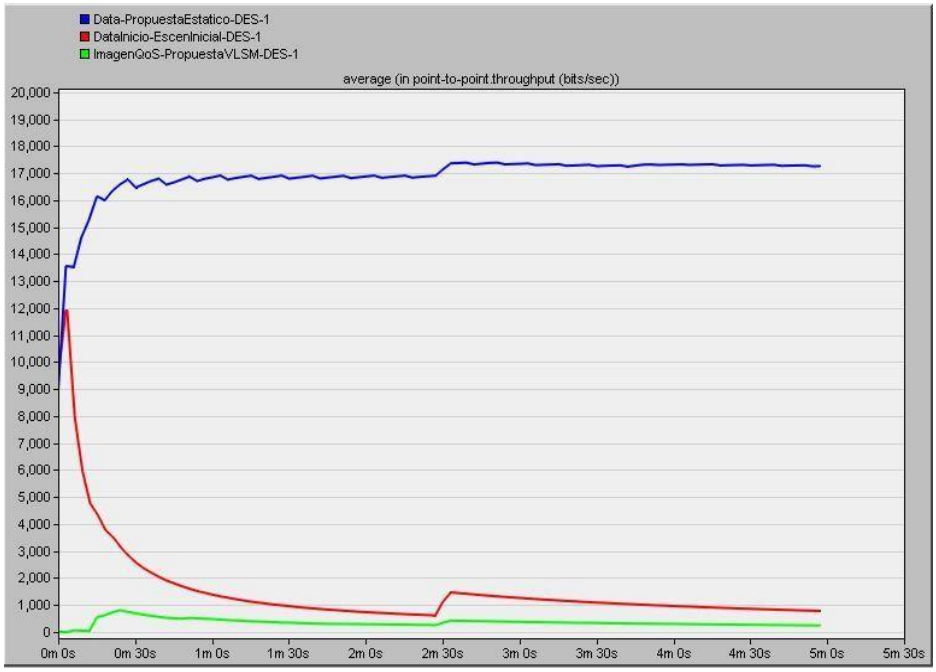


Figura 47 Gráfica comparativa throughput
Fuente: La autora.

En la figura 48 se toma en cuenta los valores máximos y mínimos que permitirán comprender la estabilidad de la red respecto a las configuraciones realizadas.

Realizando el análisis de los datos estadísticos se puede interpretar las gráficas obtenidas y de ellas llegar a una deducción; es por ello que se hace uso de las fórmulas

de varianza y desviación estándar, “la varianza representa a la desviación promedio de la media de los datos tomados, mientras que la desviación media es una medida estadística que se utiliza para determinar cuánto tienden los valores a alejarse del rango normal obtenido; lo que se desea obtener con estas medidas es que con la desviación media se conozca el comportamiento de los datos a analizar, que tan estables son y cómo estos afectan en el rendimiento de la red” (Gallegos Altamirano & Román González, 2018).

Se han utilizado las siguientes ecuaciones de varianza y desviación media para realizar los cálculos respectivos.

Valores obtenidos del throughput

```
-----------------------------------------------------
zone                : 0
statistic           : 'ImagenQoS-PropuestaVLSM-DES-1: 9300_Core <-> 9300_1 [0].point-to-point.throughput (bits/sec) -->'
length              : 101
number of values    : 101
horizontal, min     : 0
            max     : 300
vertical,   min     : 0.0
            max     : 806.518518519
initial value       : 0.0
final value         : 243.226666667
expected value      : 352.194601838
sample mean         : 352.194601838
variance            : 19,066.9651998
standard deviation  : 138.083182176
** confidence intervals valid if entries are independent samples
80% conf interval:  [       334.408708301, 369.980495376        ]
90% conf interval:  [       329.365485991, 375.023717685        ]
95% conf interval:  [        324.99395317, 379.395250507        ]
98% conf interval:  [       319.90493385, 384.484269827         ]
99% conf interval:  [       316.459055756, 387.930147921        ]
** Operations List **
Original vector     : ImagenQoS-PropuestaVLSM-DES-1: 9300_Core <-> 9300_1 [0].point-to-point.throughput (bits/sec) -->.none
---------
Operation #1
Operation type      : Filter
Filter name         : average
---------
```

Figura 48 Throughput escenario aplicado direccionamiento dinámico y VLSM
Fuente: La autora.

Ecuación 1 Ecuación de la varianza (Milton & Arnold, 2004)

$$S^2 = \frac{\sum_{i=1}^{n} (x_i - \bar{x})^2}{n-1}$$

Donde:

S^2 = Varianza

n = Total de datos a procesar

x_i = Datos de la muestra

$\bar{x}$ = Media de los datos

Ecuación 2 Ecuación de desviación media (Milton & Arnold, 2004).

$$\sigma = \sqrt{S^2}$$

Donde:

σ = Desviación media

S^2 = Varianza

Para realizar los cálculos se tomó los datos de la simulación de cada escenario colocando un tiempo de ejecución de 300 segundos.

Al procesar los 101 eventos de la simulación se obtuvieron los datos presentados en la tabla 9, de los cuales se puede concluir que los datos obtenidos del escenario aplicado VLSM y direccionamiento dinámico son los menores en los dos parámetros, "uno de los principios básicos de la desviación media es analizar el comportamiento de los datos, partiendo del hecho que mayor dispersión mayor variabilidad y a menor valor más homogeneidad" (Gallegos Altamirano & Román González, 2018).

Por lo cual se puede decir que el escenario aplicado direccionamiento dinámico y las configuraciones presentadas a lo largo de este documento es el que presenta una mayor estabilidad de la red.

Tabla 9 Resultados de varianza y desviación media obtenidos de los tres escenarios

	Estado inicial	**Estático**	**Dinámico**
Varianza	5109697,80098	281995588,28670	20295,09428
Desviación media	2260,46407	16792,72427	142,46085

Fuente: La autora.

Los datos procesados y resultados de los parámetros de varianza y desviación media se los puede encontrar en "Anexos".

CAPÍTULO IV

4.1 CONCLUSIONES

Realizado el presente trabajo se puede afirmar que los objetivos planteados se han cumplido satisfactoriamente.

- Como principal logro se ha realizado la propuesta para la implementación de la red lógica de los laboratorios del bloque D y Data Center; teniendo en cuenta los cálculos de varianza y desviación media se puede concluir que la red en la cual se ha configurado direccionamiento dinámico presenta una mayor estabilidad de la red y de igual manera permite escalabilidad y seguridad en la misma.
- Mediante la investigación y análisis del estado actual de la red, se recopiló la información de la misma y los dispositivos, conociendo así las falencias y capacidades, para así tomar las mejores decisiones sobre la configuración en cada uno de ellos.
- Muchas organizaciones, adoptan el modelo jerárquico con núcleo colapsado tomando en cuenta que este modelo reduce el costo de la red sin perder los beneficios del modelo jerárquico de tres capas. En este estudio se puede observar dicho modelo en el diseño actual, debido a razones económicas, tamaño de la red y su escalabilidad.
- La red lógica de los laboratorios del bloque D y Data Center posee enlaces redundantes, los cuales no se encuentran operativos, por lo cual es necesario la implementación de los debidos protocolos y activación para su correcto funcionamiento.

- El diseño propuesto demuestra que las configuraciones realizadas de protocolos, QoS e implementación de las VLAN se encuentran en correcto funcionamiento y conlleva a la mejora de la administración y funcionamiento de la red.

4.2 RECOMENDACIONES

- Mejorar la seguridad en dispositivos de capa 3, mediante contraseñas seguras y configuración cifrada de la información evitando así el control no autorizado de dichos dispositivos y pérdida de información.
- Implementar la capacidad para IPv6 nativo debido a que la red es escalable y debe ofrecer nuevos servicios, con dicha implementación será posible la adquisición e incorporación de dispositivos de nueva generación a la red.
- Implementar el direccionamiento dinámico haciendo uso de DHCP y de igual manera aplicar VLSM, con el fin de tener una mejor administración de las subredes y que no exista un agotamiento de direcciones IP inmediato.

GLOSARIO DE TÉRMINOS

- **Conmutación:** Es la acción por la cual se establece un camino para la comunicación entre dos dispositivos de una red.
- **Servidor:** Dispositivo de la red, el cual atiende los requerimientos de otros dispositivos, es decir que provee servicios.
- **Jitter:** Es la fluctuación o variabilidad temporal que ocurre durante el envío de señales Calvo García, 2014).
- **Flujo:** Es una corriente de paquetes IP relacionados y generados por un mismo usuario, que de igual manera requiere un mismo tipo de QoS
- **Broadcast:** Difusión masiva de paquetes a través de la red.
- **Bucle:** Es un ciclo que se repite indefinidamente hasta que uno de los elementos que lo mantiene desaparezca.
- **Redundancia:** Asegura la disponibilidad de la red en todo momento, a través del duplicado de enlaces, servidores, información, etc.
- **BPDU:** Tramas que tienen información sobre el protocolo spanning-tree (STP).

BIBLIOGRAFÍA

Aguaiza Tenelema, D. (2016). *Propuesta de rediseño de la infraestructura de red de la Universidad Laica Eloy Alfaro¨ de Manabí, para ofrecer un modelo de servicios con calidad de servicio (QoS) (Tesis de pregrado).* Potificia Universidad Católica del Ecuador, Quito.

Arévalo Padilla, L. P. (2016). *Rediseño de una red lan multiservicios para el Municipio de Tulcán.* Universidad de las Amércias, Quito.

Ariganello, E. (2016). *CCNA Routing y Switching.* Madrid: RA-MA.

Ariganello, E., & Barrientos Sevilla, E. (2010). *Redes CISCO, CCNP A fondo.* Madrid: ALFAOMEGA GPO EDR.

Calderón Zetter, M. I. (18 de Mayo de 2016). *Blog de Radioaficion,Tecnología y Internet.* Obtenido de Brandmeister XE : http://www.xe1gqp.org.mx/blog/wp-content/uploads/2016/05/Redes-de-computadoras-estandares-y-protocolos-por-XE1GNW-Ines-Calderon.pdf

Calvo García , A. L. (2014). Gestión de redes telemáticas UF1880. Málaga: IC Editorial.

Chisaguano Castellano, D. A., & Ludeña Veliz, M. J. (Febrero de 2019). *Análisis, diseño e implementación de un sistema de gestión de inventarios de activos de TI para los laboratorios de la carrera de Ingeniería en Ciencias de la Computación de la Universidad Politécnica Salesiana sede Quito campus sur.* Obtenido de Universidad Politécnica Salesiana: http://dspace.ups.edu.ec/handle/123456789/16969

Cisco. (Abril de 2014). *Cisco.* Obtenido de Cisco: https://www.cisco.com/c/dam/r/es/la/internet-of-everything-ioe/assets/pdfs/en-05_campus-wireless_wp_cte_es-xl_42333.pdf

Cisco. (19 de Septiembre de 2014). *Cisco.* Obtenido de Cisco: https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html?dtid=osscdc000283

Cisco. (5 de Junio de 2017). *Cisco.* Obtenido de Cisco: https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/5234-5.html?dtid=osscdc000283

Cisco. (13 de Julio de 2017). *Cisco Systems, Inc.* Obtenido de Cisco: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/AccessTrunk.pdf

Cisco. (4 de Mayo de 2020). *Quality of Service (QoS) Configuration Guide, Cisco IOS XE Everest 16.5.1a (Catalyst 9300 Switches).* Obtenido de Cisco: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-5/configuration_guide/qos/b_165_qos_9300_cg.pdf

Cisco. (24 de Abril de 2020). *Security Configuration Guide, Cisco IOS XE Everest 16.5.1a (Catalyst 9300 Switches).* Obtenido de Cisco: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-5/configuration_guide/sec/b_165_sec_9300_cg/configuring_ipv4_acls.html?dtid=osscdc000283#concept_EA18174B5D624C72ADB4F54AC5808D5F

CPD. (2019). *INFORME DE ACTIVIDADES P55* . Quito.

Defaz Carrera, J. A., & Gallegos Herrera, R. A. (2011). *Rediseño de la red lan del Instituto Nacional de Estadísticas y Censos Matriz Central (Tesis de pregrado).* Escuela Politécnica Nacional. Quito: Escuela Politécnica Nacional.

Editorial Team GRITS. (17 de Mayo de 2013). *laSalle Blogging*. Obtenido de laSalle Blogging: https://blogs.salleurl.edu/es/networking-and-internet-technologies/alta-redundancia-y-disponibilidad-i

EFORT. (2011). *RTP y RTCP*.

Gallegos Altamirano, B. M., & Román González, I. A. (Julio de 2018). *Análisis de los mecanismos de seguridad en un ISP de nivel tres y propuesta de implementación de IPSEC en un entorno IPv6.* Obtenido de Universidad Politécnica Salesiana: http://dspace.ups.edu.ec/handle/123456789/15809

Hallberg, B. (2006). *Fundamentos de Redes.* Madrid: McGraw-Hill Interamericana.

Hernández Cueto, C. C., & Vargas Galindo, D. E. (13 de Abril de 2018). *Análisis de tráfico de red y reasignación del ancho de banda adecuado de la red de COLTRANS.* Obtenido de Universidad Piloto de Colombia: http://repository.unipiloto.edu.co/handle/20.500.12277/2464

Huawei Technologies Co. Ltd. (13 de Agosto de 2018). *Huawei*. Obtenido de Huawei: https://support.huawei.com/enterprise/es/doc/EDOC1100027117?section=j001

IANA. (2020 de Abril de 2020). *IANA*. Obtenido de IANA: https://www.iana.org/protocols

Lagla Gallardo, C. (2019). *Propuesta de rediseño de la red de datos de la empresa COBRAFACIL FABRASILISA S.A bajo metodología PPDIOO y diseño Top-Down (Tesis de pregrado).* Universidad Politécnica Salesiana, Quito.

Loor Fonseca, D. C., & Pichoasamín Morales, L. H. (2001). *Estudio de los factores técnicos y Operativos que intervienen en la infraestructura de Calidad de Servicio en Internet (Tesis de Pregrado).* Quito: Escuela Politécnica Nacional.

Lopez Quezada, E. A. (06 de Julio de 2018). *Diseño de una red Lan en la institución educativa Túpac Amaru – Tumbes – 2017.* Obtenido de ULADECH Católica: http://repositorio.uladech.edu.pe/handle/123456789/4079

Milton, J. S., & Arnold, J. C. (2004). *Probabilidad y estadística con aplicaciones para ingeniería y ciencias computacionales.* México D.F: McGraw-Hill Interamericana.

Moreno Pérez, J. C., & Santos González, M. (2014). *Sistemas Informáticos y Redes Locales.* Madrid: RA-MA.

Olifer, N., & Olifer, V. (2009). *Redes de computadoras: principios, tecnología y protocolos para el diseño de redes.* Santa Fe: McGraw-Hill Interamericana.

R. Gavilán, I. G. (2019). *La carrera digital.* Andalucía: Exlibric.

Sánchez Galiano, G. (2015). *Estudio comparativo de servidores multimedia.* España: 3Ciencias Área de Innovación y Desarrollo, S.L.

Sepúlveda, M. (Julio de 2019). *eClassVirtual*. Obtenido de eClassVirtual: https://eclassvirtual.com/arquitectura-de-topologias-de-redes-ccna-200-301/

Shenker, S., Partridge, C., & Guerin, R. (Septiembre de 1997). *IETF Tools.* Obtenido de IETF Tools: https://tools.ietf.org/html/rfc2215

Universidad Politécnica Salesiana. (17 de Diciembre de 2014). *Universidad Politécnica Salesiana.* Obtenido de Universidad Politécnica Salesiana: https://www.ups.edu.ec/normativa/-/document_library_display/u8OILw1nqXw9/viewf/1506972

Wroclawski, J. (Septiembre de 1997). *IETF Tools.* Obtenido de IETF Tools: https://tools.ietf.org/html/rfc2211

LISTA DE REFERENCIAS

BIBLIOGRAFÍA

Ariganello, E. (2016). *CCNA Routing y Switching.* Madrid: RA-MA.

Ariganello, E., & Barrientos Sevilla, E. (2010). *Redes CISCO, CCNP A fondo.* Madrid: ALFAOMEGA GPO EDR.

Calvo García , A. L. (2014). Gestión de redes telemáticas UF1880. Málaga: IC Editorial.

Hallberg, B. (2006). *Fundamentos de Redes.* Madrid: McGraw-Hill Interamericana.

Milton, J. S., & Arnold, J. C. (2004). *Probabilidad y estadística con aplicaciones para ingeniería y ciencias computacionales.* México D.F: McGraw-Hill Interamericana.

Moreno Pérez, J. C., & Santos González, M. (2014). *Sistemas Informáticos y Redes Locales.* Madrid: RA-MA.

Olifer, N., & Olifer, V. (2009). *Redes de computadoras: principios, tecnología y protocolos para el diseño de redes.* Santa Fe: McGraw-Hill Interamericana.

Sánchez Galiano, G. (2015). *Estudio comparativo de servidores multimedia.* España: 3Ciencias Área de Innovación y Desarrollo, S.L.

IMÁGENES

Sepúlveda, M. (Julio de 2019). *eClassVirtual*. Obtenido de eClassVirtual: https://eclassvirtual.com/arquitectura-de-topologias-de-redes-ccna-200-301/

CPD. (2019). *INFORME DE ACTIVIDADES P55* . Quito.

SITIOS WEB

Calderón Zetter, M. I. (18 de Mayo de 2016). *Blog de Radioaficion,Tecnología y Internet.* Obtenido de Brandmeister XE : http://www.xe1gqp.org.mx/blog/wp-content/uploads/2016/05/Redes-de-computadoras-estandares-y-protocolos-por-XE1GNW-Ines-Calderon.pdf

Cisco. (Abril de 2014). *Cisco.* Obtenido de Cisco: https://www.cisco.com/c/dam/r/es/la/internet-of-everything-ioe/assets/pdfs/en-05_campus-wireless_wp_cte_es-xl_42333.pdf

Cisco. (19 de Septiembre de 2014). *Cisco.* Obtenido de Cisco: https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html?dtid=osscdc000283

Cisco. (5 de Junio de 2017). *Cisco.* Obtenido de Cisco: https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/5234-5.html?dtid=osscdc000283

Cisco. (13 de Julio de 2017). *Cisco Systems, Inc.* Obtenido de Cisco: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/AccessTrunk.pdf

Cisco. (4 de Mayo de 2020). *Quality of Service (QoS) Configuration Guide, Cisco IOS XE Everest 16.5.1a (Catalyst 9300 Switches).* Obtenido de Cisco: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-5/configuration_guide/qos/b_165_qos_9300_cg.pdf

Cisco. (24 de Abril de 2020). *Security Configuration Guide, Cisco IOS XE Everest 16.5.1a (Catalyst 9300 Switches).* Obtenido de Cisco: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-5/configuration_guide/sec/b_165_sec_9300_cg/configuring_ipv4_acls.html?dtid=osscdc000283#concept_EA18174B5D624C72ADB4F54AC5808D5F

Editorial Team GRITS. (17 de Mayo de 2013). *laSalle Blogging*. Obtenido de laSalle Blogging: https://blogs.salleurl.edu/es/networking-and-internet-technologies/alta-redundancia-y-disponibilidad-i

EFORT. (2011). *RTP y RTCP.*

Huawei Technologies Co. Ltd. (13 de Agosto de 2018). *Huawei*. Obtenido de Huawei: https://support.huawei.com/enterprise/es/doc/EDOC1100027117?section=j001

IANA. (2020 de Abril de 2020). *IANA*. Obtenido de IANA: https://www.iana.org/protocols

R. Gavilán, I. G. (2019). *La carrera digital.* Andalucía: Exlibric.

Shenker, S., Partridge, C., & Guerin, R. (Septiembre de 1997). *IETF Tools.* Obtenido de IETF Tools: https://tools.ietf.org/html/rfc2215

Wroclawski, J. (Septiembre de 1997). *IETF Tools.* Obtenido de IETF Tools: https://tools.ietf.org/html/rfc2211

TESIS/TRABAJOS DE TITULACIÓN

Aguaiza Tenelema, D. (2016). *Propuesta de rediseño de la infraestructura de red de la Universidad Laica Eloy Alfaro¨ de Manabí, para ofrecer un modelo de*

servicios con calidad de servicio (QoS) (Tesis de pregrado). Potificia Universidad Católica del Ecuador, Quito.

Arévalo Padilla, L. P. (2016). *Rediseño de una red lan multiservicios para el Municipio de Tulcán.* Universidad de las Amércias, Quito.

Chisaguano Castellano, D. A., & Ludeña Veliz, M. J. (Febrero de 2019). *Análisis, diseño e implementación de un sistema de gestión de inventarios de activos de TI para los laboratorios de la carrera de Ingeniería en Ciencias de la Computación de la Universidad Politécnica Salesiana sede Quito campus sur.* Obtenido de Universidad Politécnica Salesiana: http://dspace.ups.edu.ec/handle/123456789/16969

Defaz Carrera, J. A., & Gallegos Herrera, R. A. (2011). *Rediseño de la red lan del Instituto Nacional de Estadísticas y Censos Matriz Central (Tesis de pregrado).* Escuela Politécnica Nacional. Quito: Escuela Politécnica Nacional.

Gallegos Altamirano, B. M., & Román González, I. A. (Julio de 2018). *Análisis de los mecanismos de seguridad en un ISP de nivel tres y propuesta de implementación de IPSEC en un entorno IPv6.* Obtenido de Universidad Politécnica Salesiana: http://dspace.ups.edu.ec/handle/123456789/15809

Hernández Cueto, C. C., & Vargas Galindo, D. E. (13 de Abril de 2018). *Análisis de tráfico de red y reasignación del ancho de banda adecuado de la red de COLTRANS.* Obtenido de Universidad Piloto de Colombia: http://repository.unipiloto.edu.co/handle/20.500.12277/2464

Lagla Gallardo, C. (2019). *Propuesta de rediseño de la red de datos de la empresa COBRAFACIL FABRASILISA S.A bajo metodología PPDIOO y diseño Top-Down (Tesis de pregrado).* Universidad Politécnica Salesiana, Quito.

Loor Fonseca, D. C., & Pichoasamín Morales, L. H. (2001). *Estudio de los factores técnicos y Operativos que intervienen en la infraestructura de Calidad de Servicio en Internet (Tesis de Pregrado).* Quito: Escuela Politécnica Nacional.

Lopez Quezada, E. A. (06 de Julio de 2018). *Diseño de una red Lan en la institución educativa Túpac Amaru – Tumbes – 2017.* Obtenido de ULADECH Católica: http://repositorio.uladech.edu.pe/handle/123456789/4079

Universidad Politécnica Salesiana. (17 de Diciembre de 2014). *Universidad Politécnica Salesiana.* Obtenido de Universidad Politécnica Salesiana: https://www.ups.edu.ec/normativa/-/document_library_display/u8OILw1nqXw9/viewf/1506972

ANEXOS

Anexo 1

Cálculo de varianza y desviación media – Escenario inicial

x_i	n	$\bar{x}$	$x_i - \bar{x}$	$(x_i - \bar{x})^2$	S^2	σ
9504	101	1552,8914678665	9.403	88.416.409	5109697,80098	2260,46407
11.974,6666666666			11.873,6666666666	140.983.960,1111100000		
7.983,1111111111			7.882,1111111111	62.127.675,5679012000		
5.987,3333333333			5.886,3333333333	34.648.920,1111111000		
4.789,8666666667			4.688,8666666667	21.985.470,6177777000		
4.359,1111111111			4.258,1111111111	18.131.510,2345679000		
3.793,9047619048			3.692,9047619048	13.637.545,5804989000		
3.531,3333333333			3.430,3333333333	11.767.186,7777778000		
3.161,1851851852			3.060,1851851852	9.364.733,3676268600		
2.845,0666666667			2.744,0666666667	7.529.901,8711110700		
2.586,4242424242			2.485,4242424242	6.177.333,6648301100		
2.370,8888888889			2.269,8888888889	5.152.395,5679011900		
2.203,8974358974			2.102,8974358974	4.422.177,6259039900		
2.046,4761904762			1.945,4761904762	3.784.877,6077097500		
1.910,0444444444			1.809,0444444444	3.272.641,8019752900		
1.803,1666666667			1.702,1666666667	2.897.371,3611110900		
1.697,0980392157			1.596,0980392157	2.547.528,9507881400		
1.602,8148148148			1.501,8148148148	2.255.447,7379972400		
1.518,4561403509			1.417,4561403509	2.009.181,9098183900		
1.452,5333333333			1.351,5333333333	1.826.642,3511111000		
1.383,3650793651			1.282,3650793651	1.644.460,1967750100		
1.320,4848484848			1.219,4848484848	1.487.143,2956840900		
1.271,7681159420			1.170,7681159420	1.370.697,9813064300		
1.218,7777777778			1.117,7777777778	1.249.427,1604938100		
1.170,0266666667			1.069,0266666667	1.142.818,0140444300		
1.125,0256410256			1.024,0256410256	1.048.628,5134779700		
1.090,7654320988			989,7654320988	979.635,6105776450		
1.051,8095238095			950,8095238095	904.038,7505668860		
1.015,5402298851			914,5402298851	836.383,8320782000		
988,3555555556			887,3555555556	787.399,8819753090		
956,4731182796			855,4731182796	731.834,2560989710		
926,5833333333			825,5833333333	681.587,8402777770		
898,5050505051			797,5050505051	636.014,3055810640		
877,9607843137			776,9607843137	603.668,0603614000		
852,8761904762			751,8761904762	565.317,8058049900		
829,1851851852			728,1851851852	530.253,6639231820		

812,1801801802			711,1801801802	505.777,2486811130		
790,8070175439			689,8070175439	475.833,7214527550		
770,5299145299			669,5299145299	448.270,3064504350		
751,2666666667			650,2666666667	422.846,7377777780		
737,8211382114			636,8211382114	405.541,1620728400		
720,2539682540			619,2539682540	383.475,4771982860		
703,5038759690			602,5038759690	363.010,9205576590		
692,0606060606			591,0606060606	349.352,6400367310		
676,6814814815			575,6814814815	331.409,1681207140		
661,9710144928			560,9710144928	314.688,4791010300		
647,8865248227			546,8865248227	299.084,8710326440		
638,5555555556			537,5555555556	288.965,9753086420		
625,5238095238			524,5238095238	275.125,2267573700		
613,0133333333			512,0133333333	262.157,6535111110		
1.128,6797385621			1.027,6797385621	1.056.125,6450510500		
1.468,3589743590			1.367,3589743590	1.869.670,5647600100		
1.440,6540880503			1.339,6540880503	1.794.673,0756299100		
1.417,6790123457			1.316,6790123457	1.733.643,6215515700		
1.391,9030303030			1.290,9030303030	1.666.430,6336455500		
1.367,0476190476			1.266,0476190476	1.602.876,5736961200		
1.343,0643274854			1.242,0643274854	1.542.723,7936117100		
1.323,3563218391			1.222,3563218391	1.494.154,9775399600		
1.300,9265536723			1.199,9265536723	1.439.823,7342079100		
1.279,2444444444			1.178,2444444444	1.388.259,9708641900		
1.261,5519125683			1.160,5519125683	1.346.880,7417659400		
1.241,2043010753			1.140,2043010753	1.300.065,8481905200		
1.221,5026455026			1.120,5026455026	1.255.526,1785784100		
1.202,4166666667			1.101,4166666667	1.213.118,6736111000		
1.186,9948717949			1.085,9948717949	1.179.384,8615647600		
1.169,0101010101			1.068,0101010101	1.140.645,5758596000		
1.151,5621890547			1.050,5621890547	1.103.680,9130714500		
1.137,5686274510			1.036,5686274510	1.074.474,5194156100		
1.121,0821256039			1.020,0821256039	1.040.567,5429764900		
1.105,0666666667			1.004,0666666667	1.008.149,8711111000		
1.089,5023474178			988,5023474178	977.136,8908505800		
1.077,1481481481			976,1481481481	952.865,2071330430		
1.062,3926940639			961,3926940639	924.275,9121994820		
1.048,0360360360			947,0360360360	896.877,2535508370		
1.036,7288888889			935,7288888889	875.588,5535012180		
1.023,0877192982			922,0877192982	850.245,7620806300		
1.009,8008658009			908,8008658009	825.919,0136803930		
996,8547008547			895,8547008547	802.555,6450434660		
986,7679324895			885,7679324895	784.584,8302266380		
974,4333333333			873,4333333333	762.885,7877777770		
962,4032921811			861,4032921811	742.015,6317803860		

950,6666666667			849,6666666667	721.933,4444444450		
941,6224899598			840,6224899598	706.646,1706262800		
930,4126984127			829,4126984127	687.925,4242882330		
919,4666666667			818,4666666667	669.887,6844444450		
908,7751937985			807,7751937985	652.500,7637161230		
898,3295019157			797,3295019157	635.734,3346251530		
888,1212121212			787,1212121212	619.559,8025711660		
878,1423220974			777,1423220974	603.950,1887949050		
868,3851851852			767,3851851852	588.880,0224417010		
858,8424908425			757,8424908425	574.325,2409263510		
849,5072463768			748,5072463768	560.263,0978785970		
840,3727598566			739,3727598566	546.672,0780180110		
831,4326241135			730,4326241135	533.531,8183692970		
822,6807017544			721,6807017544	520.823,0352847030		
814,1111111111			713,1111111111	508.527,4567901230		
805,7182130584			704,7182130584	496.627,7598162510		
797,4965986395			696,4965986395	485.107,5119163310		
789,4410774411			688,4410774411	473.951,1171082320		
781,5466666667			680,5466666667	463.143,7655111120		
0,0000000000			-101,0000000000	10.201,0000000000		

Anexo 2

Cálculo de varianza y desviación media – Escenario direccionamiento estático

x_i	n	$\bar{x}$	$x_i - \bar{x}$	$(x_i - \bar{x})^2$	S^2	σ
8976	101	16695,804981677	8875	78765625	281995588,2867020	16792,724266381
13558,6666666666			13457,6666666666	181108792,11110900		
13527,1111111111			13426,1111111111	180260459,56790100		
14633,3333333333			14532,3333333333	211188712,11111000		
15297,0666666666			15196,0666666666	230920442,13777600		
16142,6666666666			16041,6666666666	257335069,44444200		
15997,7142857142			15896,7142857142	252705525,08163000		
16359,6666666666			16258,6666666666	264344241,77777600		
16595,5555555555			16494,5555555555	272070362,97530700		
16770,1333333333			16669,1333333333	277860006,08444300		
16469,5757575757			16368,5757575757	267930272,33149500		
16593,1111111111			16492,1111111111	271989728,90123400		
16713,0256410256			16612,0256410256	275959395,89809200		
16801,5238095238			16700,5238095238	278907495,51247100		
16579,0222222222			16478,0222222222	271525216,35604900		
16664,8333333333			16563,8333333333	274360574,69444300		

16770,3529411764			16669,3529411764	277867327,47750600		
16876,0000000000			16775,0000000000	281400625,00000000		
16712,5614035087			16611,5614035087	275943972,26254000		
16798,2666666666			16697,2666666666	278798714,13777600		
16853,2063492063			16752,2063492063	280636417,56638800		
16915,6363636363			16814,6363636363	282731996,04132000		
16765,5652173913			16664,5652173913	277707733,88468800		
16823,3333333333			16722,3333333333	279636432,11111000		
16868,4800000000			16767,4800000000	281148385,55040000		
16910,1538461538			16809,1538461538	282547653,02366700		
16789,9259259259			16688,9259259259	278520248,56104200		
16831,4285714285			16730,4285714285	279907240,18367100		
16870,0689655172			16769,0689655172	281201673,97027200		
16912,8000000000			16811,8000000000	282636619,24000000		
16801,5483870967			16700,5483870967	278908316,42975800		
16837,5000000000			16736,5000000000	280110432,25000000		
16871,2727272727			16770,2727272727	281242047,34710600		
16908,9411764705			16807,9411764705	282506886,59169300		
16810,5142857142			16709,5142857142	279207867,66448700		
16842,2222222222			16741,2222222222	280268521,49382600		
16872,2162162162			16771,2162162162	281273693,37107300		
16905,8947368421			16804,8947368421	282404487,11634300		
16821,1282051282			16720,1282051282	279562687,19592400		
16852,8000000000			16751,8000000000	280622803,24000000		
16884,4878048780			16783,4878048780	281685462,89648900		
16913,1428571428			16812,1428571428	282648147,44897800		
16832,9302325581			16731,9302325581	279957489,30719200		
16858,3636363636			16757,3636363636	280809236,04132100		
16887,1111111111			16786,1111111111	281773526,23456700		
16913,2173913043			16812,2173913043	282650653,61247500		
16839,8297872340			16738,8297872340	280188422,64599200		
16867,1666666666			16766,1666666666	281104344,69444200		
16889,3061224489			16788,3061224489	281847222,46105500		
16910,5600000000			16809,5600000000	282561307,39360000		
17154,9803921568			17053,9803921568	290838247,21606900		
17369,3846153846			17268,3846153846	298197107,22485100		
17380,3773584905			17279,3773584905	298576881,89711400		
17393,2839506172			17292,2839506172	299023084,22877300		
17327,9515151515			17226,9515151515	296767858,50538100		
17357,5238095238			17256,5238095238	297787613,98866200		
17382,4093567251			17281,4093567251	298647109,35470600		
17395,6781609195			17294,6781609195	299105892,68978600		
17331,3446327683			17230,3446327683	296884776,16396700		
17341,6888888888			17240,6888888888	297241353,36345400		
17351,6939890710			17250,6939890710	297586443,10457000		

17364,6021505376			17263,6021505376	298031959,21204700		
17304,8465608465			17203,8465608465	295972336,48915000		
17314,9583333333			17213,9583333333	296320361,50173500		
17324,7589743589			17223,7589743589	296657873,20680900		
17337,2929292929			17236,2929292929	297089793,94439200		
17279,4825870646			17178,4825870646	295100263,99408200		
17289,3725490196			17188,3725490196	295440150,88389100		
17303,8454106280			17202,8454106280	295937890,22196500		
17315,0476190476			17214,0476190476	296323435,43083800		
17262,5727699530			17161,5727699530	294519579,93839200		
17276,8148148148			17175,8148148148	295008614,55281200		
17286,0639269406			17185,0639269406	295326422,17303500		
17295,0630630630			17194,0630630630	295635804,61658700		
17243,9822222222			17142,9822222222	293881839,47142600		
17284,5614035087			17183,5614035087	295274782,50815400		
17319,7229437229			17218,7229437229	296484419,81268900		
17327,8290598290			17226,8290598290	296763639,45656900		
17307,2742616033			17206,2742616033	296055873,96551200		
17315,3333333333			17214,3333333333	296333272,11111000		
17323,1934156378			17222,1934156378	296603946,04563800		
17330,8617886178			17229,8617886178	296868137,25487200		
17311,2610441767			17210,2610441767	296193085,20870600		
17320,3809523809			17219,3809523809	296507080,38321800		
17327,8117647058			17226,8117647058	296763043,57660600		
17335,0697674418			17234,0697674418	297013160,74905100		
17290,5747126436			17189,5747126436	295481478,80155600		
17298,0909090909			17197,0909090909	295739935,73553700		
17305,4382022471			17204,4382022471	295992693,85493900		
17312,6222222222			17211,6222222222	296239939,52049300		
17290,9890109890			17189,9890109890	295495722,19792300		
17299,6521739130			17198,6521739130	295793636,59924200		
17308,1290322580			17207,1290322580	296085289,53277600		
17314,9787234042			17213,9787234042	296321063,48981300		
17275,8736842105			17174,8736842105	294976286,06858600		
17282,9166666666			17181,9166666666	295218260,34027500		
17289,8144329896			17188,8144329896	295455341,61175200		
17296,5714285714			17195,5714285714	295687676,75510100		
17259,2323232323			17158,2323232323	294404936,45801400		
17266,1600000000			17165,1600000000	294642717,82560000		
0			-101,0000000000	10201,00000000		

Anexo 3

Cálculo de varianza y desviación media – Escenario direccionamiento dinámico

x_i	n	$\bar{x}$	$x_i - \bar{x}$	$(x_i - \bar{x})^2$	S^2	σ
0	101	348,7075266	-348,7075266	121596,9391	20295,09428	142,4608518
0			-348,7075266	121596,9391		
63,111111111111			-285,5964155	81565,31252		
47,333333333333			-301,3741932	90826,40435		
37,866666666667			-310,8408599	96622,04019		
558,222222222222			209,5146956	43896,40769		
623,619047619048			274,911521	75576,3444		
731			382,2924734	146147,5352		
806,518518518519			457,8109919	209590,9043		
745,866666666667			397,1591401	157735,3826		
695,272727272727			346,5652007	120107,4383		
637,333333333333			288,6258068	83304,85633		
603,692307692308			254,9847811	65017,2386		
560,571428571429			211,863902	44886,31297		
523,200000000000			174,4924734	30447,62328		
509,666666666667			160,9591401	25907,84478		
491,450980392157			142,7434538	20375,69361		
521,185185185185			172,4776586	29748,54272		
508,210526315790			159,5029997	25441,20693		
492,800000000000			144,0924734	20762,6409		
482,412698412698			133,7051718	17877,07298		
460,484848484848			111,7773219	12494,16969		
440,463768115942			91,75624154	8419,207862		
430,444444444444			81,73691787	6680,923743		
413,226666666667			64,51914009	4162,719438		
397,333333333333			48,62580676	2364,469083		
390,024691358025			41,31716479	1707,108106		
376,095238095238			27,38771152	750,0867425		
363,126436781609			14,41891021	207,9049716		
351,022222222222			2,31469565	5,357815951		
346,150537634409			-2,556988938	6,53819243		
335,333333333333			-13,37419324	178,8690448		
325,171717171717			-23,5358094	553,9343242		
315,607843137255			-33,09968344	1095,589044		
312,304761904762			-36,40276467	1325,161275		
303,629629629630			-45,07789694	2032,016793		
299,099099099099			-49,60842747	2460,996076		
300,070175438597			-48,63735113	2365,591925		
295,863247863248			-52,84427871	2792,517792		

295,266666666667			-53,44085991	2855,925507		
288,065040650407			-60,64248592	3677,511099		
289,206349206349			-59,50117737	3540,390108		
282,480620155039			-66,22690642	4386,003134		
279,151515151515			-69,55601142	4838,038725		
277,392592592593			-71,31493398	5085,819809		
274,318840579710			-74,38868599	5533,676604		
268,482269503546			-80,22525707	6436,091872		
262,888888888889			-85,81863768	7364,838574		
261,605442176871			-87,1020844	7586,773106		
256,373333333333			-92,33419324	8525,603241		
345,934640522876			-2,77288605	7,688897044		
421,692307692308			72,98478112	5326,778275		
413,735849056604			65,02832248	4228,682725		
410,913580246914			62,20605367	3869,593114		
405,915151515151			57,20762494	3272,712352		
402,238095238095			53,53056867	2865,521782		
397,567251461988			48,85972489	2387,272716		
390,712643678161			42,00511711	1764,429863		
387,480225988701			38,77269942	1503,32222		
381,022222222222			32,31469565	1044,239555		
377,005464480874			28,29793791	800,7732899		
370,924731182796			22,21720461	493,6041807		
368,211640211640			19,50411364	380,4104488		
362,458333333333			13,75080676	189,0846866		
356,882051282051			8,17452471	66,82285423		
351,474747474747			2,767220902	7,657511522		
349,213930348259			0,506403776	0,256444784		
344,078431372549			-4,6290952	21,42852237		
340,908212560386			-7,799314012	60,82929906		
338,895238095238			-9,812288477	96,28100516		
334,122065727699			-14,58546084	212,7356681		
329,481481481481			-19,22604509	369,6408098		
324,968036529680			-23,73949004	563,5633875		
323,279279279279			-25,42824729	646,5957604		
318,968888888889			-29,73863768	884,3865713		
314,771929824561			-33,93559675	1151,624727		
313,281385281385			-35,42614129	1255,011487		
309,264957264957			-39,44256931	1555,716274		
305,350210970464			-43,3573156	1879,856816		
301,533333333333			-47,17419324	2225,404508		
300,279835390946			-48,42769118	2345,241273		
296,617886178862			-52,08964039	2713,330636		
293,044176706827			-55,66334987	3098,408518		
289,555555555556			-59,15197102	3498,955675		

286,149019607843			-62,55850696	3913,566794		
282,821705426357			-65,88582115	4340,941428		
279,570881226054			-69,13664535	4779,87573		
276,393939393939			-72,31358718	5229,254891		
273,288389513109			-75,41913706	5688,046235		
270,251851851852			-78,45567472	6155,292896		
267,282051282051			-81,42547529	6630,108026		
264,376811594203			-84,33071498	7111,669489		
261,534050179211			-87,17347639	7599,214986		
258,751773049645			-89,95575352	8092,037592		
256,028070175439			-92,6794564	8589,481638		
253,361111111111			-95,34641546	9090,938941		
250,749140893471			-97,95838568	9595,845325		
248,190476190476			-100,5170504	10103,67742		
245,683501683502			-103,0240249	10613,9497		
243,226666666667			-105,4808599	11126,21181		
0			-348,7075266	121596,9391		

Anexo 3

Políticas de seguridad de la información (Universidad Politécnica Salesiana, 2014)

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

4.3 CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

El proceso de escoger los controles (protección) está definido en la metodología de evaluación y tratamiento de riesgos.

Los controles seleccionados y su estado de implementación se detallan en la Declaración de Aplicabilidad.

Los controles seleccionados y aplicados buscarán cumplir los siguientes requerimientos:

4.3.1 Evaluación de Riesgo de la Información

4.3.1.1 El grado de control de la seguridad requerida depende de la sensibilidad y criticidad de la información. El primer paso para determinar el nivel adecuado de seguridad es un proceso de evaluación de riesgos, cuyo fin será identificar y clasificar la naturaleza de la información que la UPS posee, las consecuencias adversas de las brechas de seguridad y la probabilidad de que ocurran esas consecuencias.

4.3.1.2 Dada la naturaleza descentralizada de la estructura de la UPS, la evaluación del riesgo debe llevarse a cabo en primera instancia por sus diferentes departamentos y ésta debe ser coherente con los principios generales de esta política.

4.3.1.3 La evaluación del riesgo debe identificar los activos de información del departamento, definir la propiedad de dichos activos, y clasificarlas en función de su sensibilidad y/o criticidad para el departamento o la UPS en su conjunto. En la evaluación de riesgos, los departamentos deben considerar el valor de los activos, las amenazas a ese activo y su vulnerabilidad.

4.3.1.4 Cuando sea práctico, los activos de información deben ser etiquetados y manejados de acuerdo con su criticidad y sensibilidad.

4.3.1.5 Se debe definir, documentar e implementar normas para el uso aceptable de los activos de información.

4.3.1.6 Las evaluaciones de riesgos de seguridad de información deben ser repetidos periódicamente como parte de la ejecución operacional normal y cuando se realicen cambios en la infraestructura, los sistemas informáticos y los procesos de la UPS.

4.3.2 Datos Personales

Todo lo referente a Datos Personales, estará contemplado en la "Política de Datos Personales de la UPS y clasificación de la información".

4.3.3 Protección de Sistemas de Información y Activos

4.3.3.1 Después de haber completado una evaluación de riesgo de sus activos de información, los departamentos deben elaborar sus lineamientos de seguridad que se enmarcarán en las Políticas establecidas en este documento, la determinación de controles y procedimientos adecuados. Los propietarios de la información

Turuhuayco 3-69 y Calle Vieja • PBX: (+593 7) 2050000 • Fax: 4088958 • Casilla Postal: 2074
e-mail: rector@ups.edu.ec • www.ups.edu.ec • Cuenca - Ecuador

deben tener constancia de que los controles reducen cualquier riesgo residual a un nivel aceptable.

4.3.3.2 La información confidencial debe ser manejada de acuerdo con los requisitos establecidos en el siguiente punto.

4.3.4 PROTECCIÓN DE INFORMACIÓN CONFIDENCIAL

El tratamiento de la Información Confidencial, estará contemplado en el documento "Política de Datos Personales de la UPS y clasificación de la información".

4.3.5 ACCESO REMOTO

4.3.5.1 Cuando se requiera de acceso remoto, éste debe ser controlado mediante una política de control de acceso definida y los controles deben ser estrictos manteniendo el principio del mínimo acceso necesario.

4.3.5.2 Todo acceso remoto debe ser controlado por protocolos de control de acceso seguro usando los niveles apropiados de encriptación y autentificación.

4.3.6 COPIA DE INFORMACIÓN

4.3.6.1 El número de copias realizadas de información confidencial, ya sea en dispositivos o medios portátiles o como copias físicas, deben ser las mínimas requeridas y cuando sea necesario, se debe llevar un registro de esa distribución. Cuando ya no sea necesaria la copia debe ser eliminada o, en el caso de copias físicas, deben ser destruidas.

4.3.6.2 Todas las copias deben ser físicamente seguras.

4.3.7 RETIRO DE INFORMACIÓN CONFIDENCIAL

4.3.7.1 Se debe definir políticas y procedimientos para el retiro o destrucción de información confidencial.

4.3.7.2 Documentos confidenciales deben ser triturados de forma segura luego de su retiro.

4.3.8 USO DE DISPOSITIVOS O MEDIOS PORTÁTILES

4.3.8.1 Se deben definir procedimientos para la administración de medios removibles con el fin de asegurar que ellos estén apropiadamente protegidos de accesos no autorizados.

4.3.8.2 El dueño de la información debe revisar los permisos sobre los activos de información a su cargo antes de que éstos sean llevados fuera de la UPS.

4.3.8.3 En el caso de datos personales, se recomienda que todos los dispositivos y medios portátiles deben ser encriptados cuando la pérdida de dicha información pueda causar daño o angustia a los individuos.

Turuhuayco 3-69 y Calle Vieja • PBX: (+593 7) 2050000 • Fax: 4088958 • Casilla Postal 2074
e-mail: rector@ups.edu.ec • www.ups.edu.ec • Cuenca - Ecuador

4.3.8.4 La frase de encriptación de un dispositivo no debe ser almacenada en el mismo dispositivo.

4.3.9 INTERCAMBIO DE INFORMACIÓN Y USO DEL CORREO ELECTRÓNICO

4.3.9.1 Se deben implementar controles para asegurar que los mensajes electrónicos son protegidos adecuadamente.

4.3.9.2 El correo electrónico debe ser apropiadamente protegido del uso y acceso no autorizado.

4.3.9.3 El correo electrónico solo debe ser utilizado para enviar información confidencial cuando el destinatario es de confianza, el dueño de la información ha dado su permiso y los controles adecuados se han adoptado.

4.3.9.4 Se debe proveer una guía para la administración de los riesgos asociados con el uso de correo electrónico.

4.3.10 CONTROLES CRIPTOGRÁFICOS

4.3.10.1 Se deben definir procedimientos para soportar el uso de técnicas criptográficas para asegurar que solo el personal autorizado pueda tener acceso a información confidencial.

4.3.10.2 Se debe definir una política de criptografía y administración de claves, y verificar su cumplimiento con el fin de asegurar que los datos están apropiadamente asegurados y que los requerimientos tanto internos como externos han sido cumplidos.

4.3.11 DISEÑO Y DESARROLLO DE SISTEMAS

4.3.11.1 Una evaluación de riesgos debe ser llevada a cabo como parte del diseño y desarrollo de cualquier sistema que sea utilizado para almacenar información confidencial. La evaluación de riesgos debe ser repetida periódicamente en todos los sistemas existentes.

4.3.12 RESPALDO DE INFORMACIÓN

4.3.12.1 Los dueños de la información deben asegurarse que los respaldos y los procedimientos de recuperación sean definidos. Las copias de respaldo de todo activo de información importante deben ser probadas regularmente de acuerdo a una apropiada política de respaldo.

4.3.13 ETIQUETADO DE PROTECCIÓN DE COPIAS FÍSICAS

4.3.13.1 Los documentos que contienen información confidencial deben ser etiquetados como "Confidencial" o con una designación adecuada dependiendo de la clasificación adoptada por el departamento.

Turuhuayco 3-69 y Calle Vieja • PBX: (+593 7) 2050000 • Fax: 4088958 • Casilla Postal: 2074
e-mail: rector@ups.edu.ec • www.ups.edu.ec • Cuenca - Ecuador

4.3.14 ALMACENAMIENTO DE COPIAS FÍSICAS

a. Cuando sea práctico, los documentos con información confidencial deben ser almacenados en armarios o gavetas, cuando no sea necesario y la información sea almacenada en estanterías abiertas, el espacio físico debe ser cerrado cuando se abandone por un tiempo considerable.
b. Las llaves de los armarios o gavetas, no deben ser dejados a la vista cuando el espacio físico no esté ocupado.

4.3.15 TRASLADO DE INFORMACIÓN CONFIDENCIAL FUERA DE LAS INSTALACIONES

4.3.15.1 La información confidencial no debe ser llevada fuera de la UPS a menos que esta pueda ser retomada en el mismo día o almacenada de manera segura durante la noche.

4.3.16 TRANSMISIÓN DE INFORMACIÓN CONFIDENCIAL

a. Si documentos confidenciales son enviados por fax, el remitente debe asegurarse de utilizar el número correcto y el destinatario se encuentre cerca de la máquina de destino listo para tomar la información inmediatamente luego de ser impresa.
b. Si documentos confidenciales son enviados mediante correo externo, de preferencia debe ser enviado por correo certificado y el remitente debe asegurarse de que los documentos sean adecuadamente sellados.
c. Si documentos confidenciales son enviados mediante correo interno, los documentos deben ser marcados como "Confidencial" con el nombre del destinatario claramente escrito.

4.4 CONTINUIDAD DEL NEGOCIO

La gestión de la continuidad del negocio está reglamentada en la política de gestión de la continuidad del negocio.

4.5 RESPONSABILIDADES

Las responsabilidades para el Plan de Seguridad de la Información son las siguientes:

4.5.1 COMITÉ INFORMÁTICO DE LA UNIVERSIDAD POLITÉCNICA SALESIANA

El Comité Informático debe revisar el Plan de Seguridad de la Información al menos una vez por año o cada vez que se produzca una modificación significativa; y debe elaborar minutas de dichas reuniones. Los objetivos de las verificaciones por parte del Comité Informático son:

a. Establecer la conveniencia, adecuación y eficacia del Plan de Seguridad de la Información.

Turuhuayco 3-69 y Calle Vieja • PBX: (+593 7) 2050000 • Fax: 4088958 • Casilla Postal: 2074
e-mail: rector@ups.edu.ec • www.ups.edu.ec • Cuenca - Ecuador

b. Asegurar que los usuarios sean conscientes de esta política.
c. Supervisar el cumplimiento de la presente política.
d. Revisar de forma periódica el presente documento, teniendo en cuenta los cambios pertinentes en legislación, políticas organizacionales y obligaciones contractuales.
e. Asegurar que existe una dirección clara y el apoyo necesario para las iniciativas de seguridad de la información.

4.5.2 SECRETARIO TÉCNICO DE TECNOLOGÍAS DE LA INFORMACIÓN

a. El Secretario Técnico de Tecnologías de la Información es el responsable de garantizar que el Plan de Seguridad de la Información sea implementado y mantenido de acuerdo con esta política y de garantizar que todos los recursos necesarios estén disponibles.
b. El Secretario Técnico de Tecnologías de la Información es el responsable de la coordinación operativa del Plan de Seguridad de la Información, como también de informar su desempeño.
c. El Secretario Técnico de Tecnologías de la Información es el encargado de definir aspectos sobre la seguridad de la información y comunicará a la parte interesada (tanto interna como externa) cuando el caso lo amerite.
d. El Secretario Técnico de Tecnologías de la Información es el responsable de adoptar e implementar el plan de capacitación y concienciación, que corresponde a todas las personas que cumplen una función en la gestión de la seguridad de la información.

4.5.3 CONSEJO DE SEGURIDAD DE LA INFORMACIÓN

a. El Consejo de Seguridad de la Información posee la responsabilidad última sobre la seguridad de la información en la Universidad Politécnica Salesiana, siendo el Consejo responsable de asegurar que la UPS cumpla con los requisitos externos pertinentes, incluidos los de carácter legislativo, este Consejo será nombrado por el Rector o su delegado.

4.5.4 DIRECTORES DE DEPARTAMENTOS

a. Los directores de departamentos son responsables de la seguridad de la información dentro de su área de gestión, debiendo garantizar que cada departamento ha puesto en marcha una política local de seguridad de la información para satisfacer sus propias necesidades, en consonancia con los requisitos de esta política.
b. Los directores de departamentos deben definir de forma clara las funciones y responsabilidades específicas vinculadas a la seguridad de la información dentro de su área de gestión.
c. El jefe del departamento debe aprobar la política, garantizar que se aplique y revisarla con regularidad.

Turuhuayco 3-69 y Calle Vieja • PBX: (+593 7) 2050000 • Fax: 4088958 • Casilla Postal: 2074
e-mail: rector@ups.edu.ec • www.ups.edu.ec • Cuenca - Ecuador

4.5.5 USUARIOS Y PARTES EXTERNAS

a. Los usuarios de la información de la Universidad Politécnica Salesiana serán conscientes de sus propias responsabilidades individuales para cumplir con la presente política institucional y las políticas departamentales de seguridad de la información.
b. Acuerdos con terceros relacionados con el acceso, tratamiento, la comunicación o la gestión de la información de la Universidad, o los sistemas de información, deben cubrir todos los requisitos de seguridad pertinentes, y serán tratados en acuerdos contractuales.
c. Todos los incidentes o debilidades de seguridad deben ser informados al Secretario Técnico de Tecnologías de la Información.

4.5.6 OTROS

a. La Secretaría Técnica de Gestión de Talento Humano implementará programas de capacitación y concienciación de empleados sobre seguridad de la información.
b. La protección de la integridad, disponibilidad y confidencialidad de los activos es responsabilidad del propietario de cada activo.

4.6 COMUNICACIÓN DE LA POLÍTICA

El Secretario Técnico de Tecnologías de la Información debe asegurarse de que todos los empleados, docentes y estudiantes de la Universidad Politécnica Salesiana, como también los participantes externos correspondientes, estén familiarizados con esta política.

5. APOYO PARA LA IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN

A través del presente documento, el Consejo Superior de la Universidad Politécnica Salesiana respalda la implementación y mejora continua del Plan de Seguridad de la Información y se contará con el apoyo de los recursos adecuados para lograr todos los objetivos establecidos en esta política, como también para cumplir con todos los requisitos identificados.

5.1 COMPROMISOS

5.1.1 La Universidad Politécnica Salesiana reconoce el papel de la seguridad de la información para garantizar que los usuarios tengan acceso a la información que necesitan para llevar a cabo su trabajo. Los sistemas informáticos y los sistemas de información sustentan todas las actividades de la Universidad Politécnica Salesiana y son esenciales para sus funciones administrativas, actividades de investigación y docencia.

Turuhuayco 3-69 y Calle Vieja • PBX: (+593 7) 2050000 • Fax: 4088958 • Casilla Postal: 2074
e-mail: rector@ups.edu.ec • www.ups.edu.ec • Cuenca - Ecuador