UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TEMA:

Diseño e implementación de buenas prácticas y procedimientos de verificación de seguridad informática aplicada al sistema LAN/WAN para la Migración a Datacenter alterno de Credimatic

AUTOR:

Ing. Alex Daniel Zambrano Herrera

Trabajo de titulación previo a la obtención del grado de

Magister en Telecomunicaciones

TUTOR:

MSc. Manuel Romero Paz

Guayaquil, a los 21 días del mes de junio del año 2021

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

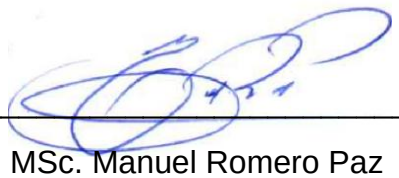
CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por Alex Daniel Zambrano Herrera como requerimiento parcial para la obtención del Título de Magíster en Telecomunicaciones.

TUTOR

MSc. Manuel Romero Paz

DIRECTOR DEL PROGRAMA



MSc. Manuel Romero Paz

Guayaquil, a los 21 días del mes de junio del año 2021

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

YO, Alex Daniel Zambrano Herrera

DECLARO QUE:

El trabajo de Titulación **"**Diseño e implementación de buenas prácticas y procedimientos de verificación de seguridad informática aplicada al sistema LAN/WAN para la Migración a Datacenter alterno de Credimatic**"** Previa a la obtención del Título de **Magíster en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 21 días del mes de junio del año 2021

EL AUTOR

Ing. Alex Daniel Zambrano Herrera

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

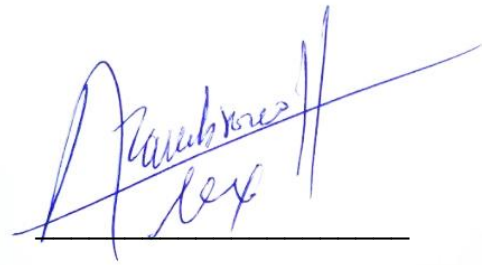
AUTORIZACIÓN

YO, Alex Daniel Zambrano Herrera

Autorizo a la Universidad Católica de Santiago de Guayaquil a la **publicación**, en la biblioteca de la institución del Trabajo de Titulación, **"**Diseño e implementación de buenas prácticas y procedimientos de verificación de seguridad informática aplicada al sistema LAN/WAN para la Migración a Datacenter alterno de Credimatic**"**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

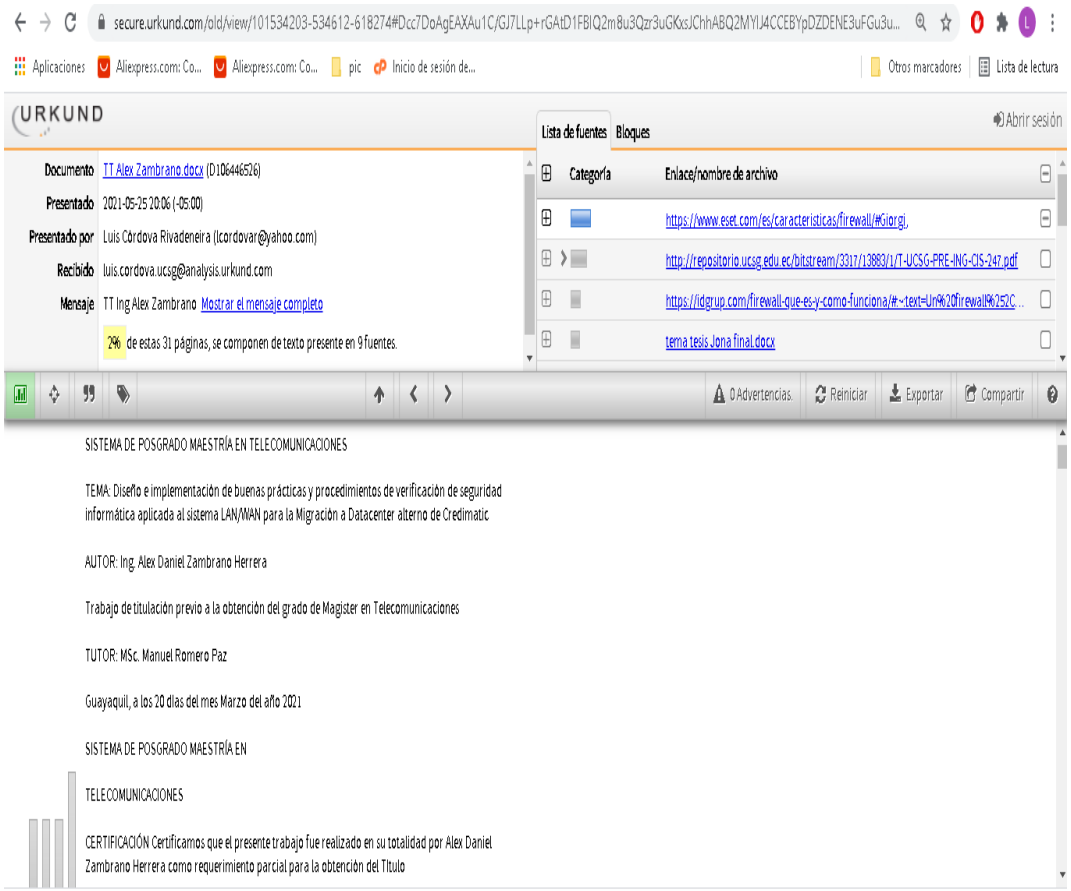
Guayaquil, a los 21 días del mes de junio del año 2021

EL AUTOR



Ing. Alex Daniel Zambrano Herrera

REPORTE URKUND



Dedicatoria

A Dios por haberme permitido tener esta experiencia y la bendición de salir adelante, a mis padres que me han dado la mayor enseñanza que se puede dar a un hijo amor y educación, a mis hermanos, dedico también este trabajo a mis amigos que me han empujado y soportado durante todo este proceso y como dejar de lado a la Universidad Católica de Santiago de Guayaquil por permitirme seguir creciendo profesionalmente.

Agradecimientos

El presente trabajo de tesis se da por el esfuerzo y la lucha constante de ser cada día mejor y superar las barreras que nos pone el destino, es por ello mi agradecimiento al Dios todo poderoso por contar con sus múltiples bendiciones siempre. A mis padres José Zambrano y Eloísa Herrera que son el mayor regalo de la vida que he tenido hasta el día de hoy ya que ellos han sido y serán por siempre el mayor de mis ejemplos. A mis hermanos Roxana, Emilio que con sus buenos consejos y ejemplo de vida han hecho de mí, el más grande admirador de todas sus hazañas tanto en lo personal como profesional. Un agradecimiento especial a todos mis amigos por su incondicional apoyo y empuje, A todos los docentes de la Maestría en Telecomunicaciones, con quienes hemos compartido muchos momentos de conocimiento y alegría dentro y fuera del salón de clase y por supuesto a todos mis compañeros de clase.

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

MSc. Manuel Romero Paz

TUTOR

f. _____

MSc. Manuel Romero Paz

DIRECTOR DEL PROGRAMA

f. _____

MSc. Luis Córdova Rivadeneira

REVISOR

_____

MSc. Edgar Quezada Calle

REVISOR

RESUMEN:

En el presente trabajo de investigación se realiza un análisis del estado actual de los componentes de red la cual deriva en un dimensionamiento y con esto proponer una posible solución a la problemática que la empresa está atravesando en estos momentos que conlleven a una mejora a nivel global de las comunicaciones externas e internas, con el fin de otorgar un mejor servicio tanto a los clientes internos como a los externos, se evalúa una solución convergente a todo nivel, que les permita otorgar niveles de disponibilidad de un 99.9%, que se acoplen a las siguientes características: cumplimiento de la Norma PCI, equipos con soporte y actualizaciones por 5 años, cableado estructurado certificado con soporte a 10 años, descongestión de backbone de red y capacidades que permitan el normal funcionamiento por los próximos 5 años, simplicidad en la administración de la red que conlleva a que la topología se simplifique, reduce el tiempo de resolución de problemas, abarata los costos de futuras implementaciones de sistemas de seguridad y permite una adaptación a cambios más eficiente, facilidad de integración o crecimiento con nuevos clientes, trasladando el centro de cómputo se podrá diseñar un sistema de interconexión a través de fibra óptica sostenible y permitirá la integración con nuevos clientes y asociados.

Palabras clave: convergencia, alta disponibilidad, tiempos de respuesta, integración, escalabilidad, seguridad

ABSTRACT

In this thesis, an analysis of the current state of the network components is carried out, which results in a dimensioning and with this propose a possible solution to the problems that the company is going through at the moment that lead to a global improvement to the External and internal communications in order to provide better services to both internal and external customers, a convergent solution is evaluated at all levels, which allows them to grant availability levels of 99.9%, which are coupled with the following characteristics , Compliance with PCI Standard, Equipment with support and updates for 5 years, Structured cabling certified with support for 10 years, Decongestion of network Backbone and capacities that allow normal operation for the next 5 years, Simplicity in the administration of the network that entails simplifies topology, reduces troubleshooting time, lowers costs for future s deployments safety systems and allows more efficient adaptation to changes. Ease of integration or growth with new clients: Moving the computer center will allow the design of an interconnection system through sustainable fiber optics and allow integration with new clients and associates.

Keywords: convergence, high availability, response times, integration, scalability, security

INDICE GENERAL

ÍNDICE DE FIGURAS

CAPITULO 2

CAPITULO 3

INDICE DE TABLAS

CAPITULO 2

CAPITULO 3

Capítulo 1: Diseño metodológico.

Actualmente las tecnologías existentes como IP (Internet Protocol), han sido diseñadas para que brinden seguridad y sean aptos de restablecer la conectividad luego de que se presente algún eventual corte o daño en los componentes de red. Pese a esto, el tiempo que demande la solución podría no estar acorde a los SLA (Service Level Agreement) de servicio de alta prioridad. Por esta razón se analiza la posibilidad para que un proveedor de servicios cotice e implemente un sistema de redes LAN (Local Area Network) y WAN (Wide Area Network) convergente, modular y escalable que pueda brindar a los clientes la seguridad necesaria al momento de utilizar los servicios que la compañía ofrece, adaptando protocolos como IP y MPLS (Multiprotocol Label Switching).

Toda empresa tiene elaborada su propia estructura interna, en cuanto a infraestructura y el recurso humano, todo esto va ligado a las necesidades o a la razón de ser de la misma, en base a estas estructuras se definen servicios de comunicaciones que tratan de satisfacer los requerimientos de cada organización, enfocándose en la transmisión de información interna y externa para sus clientes y/o proveedores, que la mayoría de las veces no son cubiertos a cabalidad de manera total o eficiente, ante ello cada día se van desarrollando nuevas y mejores soluciones tecnológicas en la búsqueda de la integridad de los datos, en donde debe primar la confidencialidad de la información sensitiva de cada empresa.

Existen múltiples alternativas a nivel de comunicaciones, pero entre las que más se destaca es la creación de redes convergentes, que estén distribuidas de manera adecuada, así como también tener protocolos de redundancia que permitan tener varios caminos, que a la vez se suman para tener mayor ancho de banda en la transmisión de datos, además con este protocolo de redundancia se tiene control de fallos, ya que al malograrse uno de los caminos de transmisión se garantiza que la comunicación continúe. Utiliza LACP (Link Aggregation Control Protocol), para controlar los enlaces y formar el Eth-Trunk, lo que ayuda a incrementar

el ancho de banda del enlace. Se basa en el estándar IEEE 802.3ad, por lo que LACP permite establecer enlaces Eth-Trunk entre dispositivos de los diferentes proveedores (HdezF, 2019), ya que la misma está caracterizada por la simplicidad de migración. MPLS estudia el transporte de paquetes y tiene como objetivo el mejoramiento del rendimiento de enrutamiento en la capa de red, por lo que optimiza la escalabilidad y flexibilidad en la prestación de servicios de encaminamiento del tráfico. Si se habla de seguridad, se tiene la red privada virtual VPN (Virtual Private Network) de punto a punto para otorgar un canal cifrado y seguro de comunicación para la compañía.

Por lo expuesto, el presente proyecto de titulación va direccionado a gestionar de manera adecuada los recursos que sean necesarios para la ejecución eficiente de los procesos internos en el datacenter, cuyo presupuesto estará financiado por la empresa.

1.1. Antecedentes.

La comunicación es la base fundamental en las redes de datos, desde los inicios del tiempo ha sido parte indispensable para el emisor y el receptor, de esta forma puede mantener una relación por medio del mensaje a través del canal.

Con la evolución tecnológica y el desarrollo de las comunicaciones, se crea la necesidad de que los tiempos de respuesta para las transacciones sean más cortos, por ello se ve la necesidad de realizar una actualización a nivel de infraestructura de la parte neurálgica, en cuanto al core de servicios de la compañía y así poder brindar un mejor servicio, apegado a las buenas prácticas y como las normas internacionales lo establecen, ya que existe información valiosa que es sensitiva y que debe estar a buen recaudo, disponible y a tiempo para mantener la integridad de la información.

Con la información que se maneja, se plantean nuevas tecnologías que puedan abastecer la demanda de recursos, para poder tener la información

de primera mano y de manera eficaz, por ello con el diseño de una infraestructura con MPLS, usando una VPN se espera cubrir todas las necesidades a nivel de comunicación con la matriz y satisfacer las expectativas de la disponibilidad de acceso a los servidores, para que el enlace de comunicación no se vea colapsado por la cantidad de concurrencias en un día determinado por el aumento de transaccionalidad en las aplicaciones.

1.2. Justificación.

Las compañías que están formalmente desarrolladas tienen la necesidad de estar comunicadas con todos sus colaboradores y clientes para agilizar el trabajo diario, generando que los datos de consulta estén disponibles en todo momento. El tener un esquema de servicios modular y escalable permitirá tener conexiones seguras entre equipos, de donde se podrá acceder a los recursos de los mismos de manera confidencial, así como también mejorar los tiempos de respuesta al reporte de fallos.

El diseño de la red de datos para la compañía, tratará de cumplir cualquier tipo de necesidad a nivel de las comunicaciones, ya que en la actualidad la misma no está cubierta en la infraestructura que posee. También debe tomarse en cuenta la calidad de servicio, por lo que con la metodología planteada se va a poder contar con clases de servicio QoS (Quality of Service) para poder priorizar tráfico, gestionar de manera eficiente el ancho de banda de las conexiones, para complementar las necesidades de cada servicio en particular.

El presente trabajo, expone que para tener un servicio óptimo se debe realizar la inversión de nuevos recursos de hardware los cuales permitirán ayudar a controlar, gestionar y ejecutar de mejor manera la resolución de problemas, así como también a la optimización de recursos físicos y lógicos de la red.

1.3. Definición del Problema.

La compañía Credimatic tiene la necesidad de contar con procedimientos de verificación de seguridad informática para las redes LAN/WAN acorde a los estándares y buenas prácticas que permitan gestionar de manera adecuada los recursos tecnológicos.

1.4. Objetivo General.

Diseñar e implementar procedimientos de verificación de seguridad informática aplicada para las comunicaciones LAN/WAN alineado a las buenas prácticas internacionales para la migración a un Datacenter alterno de Credimatic.

1.4.1. Objetivos específicos.

- Determinar el estado actual del datacenter de la empresa en estudio, a fin de determinar y dimensionar el hardware a utilizar.

- Establecer los equipos y servicios, bajo especificaciones técnicas para la infraestructura de red y servidores del centro de cómputo.

- Diseñar la comunicación unificada de datacenters con la finalidad de activar el ambiente de producción y la continuidad de servicios.

1.5. Hipótesis

Con la implementación de un nuevo datacenter se mejorará sustancialmente los tiempos de respuesta en la atención a incidencias, aislando de manera eficiente los ambientes de producción y desarrollo, logrando una total independencia de tráfico transaccional.

1.6. Técnicas y métodos empleados en la investigación.

- **Método de observación documental y científica:** Se utiliza con el objetivo de recopilar y analizar información a fin de lograr la definición del problema, estudiar las diferentes tecnologías y la diferencia para establecer cuál es el diseño para la disposición de equipos de comunicación por tecnología y poder sustentar el marco teórico.
- **Método analítico:** Se recurre con el fin de evaluar y analizar los elementos de forma separada, para evidenciar las conexiones entre ellos.

Capítulo 2: Topología de una Red

Es la representación gráfica de cómo se encuentran conectados los dispositivos de red, distribuidos de acuerdo a sus características físicas y lógicas (Reyna, 2013).

2.1. Tipos de Topología de Red

- Topología Física: denota la disposición física de los dispositivos conectados.
- Topología Lógica: demuestra el funcionamiento de la red en forma real.

2.2. Diseño de las LAN. Red Jerárquica

La jerarquía de una red LAN, fue diseñada con el fin de que su estructura sea confiable, flexible, escalable y de alta disponibilidad, está compuesta por tres capas bien definidas tal como lo muestra la figura 2.1.

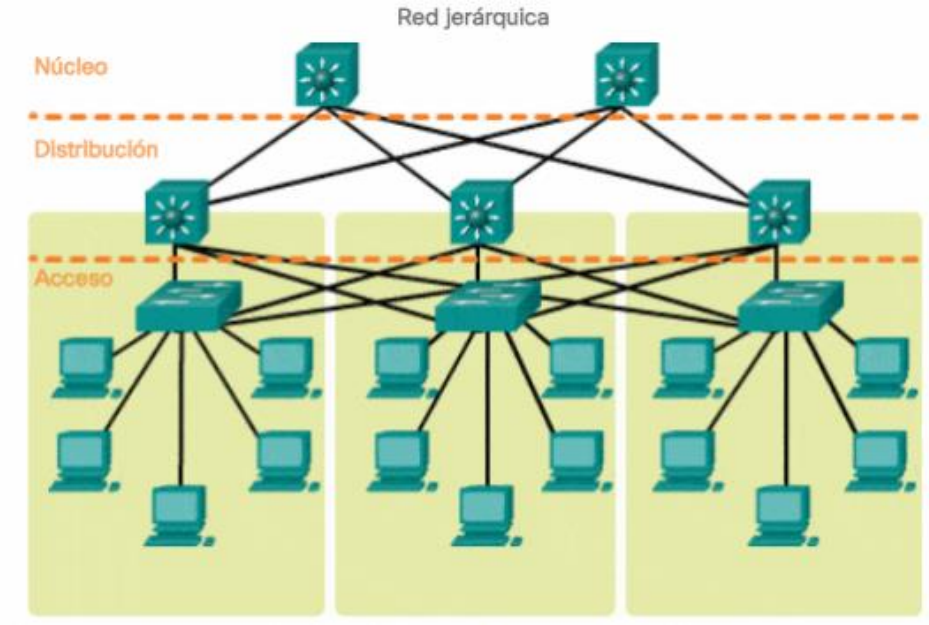


Figura 2: 1: Diseño de red jerárquico
Fuente: (Walton, 2018)

2.2.1. Capa de núcleo

Es la capa fundamental de un sistema de red jerárquico, es la encargada de proporcionar un transporte rápido entre los switches de distribución, capaz de lograr confiabilidad y tolerancia a fallos y de obtener escalabilidad mediante equipos más rápidos (Walton, 2018).

Su única función es conmutar tráfico tan rápido como sea posible y se encarga de trasladar gran cantidad de este de manera confiable y veloz, por lo que es de mucha importancia la **latencia** y la **velocidad**.

2.2.2. Capa de distribución

Es la encargada del enrutamiento de paquetes, establece una comunicación entre las capas de núcleo y de acceso, controlando el tráfico que circula entre ellas, dirige el filtrado entrante y saliente mediante políticas de seguridad configuradas previamente, brindando seguridad a la información dentro de la red (Reyna, 2013), la capa de distribución es el límite entre los dominios del enlace de datos y la red enrutada (Walton, 2018).

2.2.3. Capa de acceso

Provee un punto de acceso o conectividad entre los usuarios y los hosts de la red o dispositivos finales, esta capa se encarga de la conmutación y está directamente conectada con la capa de distribución (Reyna, 2013).

La capa de acceso cumple varias funciones, incluidas las siguientes:

- Switching de capa 2
- Alta disponibilidad
- Seguridad del puerto
- Clasificación y marcación de QoS y límites de confianza
- Inspección del protocolo de resolución de direcciones

- Listas de control de acceso virtual
- Árbol de expansión (Walton, 2018)

2.2.4. Ventajas de un diseño jerárquico

Dentro del diseño jerárquico de red, las capas presentan diferentes funciones y cada una realiza una actividad específica. Al dividir una red en sectores se obtienen varias ventajas tales como:

- Escalabilidad, la cual permite que la red pueda extenderse con mayor facilidad, redundancia en la capa del núcleo y distribución.
- Fácil implementación del diseño.
- Seguridad de configuración de políticas establecidas a nivel de acceso y distribución.
- Estabilidad entre los switch en los diferentes niveles que permiten su administración ordenada.
- Fácil mantenimiento por modularidad.

2.3. EtherChannel o Link aggregation

EtherChannel es una tecnología de Cisco, construida de acuerdo con los estándares IEE 802.3, que puede ser utilizada tanto en puertos de capa 2 y 3 (Barbosa, 2016).

Este protocolo da lugar a la agrupación lógica de algunos enlaces físicos Ethernet, su agrupación es vista como un único enlace y da paso a sumar la velocidad nominal de cada puerto físico Ethernet usado y como resultado obtener un enlace troncal de alta velocidad con un tope máximo de 8 puertos que pueden ser agrupados para formar un EtherChannel.

Al aparentar un solo puerto, el protocolo Spanning-Tree no los bloquea, permitiendo que haya más de un enlace de soporte por si el que está activo falla, puede haber dos, cuatro y hasta ocho puertos activos (Barbosa, 2016).

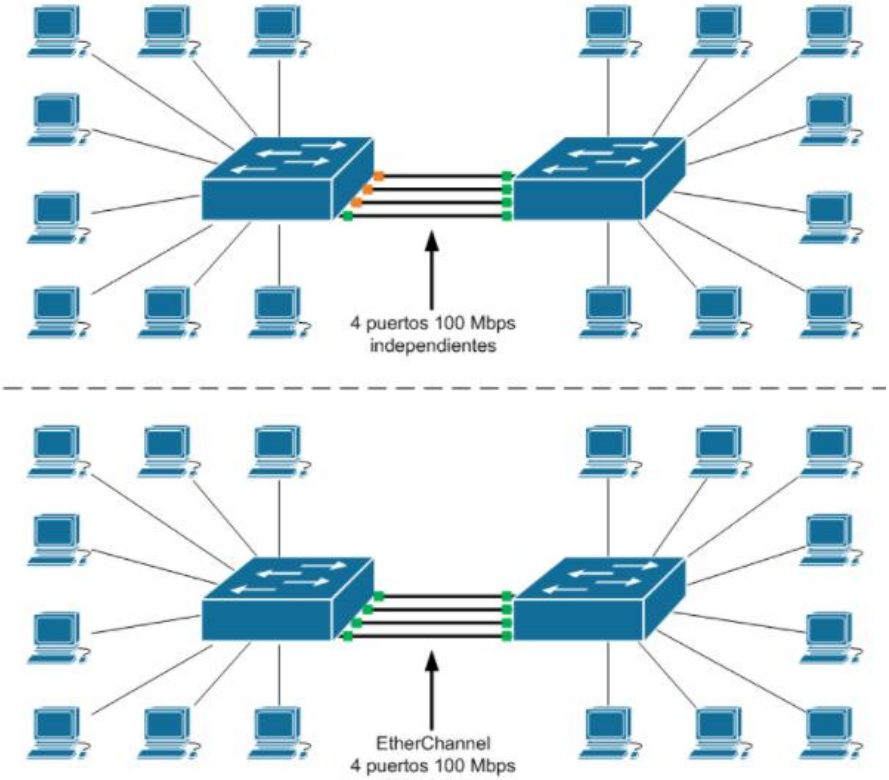


Figura 2: 2: Ethernet Channel
Fuente: (Barbosa, 2016)

2.3.1.1. Ventajas

- Permite el uso de la red en cualquier lugar donde puedan ocurrir cuellos de botella.
- Permite un crecimiento escalable y a medida.
- Es posible agregar el ancho de banda de cualquiera de los enlaces que se tiene en el EtherChannel.
- El incremento de la capacidad no requiere una actualización de hardware.
- Considerando que el enlace está compuesto por varios enlaces Ethernet, se puede hacer reparto de carga entre estos enlaces obteniendo mayor rendimiento y caminos paralelos redundantes.
- Permite robustez y convergencia rápida cuando un enlace falla, la tecnología EtherChannel redirige el tráfico del enlace fallido a los otros

enlaces, proporcionando una recuperación completamente transparente para los usuarios y las aplicaciones de red mediante la redistribución de la carga.

- La tecnología EtherChannel está disponible para todas las velocidades de los enlaces Ethernet.
- Permite a los administradores de red desplegar redes escalables sin problemas.

2.3.1.2. Protocolos

Hay dos protocolos para agrupar puertos:

PAgP (Port Aggregation Protocol): propietario de Cisco Systems. Modos de funcionamiento:

- On: fuerza a los puertos a establecer el canal.
- Off: evita que los puertos establezcan un canal.
- Auto: espera a recibir paquetes para negociar el canal.
- Desirable: establece que el puerto negocie el establecimiento del canal mediante PAgP.

LACP (Link Aggregation Control Protocol)**:** basado en estándares. Modos de funcionamiento:

- On: fuerza los puertos a establecer el canal.
- Off: evita que se establezca el canal.
- Passive: pone el puerto en espera de recibir paquetes LACP para negociar el canal.
- Active: establece que el puerto envíe paquetes para iniciar la negociación del canal.

Es necesario que los dos dispositivos usen el mismo protocolo para que establezcan un EtherChannel (Barbosa, 2016)

2.3.1.3. RSTP (Rapid Spanning Tree Protocol)

Es el protocolo que previene loops en una red de switches. Éste suplanta a su antecesor, el protocolo STP (Spanning Tree Protocol), RSTP trae consigo varias mejoras respecto a este, principalmente en lo que tiene que ver a los tiempos de convergencia.

2.3.1.3.1. Roles de Puertos en RSTP

Los puertos raíz y designados forman parte de la topología activa. Los puertos alternativos y de respaldo no están incluidos en la topología activa.

La siguiente tabla muestra los distintos roles de los puertos en RSTP.

Tabla 2. 1: Roles de Puerto RSTP

Funciones	**Rol del Puerto**
Puerto con la mejor ruta desde el switch que no es raíz al switch raíz	Puerto raíz
Puerto que remplaza al puerto raíz cuando este falla	Puerto alternativo
Puerto designado del switch para reenviar a un dominio de colisión	Puerto designado
Puerto que remplaza al designado cuando el puerto designado falla	Puerto de respaldo
Puerto que está administrativamente deshabilitado	Puerto deshabilitado

Fuente: *(Suárez, 2020)*

2.3.1.3.2. Estados de los Puertos en RSTP

RSTP monitorea el estado de todas las trayectorias:

- Si una dirección activa se cae, RSTP activa las direcciones redundantes.
- Configura de nuevo la topología de la red adecuadamente.

Tabla 2. 2: Estados de Puertos RSTP

Función	**Estado RSTP**
El puerto esta administrativamente deshabilitado	Discarding
Estado estable que ignora las tramas de datos de entrada y no es usado para reenviar tramas de datos.	Discarding
Estado intermedio sin aprendizaje de MAC (Media Access Control) y sin reenvío	Not used
Estado intermedio con aprendizaje de MAC y sin reenvío	Learning
Estado estable que permite el aprendizaje de MAC y el reenvío de tramas de datos	Forwarding

Fuente: *(Suárez, 2020)*

2.3.2. MPLS (Multi-Protocol Label Switching)

Es un estándar IP de conmutación que proporciona varias de las características de las redes orientadas y no orientadas a conexión, la dirección de destino junto a otros parámetros de cabecera son evaluados cada vez que el paquete pasa un router. El camino del paquete se acopla en función del estado de las tablas de enrutamiento de cada dispositivo, como el camino no se predice, difícilmente se puede guardar recursos para que garanticen la calidad del servicio. Adicionalmente, la búsqueda de enrutamiento en las tablas da como resultado que cada nodo pierda cierto tiempo, esto aumenta en función del crecimiento de la tabla.

No obstante, MPLS asigna una etiqueta que se anuncia entre los enrutadores a cada uno de los miembros de la tabla y conectarla con sus nodos vecinos. Esta etiqueta tiene un valor corto y con un tamaño fijo que lo transporta en la cabecera del paquete IP, permitiendo que los enrutadores reenvíen el tráfico mirando en la etiqueta y no la dirección IP de destino.

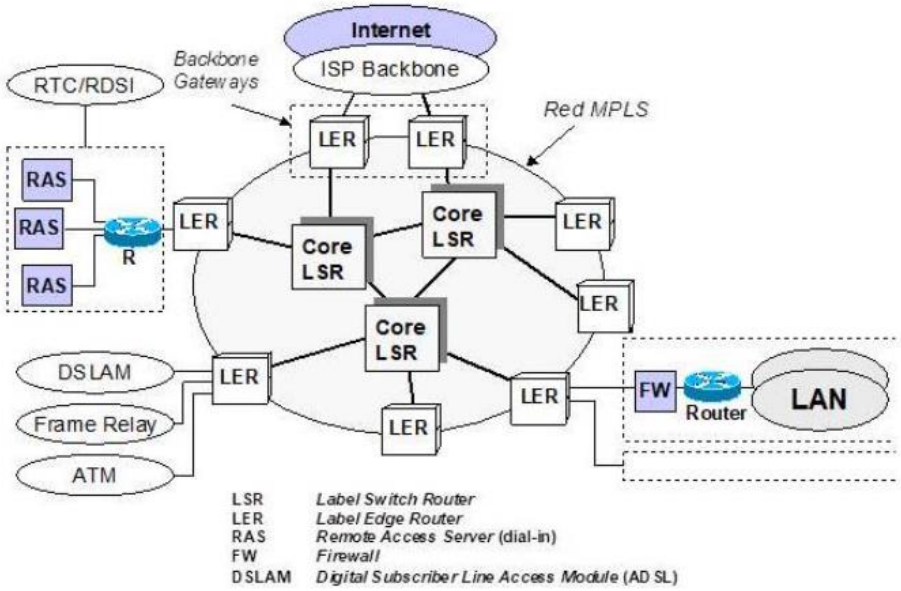


Figura 2: 3: Ejemplo de una red MPLS
Fuente: (Huidobro & Millán, 2002)

2.3.3. Beneficios de MPLS

La migración IP está produciendo cambios en el área de telecomunicaciones, lo cual se traduce en uno de los retos más importantes para los ISP (Internet Service Provider).

MPLS incorpora la conmutación a nivel 2 y 3, por medio de la conmutación por etiquetas, pero actualmente esto no es una ventaja, no es percibida como el principal beneficio, por las características de los gigarouters que realizan las búsquedas de rutas en las tablas a velocidades suficientes. Los beneficios que proporcionan a las redes IP son:

- Realiza ingeniería de tráfico, permite a los ISP mover parte del tráfico de datos, desde el camino más corto hacia otros caminos físicos menos congestionados o menos propensos a fallos.
- Calidad y clases de servicio.
- Crear redes virtuales privadas basadas en IP
- Finalmente, el modelo MPLS simplifica las tareas de monitorización del tráfico, ya que los paquetes pertenecientes a una misma clase de equivalencia FEC (Forward Equivalent Class) son fácilmente identificables gracias a su etiqueta (Tapasco, 2008).

2.4. Virtualización

Crea una representación enfocada en software o virtual, de una entidad física, por ejemplo, aplicaciones, servidores, redes y almacenamientos virtuales. Reduce eficientemente los gastos de TI (Tecnologías de Información) y, a la vez, aumenta la eficiencia y agilidad para empresas de cualquier tamaño.

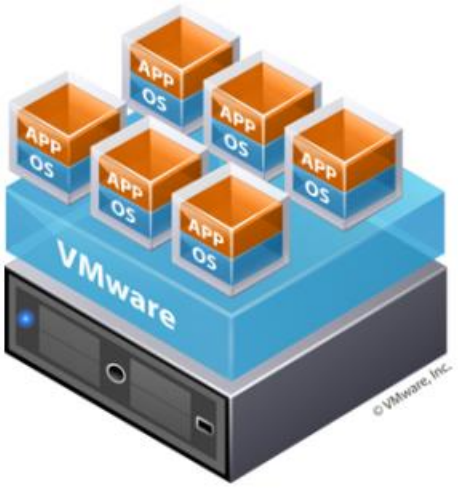


Figura 2: 4: Esquema Virtualización
Fuente: (VMWARE, 2020)

2.4.1. Ventajas de la virtualización

La virtualización puede mejorar la agilidad, flexibilidad y escalabilidad de la infraestructura de TI, a la vez que permite disfrutar de ahorros importantes.

Algunas ventajas de la virtualización son: mayor movilidad de las cargas de trabajo, aumento del rendimiento y disponibilidad de los recursos o la automatización de las operaciones, simplifican la gestión de la infraestructura de TI y permiten reducir los costos de propiedad y operativos. Otras ventajas son (VMWARE, 2020):

- Reducción de la inversión en capital y gastos operativos
- Reducción o eliminación del tiempo de inactividad
- Aumento de la productividad, la eficiencia, la agilidad y la capacidad de respuesta del departamento de TI.
- Distribución más rápida de las aplicaciones y recursos.
- Mejora de la continuidad del negocio y capacidad de recuperación ante desastres.
- Gestión simplificada del centro de datos.
- Disponibilidad de un auténtico centro de datos definido por software.

2.4.2. Principales características de las máquinas virtuales

Las máquinas virtuales tienen las siguientes características, que ofrecen varias ventajas:

2.4.2.1. Creación de particiones

- Ejecuta varios sistemas operativos en una sola máquina física.
- Distribuye los recursos del sistema entre las máquinas virtuales.

2.4.2.2. Aislamiento

- Permite aislar la seguridad y los fallos a nivel de hardware.
- Garantiza el rendimiento gracias a los controles avanzados de recursos.

2.4.2.3. Encapsulación

- Guarda el estado completo de una máquina virtual en archivos.
- Transfiere y copia máquinas virtuales con la misma facilidad que si fueran archivos.

2.4.2.4. Independencia del hardware

- Suministra o migra cualquier máquina virtual a un servidor físico.

2.4.3. Tipos de virtualización

La virtualización es un contenedor de software aislado que incluye un sistema operativo y una aplicación. Cada máquina virtual es autónoma, también es posible ejecutar varios sistemas operativos y aplicaciones en un solo servidor físico.

Para gestionar todas las máquinas virtuales en el mismo host se utiliza una capa ligera de software, llamada «hipervisor», la cual tiene como función desvincular las máquinas virtuales del host y la potestad de asignar recursos informáticos de forma dinámica a cada máquina virtual según las necesidades (VMWARE, 2020)

2.4.3.1. Virtualización de servidores

La virtualización de servidores permite ejecutar múltiples sistemas operativos en un solo servidor físico, por medio de máquinas virtuales que ofrecen un elevado rendimiento. Entre las ventajas principales, se incluyen las siguientes:

- Mayor eficiencia del entorno de TI.
- Reducción de los costos operativos.
- Implementación más rápida de las cargas de trabajo.

- Mejora del rendimiento de las aplicaciones.
- Mayor disponibilidad del servidor.
- Eliminación de la complejidad y la proliferación de servidores (VMWARE, 2020).

2.4.3.2. Virtualización de red

Al reproducir una red física en su totalidad, su virtualización permite ejecutar las aplicaciones en una red virtual del mismo modo que en una física, pero con mayores ventajas operativas y toda la independencia del hardware que ofrece la virtualización.

La virtualización de red muestra los dispositivos y servicios lógicos (puertos, conmutadores, enrutadores, cortafuegos, equilibradores de carga, VPN, etc.) a las cargas de trabajo vinculadas (VMWARE, 2020).

2.4.3.3. Virtualización de escritorios

Implementar los escritorios como un servicio gestionado permite a las organizaciones de TI responder más rápido a las necesidades cambiantes del entorno de trabajo y a las nuevas oportunidades. Los escritorios y las aplicaciones virtuales levantadas también pueden distribuirse de forma rápida y sencilla a sucursales, empleados subcontratados o en otros países y trabajadores móviles que utilizan tabletas iPad y Android.

2.5. Firewall

Cuando se habla de firewall en seguridad informática, se trata de un sistema basado en un software o hardware, el cual funciona como entrada de seguridad entre redes internas y externas de confianza e inseguras**.** Esto se lleva a cabo por medio del filtrado de contenido y basado en algoritmos de revisión, controla la comunicación que se considere dañina o potencialmente no deseada.

Los firewalls de red operan con un hardware que cumple con la protección de acceso de las redes externas hacia las internas, se puede escalar fácilmente para adaptarse a empresas de cualquier tamaño.

Figura 2: 5: Protección Firewall
Fuente: *(ESET, 2020)*

Los firewalls basados en host operan directamente en el dispositivo del usuario (o endpoint), otorga varias posibilidades de filtrado que pueden ser personalizadas por el administrador de redes y seguridades

Muchos de los sistemas operativos facilitan su propio firewall para host. A pesar de eso tienden a mostrar funcionalidades básicas y, por lo general, han sido investigados exhaustivamente por los posibles atacantes (ESET, 2020).

2.5.1. Funciones de un Firewall

- Crear una barrera que permita o bloquee intentos para acceder a la información en su equipo.
- Evitar que usuarios no autorizados accedan a los equipos y redes de la organización que se conectan a Internet.

- Supervisar la comunicación entre equipos y otros de Internet.
- Visualizar y bloquear aplicaciones que puedan generar riesgo
- Advertir de intentos de conexión desde otros equipos.
- Advertir de intentos de conexión mediante las aplicaciones en su equipo que se conectan a otros equipos.
- Detectar aplicaciones y actualizar rutas para añadir futuras fuentes de información
- Hacer frente a los cambios en las amenazas para la seguridad (ID Group, 2020)

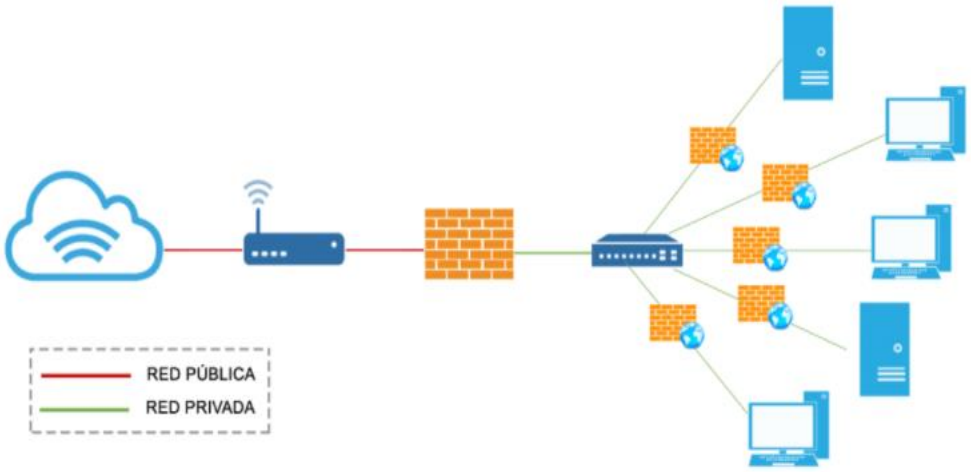


Figura 2: 6: Función de Firewall
Fuente: *(ID Group, 2020)*

Los firewalls de tercera generación fueron creados con la finalidad de filtrar la información en las capas del modelo OSI (Open Systems Interconnection), incluida la de aplicación, lo que les permite reconocer y comprender las aplicaciones, así como algunos de los protocolos más utilizados, como el de transferencia de archivos (FTP, File Transfer Protocol) y el de transferencia de hipertexto (HTTP, Hypertext Transfer Protocol). Basándose en esta información, el firewall puede detectar ataques que intentan eludirlo a través de un puerto permitido o el uso incorrecto de un protocolo.

Combinan todos los enfoques utilizados anteriormente con una inspección más profunda del contenido filtrado, comparándolo con una base de datos de detección para identificar el tráfico potencialmente dañino.

Estos firewalls vienen con sistemas de seguridad adicionales incorporados, tales como redes privadas virtuales (VPN), sistemas de prevención y detección de intrusos (IPS/IDS, Intrusion Prevention System/Intrusion Detection Systems), administración de identidades, control de aplicaciones y filtrado web (ESET, 2020).

2.5.2. Beneficios que ofrece un firewall

El principal beneficio para los usuarios es un mayor nivel de seguridad, por ende cuando se implementa un firewall se amplía el perímetro de seguridad y se obtiene mayor protección para la red corporativa frente al tráfico malicioso. Reduce el riesgo de que los dispositivos detrás del firewall se conviertan en parte de una red de bots: un gran grupo de dispositivos conectados a Internet esclavizados por los atacantes con malos propósitos.

2.5.3. NAT (Network Address Traslator)

Es el proceso fundamental entre los dispositivos e Internet, forma parte del router, módem o equipo que se utiliza para conectarse a la red. Es conocido también como enmascaramiento de direcciones IP. Cada uno de los dispositivos que hay conectados en la red tienen una dirección IP única. En este grupo se puede mencionar ordenadores, móviles o cualquier otro equipo, esto es necesario para que esté conectado a Internet y el router lo detecte y pueda funcionar con normalidad. El traductor de direcciones de red lo que hace (ya sea en el router, módem o dispositivo que sea) es proporcionar una dirección IP pública a toda esa red, a todo el conjunto de equipos (Jiménez, 2020).

La idea es sencilla, hacer que redes de ordenadores utilicen un rango de direcciones especiales (IPs privadas) y se conecten a Internet usando

una única dirección (IP pública). Gracias a este proceso, las grandes empresas sólo utilizarían una dirección IP y no tantas como máquinas hubiese en dicha empresa. También se utiliza para conectar redes domésticas a Internet (Alcoba, 2011).

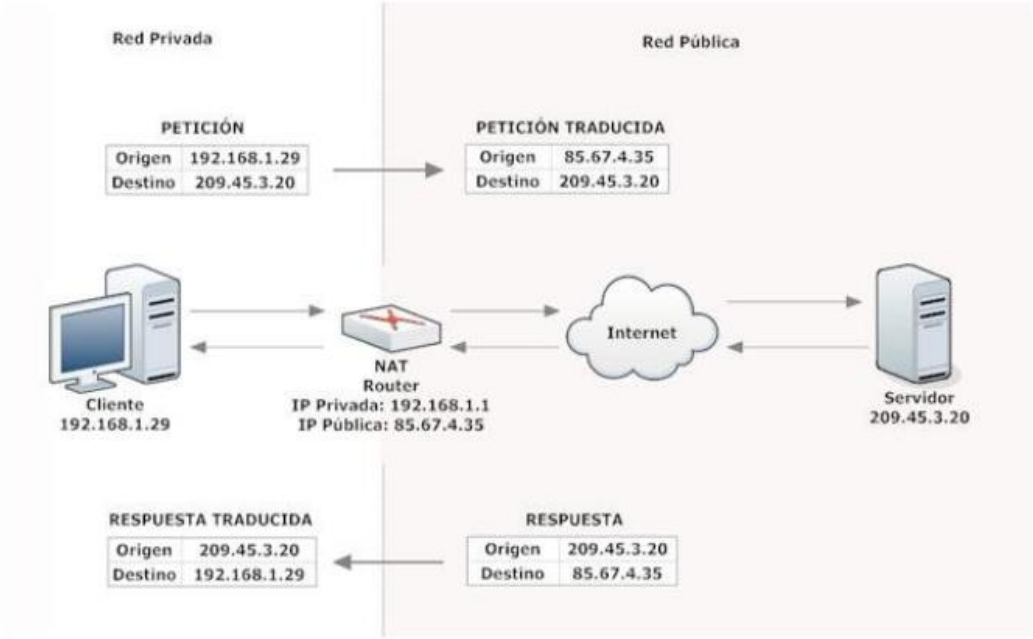


Figura 2: 7 : Nateo de redes internas
Fuente: *(Alcoba, 2011)*

Hay que tener en cuenta que NAT actúa únicamente sobre direcciones IPv4. A pesar de que existe también la opción de IPv6, más adaptados y con mejores características, en este caso no se necesitaría traducir las direcciones de red.

2.5.3.1. Funcionamiento

En NAT existen varios tipos de funcionamientos, los cuales se detallan a continuación:

Estática

Una dirección IP privada se traduce siempre en una misma dirección IP pública. Este modo de funcionamiento permitiría a un host dentro de la red ser visible desde Internet (Ver figura 2.7).

Dinámica

El router tiene asignadas varias direcciones IP públicas, de modo que cada IP privada se contrasta usando una de las públicas que el router tiene asignadas, de modo que a cada IP privada le corresponde al menos una pública. Cada vez que un host requiera una conexión a Internet, el router le asignará una dirección IP pública que no esté siendo utilizada. Así se aumenta la seguridad ya que dificulta que un host externo ingrese a la red, ya que las direcciones IP públicas van cambiando (Alcoba, 2011).

Sobrecarga

La NAT con sobrecarga o PAT (Port Address Translation) es la más común de todos los tipos, ya que es utilizada en los hogares. Se pueden mapear múltiples direcciones IP privadas a través de una pública, con lo que se evita contratar más de una IP pública. Además del ahorro económico, también se economizan direcciones IPv4, ya que aunque la subred tenga muchas máquinas, todas salen a Internet a través de una misma dirección IP pública (Alcoba, 2011).

Solapamiento

Cuando una dirección IP privada de una red es una pública en uso, el router se encarga de reemplazarla por otra para evitar el conflicto de direcciones (Alcoba, 2011).

2.5.3.2. Ventajas de la NAT

- Gran ahorro de direcciones IPv4 que supone, se puede conectar múltiples máquinas de una red a Internet usando una única dirección IP pública.
- Brinda seguridad ya que los dispositivos conectados a la red mediante NAT no son visibles desde el exterior, por lo tanto un atacante externo no podría tener la visibilidad que una máquina está conectada o no a la red.

- Mantenimiento de la red, sólo sería necesario modificar la tabla de reenvío de un router para desviar todo el tráfico hacia otra máquina, mientras se llevan a cabo tareas de mantenimiento (Alcoba, 2011).

2.5.3.3. Desventajas de la NAT

- Checksums TCP (Transmission Control Protocol) y UDP (User Datagram Protocol): El router tiene que volver a calcular el checksum de cada paquete que modifica. Por lo que se necesita mayor potencia de computación.
- No todas las aplicaciones y protocolos son compatibles con NAT. Algunos introducen el puerto de origen dentro de la zona de datos de un paquete, por lo que el router no lo modifica y la aplicación no funciona correctamente (Alcoba, 2011).

2.5.4. Alta Disponibilidad

Es la facultad de garantizar la continuidad de la operatividad en cuanto a los servicios, incluso en situaciones de deficiencias (hardware, software, corte de energía, etc.). Aplicado a la implementación de un firewall, este concepto indica que si ocurre un desperfecto (por ejemplo, su hardware sufre pérdida de funciones debido a un corte de energía o un error en las interfaces físicas), habrá un sistema con similares características, configuraciones que estará disponible en modo backup, listo para controlar el tráfico filtrado dentro del perímetro de la compañía.

Existen dos maneras posibles de activar HA (High Aviality), Activo-Activo y Activo-Pasivo. En el caso de Activo-Activo el firewall, los dispositivos trabajan activamente dando seguimiento la red, mientras que la opción de Activo – Pasivo el nodo secundario está en espera, y solo funcionará si el primer nodo presenta alguna anomalía para trabajar.

Sin embargo, en Activo-Activo, las conexiones y las sesiones de autenticación se replican entre las instancias de los dispositivos, mientras

que en Activo-Pasivo, el usuario debe rehabilitar todas las conexiones (Blockbit, 2019).En cualquier caso, la opción de conmutación por error es vital para conservar la seguridad del entorno, pues protege a los usuarios, dispositivos y datos.

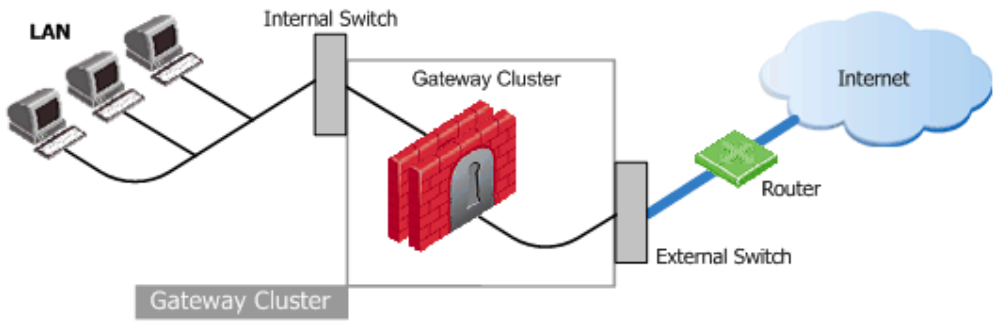


Figura 2: 8: Cluster de Firewall
Fuente: *(Check Point Software Technologies Ltd., 2013)*

Capítulo 3: Diseño y Análisis de la Propuesta

En esta última década la tecnología Ethernet ha crecido velozmente, lo que se traduce con la demanda de enlaces muchos más rápidos con características sobresalientes sobre la transmisión de datos. Esta evolución ha provocado que sea dominante en las redes de área local y de área amplia, que da como resultado afianzamiento con bases sólidas en el ámbito empresarial con aproximadamente 95% del tráfico en todas las empresas. Ethernet no fue diseñada pensando en la calidad de los servicios, es aquí donde se plantea las mejoras que se pueden implementar para robustecer y sacar el mejor provecho a las comunicaciones que maneja la compañía. En el presente capítulo se trata del diseño e implementación de buenas prácticas y procedimientos de verificación de seguridad informática aplicada al sistema LAN/WAN para la migración a datacenter alterno de Credimatic, estableciendo aspectos técnicos tales como el tráfico de datos entre la oficina matriz y el centro de datos, configuraciones generales así como equipos mínimos necesarios para cumplir con una implementación de esta magnitud.

3.1. Situación actual en la compañía

La compañía presenta el estado actual que está resumido en los puntos que se detallan a continuación:

Infraestructura segmentada por VLAN (Virtual Local Area Network): Se disminuye el alcance PCI (Payment Card Industry) por medio de segmentos de red, cada segmento de red tiene una VLAN asignada.

Topología Estrella: Los firewalls tanto internos como externos concentran todas las redes.

Ineficiente uso de puertos: Los switches de centro de cómputo proporcionan una capacidad de 864 puertos para conexión de equipos de

red. Sólo se usan 267. El porcentaje de utilización es del 31%, Esto ocurre porque los switches no “conocen” todas las VLANs.

Escalabilidad: La cantidad de redes que pueden ser protegidas se ven limitadas por el número de interfaces que soporta cada servidor firewall. Los firewalls principales de la compañía se encuentran en la ciudad de Guayaquil, cada uno de ellos cuenta con 20 interfaces de red disponibles con tasas de transferencia de hasta 1Gbps en cobre. Cada nodo del clúster de firewalls externos utiliza 13 de sus 20 interfaces, mientras que en el clúster de firewalls internos se consumen 11 de 20 interfaces por nodo.

Administración: Al existir mayor cantidad de conexiones físicas, la administración de la infraestructura de red se vuelve compleja. Esto incrementa el tiempo de resolución de problemas y ralentiza el proceso de implementación de cambios.

Costos: El diseño actual requiere que se implemente mayor cantidad de dispositivos de red debido a que los switches no concentran todas las VLANs de la compañía, por tal motivo los costos de mantenimiento se multiplican.

A continuación, se presenta:

Figura 3. 1: Segmentación de redes Guayaquil

Figura 3. 2: Segmentación de redes Quito

Tabla 3. 1: Redes y VLANs actuales

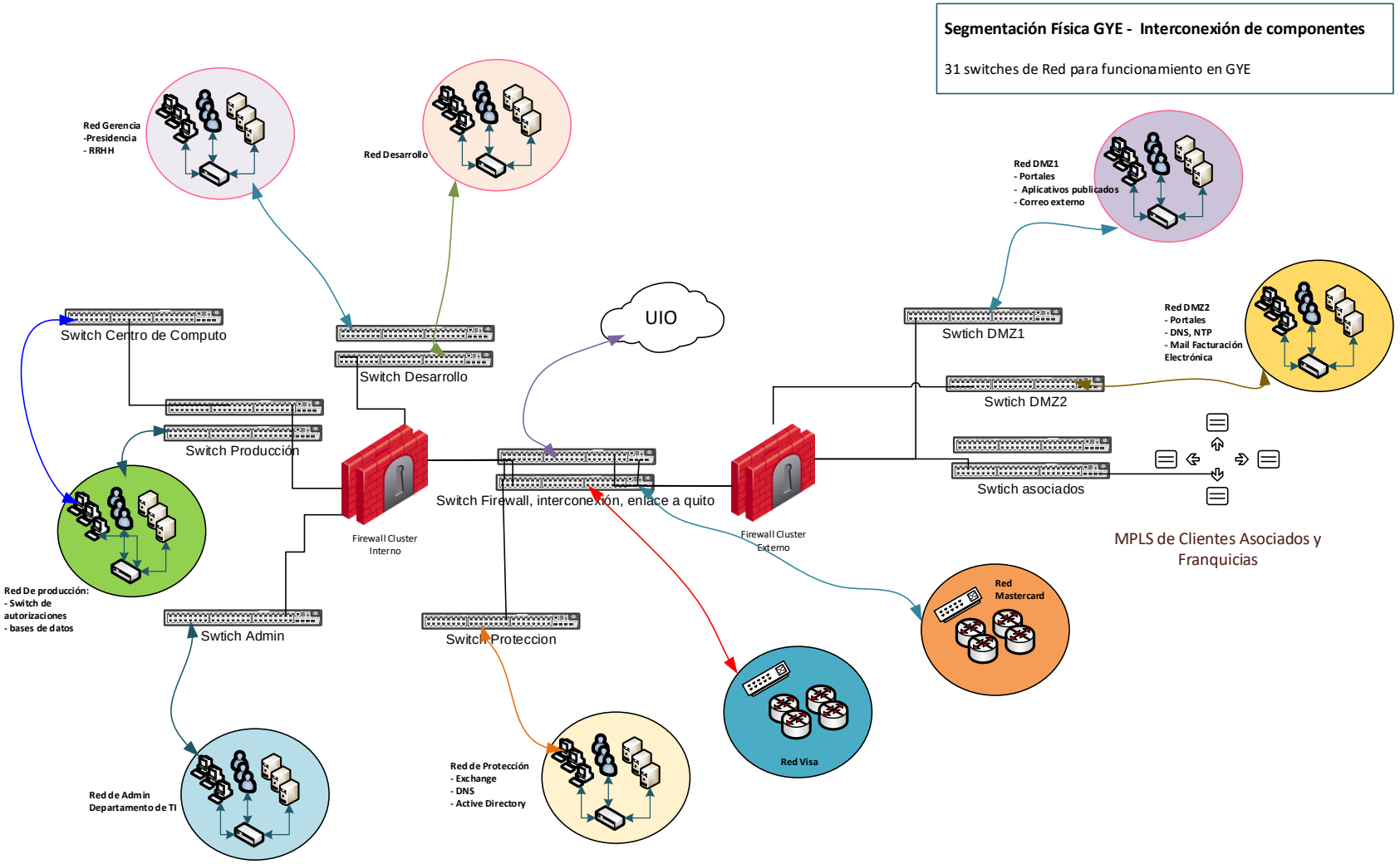


Figura 3. 1: Segmentación de redes Guayaquil
Fuente: Autor

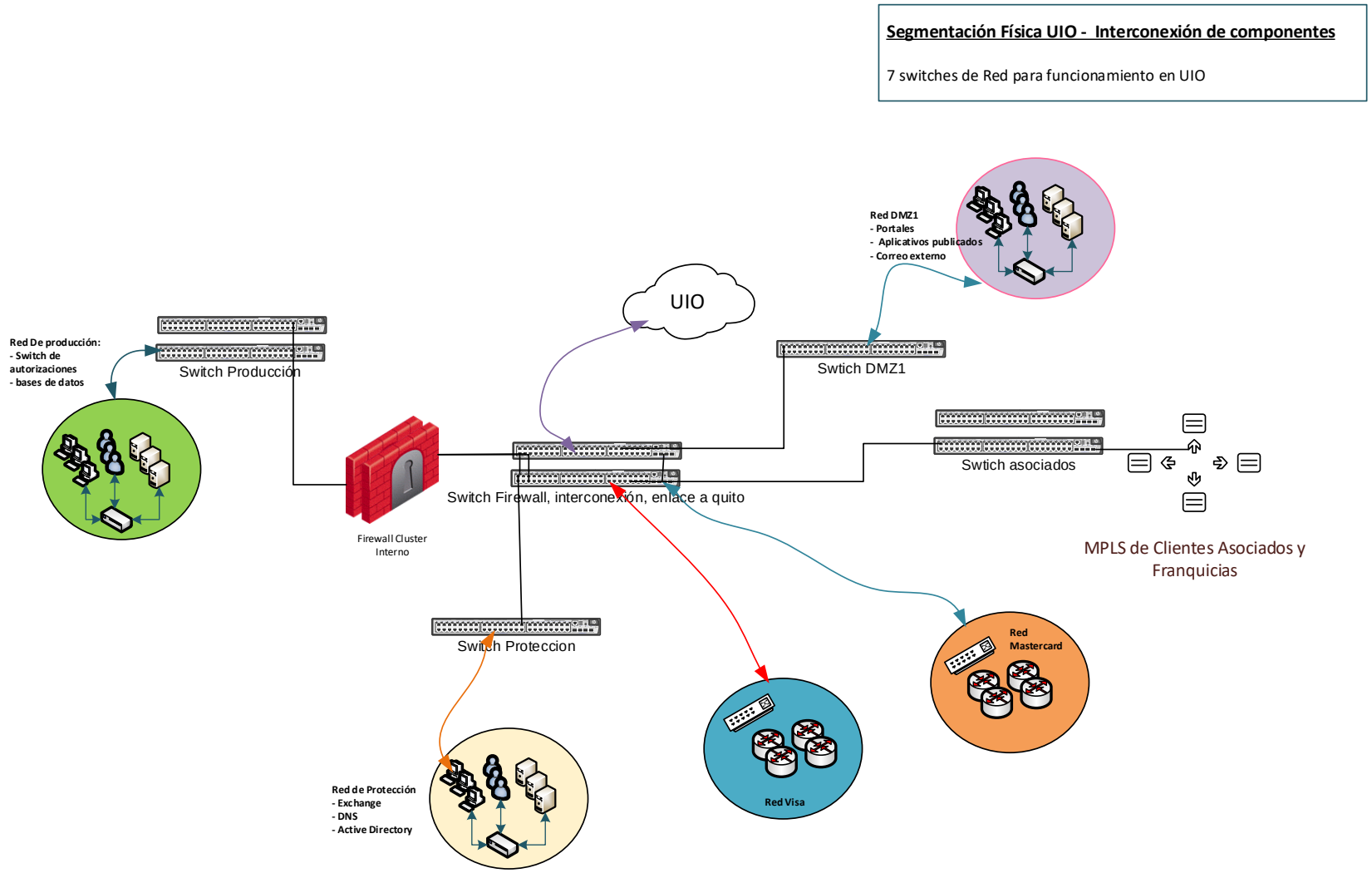


Figura 3. 2: Segmentación de redes Quito
Fuente: Autor

Redes actuales Oficina

Tabla 3. 1: Redes y VLANs Actuales

DESCRIPCION	VLAN	NOMBRE	RED	MASCARA	GATEWAY
OFIC-ACTUAL-GYE FIREWALL INTERNO	118	PRODUCCION	182.27.118.0	24	182.27.118.76
	117	PROTECCION	182.27.117.0	24	182.27.117.1
	88	FW_INTERNO_UIO	20.221.88.0	24	20.221.88.24
	116	HEARTBEAT_SYBASE	182.27.116.0	24	182.27.116.14
	24	INTERCONEXION_DESARROLLO	182.27.160.0	24	182.27.160.24
	131	USUARIOS_AVANZADOS	182.27.131.0	24	182.27.131.1
	85	CONEXION_FW_EXTERNO	20.221.85.0	24	20.221.85.12
	114	SENTINEL	182.27.114.0	24	182.27.114.14
	157	AUTORIZACIONES	182.27.157.0	24	182.27.157.1
	110	HEARTBEAT_SQL	182.27.110.0	25	182.27.110.1
	113	PREPRODUCCION	182.27.113.0	24	182.27.113.1
	155	GERENCIA_TMP	182.27.155.0	24	182.27.155.1
DESCRIPCION	VLAN	NOMBRE	RED	MASCARA	GATEWAY
OFIC-ACTUAL-GYE FIREWALL EXTERNO	150	DMZ1	20.221.150.0	24	20.221.150.14
	86	FW_EXTERNO	20.221.86.0	24	20.221.86.22
	89	VISA	20.221.89.0	24	20.221.89.14
	90	MASTERCARD	20.221.90.0	24	20.221.90.14
	11	INTERNET CENTURY LINK	200.51.10.0	28	200.51.10.194
	100	ASOCIADOS	20.221.100.0	24	20.221.100.25
	121	SFTP_MNET	20.221.121.0	24	20.221.121.15
	15	PAYPHONE_PRD	190.226.103.144	29	190.226.103.150
	17	PAYPHONE_DESA	190.226.103.136	29	190.226.103.140
	29	WIPS	182.27.121.0	24	182.27.121.3

	151	DMZ2	20.221.151.0	24	20.221.151.15
	152	DMZ_DESARROLLO	20.221.152.0	24	20.221.152.14
OFIC-ACTUAL-GYE DESARROLLO	119	PROTECCION_ANTIGUA	182.27.119.0	24	182.27.119.1
	125	DESARROLLO	182.27.125.0	24	182.27.125.1
	22	GERENCIA	182.27.150.0	24	182.27.150.1
	23	AVANZADOS_ANTIGUA	182.27.130.0	24	182.27.130.1
	24	INTERCONEXION_FW_INTERNO	182.27.160.0	24	182.27.160.1
OFIC-ACTUAL-UIO	233	AUTORIZACIONES_UIO	182.27.233.0	24	182.27.233.1
	234	ADMINISTRACION_UIO	182.27.234.0	24	182.27.234.1
DC-UIO-IÑQ	6	MASTERCARD_UIO	30.221.90.0	24	30.221.90.1
	210	CONEXION_QUITO_GUAYAQUIL	30.221.85.0	24	30.221.85.1
	211	ASOCIADOS_UIO	20.221.211.0	24	20.221.211.1
	213	VISA_UIO	30.221.89.0	24	30.221.89.1
	230	PRODUCCION_UIO	182.27.230.0	24	182.27.230.1
	231	PROTECCION_UIO	182.27.231.0	24	182.27.231.1
	232	DMZ_UIO	182.27.232.0	24	182.27.232.1

Fuente: Autor

3.2. Equipos a utilizar en la implementación

La implementación de esta solución va a depender mucho de la necesidad del cliente, situación económica o infraestructura propia de la empresa, para este caso se menciona los más destacados que se pueden aplicar en una estructura como la que se plantea en el proyecto actual, los mismos se destacarán a nivel de capa 2 y 3.

Para la distribución del tráfico, se ha dimensionado de tal manera para unificar redes ya que actualmente están separados los ambientes, si bien es cierto pero el sitio de contingencia que se encuentra en Quito maneja otro direccionamiento distinto al de producción y esto hace de que las pruebas de contingencia sea largas y no convergen de manera automática, por tal motivo se plantea un clúster geográfico dividiendo los ambientes de producción, contingencia y continuidad, se ha distribuido de la siguiente manera:

DC Telconet:

- Rack Wan: a este rack van a llegar todas las conexiones externas que interactúan con la compañía, es decir los proveedores de internet, los routers de clientes y franquicias.
- Rack de Core: en esta ubicación se tendrán los equipos que manejarán el tráfico interno de la compañía que tienen vinculación con el ambiente de producción, protección, DMZ (DeMilitarized Zone).
- Rack distribución: direcciona el tráfico para las diferentes VLANs de interés

DC Century Link:

- Rack Wan: se aplica el mismo concepto que en el datacenter de Telconet pero con la particularidad de que este ambiente es de contingencia

- Rack de Core: lleva relación con el core principal a diferencia que estos equipos son de contingencia

Oficina Matriz:

- Rack Wan
- Rack Core y Distribución

Switch de Red Core Guayaquil. – Se debe considerar la renovación de los equipos CORE de la red en la compañía. En el rediseño de la red se ha considerado una optimización en los equipos a considerar, reduciendo la cantidad de dispositivos y puertos de red, mejorando las velocidades y optimizando el cableado de datos y la complejidad de administración. Para cumplir estas iniciativas se requieren 2 equipos Switch de red (primario y secundario) con las siguientes características y funcionalidades para la ciudad de Guayaquil:

Tipo Configuración Cantidad Apilable Tecnología Non-Blocking Puertos 10G BASE-T Puertos 10G BASE-SR Puertos 40G, BASE-SR Puertos 1000 BASE-T, Fuente, ventiladores Redundante Soporte y garantía, Modular.

Estos equipos serán colocados en el denominado Rack 3. Deberán poseer una configuración de tipo stack por lo que deben incluirse todos los módulos y/o elementos necesarios. A su vez, deberán contemplarse todos los componentes redundantes para garantizar el continuo funcionamiento del equipo, es decir, fuentes de poder, ventiladores, supervisoras, etc.

Cada switch core debe poseer al menos dos slots libres que permitan el crecimiento futuro de conexiones 10GB (Base-SR) o 40GB (Base-SR).

Switch de Red ToR LAN Guayaquil. – En el rediseño de la red se ha considerado colocar 2 switch en stack por cada rack de servidores, se necesitan estos equipos ToR para dos racks, por lo que se requieren 4

switches de red con las siguientes características para la ciudad de Guayaquil:

Tipo Configuración Cantidad Apilable Tecnología Non-BlockingPuertos 10G BASE-T Puertos 10G BASE-SR,Fuente Redundante.

Cada pareja de equipos switch stack serán colocados en los racks 1 y otra pareja en el rack 2. Deberán poseer una configuración de tipo stack por lo que deben incluirse todos los módulos y/o elementos necesarios. A su vez, deberán contemplarse todos los componentes redundantes para garantizar el continuo funcionamiento del equipo, es decir, fuentes de poder, ventiladores, etc.

Switch de Red ToR WAN Guayaquil. – Para habilitar la conectividad WAN de los equipos alojados en el Datacenter Guayaquil, se requieren 2 switch de red para el rack de comunicaciones WAN con las siguientes características:

Tipo Configuración Cantidad Apilable Tecnología Non-Blocking Puertos 10G BASE-T Puertos 10G BASE-SR, Fuente Redundante.

Estos equipos serán colocados en el rack 4. Deberán poseer una configuración de tipo stack por lo que deben incluirse todos los módulos y/o elementos necesarios. A su vez, deberán contemplarse todos los componentes redundantes para garantizar el continuo funcionamiento del equipo, es decir, fuentes de poder, ventiladores, etc.

Switch de Red Core Quito. – Para el Datacenter de la ciudad de Quito, se requieren 2 switch CORE de red, estos equipos serán configurados en stack y permitirán conectar y concentrar las redes del datacenter en la ciudad de Quito, se requieren 2 equipos con las siguientes características:

Tipo Configuración Cantidad Apilable Tecnología Non-Blocking, Puertos 10G BASE-T Puertos 10G BASE-SR, Fuente Redundante.

Estos equipos son colocados en el rack 2 del datacenter Quito. Deberán poseer una configuración de tipo stack por lo que deben incluirse todos los módulos y/o elementos necesarios. A su vez, deberán contemplarse todos los componentes redundantes para garantizar el continuo funcionamiento del equipo, es decir, fuentes de poder, ventiladores, etc.

Switch de Red ToR WAN Quito. - Se requiere 1 switch de red para las conexiones WAN en el Datacenter de la ciudad de Quito, el equipo debe tener las siguientes características:

Tipo Configuración Cantidad Apilable Tecnología Non-Blocking, Puertos 10G BASE-T, Puertos 10G BASE-SR, Puertos 1000 BASE-T, Fuente Redundante.

Este equipo será colocado en el rack 4 del Datacenter Quito. Deberán contemplarse todos los componentes redundantes para garantizar el continuo funcionamiento del equipo, es decir, fuentes de poder, ventiladores, etc.

Switch de Red ToR Oficina Guayaquil. – Para las redes de la oficina Guayaquil se ha considerado implementar equipos de red que permitan integrar a esta oficina con los Datacenter de Guayaquil y Quito. Para esta parte se ha considerado colocar 2 switches principales y 2 switches de distribución con las siguientes características para la ciudad de Guayaquil:

Tipo Configuración Cantidad Apilable Tecnología Non-Blocking, Puertos 10G BASE-T, Puertos 10G BASE-SR Puertos 1000, BASE-T, Fuente Redundante.

Deberán poseer una configuración de tipo stack por lo que deben incluirse todos los módulos y/o elementos necesarios. A su vez, deberán

contemplarse todos los componentes redundantes para garantizar el continuo funcionamiento del equipo, es decir, fuentes de poder, ventiladores, etc.

3.3. Listado de Equipos Instalados

A continuación, se detalla el listado de equipos Instalados en Credimatic, en las localidades de DC-GYE y DC-UIO, que componen la infraestructura de red implementada y su distribución:

Tabla 3. 2: Listado de equipos a Instalar

LOCALIDAD	NOMBRE	FABRICANTE	NUMERO PARTE	MODELO	NUMERO SERIE
DC-GYE	SWC1DCGR7	HPE	JH398A	HPE FF 5940 4-slot Switch	CN94HLM0CW
	SWC2DCGR7	HPE	JH398A	HPE FF 5940 4-slot Switch	CN94HLM0DN
	SWT1DCGR5	HPE	JG898A	HPE 5700 32XGT 8XG 2QSFP+ Swch	CN94GN502M
	SWT2DCGR5	HPE	JG898A	HPE 5700 32XGT 8XG 2QSFP+ Swch	CN94GN500H
	SWT1DCGR6	HPE	JG898A	HPE 5700 32XGT 8XG 2QSFP+ Swch	CN94GN501N
	SWT2DCGR6	HPE	JG898A	HPE 5700 32XGT 8XG 2QSFP+ Swch	CN94GN506X
	SWW1DCGR8	HPE	JG934A	HPE 5130 48G 4SFP+ EI Switch	CN89GPX0KZ
	SWW2DCGR8	HPE	JG934A	HPE 5130 48G 4SFP+ EI Switch	CN89GPX0H2
DC-UIO	SWC1DCQR2	HPE	JH397A	HPE FF 5940 2-slot Switch	CN94HLL00P
	SWC2DCQR2	HPE	JH397A	HPE FF 5940 2-slot Switch	CN95HLL00D
	SWW1DCQR3	HPE	JG934A	HPE 5130 48G 4SFP+ EI Switch	CN89GPX0GF
	SWW2DCQR3	HPE	JG934A	HPE 5130 48G 4SFP+ EI Switch	CN89GPX0KT

Fuente: Autor

3.4. Implementación Diseño Lógico

A continuación, se detallan las fases que se sugiere implementar:

- Fase 1. Integración de localidad OFIC-ACTUAL con DC-GYE
- Fase 2. Integración de localidad DC-GYE con DC-UIO

3.4.1. Fase 1

Esta fase comprende la integración del centro de datos OFIC-ACTUAL-GYE con el centro de datos denominado DC-GYE localizado en las instalaciones de Telconet a través de enlaces extendidos de capa 2 entre ambas localidades por los carriers Telconet y Century-Link en modalidad activo-activo.

3.4.1.1. Descripción de Implementación Fase 1

a) En el centro de datos DC-GYE, en el rack 7 se encuentra el switch Core, modelo HPE 5940 4-slot llamado SWCSDCGR7, compuesto de dos miembros en modalidad de stack con anillo mediante un enlace virtual IRF (Intelligent Resilient Framework) entre ambos miembros, compuesto por dos conexiones físicas de 40 Gbps con cables DAC QSFP+ de 3 metros cada uno, agregando un total de 80 Gbps.

b) En el rack 5 se encuentra el switch ToR, modelo HPE 5700 32XGT 8XG 2QSFP+ llamado SWTSDCGR5, compuesto de dos miembros en modalidad de stack con anillo mediante un enlace virtual IRF entre ambos miembros, compuesto por cuatro conexiones físicas de 10 Gbps con cables DAC SFP+ de 1.2 metros cada uno, agregando un total de 40 Gbps.

c) En el rack 6 se encuentra el switch ToR, modelo HPE 5700 32XGT 8XG 2QSFP+ llamado SWTSDCGR6, compuesto de dos miembros en modalidad de stack con anillo, mediante un enlace virtual IRF entre ambos miembros compuesto por cuatro conexiones físicas de 10 Gbps con cables DAC SFP+ de 1.2 metros cada uno, agregando un total de 40 Gbps.

d) En el rack 8 se encuentra el switch ToR, modelo HPE 5130 48G 4SFP+ llamado SWWDCGR8, compuesto de dos miembros en modalidad de stack con anillo mediante un enlace virtual IRF entre ambos miembros,

compuesto por dos conexiones físicas de 10 Gpbs con cables de fibra óptica cada uno, agregando un total de 20 Gbps.

e) El switch ToR SWTSDCGR5 dispone de 4 puertos QSFP+ y esta conectado al switch core SWCSDCGR7 mediante un enlace agregado compuesto por dos conexiones físicas de 40 Gbps con cables DAC QSFP+ de 5 metros cada uno, agregando un total de 80 Gbps. Los dos puertos QSFP+ restantes son utilizados para conectar el equipo HPE Synergy de producción.

f) El switch ToR SWTSDCGR6 dispone de 4 puertos QSFP+ y esta conectado al switch core SWCSDCGR7 mediante un enlace agregado compuesto por dos conexiones físicas de 40 Gbps con cables DAC QSFP+ de 5 metros cada uno, agregando un total de 80 Gbps. Los dos puertos QSFP+ restantes son utilizados para conectar el equipo HPE Synergy de contingencia local.

g) El switch ToR SWWDCGR8 está conectado al switch core SWCSDCGR7 mediante un enlace agregado entre ambos, compuesto por dos conexiones físicas de 10 Gbps con cables de fibra óptica de 5 metros cada uno, agregando un total de 20 Gbps.

h) El switch core SWCSDCGR7 de DC-GYE está conectado al switch core SWPRDP3R1U03 de OFIC-ACTUAL-GYE. La conexión entre ambos switches se realiza mediante un enlace agregado de capa 2 extendido en modo activo – activo, conformado por los carriers Telconet y Century-Link cada uno aportando con un ancho de banda de 1.9 Gbps. Este enlace se realiza mediante la agregación de dos conexiones físicas de 1 Gbps y dos conexiones físicas de 900 Mbps con cables UTP CAT-6A que llegan a cada uno de los switches mencionados. Este enlace agregado está funcionando con el protocolo LACP en modo activo.

i) Por el enlace agregado activo de capa 2 entre ambas localidades, DC-GYE y OFIC-ACTUAL-GYE, que opera en modo troncal, atraviesan las VLANs.

Tabla 3. 3: VLANs Extendidas

DESCRIPCION	VLAN	NOMBRE	RED	MASCARA	GATEWAY
DC-GYE / DC-UIO (VLAN EXTENDIDAS)	4	PRODUCCION	182.27.118.0	24	182.27.118.76
	6	DMZ1	20.221.150.0	24	20.221.150.14
	7	PROTECCION	182.27.117.0	24	182.27.117.1
	110	HEARTBEAT_SQL	182.27.110.0	25	N/A
	151	DMZ2	20.221.151.0	24	20.221.151.15
	200	MGMT_DC	182.20.1.0	24	182.20.1.1

: Fuente: Autor

j) En esta fase, los clusters HA de firewall interno y externo Check Point ubicados en OFIC-ACTUAL-GYE son los Gateways de cada VLAN de capa 2 extendida detallada en la tabla 3.3, y otorgan conectividad hacia las VLANs no extendidas, franquicias, clientes e Internet.

k) Adicional a los enlaces de capa 2 extendidos, existen dos enlaces de capa 3 enrutados con una capacidad de 100 Mbps y una conexión física cada uno, provistos también por los carriers Telconet y Century Link.

3.4.2. Fase 2

En la segunda fase se realizó la integración del centro de datos DC-GYE con el centro de datos alterno localizado en DC-UIO, a través de dos enlaces extendido de capa 2 entre ambas localidades en modalidad activo-activo y enlaces de capa 3 en modalidad activo-activo.

3.4.2.1. Descripción de Implementación Fase 2

a) En el centro de datos DC-UIO, en el rack 2 se instaló el switch core llamado SWCSDCQR2, compuesto de dos miembros en modalidad de stack con anillo mediante un enlace virtual IRF, compuesto por dos

conexiones físicas de 40 Gpbs con cables DAC QSFP+ de 3 metros cada uno, agregando un total de 80 Gbps.

b) En el rack 3 de DC-UIO se encuentra el switch ToR llamado SWWSDCQR3, compuesto de dos miembros en modalidad de stack con anillo mediante un enlace virtual IRF, compuesto por dos conexiones físicas de 10 Gpbs con cables de fibra óptica cada uno, agregando un total de 20 Gbps.

c) El switch core SWCSDCQR2 se conecta con el switch ToR SWWSDCQR3 mediante un enlace agregado entre ambos stack compuesto por dos conexiones físicas de 10 Gbps con cables DAC SFP+ de 3 metros cada uno, agregando un total de 20 Gbps.

d) El switch core SWCSDCQR2 de DC-UIO se conecta con el SWCSDCGR7 de DC-GYE mediante dos enlaces de capa 2 extendido, en modo activo/activo con un ancho de banda de 900 Mbps cada uno provistos por los carrier Telconet y Century Link. Estos dos enlaces forman un enlace lógico usando el protocolo LACP en modo activo y se realiza mediante la conexión física con cables UTP CAT-6A entre ambos switches a través de los equipos de los carriers. Por este enlace de capa 2 entre ambas localidades, que opera en modo troncal, atraviesan las mismas VLANs de capa 2 extendidas que vienen de DC-GYE, detalladas en la tabla 3.3.

e) Adicional a los enlaces de capa 2 extendidos, existen dos enlaces de capa 3 enrutados con una capacidad de 100 Mbps y una conexión física cada uno, provistos también por los carriers Telconet y Century Link.

3.4.3. Nomenclatura de Equipos

Tal como se ha detallado en el listado en la tabla 3.2, se detalla la estructura de nombre a utilizar para cada equipo switch de red, en base a un estándar definido por el cliente:

SW[FUNCION][MIEMBRO_STACK][LOCALIDAD][RACK]

Tabla 3. 4: Nomenclatura de equipos

Token	Descripción	Valor / Ejemplo
FUNCION	En 1 solo caracter, se detalla la función o uso del switch.	C = Core T = ToR W = WAN
MIEMBRO_STACK	En 1 solo caracter, se detalla el miembro del stack de switches.	1 = Miembro 1 2 = Miembro 2 S = Stack*
LOCALIDAD	Detalla la localidad donde está ubicado el switch.	DCG = DC-GYE DCQ = DC-UIO
RACK	Detalla el número o identificador de rack donde está ubicado el switch.	R7 = Rack 7

Fuente: Autor

Por ejemplo, el switch llamado SWC1DCGR7 cumple la función de miembro 1 del stack de switch Core, está ubicado en el centro de datos principal DCGYE en el rack R7. En caso de referirse al stack de switches y no al miembro en sí, se utiliza el caracter S.

3.4.4. Direccionamiento IP Administración Equipos

Las direcciones IP utilizadas para administración de los nuevos equipos de infraestructura de red son las siguientes:

Tabla 3. 5: Direccionamiento de equipos en DataCenter

LOCALIDAD	NOMBRE	DIRECCION IP	MASCARA	GATEWAY	VLAN
DC-GYE	SWCSDCGR7	182.20.1.10	24	182.20.1.1	200
	SWTSDCGR5	182.20.1.11	24	182.20.1.1	200
	SWTSDCGR6	182.20.1.12	24	182.20.1.1	200
	SWWSDCGR8	182.20.1.13	24	182.20.1.1	200
DC-UIO	SWCSDCQR2	182.20.1.20	24	182.20.1.1	200
	SWWSDCQR3	182.20.1.21	24	182.20.1.1	200

Fuente: Autor

3.5. Instalación física de los equipos

A continuación, se muestra la distribución de los equipos de cada localidad.

3.5.1. DC-GYE

Para el DC-GYE ubicado en el Data Center de telconet, se tienen cuatro racks donde se disponen de los equipos de comunicaciones y han sido numerados del cinco al ocho de la siguiente manera:

3.5.1.1. Rack 5

En este rack en la parte frontal se encuentran los dos switches modelo HPE 5700 configurados en stack con nombre SWTSDCGR5 mediante 4 cables DAC SFP+ de 10Gb cada uno. Está ubicado en las dos primeras unidades de rack usando la topología Top of the Rack (ToR) y se conecta al switch Core en el rack 7 mediante dos cables DAC QSF+ formando un enlace agregado de 80Gb

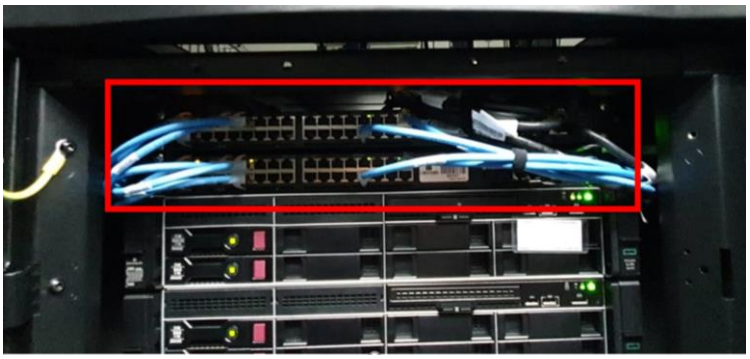


Figura 3. 3: Equipos Rack 5
Fuente: Autor

3.5.1.2. Rack 6

En este rack en la parte frontal se encuentran los dos switches modelo HPE 5700 configurados en stack con nombre SWTSDCGR6, mediante 4 cables DAC SFP+ de 10Gb cada uno. Está ubicado en las dos primeras unidades de rack usando la topología Top of the Rack (ToR) y se conecta al switch Core en el rack 7 mediante dos cables DAC QSF+ formando un enlace agregado de 80Gb.

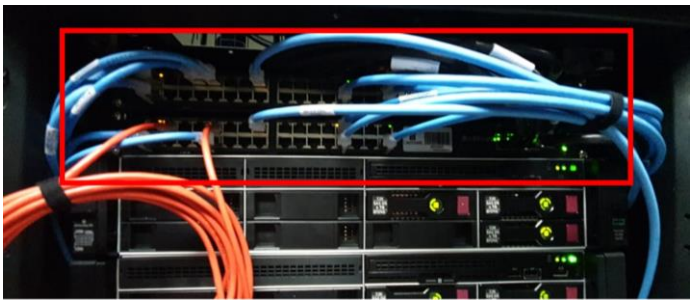


Figura 3. 4: Equipos Rack 6
Fuente: Autor

3.5.1.3. Rack 7

En este rack en la parte frontal se encuentran los dos switches de Core modelo HPE 5940 4-slot con nombre SWC1DCGR7, configurados en stack mediante el protocolo IRF. Está ubicado en las 4 primeras unidades de rack al ser un equipo de 2 unidades de rack cada uno. Integra a los equipos en los racks 5, 6 y 8 que corresponden al ToR1, ToR2 y ToR WAN respectivamente. Además, permite la comunicación al DC-UIO en Carcelén y Oficinas actuales de Credimatic.

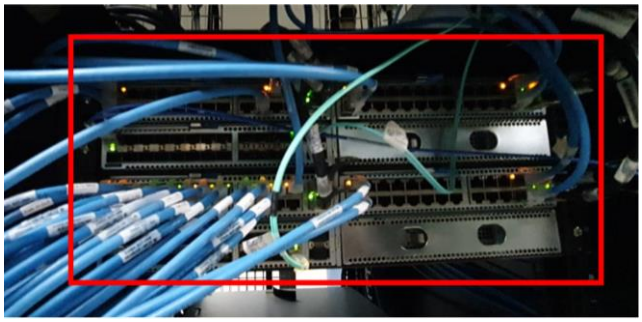


Figura 3. 4: Equipos Rack 7
Fuente: Autor

3.5.1.4. Rack 8

En este rack en la parte frontal se encuentran los dos switches modelo HPE5130 configurados en stack con nombre SWWSDCGR8, mediante 2 cables de fibra y modulos SFP+ de 10Gb cada uno. Está ubicado en las dos primeras unidades de rack y se conecta al switch Core en el rack 7 mediante dos cables fibra y SFP+ de 10 Gb formando un enlace agregado de 20Gb.

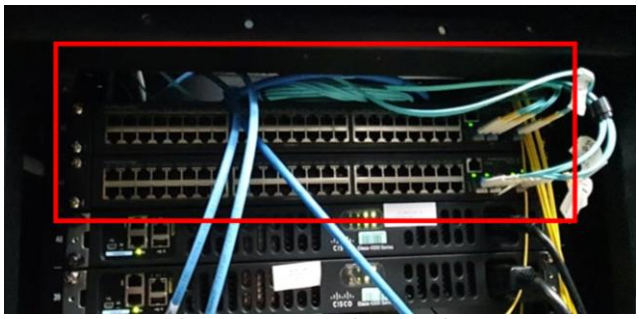


Figura 3. 5: Equipo Rack 8
Fuente: Autor

3.5.2. DC-UIO

Para el DC-UIO ubicado en el Data Center de Century Link, se tienen dos racks donde se disponen de los equipos de comunicaciones y han sido numerados del dos al tres de la siguiente manera:

Rack 2

En este rack en la parte frontal se encuentran los dos switches de Core modelo HPE 5940 2-slot con nombre SWCSDCQR2, configurados en stack mediante el protocolo IRF.

Rack 3

En este rack se encuentran los dos switches modelo HPE 5130 configurados en stack con nombre SWWSDCQR3 mediante modulos SFP+ de 10Gb cada uno.

3.6. Conexiones Stack Switches

A continuación, se detalla las conexiones de stacking IRF para los nuevos equipos adquiridos por Credimatic, distribuidos por localidad en la Tabla 3. 6: Detalle de Stack de Switches.

3.7. Conexiones entre Switches

En la Tabla 3. 7 se detalla las conexiones entre los switches nuevos equipos adquiridos por Credimatic, distribuidos por localidad.

Tabla 3. 6: Detalle de Stack de Switches

	ORIGEN			MEDIO		DESTINO		
LOCALIDAD	**EQUIPO**	**PUERTO**	**TIPO**	**VELOCIDAD**	**CABLE**	**EQUIPO**	**PUERTO**	**TIPO**
DC-GYE	SWC1DCGR7	1/1/25	IRF	40 Gbps	DAC QSFP+	SWC2DCGR7	2/1/25	IRF
	SWC1DCGR7	1/2/25	IRF	40 Gbps	DAC QSFP+	SWC2DCGR7	2/2/25	IRF
	SWT1DCGR5	1/0/37	IRF	10 Gbps	DAC SFP+	SWT2DCGR5	2/0/37	IRF
	SWT1DCGR5	1/0/38	IRF	10 Gbps	DAC SFP+	SWT2DCGR5	2/0/38	IRF
	SWT1DCGR5	1/0/39	IRF	10 Gbps	DAC SFP+	SWT2DCGR5	2/0/39	IRF
	SWT1DCGR5	1/0/40	IRF	10 Gbps	DAC SFP+	SWT2DCGR5	2/0/40	IRF
	SWT1DCGR6	1/0/37	IRF	10 Gbps	DAC SFP+	SWT2DCGR6	2/0/37	IRF
	SWT1DCGR6	1/0/38	IRF	10 Gbps	DAC SFP+	SWT2DCGR6	2/0/38	IRF
	SWT1DCGR6	1/0/39	IRF	10 Gbps	DAC SFP+	SWT2DCGR6	2/0/39	IRF
	SWT1DCGR6	1/0/40	IRF	10 Gbps	DAC SFP+	SWT2DCGR6	2/0/40	IRF
	SWW1DCGR8	1/0/49	IRF	10 Gbps	SFP+	SWW2DCGR8	2/0/49	IRF
	SWW1DCGR8	1/0/50	IRF	10 Gbps	SFP+	SWW2DCGR8	2/0/50	IRF
DC-UIO	SWC1DCQR2	1/0/1	IRF	40 Gbps	DAC QSFP+	SWC2DCQR2	1/0/1	IRF
	SWC1DCQR2	1/0/2	IRF	40 Gbps	DAC QSFP+	SWC2DCQR2	1/0/2	IRF
	SWW1DCQR3	1/0/49	IRF	10 Gbps	SFP+	SWW2DCQR3	2/0/49	IRF
	SWW1DCQR3	1/0/50	IRF	10 Gbps	SFP+	SWW2DCQR3	2/0/50	IRF

Fuente: Autor

Tabla 3. 7: Interconexión de Switches

ORIGEN					MEDIO		DESTINO			
LOCALIDAD	**EQUIPO**	**PUERTO**	**TIPO**	**LAG**	**VELOCIDAD**	**CABLE**	**EQUIPO**	**PUERTO**	**TIPO**	**LAG**
DC-GYE	SWC1DCGR7	1/1/23	Troncal	BAGG10	1 Gbps	CAT 6A	SWPRDP3R1U03	1/0/47	Troncal	BAGG10
	SWC1DCGR7	1/2/23	Troncal	BAGG10	1 Gbps	CAT 6A	SWPRDP3R1U03	1/0/48	Troncal	BAGG10
	SWC1DCGR7	2/1/23	Troncal	BAGG10	1 Gbps	CAT 6A	SWPRDP3R1U03	2/0/47	Troncal	BAGG10
	SWC1DCGR7	2/2/23	Troncal	BAGG10	1 Gbps	CAT 6A	SWPRDP3R1U03	2/0/48	Troncal	BAGG10
	SWC1DCGR7	1/1/26	Troncal	BAGG1	40 Gbps	DAC QSFP+	SWT1DCGR5	1/0/41	Troncal	BAGG1
	SWC2DCGR7	2/1/26	Troncal	BAGG1	40 Gbps	DAC QSFP+	SWT2DCGR5	2/0/41	Troncal	BAGG1
	SWC1DCGR7	1/2/26	Troncal	BAGG2	40 Gbps	DAC QSFP+	SWT1DCGR6	1/0/41	Troncal	BAGG1
	SWC2DCGR7	2/2/26	Troncal	BAGG2	40 Gbps	DAC QSFP+	SWT2DCGR6	2/0/41	Troncal	BAGG1
	SWC1DCGR7	1/3/24	Troncal	BAGG3	10 Gbps	SFP+	SWW1DCGR8	1/0/52	Troncal	BAGG1
	SWC2DCGR7	2/3/24	Troncal	BAGG3	10 Gbps	SFP+	SWW2DCGR8	2/0/52	Troncal	BAGG1
	SWC1DCGR7	1/2/24	Troncal	BAGG20	1 Gbps	CAT 6A	SWC1DCQR2	1/1/23	Troncal	BAGG20
	SWC2DCGR7	2/2/24	Troncal	BAGG20	1 Gbps	CAT 6A	SWC2DCQR2	2/1/23	Troncal	BAGG20
DC-UIO	SWC1DCQR2	1/1/26	Troncal	BAGG1	10 Gbps	DAC SFP+	SWW1DCQR3	1/0/52	Troncal	BAGG1
	SWC2DCQR2	2/1/26	Troncal	BAGG1	10 Gbps	DAC SFP+	SWW2DCQR3	2/0/52	Troncal	BAGG1

Fuente: Autor

También se puede corroborar los equipos conectados al switch core en DC-GYE y los tipos de puertos utilizados:

```
[SWCSDCGR7]display lldp neighbor-information list
Chassis ID : * -- -- Nearest nontpmr bridge neighbor
             # -- -- Nearest customer bridge neighbor
             Default -- -- Nearest bridge neighbor
Local Interface Chassis ID      Port ID                 System Name
XGE1/1/23       4001-c6a5-d480  GigabitEthernet1/0/47   SWPRDP3R1U03
FGE1/1/25       4cae-a349-59fc  FortyGigE2/1/25         SWCSDCGR7
FGE1/1/26       ec9b-8bfa-1b35  FortyGigE1/0/41         SWTSDCGR5
XGE1/2/23       4001-c6a5-d480  GigabitEthernet1/0/48   SWPRDP3R1U03
XGE1/2/24       4cae-a34e-1fc7  Ten-GigabitEthernet1/1/23 SWCSDCQR2
FGE1/2/25       4cae-a349-59fc  FortyGigE2/2/25         SWCSDCGR7
FGE1/2/26       ec9b-8bfa-10c7  FortyGigE1/0/41         SWTSDCGR6
XGE1/3/24       ec9b-8ba0-217e  Ten-GigabitEthernet1/0/52 SWWDCGR8
XGE2/1/23       4001-c6a5-d480  GigabitEthernet2/0/47   SWPRDP3R1U03
FGE2/1/25       4cae-a349-59fc  FortyGigE1/1/25         SWCSDCGR7
FGE2/1/26       ec9b-8bfa-1b35  FortyGigE2/0/41         SWTSDCGR5
XGE2/2/23       4001-c6a5-d480  GigabitEthernet2/0/48   SWPRDP3R1U03
XGE2/2/24       4cae-a34e-1fc7  Ten-GigabitEthernet2/1/23 SWCSDCQR2
FGE2/2/25       4cae-a349-59fc  FortyGigE1/2/25         SWCSDCGR7
FGE2/2/26       ec9b-8bfa-10c7  FortyGigE2/0/41         SWTSDCGR6
XGE2/3/24       ec9b-8ba0-217e  Ten-GigabitEthernet2/0/52 SWWDCGR8
[SWCSDCGR7]
```

Figura 3. 6: Identificación de Conexiones
Fuente: Autor

3.8. Enlace entre DC-GYE y DC-UIO

Se muestra el enlace formado entra el DC-GYE ubicado en Telconet y DT-UIO ubicado en Carcelen. Para el enlace agregado se usó el protocolo LACP en modo activo a través de los carriers Telconet y Century Link; cada uno de 900 Megas.

```
[SWCSDCGR7]display link-aggregation verbose Bridge-Aggregation 20
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation20
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x8000, 4cae-a349-59fc
Local:
  Port              Status  Priority Index    Oper-Key              Flag
  XGE1/2/24(R)      S       32768    11       6                     {ABCDEF}
  XGE2/2/24         S       32768    12       6                     {ABCDEF}
Remote:
  Actor             Priority Index    Oper-Key SystemID              Flag
  XGE1/2/24         32768    5        3        0x8000, 4cae-a34e-1fc7 {ABCDEF}
  XGE2/2/24         32768    2        3        0x8000, 4cae-a34e-1fc7 {ABCDEF}
[SWCSDCGR7]
```

Figura 3. 7: Enlace DCGYE- DCUIO
Fuente: Autor

El estado de los puertos muestra una S que para el caso significa SELECTED, es decir forma parte del enlace agregado y ese encuentra activo.

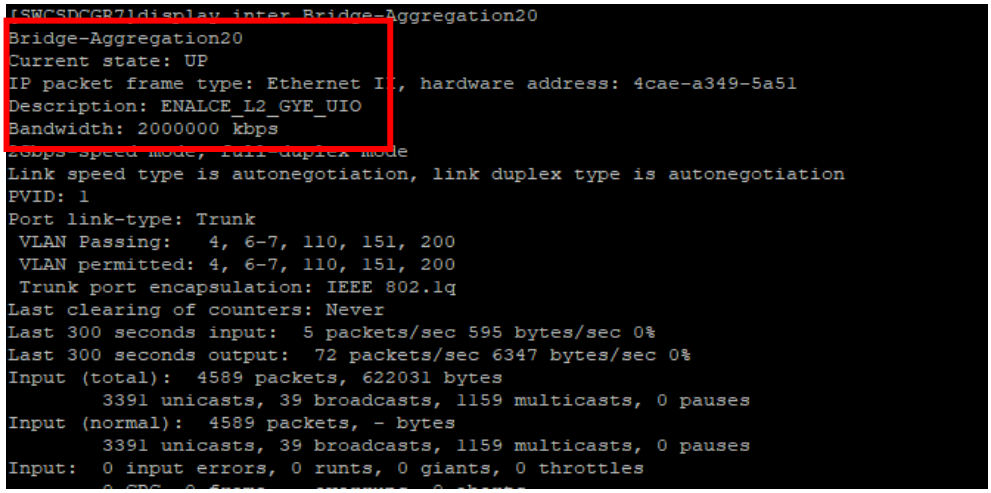


Figura 3. 8: Ancho de banda de enlace
Fuente: Autor

La imagen muestra el estado del enlace y el ancho de banda del enlace agregado.

3.8.1.1. Rack 2

En este rack en la parte frontal se encuentran los dos switches de Core modelo HPE 5940 2-slot con nombre SWCSDCQR2, configurados en stack mediante el protocolo IRF. Está ubicado en las unidades de rack 40 y 37; primario y secundario respectivamente. Integra al switche ToR ubicado en el rack 3 que corresponden al ToR1. Es el encargado de establecer la comunicación con el DC-GYE.

Figura 3. 9: Equipo Rack 2
Fuente: Autor

3.8.1.2. Rack 3

En este rack se encuentran los dos switches modelo HPE 5130 configurados en stack con nombre SWWSDCQR3 mediante módulos SFP+ de 10Gb cada uno. Está ubicado en las unidades de rack usando 40 y 41 usando la topología Top of the Rack (ToR) y se conecta al switch Core en el rack 2 mediante dos cables DAC SFP+ formando un enlace agregado de 20Gb.

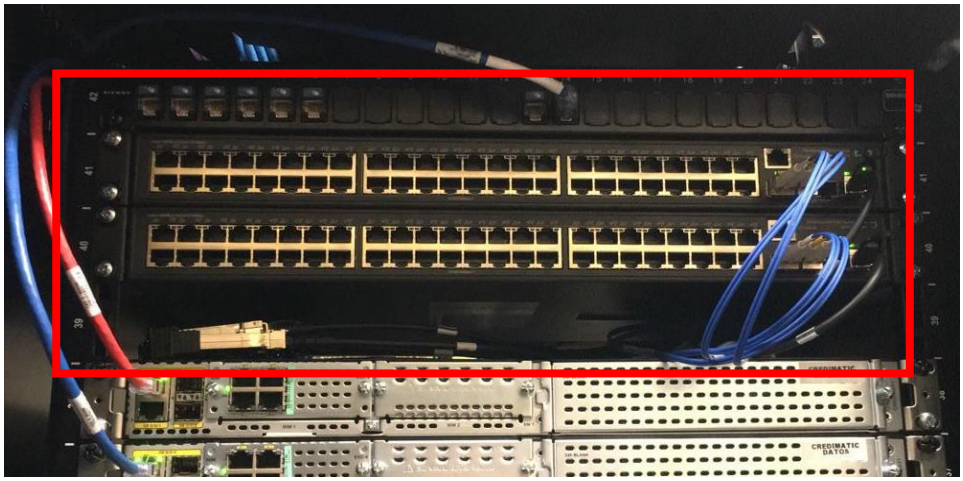


Figura 3. 10: Equipo Rack 3
Fuente: Autor

En la figura 3.12 se muestra la conexión entre Datacenters de Guayaquil y Quito.

3.9. Actualización Plataforma CheckPoint a Version R80.xx

La migración de los equipos Check Point será de la versión R77.30 a R80.XX., a continuación en la tabla 3.8 se detallan todos los equipos con su versión correspondiente, los cuales se alojan en un servidor físico cada uno.

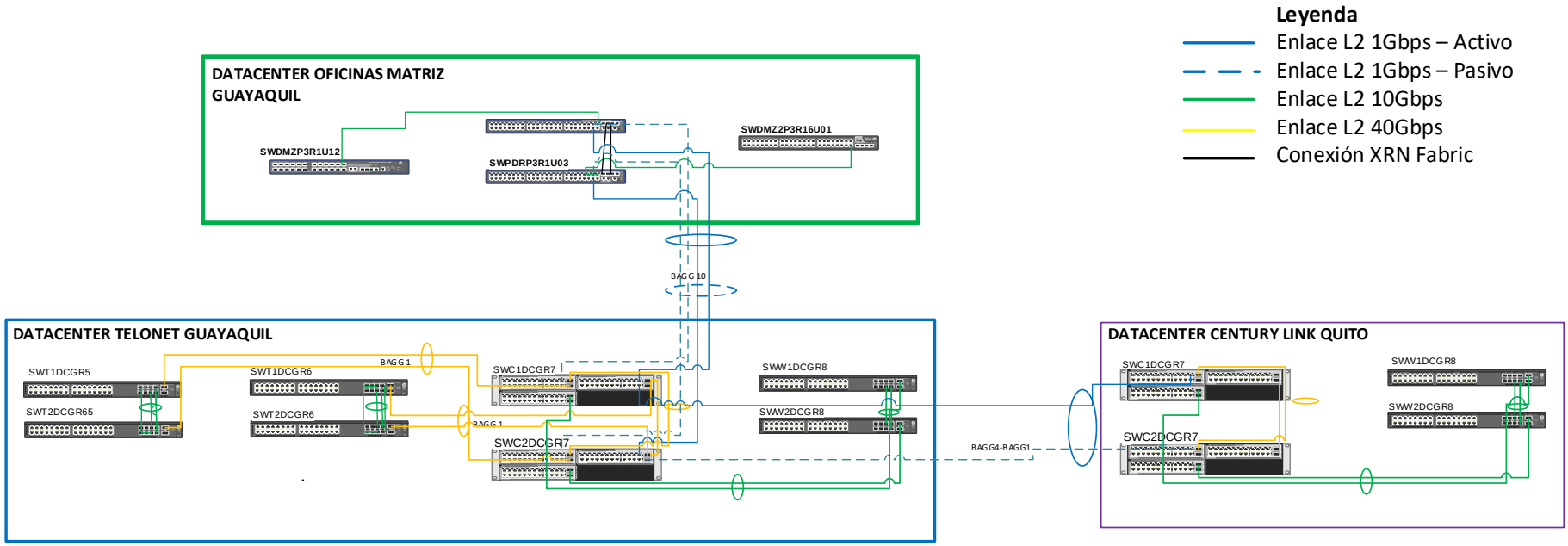


Figura 3. 11: Conexión entre Datacenters

Fuente: Autor

Tabla 3. 8: Versiones Actuales de Solucion Firewall Checkpoint

Ciudad	Equipo	Version Actual
Guayaquil	Security Manager (SMC)	R77.30
Guayaquil	Security Gateway (Odisea001)	R77.30
Guayaquil	Security Gateway (Odisea002)	R77.30
Guayaquil	Security Gateway (Olimpo01)	R77.30
Guayaquil	Security Gateway (Olimpo02)	R77.30
Quito	Security Manager (SMC UIO)	R80.10
Quito	Security Gateway (Zeus01)	R77.30
Quito	Security Gateway (Zeus02)	R77.30
Quito	Security Gateway (FW Oficina UIO)	R77.30

Fuente: Autor

3.9.1. Estado actual

Se muestra gráficamente como está actualmente estructurada la distribución de los servidores que alojan los gateways y manager de la solución checkpoint en la versión R70.30.

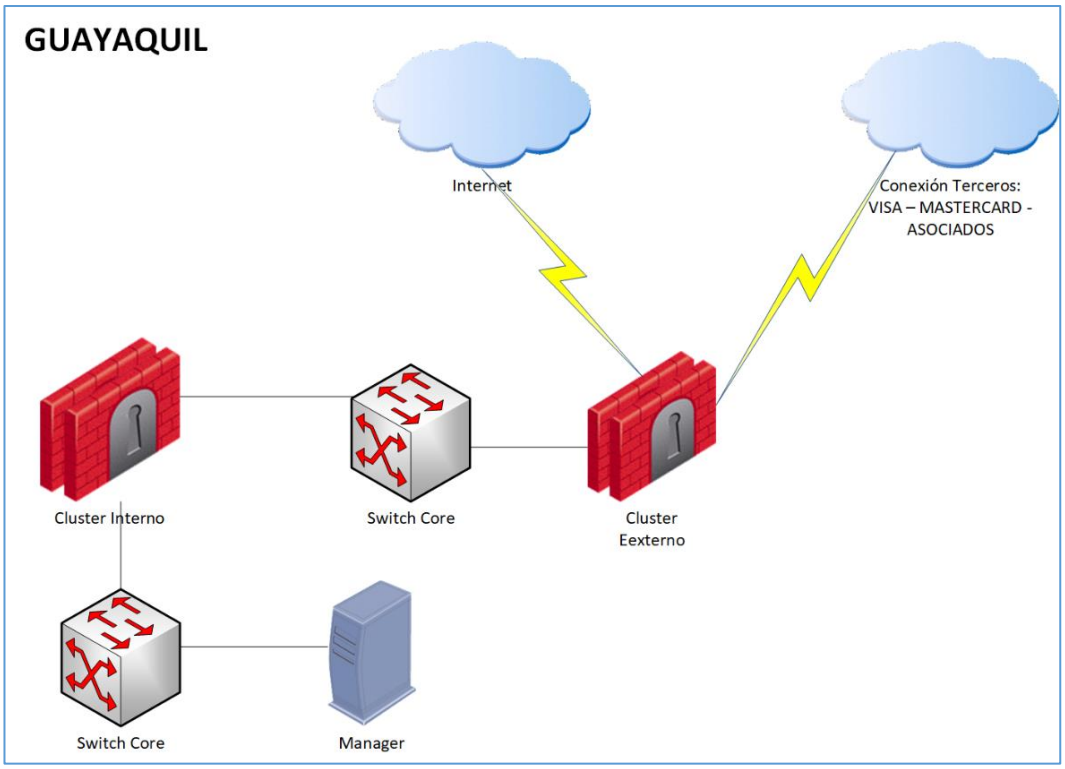


Figura 3. 12: Situación Actual Guayaquil
Fuente: Autor

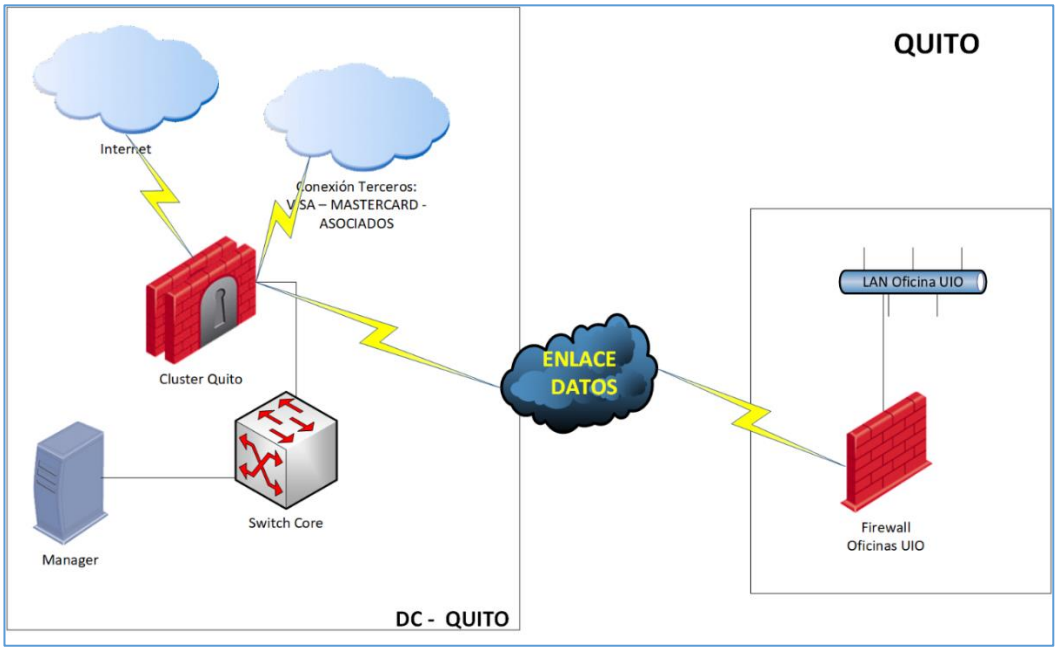


Figura 3. 14: Situación Actual Quito
Fuente: Autor

Las redes que están en uso en los FWs internos y externos son las siguientes:

Tabla 3. 9: Detalle de Interfaces Firewall Clúster Interno

Interfaz	crdodisea	odisea001	odisea002	VLAN	RED	Observaciones
Eth0	182.27.160.24	182.27.160.25	182.27.160.26	24	182.27.160.0/24	Interconexión Desarrollo (125,124,119)
Eth3	10.121.85.12	10.121.85.10	10.121.85.11	30	10.121.85.0/24	Interconexión Firewall Externo
Eth4	10.121.88.24	10.121.88.25	10.121.88.26	12	10.121.88.0/24	FW INTERNO
Eth5	182.27.118.76	182.27.118.74	182.27.118.75	4	182.27.118.0/24	PRODUCCIÓN
Eth6	182.27.117.1	182.27.117.15	182.27.117.16	7	182.27.117.0/24	PROTECCIÓN
Eth7	182.27.114.14	182.27.114.15	182.27.114.16	40	182.27.114.0/24	SENTINEL
Eth8	182.27.113.1	182.27.113.14	182.27.113.15	113	182.27.113.0/24	PREPRODUCCIÓN
Eth10	182.27.131.1	182.27.131.14	182.27.131.16	25	182.27.131.0/24	USUARIOS AVANZADOS**(IDS/SIT/Monitoreo)**
Eth11	182.27.155.1	182.27.155.15	182.27.155.16	155	182.27.155.0/24	GERENCIA/Contabilidad/ RRHH
Eth12	182.27.157.1	182.27.157.16	182.27.157.16	157	182.27.157.0/24	AUTORIZACIONES
Eth1		182.27.116.14	182.27.116.15	16	182.27.116.0/24	***SYNC***

Fuente: Autor

Tabla 3. 10: Detalle de Interfaces Clúster Firewall Externo

Interfaz	crdolimpo	crdolimpo01	crdolimpo02	VLAN	RED	Observación
Eth0	20.221.90.14	20.221.90.15	20.221.90.16	10	20.221.90c.0/24	MASTERCARD
Eth2	200.51.10.194	200.51.10.203	200.51.10.203	11	200.51.10.0/28	INTERNET
Eth4	20.221.150.14	20.221.150.15	20.221.150.16	6	20.221.150.0/24	DMZ1
Eth5	182.27.121.3	182.27.121.1	182.27.121.2	29	182.27.121.0/24	WIPS
Eth6	20.221.100.25	20.221.100.15	20.221.100.16	13	20.221.100.0/24	ASOCIADOS
Eth7	20.221.86.22	20.221.86.20	20.221.86.21	8	20.221.86.0/24	FW EXTERNO
Eth8	20.221.89.14	20.221.89.15	20.221.89.16	9	20.221.89.0/24	VISA
Eth9	20.221.151.15	20.221.151.14	20.221.151.16	151	20.221.151.0/24	DMZ2
Eth10	190.226.103.149	190.226.103.148	190.226.103.150	15	190.226.103.144/29	PAYPHONE PRD
Eth11	20.221.121.2	20.221.121.3	20.221.121.15	14	20.221.121.0/24	SFTP MNET
Eth12	190.226.103.137	190.226.103.139	190.226.103.140	17	190.226.103.136/29	PAYPHONE DESA
Eth13	20.221.152.14	20.221.152.15	20.221.152.16	152	20.221.152.0/24	DMZ DESARROLLO
Eth1		10.121.87.1	10.121.87.2		10.121.87.0/24	***SYNC***

Fuente: Autor

Las redes que están en uso en los FWs DataCenter y Oficinas son las siguientes:

Tabla 3. 11: interfaces Firewall UIO Datacenter

Interfaz	Zeus	Zeus01	zeus02	Observaciones
Eth0	20.221.211.25/24	20.221.211.30/24	20.221.211.31/24	Asociados
Eth1	10.121.214.15/24	10.121.214.16/24	10.121.214.14/24	conexión oficinas uio hacia Datacenter
Eth2	182.27.230.14/24	182.27.230.100/24	182.27.230.101/24	Red Extendida **producción RED118 - FW Interno GYE**
Eth3	182.27.231.14/24	182.27.231.100/24	182.27.231.101/24	Red Extendida **Protección RED 117 - FW Interno GYE**
Eth4	30.221.89.14/24	30.221.89.13/24	30.221.89.12/24	VISA
Eth5	182.27.232.14/24	182.27.232.100/24	182.27.232.101/24	DMZ RED150
Eth6	200.31.26.227/28	200.31.26.229/28	200.31.26.229/28	Internet
Eth7	30.221.90.14/24	30.221.90.58/24	30.221.90.57/24	MasterCard
Eth8	190.216.103.206/29	190.216.103.204/29	190.216.103.205/29	Payphone

Fuente: Autor

Tabla 3. 12: Interfaces Firewall oficinas Quito

Interfaz	FW Oficina	Observaciones
Eth0	10.121.212.15/24	Conexión oficina century Link
Eth1	182.27.235.3/24	Sentinel usuario
Eth2	182.27.233.0/24	Autorizaciones, Vlan **extendida de la red 157 GYE**
Eth3	30.221.85.25/24	Enlace quito - gye
Eth5	182.27.234.3/24	Red administrativa UIO

Fuente: Autor

3.9.2. Solución propuesta

Se debe migrar de la versión R77.30 a versión R80.xx toda la plataforma CheckPoint, debido a que los equipos actuales tienen limitantes de hardward y ya terminó su tiempo de vida útil, para esto se va a implementar 8 servidores marca HP modelo HPE ProLiant DL380 Gen10, se implementará como sistema operativo en cada host vmware ESXi para virtualizar los gateways. Adicional se realizará la migración del DC Guayaquil a Telconet, como último punto tener un mirror site con el DataCenter en Century Link UIO.

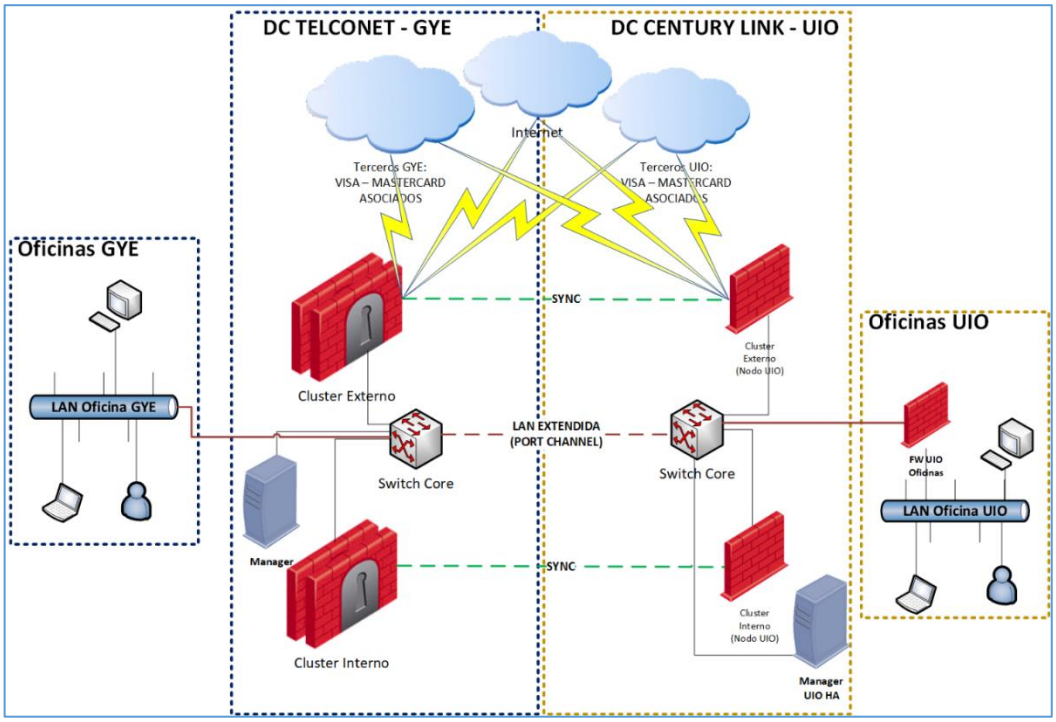


Figura 3. 13: Diagrama de Red de la Solución Propuesta
Fuente: Autor

Tabla 3. 13: Hardware a utilizar

Ciudad	Equipo	Ubicación	Observación
Guayaquil	Security Manager (SMC)	DC Telconet	Virtual
Guayaquil	Security Gateway (FWInterno01)	DC Telconet	HP Proliant DL380 G10
Guayaquil	Security Gateway (FWInterno02)	DC Telconet	HP Proliant DL380 G10
Quito	Security Gateway (FWInterno03)	DC CenturyLink	HP Proliant DL380 G10
Guayaquil	Security Gateway (FWExterno01)	DC Telconet	HP Proliant DL380 G10
Guayaquil	Security Gateway (FWExterno02)	DC Telconet	HP Proliant DL380 G10
Quito	Security Gateway (FWExterno03)	DC CenturyLink	HP Proliant DL380 G10
Guayaquil	Security Gateway (FWOficina01)	Oficinas Matriz	HP Proliant DL380 G10
Guayaquil	Security Gateway (FWOficina02)	Oficinas Matriz	HP Proliant DL380 G10

Fuente: Autor

3.9.3. Consideraciones

- Se tienen extendidas las redes directamente conectadas de los Firewalls Externos (UIO y GYE) e Internos, en los Data Centers de Telconet y Century Link. Esto incluye las redes internas y las redes externas como: Visa, MasterCard, Asociados, etc.
- Los requerimientos recomendados para la interfaz Sync en los Firewalls (Red extendida) son: 20ms y 3% de paquetes perdidos.
- Se tiene Cluster de 3 nodos para Externo e Interno distribuidos: 2 Firewalls en GYE y 1 Firewall en UIO.
- El Manager HA en UIO puede ser manejado como un Security Manager secundario, o en su defecto puede ser una réplica de VM del Manager GYE (esta opción sería manejada por la replicación de VMware)
- Se manejarán 3 etapas para llegar al diseño final (se dispone de un cronograma a detalle de cada etapa):
    - Upgrade de plataforma actual a R80.xx
        - Se actualizarán los equipos como se encuentran desplegados actualmente en versión R80.xx

        - Para los FWs GYE se actualizará a la versión R80.10, pero se tendrá instalado VMware sobre los Servers. El Security Gateway será una VM sobre ESX.
        - Se deberá revisar como quedarán las conexiones de cada FW (visto desde la óptica de VM), conexiones a los VSwitch en VMware, conexiones físicas de las interfaces hacia los switches
    - Migración a DC Telconet
        - Redes directamente conectadas a los Firewalls extendidas en DC Telconet
        - Migrar 1 FW a la vez a DataCenter Telconet
        - Migrar el Manager a DataCenter Telconet
    - Mirror Site con DC CenturyLink
        - Redes directamente conectadas a los Firewall extendidas en los DCs (Redes de Telconet extendidas en CenturyLink y viceversa)
        - Realizar revisión de redes extendidas y hacer merge de políticas de seguridad de UIO y GYE.
        - Manager HA en UIO (opción Manager Secundario o replica de VM por VMware)

3.9.4. Tabla de Direccionamiento Unificado:

A continuación se detallará la configuración de las interfaces de los servidores en el cual será manejado como sistema operativo núcleo VMWare ESXi versión 6.7.

Tabla 3. 14: Detalle Interfaces Firewall Externo
Tabla 3. 15: Detalle de Configuración de Interfaces Firewall Interno
Tabla 3. 16: Detalle de configuración de interfaces Firewall Oficina

Tabla 3. 16: Detalle Interfaces Firewall Externo

VMWARE SERVER (VM FW Externo)											
Interface	**VLAN**	**FWEXTERNO**	**FWEXTERNO01**	**FWEXTERNO02**	**FWEXTERNO03**	**RED**	**Descripción**	**VMWare (Nic Fisica)**	**Velocidad**	**GroupPort**	**VMSwitch**
eth0	VLAN10:	20.221.90.14	20.221.90.15	20.221.90.16	20.221.90.17	20.221.90.0/24	MASTERCARD	Nic 0	1000 Mbps	MASTERCARD	Vswitch1
eth1	VLAN11:	200.51.10.194	200.51.10.203	200.51.10.203	200.51.10.204	200.51.10.0/28	INTERNET	Nic2	1000 Mbps	INTERNET	Vswitch2
eth2			10.121.87.1	10.121.87.2	10.121.87.3	10.121.87.0/24	Sync	Nic3	1000 Mbps	FWSYNC	Vswitch3
eth3	VLAN6:	20.221.150.14	20.221.150.15	20.221.150.16	20.221.150.17	20.221.150.0/24	DMZ1	Nic4	10 Gbps	DMZ1	Vswitch4
eth4	VLAN29:	182.27.121.3	182.27.121.1	182.27.121.2	182.27.121.3	182.27.121.0/24	WIPS	Nic 5	10 Gbps	WIPS_PAYPHONE_DMZ	Vswitch5
eth5	VLAN13:	20.221.100.25	20.221.100.15	20.221.100.16	20.221.100.17	20.221.100.0/24	ASOCIADOS	Nic 6	10 Gbps	ASOCIADOS	Vswitch6
eth6	VLAN8:	20.221.86.22	20.221.86.20	20.221.86.21	20.221.86.22	20.221.86.0/24	FW EXTERNO	Nic 7	10 Gbps	FWEXTERNO	Vswitch7
eth7	VLAN9:	20.221.89.14	20.221.89.15	20.221.89.16	20.221.89.17	20.221.89.0/24	VISA	Nic 8	10 Gbps	VISA	Vswitch8
eth8	VLAN151:	20.221.151.15	20.221.151.14	20.221.151.16	20.221.151.17	20.221.151.0/24	DMZ2	Nic 9	10 Gbps	DMZ2	Vswitch9
eth9	VLAN15:	190.226.103.150	190.226.103.149	190.226.103.148	190.226.103.149	190.226.103.144/29	PAYPHONE PRD	Nic 10	1000 Mbps	PAYPHONE_PRD-SFTP MNET	Vswitch10
eth9	VLAN14:	20.221.121.15	20.221.121.2	20.221.121.3	20.221.121.4	20.221.121.0/24	SFTP MNET	Nic 10	1000 Mbps	PAYPHONE_PRD-SFTP MNET	Vswitch10
eth4	VLAN17:	190.226.103.140	190.226.103.137	190.226.103.138	190.226.103.149	190.226.103.136/29	PAYPHONE DESA	Nic 5	10 Gbps	WIPS_PAYPHONE_DMZ	Vswitch5
eth4	VLAN152:	20.221.152.14	20.221.152.15	20.221.152.16	20.221.152.17	20.221.152.0/24	DMZ DESARROLLO	Nic 5	10 Gbps	WIPS_PAYPHONE_DMZ	Vswitch5

Fuente: Autor

Tabla 3. 17: Detalle de Configuración de Interfaces Firewall Interno

VMWARE SERVER (VM FW Interno)										
Interface	**VLAN**	**FWINTERNO**	**FWINTERNO01**	**FWINTERNO02**	**FWINTERNO03**	**RED**	**Descripción**	**VMWare (Nic Fisica)**	**Velocidad**	**VMSwitch**
eth0	VLAN24	182.27.160.24	182.27.160.25	182.27.160.26	182.27.160.27	182.27.160.24/24	interconexion Desarrollo	Nic 0	1000 Mbps	Vswitch1
eth1	VLAN16		182.27.16.14	182.27.16.15	182.27.16.16	182.27.16.0/24	RED HEARBEAT SYBASE	Nic 3	1000 Mbps	Vswitch2
eth2	VLAN30	10.121.85.12	10.121.85.10	10.121.85.11	10.121.85.13	10.121.85.12/24	CONEXIÓN FW EXTERNO	Nic 2	1000 Mbps	Vswitch3
eth3	VLAN12	10.121.88.24	10.121.88.25	10.121.88.26	10.121.88.27	10.121.88.24/24	FW INTERNO UIO	Nic 9	1000 Mbps	Vswitch4
eth4	VLAN4	182.27.118.76	182.27.118.74	182.27.118.75	182.27.118.76	182.27.118.76/24	PRODUCCION	Nic 4	1000 Mbps	Vswitch5
eth5	VLAN7	182.27.117.1	182.27.117.15	182.27.117.16	182.27.117.17	182.27.117.1/23	PROTECCION	Nic 5	1000 Mbps	Vswitch0
eth6	VLAN40	182.27.114.14	182.27.114.15	182.27.114.16	182.27.114.17	182.27.114.14/24	SENTINEL	Nic 6	1000 Mbps	Vswitch7
eth7	VLAN113	182.27.113.1	182.27.113.14	182.27.113.15	182.27.113.16	182.27.113.1/24	PREPRODUCCION	Nic 7	1000 Mbps	Vswitch8
eth3	VLAN25	182.27.131.1	182.27.131.14	182.27.131.16	182.27.131.18	182.27.131.1/24	USUARIOS AVANZADOS	Nic 9	1000 Mbps	Vswitch4
eth8	VLAN155	182.27.155.1	182.27.155.15	182.27.155.16	182.27.155.17	182.27.155.1/24	GERENCIA TMP	Nic 8	1000 Mbps	Vswitch9
eth7	VLAN157	182.27.157.1	182.27.157.15	182.27.157.16	182.27.157.17	182.27.157.1/24	AUTORIZACIONES	Nic 7	1000 Mbps	Vswitch8

Fuente: Autor

Tabla 3. 18: Detalle de configuración de interfaces Firewall Oficina

VMWARE SERVER (VM FW OFCINA MATRIZ)									
VLAN	**IF Firewall**	**FWOficina**	**FWOficina01**	**FWOficina02**	**RED**	**DESCRIPCION**	**VMWare (Nic Fisica)**	**Velocidad**	**VMSwitch**
VLAN17	ETH0		182.27.17.14	182.27.17.15	182.27.17.0/24	Heartbeat	Nic 2	1000 Mbps	Vswitch2
VLAN155	ETH1	182.27.155.1	182.27.155.15	182.27.155.16	182.27.155.1/24	GERENCIA TMP	Nic 3	1000 Mbps	Vswitch3
VLAN 218	ETH2	182.27.218.1	182.27.218.2	182.27.218.3	182.27.218.0/24	RESPALDO Y OFUSCACION	Nic 4	10 Gbps	Vswitch4
VLAN40	ETH2	182.27.114.14	182.27.114.15	182.27.114.16	182.27.114.14/24	SENTINEL	Nic 4	10 Gbps	Vswitch4
VLAN 221	ETH2	182.27.221.1	182.27.221.2	182.27.221.3	182.27.221.0/24	CDC-CDP	Nic 4	10 Gbps	Vswitch4
VLAN113	ETH3	182.27.113.1	182.27.113.14	182.27.113.15	182.27.113.1/24	PREPRODUCCION-AUTORIZACIONES	Nic 5	10 Gbps	Vswitch5
VLAN 219	ETH3	182.27.219.1	182.27.219.2	182.27.219.3	182.27.219.0/24	INTERCAMBIO DESARROLLO	Nic 5	10 Gbps	Vswitch5
VLAN 201	ETH4	182.30.2.1	182.30.2.2	182.30.2.3	182.30.2.0/24	ADMINISTRACION EQUIPOS	Nic 6	10 Gbps	Vswitch6
VLAN25	ETH5	182.27.131.1	182.27.131.14	182.27.131.16	182.27.131.1/24	USUARIOS_AVANZADOS	Nic 7	10 Gbps	Vswitch7
VLAN 220	ETH6	182.27.220.1	182.27.220.2	182.27.220.3	182.27.220.0/24	CAMARAS	Nic 8	10 Gbps	Vswitch8
VLAN30	ETH7	10.121.85.15	10.121.85.16	10.121.85.17	10.121.85.0/24	CONEXIÓN FW ODISEA	Nic 9	10 Gbps	Vswitch9
VLAN24	ETH8	182.27.160.24	182.27.160.25	182.27.160.26	182.27.160.0/24	interconexion Desarrollo	Nic 10	10 Gbps	Vswitch10
VLAN217	ETH9	182.27.217.1	182.27.217.2	182.27.217.3	182.27.217.0/24	PROTECCION	Nic 11	10 Gbps	Vswitch11

Fuente: Autor

CONCLUSIONES

El presente trabajo de titulación propone el diseño e implementación de buenas prácticas y procedimientos de verificación de seguridad informática aplicada al sistema LAN/WAN para la migración a Datacenter alterno de Credimatic, donde se evaluó la arquitectura para realizar ingeniería de tráfico, estableciendo su viabilidad en un periodo de mediano a largo plazo, esto debido a la estructura organizacional.

Para poder definir el diseño se necesitó dimensionar la nueva solución teniendo en cuenta una holgura en cuanto a crecimiento facilitando la realización de la configuración específica de cada uno de los componentes en cuanto a comunicación se refiere.

Todos los componentes de la solución deben cumplir las normas de Seguridad de Datos de la Industria de Tarjetas de Pago PCI DSS, los cuales están amparados en la versión 3.2.1 vigente desde mayo de 2018, estas actividades se contemplaron en el cronograma de trabajo, esta norma indica 12 requisitos que deben cumplirse para una institución procesadora de tarjetas.

La propuesta se enfoca en diseñar una red jerárquica permitiendo agrupar equipos con funciones específicas, separándolo en tres niveles para facilitar el diseño, la implementación y mantenimiento de la red, que se traduce en una red más confiable y escalable. Se reutilizaron las VLANs de producción para impactar en menor escala la afectación y configuración de los servicios principales a nivel interno y externo. Cabe indicar que el proceso estará bajo políticas de seguridad con las listas de control de acceso y asegurando los puertos de los Switches de Acceso para cualquier intruso que intente acceder a la red.

Finalmente, se establece que al ejecutar el presente proyecto con enfoque Ethernet, representará el uso de tecnología de área local más extendida actualmente ya que combina fácil administración e implementación, costos relativamente bajos y velocidad, permitiendo un mayor aprovechamiento de ancho de banda disponible en la red.

RECOMENDACIONES

Mantener el control de las actividades de trabajo mediante indicadores de gestión.

Potenciar las capacidades del personal con inducción frecuente.

Efectuar reuniones periódicas que permitan prevenir problemas futuros.

Incentivar al personal, pieza clave para crear compromiso y lealtad a la empresa.

Mantener controles permanentes para mantener la estabilidad y confiabilidad del sistema propuesto, generando mantenimientos periódicos, actualizaciones de parches de seguridad para corregir o mitigar vulnerabilidades.

BIBLIOGRAFÍA

Alcoba, J. (2011). *NAT (Network Address Translation): Qué es y cómo funciona.* Obtenido de xataka movil: https://www.xatakamovil.com/conectividad/nat-network-address-translation-que-es-y-como-funciona

Barbosa, R. (2016). *EtherChannel o Link aggregation – Uniendo ancho de banda*. Obtenido de Sea CCNA: https://seaccna.com/etherchannel-link-aggregation/

Blockbit. (2019). *¿Qué es alta disponibilidad?* Obtenido de https://www.blockbit.com/es/blog/que-es-alta-disponibilidad/

Checkpoint. (2019). *Checkpoint Documentation.* Obtenido de Gaia R80.20 Administration Guide: https://sc1.checkpoint.com/documents/R80.20_GA/WebAdminGuides/EN/CP_R80.20_Gaia_AdminGuide/html_frameset.htm

Checkpoint. (2019). *R80.20 mgmt VM in VMware*. Obtenido de https://community.checkpoint.com/t5/General-Management-Topics/R80-20-mgmt-VM-in-VMware/td-p/46915

Check Point Software Technologies Ltd. (2013). *Introduction to ClusterXL*. Obtenido de ClusterXL Gateway Cluster Solution: https://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/index.html

ESET. (2020). *Firewall.* Obtenido de ESET: https://www.eset.com/es/caracteristicas/firewall/#

Giorgi, A. (2014). *Especialistas en Virtualización VMware y Formación Oficial VMware y OpenStack*. Obtenido de https://www.josemariagonzalez.es/vmware-nsx/conceptos-fundamentales-de-vmware-nsx.html

HdezF, G. (2019). *Cuál es la diferencia entre los procolos de capa 2 LACP y PagP*. Obtenido de Comunidad Huawei Enterprise: https://forum.huawei.com/enterprise/es/cu%C3%A1l-es-la-diferencia-entre-los-procolos-de-capa-2-lacp-y-pagp/thread/559641-100237#:~:text=LACP%2C%20conocido%20como%20Link%20Aggregation,dispositivos%20de%20los%20diferentes%20proveedores.

Huidobro, J., & Millán, R. (2002). *Que es MPLS (MultiProtocol Label Switching).* Obtenido de Ramón Millan : https://www.ramonmillan.com/tutoriales/mpls.php

ID Group. (2020). *Qué es un Firewall y cómo funciona?* Obtenido de https://idgrup.com/firewall-que-es-y-como-

funciona/#:~:text=Un%20firewall%2C%20tambi%C3%A9n%20llamado%20cortafuegos,ordenadores%20de%20una%20misma%20red.

Jiménez, J. (2020). *Qué es NAT y cómo actúa en nuestra red.* Obtenido de RZ redes zone: https://www.redeszone.net/tutoriales/redes-cable/que-es-nat-red/

LP, H. P. (2020). *HP E8212 zl Switch Base System - How to Configure LACP Passive Mode*. Obtenido de https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-c02933349

Reyna, B. (2013). *Topologías de red. Introducción a las ciencias computacionales*. Obtenido de Universidad Autónoma de Coahuila: http://sistemas.paec.uadec.mx/courses/670162A/document/SegundoParcial/Topologias_de_Red.pdf

Ruostemaa, J. (2020). *How to install HAProxy load balancer on CentOS*. Obtenido de https://upcloud.com/community/tutorials/haproxy-load-balancer-centos/

soporte, H. P. (2020). *HP 5830 Switch Series - Aggregation Configuration Examples*. Obtenido de https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=c03152927

soporte, H. P. (2020). *HP 5830 Switch Series - Configuring an Aggregate Interface*. Obtenido de https://support.hpe.com/hpesc/public/docDisplay?docId=c03152925&docLocale=en_US

Standard, P. C. (2018). *PCI DSS Quick Reference Guide*. Obtenido de https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

Suárez, M. (2020). *RSTP: Conceptos.* Obtenido de CCNA desde cero: https://ccnadesdecero.com/curso/rstp/

Tapasco, M. (2008). *MPLS, El Presente de las Redes IP. .* Obtenido de Universidad Tecológica de Pereira: https://core.ac.uk/download/pdf/71395663.pdf

VMWARE. (2020). *Virtualización.* Obtenido de vmware: https://www.vmware.com/latam/solutions/virtualization.html

Walton, A. (2018). *Diseño Jerárquico de Redes*. Obtenido de CNNA desde cero: https://ccnadesdecero.es/diseno-jerarquico-de-redes/

GLOSARIO DE TÉRMINOS

BACKBONE: Se refiere a las principales conexiones troncales de Internet. Está compuesta por enrutadores comerciales, gubernamentales de gran capacidad interconectados que llevan los datos a través de países, continentes y océanos del mundo mediante cables de fibra óptica.

BGP: Border Gateway Protocol: Protocolo de gateway fronterizo

CE: Customer Edge: Router de cliente

CN: Customer Network: Red cliente

CoS: Quality of Service: Calidad de Servicio

DSL: Digital Subscriber Line: Línea de Abonado Digital.

EIGRP: Enhanced Interior Gateway Routing Protocol: Protocolo de enrutamiento de gateway interior mejorado

ETHERNET: Estándar de redes de área local para computadores con acceso al medio por detección de la portadora con detección de colisiones

FEC: Forward Error Correction: Corrección de errores

FIB: Forwarding information base: Base de información de envío

FIFO: First In First Out que indica que las posiciones se cierran en el orden que fueron abiertas**.**

FO: Fiber optic: Fibra Óptica.

IEEE: Institute of Electrical and Electronics Engineers: Instituto de ingenieros eléctricos y electrónicos

IETF: Internet Engineering Task Force: Grupo de trabajo de Ingeniería de Internet IGP Interior Gateway Protocol: Protocolo de pasarela interno

IOS: Internetwork Operating System: es el software utilizado en los enrutadores y switches IP Internet Protocol: Protocolo de Internet.

IPSEC: Internet Protocol security es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando cada paquete en un flujo de datos**.**

IPV6: Internet Protocol versión 6: Protocolo de Internet versión 6, es una versión del protocolo Internet Protocol (IP) y diseñada para reemplazar a Internet Protocol versión 4 (IPv4)

IS-IS: Intermediate System to Intermediate System: Sistema intermedio a Sistema intermedio

ISP: Internet service Provider: Proveedor de servicios de Internet

ITU: Internacional Telecommunications Unión: Unión Internacional de Telecomunicaciones.

L2TP: Layer 2 Tunneling Protocol: Protocolo de túnel de capa 2

LAN: Local Area Network: Red de Área Local.

LDP: Label Distribution Protocol: Protocolo de Distribución de Etiquetas

LER: Label Edge Router - Enrutadores de Etiquetas de Borde

LFIB: Label Forwarding Instance Base: Base de información de envío de etiquetas

LIB: Label Information Base: Base de información de etiquetas

LSP: Label Switched Path: Caminos conmutados mediante etiquetas

LSR: Label Switching Router - Enrutadores Conmutadores de Etiquetas

MAC: Media Access Control: Control de Acceso al Medio.

MAN Metropolitan Área Network: Red de Área Metropolitana.

MPLS: Multiprotocol Label Switching: Conmutación Multi-Protocolo mediante Etiquetas 88

MULTICAST: Método para transmitir datagramas IP a un grupo de receptores interesados.

OSI: Open Systems Interconnection: Interconexión de Sistemas Abiertos.

OSPF: Open Shortest Path First: El camino más corto primero

PDU: Packet data unit: Unidad de datos de protocolo se utilizan para el intercambio de datos entre unidades disparejas, dentro de una capa del modelo OSI.

PE: Provider Edge: Router de proveedor PHP Remoción en el penúltimo salto

POP: Es una operación donde la etiqueta es retirada del paquete lo cual puede revelar una etiqueta interior.

PPP: Point-to-point Protocol: Protocolo punto a punto

PPTP: Point-To-Point Tunneling Protocol: Protocolo punto a punto de túnel

PUSH: Es una operación de aplicar nueva etiqueta la que es empujada encima de otra si existe.

RAS: Servidor de acceso remoto, se utiliza para conectarse a las LAN o WAN mediante internet, modem, vpn.

RDSI: Integrated Services Digital Networks: Red Digital de Servicios Integrados **RFC:** Request For Comments: Petición de comentarios

RIB: Routing Information Base: Base de información de ruteo

RIP: Routing Information Protocol: Protocolo de Información de enrutamiento

ROUTER: Es un dispositivo que proporciona conectividad a nivel de red en el modelo OSI, su función principal consiste en encaminar paquetes de datos de una red a otra

RSVP: Resource Reservation Protocol: Protocolo de reserva de recursos

SA: Autonomous System: Sistema Autónomo, es definido como un grupo de redes IP que poseen una política de rutas propia e independiente

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Zambrano Herrera Alex Daniel**, con C.C: # **0924215296** autor/a del trabajo de titulación: **Diseño e implementación de buenas prácticas y procedimientos de verificación de seguridad informática aplicada al sistema LAN/WAN para la Migración a Datacenter alterno de Credimatic,** previo a la obtención del título de **Magíster en Telecomunicaciones** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, a los 21 días del mes de junio del 2021

Zambrano Herrera Alex Daniel

C.C: 0924215296

Presidencia de la República del Ecuador

Plan Nacional de Ciencia, Tecnología, Innovación y Saberes

SENESCYT
Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TÍTULO Y SUBTÍTULO:	Diseño e implementación de buenas prácticas y procedimientos de verificación de seguridad informática aplicada al sistema LAN/WAN para la Migración a Datacenter alterno de Credimatic.	
AUTOR(ES)	Zambrano Herrera Alex Daniel	
REVISOR(ES)/TUTOR	MSc. Edgar Quezada Calle; MSc. Luis Córdova Rivadeneira / MSc. Manuel Romero Paz	
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil	
FACULTAD:	Sistema de Posgrado	
PROGRAMA:	Maestría en Telecomunicaciones	
TITULO OBTENIDO:	Magister en Telecomunicaciones	
FECHA DE PUBLICACIÓN:	**Guayaquil, a los 21 días del mes de junio del 2021**	**No. DE PÁGINAS: 80**
ÁREAS TEMÁTICAS:	Topología de Red, Diseño de las LAN, diseño jerárquico, Protocolos, RSTP, MPLS	
PALABRAS CLAVES/ KEYWORDS:	convergencia, alta disponibilidad, tiempos de respuesta, integración, escalabilidad, seguridad	

RESUMEN/ABSTRACT: En el presente trabajo de investigación se realiza un análisis del estado actual de los componentes de red la cual deriva en un dimensionamiento y con esto proponer una posible solución a la problemática que la empresa está atravesando en estos momentos que conlleven a una mejora a nivel global de las comunicaciones externas e internas, con el fin de otorgar un mejor servicio tanto a los clientes internos como a los externos, se evalúa una solución convergente a todo nivel, que les permita otorgar niveles de disponibilidad de un 99.9%, que se acoplen a las siguientes características: cumplimiento de la Norma PCI, equipos con soporte y actualizaciones por 5 años, cableado estructurado certificado con soporte a 10 años, descongestión de backbone de red y capacidades que permitan el normal funcionamiento por los próximos 5 años, simplicidad en la administración de la red que conlleva a que la topología se simplifique, reduce el tiempo de resolución de problemas, abarata los costos de futuras implementaciones de sistemas de seguridad y permite una adaptación a cambios más eficiente, facilidad de integración o crecimiento con nuevos clientes, trasladando el centro de cómputo se podrá diseñar un sistema de interconexión a través de fibra óptica sostenible y permitirá la integración con nuevos clientes y asociados.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO AUTOR/ES:	**Teléfono:** +593- 988770681	**E-mail:** azambranoh85@gmail.com
CONTACTO CON LA INSTITUCIÓN (COORDINADOR DEL PROCESO UTE):	**Nombre:** Romero Paz Manuel de Jesús	
	Teléfono: +593-994606932	
	E-mail: manuel.romero@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	