**PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR**

**FACULTAD DE INGENIERÍA**

**MAESTRÍA EN REDES DE COMUNICACIÓN**

# "DISEÑO E IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA DE RED PARA UN DATACENTER ALTERNO COMO SITIO DE RECUPERACIÓN ANTE DESASTRES, PARA UNA ENTIDAD PRIVADA"

**Informe final caso de estudio previo la obtencion del título de:**

**Magíster en Redes de Comunicaciones**

**DAVID FERNANDO SILVA VIZCARRA**

**Quito – Octubre 2017**

# Autoría

Yo, David Fernando Silva Vizcarra, portador de la cédula de ciudadanía No.1716457328, declaro bajo juramento que la presente investigación es de total responsabilidad del autor, y que se he respetado las diferentes fuentes de información realizando las citas correspondientes. Esta investigación no contiene plagio alguno y es resultado de un trabajo serio desarrollado en su totalidad por mi persona.

_____

DAVID FERNANDO SILVA VIZCARRA

# Contenido


**1. INTRODUCCIÓN ..... 11**

**2. JUSTIFICACIÓN ..... 13**

**3. ANTECEDENTES ..... 14**

**4. OBJETIVOS ..... 16**

**5. DESARROLLO CASO DE ESTUDIO ..... 17**

5.1. ANÁLISIS DE LA INFRAESTRUCTURA ACTUAL DEL DATACENTER PRINCIPAL ..... 17

*5.1.1. Desafíos en la Red ..... 17*

*5.1.2. Marco de Evaluación de la Infraestructura de Red ..... 19*

*5.1.3. Estado Actual de la Red ..... 20*

*5.1.3.1. Capa Core del Datacenter Principal ..... 23*

*5.1.3.1.1. Características Nexus 7009. ..... 25*

*5.1.3.1.2. Análisis consumo CPU, Memoria. ..... 27*

*5.1.3.2. Capa Agregación y Acceso del Datacenter Principal. ..... 28*

*5.1.3.2.1. Características Nexus 5548 ..... 30*

*5.1.3.2.2. Características Extensores Nexus 2000 ..... 32*

*5.1.3.2.3. Análisis consumo CPU, Memoria ..... 33*

*5.1.3.3. Componentes de Seguridad de la Red del DCP. ..... 34*

*5.1.3.3.1. Características Firewall. ..... 34*

*5.1.3.3.2. Características IPS ..... 37*

*5.1.3.3.3. Características DDoS ..... 38*

*5.1.3.3.4. Análisis de la infraestructura de Seguridad ..... 41*

*5.1.3.3.5. Características Balanceador de Carga F5 ..... 42*

5.2. DISEÑO DEL MODELO DE RED A IMPLEMENTAR EN EL DATACENTER ALTERNO 45

*5.2.1. Capa Core DCA ..... 47*

***5.2.1.1. Características Cisco Nexus 7700 ..... 48***

*5.2.2. Capa Agregación DCA ..... 51*

*5.2.3. Capa Acceso DCA ..... 54*

***5.2.3.1. Características Cisco 9372*** ..... 55

***5.2.3.2. Características Cisco 2248*** ..... 57

*5.2.4. Diseño de la Zona de DMZ ..... 59*

*5.2.5. Diseño de la Zona de Administración Fuera de Banda (Out-of-Band) ..... 61*

***5.2.5.1. Características Switch 2960X*** ..... 62

*5.2.6. Diseño de la zona de entrada/salida hacia Internet. ..... 63*

***5.2.6.1. Características Routers ISR 4431*** ..... 64

***5.2.6.2. Características Switches Cisco 3548*** ..... 65

*5.2.7. Diseño de la zona de Acceso de Terceros. ..... 66*

***5.2.7.1. Características Cisco ASR 1006*** ..... 68

***5.2.7.2. Características Cisco 4500X*** ..... 70

*5.2.8. Diseño de la arquitectura para implementación de Dispositivos de Seguridad en el DCA . ..... 72*

***5.2.8.1. Diseño Equipamiento de Seguridad Anti DDoS*** ..... 73

*5.2.8.2. Diseño Equipamiento de Seguridad IPS* ..... 81

*5.2.9. Diseño de la arquitectura para Firewalls ..... 90*

***5.2.9.1. Firewall Borde*** ..... 92

***5.2.9.2. Firewall Terceros*** ..... 95

***5.2.9.3. Firewall Principal*** ..... 97

***5.2.9.4. Características Firewall CheckPoint*** ..... 100

***5.2.9.5. Configuración Políticas de seguridad Firewall CheckPoint*** ..... 104

*5.2.10. Diseño de la arquitectura para Equipamiento F5 ..... 105*

***5.2.10.1. Características equipamiento F5*** ..... 107

***5.2.10.2. Funcionalidad del LTM F5*** ..... 108

***5.2.10.3. Funcionalidad del GTM F5*** ..... 111

*5.2.11. Dispositivos de Red considerados en el Diseño del Datacenter Alterno ..... 112*

*5.2.12. Cableado Requerido Equipos de Red en el Datacenter Alterno ..... 114*

5.3. CONFIGURACIONES DE EQUIPOS DE RED EN EL DATACENTER ALTERNO ..... 117

*5.3.1. Configuraciones Iniciales de los equipos de Red ..... 117*

*5.3.2. Configuración de Spanning Tree ..... 119*

*5.3.3. Configuración de VLANs ..... 119*

*5.3.4. Configuración de PortChannels y VPCs ..... 119*

*5.3.5. Configuración de Puertos Troncales y de Acceso. ..... 120*

*5.3.6. Configuración del enrutamiento ..... 120*

*5.3.7. Configuración de Túneles ..... 121*

*5.3.8. Configuración HSRP ..... 121*

*5.3.9. Configuración PBR ..... 122*

5.4. INTERCONEXIÓN DEL DATACENTER PRINCIPAL CON EL DATACENTER ALTERNO 124

*5.4.1. Características equipos de Interconexión de Datacenters ..... 129*

***5.4.1.1. Dispositivo de Encripción PL 1000 TE*** ..... 129

***5.4.1.2. Switch Óptico CTCFRM220*** ..... 130

***5.4.1.3. Dispositivo de Transporte PL 2000*** ..... 132

*5.4.2. Configuración en Equipos de Core para la Interconexión DC ..... 135*

*5.4.3. Diagrama del Diseño para la Interconexión de los Datacenters ..... 140*

5.5. PLAN PARA LA RECUPERACIÓN DE DESASTRE DE IT ..... 141

*5.5.1. Introducción ..... 141*

***5.5.1.1. Objetivo*** ..... 141

***5.5.1.2. Supuestos*** ..... 142

***5.5.1.3. Alcance*** ..... 143

***5.5.1.4. Responsabilidades de equipo de recuperación*** ..... 143

***5.5.1.5. Respaldo*** ..... 143

*5.5.2. Gestión de Crisis ..... 144*

***5.5.2.1. Identificación del evento*** ..... 144

***5.5.2.2. Centro de Gestión de Crisis (CMC)*** ..... 144

***5.5.2.3. Convocatoria de BCP*** ..... 145

***5.5.2.4. Roles y responsabilidades del Equipo de Recuperación*** ..... 145

*5.5.3. Procedimiento de Recuperación de Desastres - Fail over. ..... 147*

5.5.3.1. Plan de reubicación del personal ..... 147

***5.5.3.2. Pasos de Recuperación Común*** ..... 147

*5.5.4. Procedimiento de Recuperación de Desastres – Retorno a la normalidad ..... 149*

***5.5.4.1. Procedimiento Switch-Back*** ..... 149

*5.5.5. Lista de verificación de Recuperación ..... 150*

*5.5.6. Registro de recuperación y Mejora Continua ..... 152*

***5.5.6.1. Resultado de los parámetros de recuperación archivados*** ..... 152

***5.5.6.2. Mejora continua*** ..... 153

5.6. CONCLUSIONES Y RECOMENDACIONES ..... 154

BIBLIOGRAFÍA: ..... 158

# Índice de Figuras

*Figura 1.* Diagrama Red Actual de la Empresa ..... 21
*Figura 2.* Conexión LAN DCP ..... 22
*Figura 3.* Conexión Lógica VDCs ..... 24
*Figura 4.* Cisco Nexus 7000 Series ..... 26
*Figura 5.* Conexiones Capa Agregación - Acceso (Cisco 5548 y Cisco 2000) ..... 29
*Figura 6.* Conexiones DMZ ..... 29
*Figura 7.* Cisco Nexus 5548UP Switch ..... 30
*Figura 8.* Cisco Nexus 2000 Series ..... 32
*Figura 9.* Conexiones de las 3 zonas de Firewall ..... 35
*Figura 10.* Conexiones Equipo Anti-DDoS ..... 40
*Figura 11.* Conexiones Equipo F5 ..... 43
*Figura 12.* Arquitectura de Red Propuesta para DCA ..... 46
*Figura 13.* Conexiones Capa Core DCA ..... 48
*Figura 14.* Cisco Nexus 7700 ..... 49
*Figura 15.* Conexiones Capa Agregación DCA ..... 53
*Figura 16.* Conexiones Capa Acceso DCA ..... 55
*Figura 17.* Cisco Nexus 9372PX Switch ..... 56
*Figura 18.* Cisco Nexus N2248PQ ..... 58
*Figura 19.* Arquitectura Zona DMZ ..... 60
*Figura 20.* Arquitectura Zona de Administración Fuera de Banda ..... 62
*Figura 21.* Arquitectura Zona para la Salida de Internet ..... 64
*Figura 22.* Arquitectura Zona de Acceso de Terceros ..... 67
*Figura 23.* Cisco ASR1006 ..... 69
*Figura 24.* Cisco 4500X ..... 71
*Figura 25.* Arquitectura Equipo Anti-DDoS ..... 75
*Figura 26.* Conexión IPS – VDC ..... 82
*Figura 27.* Conexión IPS Internet y DMZ ..... 83
*Figura 28.* Conexión IPS – Terceros ..... 83
*Figura 29.* Equipo IPS HP Tipping Point ..... 87
*Figura 30.* Consola Administración HP SMS ..... 89
*Figura 31.* Consola Administración Firewall ..... 92
*Figura 32.* Ubicación Lógica del Firewall Borde ..... 92
*Figura 33.* Conexiones Lógicas del Firewall Borde ..... 93
*Figura 34.* Conexiones Físicas del Firewall Borde ..... 94
*Figura 35.* Ubicación Lógica del Firewall Terceros ..... 95
*Figura 36.* Conexiones Lógicas del Firewall Terceros ..... 96
*Figura 37.* Conexiones Físicas del Firewall Terceros ..... 96
*Figura 38.* Ubicación Lógica del Firewall Principal ..... 98
*Figura 39.* Conexiones Lógicas del Firewall Principal ..... 98
*Figura 40.* Conexiones Físicas del Firewall Principal ..... 99
*Figura 41.* Mapa de los reléase de software para Checkpoint ..... 101
*Figura 42.* Conexiones de los Modulo GTM y LTM del F5 en el DCA ..... 106
*Figura 43.* Equipo BIG IP - F5 ..... 107
*Figura 44.* Conexiones LTM F5 ..... 110
*Figura 45.* Esquema de Conexión de GTM para redundancia de Datacenters ..... 112
*Figura 46.* Ubicación en los Racks Equipos de Red Fila B ..... 113

*Figura 47.* Ubicación en los Racks Equipos de Red Fila A.....114
*Figura 48.* Diagrama de Bloque Interconexión Datacenters .....126
*Figura 49.* Diagrama Lógico de la Interconexión Datacenters.....127
*Figura 50.* Diagrama Conexiones Físicas dispositivos de la Interconexión Datacenters.....128
*Figura 51.* Dispositivo de Encripción PL 1000 TE .....130
*Figura 52.* Dispositivo Switch Óptico FRM220.....131
*Figura 53.* Dispositivo Trasportador PL2000.....132
*Figura 54.* Agregación de servicios en el equipo PL 2000.....133
*Figura 55.* Diseño de red de la Interconexión de Datacenters.....140

# Índice de Tablas


Tabla 1 *Cantidad de Dispositivos de Red, Seguridad en el DCP* ..... 22
Tabla 2 *Cantidad Equipos Core DCP* ..... 25
Tabla 3 *Especificaciones Técnicas Cisco Nexus 7009* ..... 26
Tabla 4 *Consumo Promedio de CPU y Memoria, Equipos Core* ..... 27
Tabla 5 *Cantidad Equipos Capa Agregacion, Acceso y DMZ* ..... 30
Tabla 6 *Características técnicas equipos Cisco Nexus 5548* ..... 30
Tabla 7 *Consumo Promedio de CPU y Memoria, Equipos Agregación - Acceso* ..... 33
Tabla 8 *Cantidad Equipos Firewall en DCP* ..... 35
Tabla 9 *Características Técnicas Firewall Checkpoint* ..... 36
Tabla 10 *Cantidad de equipos IPS* ..... 37
Tabla 11 *Características Técnicas IPS Tipping Point* ..... 37
Tabla 12 *Cantidad de equipos IPS* ..... 40
Tabla 13 *Características Técnicas Anti DDoS* ..... 41
Tabla 14 *Cantidad de Equipo F5 en DCP* ..... 43
Tabla 15 *Características F5 - LTM* ..... 44
Tabla 16 *Cantidad Equipos Capa Core* ..... 48
Tabla 17 *Características Técnicas Cisco Nexus 7710* ..... 50
Tabla 18 *Criterios para la Agrupación de los Aplicativos en VDCs* ..... 51
Tabla 19 *Asignación de Interfaces del Cisco 7710 a las VDCs* ..... 53
Tabla 20 *Cantidad Equipos Capa Acceso* ..... 55
Tabla 21 *Especificaciones Técnicas Cisco Nexus 9372* ..... 56
Tabla 22 *Especificaciones adicionales Cisco Nexus 9372* ..... 57
Tabla 23 *Especificaciones Técnicas Cisco Nexus 2248* ..... 58
Tabla 24 *Criterios Categorización DMZ* ..... 59
Tabla 25 *Cantidad Equipos Capa Acceso* ..... 61
Tabla 26 *Cantidad Equipos zona Administración fuera de Banda.* ..... 62
Tabla 27 *Cantidad Equipos Interconexión hacia Internet* ..... 64
Tabla 28 *Especificaciones Técnicas Cisco ISR 4431* ..... 65
Tabla 29 *Especificaciones técnicas Switch Cisco 3548* ..... 66
Tabla 30 *Cantidad Equipos Conexión Acceso Terceros* ..... 67
Tabla 31 *Especificaciones Técnicas Cisco ASR 1006* ..... 69
Tabla 32 *Especificaciones Técnicas Cisco 4500X* ..... 71
Tabla 33 *Cantidad Equipos Anti-DDoS* ..... 75
Tabla 34 *Especificaciones técnicas equipo Anti-DDos Radware* ..... 77
Tabla 35 *Principales servicios dentro de la Infraestructura del DCA* ..... 79
Tabla 36 *Tabla de Políticas a implementar en Equipo Anti-DDoS* ..... 80
Tabla 37 *Detalle de los módulos habilitados* ..... 81
Tabla 38 *Distribución Interfaces Equipos IPS* ..... 84
Tabla 39 *Cantidad Equipos IPS* ..... 84
Tabla 40 *Especificaciones técnicas IPS Tipping Point* ..... 87
Tabla 41 *Especificaciones técnicas Consola Administración Tipping Point* ..... 89
Tabla 42 *Zonas a Proteger con los Firewalls en DCA* ..... 90
Tabla 43 *Detalle de Firewalls en el DCA* ..... 91
Tabla 44 *Interfaces Firewall Borde* ..... 94
Tabla 45 *Interfaces Firewall Terceros* ..... 97
Tabla 46 *Interfaces Firewall Principal* ..... 99
Tabla 47 *Especificaciones Hardware para Servidores Firewall* ..... 100
Tabla 48 *Equipamiento F5 en el DCA* ..... 106

Tabla 49 *Especificaciones Técnicas equipo F5 5250v* .....107
Tabla 50 *Nomenclatura, Posición de Equipos de Red a implementar en el DCA*.....112
Tabla 51 *Cableado Necesario Para la Conexión de los Equipos de Red en el DCA* 114
Tabla 52 *Configuraciones a aplicar en los equipos de Red*.....117
Tabla 53 *Configuraciones de acceso a los equipos de Red* .....118
Tabla 54 *Funcionalidades a configurar en los equipos*.....119
Tabla 55 *Equipos de Interconexión de los Datacenters*.....125
Tabla 56 *Cantidad Equipos de Interconexión de los Datacenters*.....125
Tabla 57 *Conexiones Físicas Equipos de Interconexión de los Datacenters* .....127
Tabla 58 *Especificaciones Técnicas equipo PL 2000* .....134
Tabla 59 *Plan de Reubicación del Personal* .....147
Tabla 60 *Registro de Recuperación* .....152
Tabla 61 *Resultado de los Parámetros de Recuperación* .....152
Tabla 62 *Cuadro de Mejora Continua* .....153

# 1. INTRODUCCIÓN

El presente trabajo trata sobre el análisis, diseño e implementación de un Datacenter Alterno para una institución financiera. Debido a la criticidad de las aplicaciones de hoy en día las instituciones no pueden darse el lujo de perder información o de paralizar sus negocios debido a un imprevisto en su centro de Datos, por lo cual se crea la necesidad de poseer un Datacenter Alterno al Principal.

La institución busca implementar una arquitectura de alta disponibilidad para su centro de datos principal, localizado en Quito, Ecuador y a su vez tener un nuevo sitio para Recuperación de Desastres Informáticos. Se pretende replicar la infraestructura de Red de su Centro de Datos Principal considerando las mejores prácticas, optimizando y mejorando el diseño actual.

Para lograr los objetivos planteados se realizará un análisis de la infraestructura de red actual, lo cual servirá de línea base, de la que se partirá para crear un diseño óptimo para el Datacenter Alterno. Se revisará las características de los equipos actuales y sus configuraciones. El enfoque es analizar los vacíos, desafíos y problemas en la infraestructura. El análisis y la evaluación se llevarán a cabo sobre el conjunto general de Infraestructura de TI con varias dimensiones y atributos claves. Examinando sus posibles fallas en el diseño actual. Luego de lo cual se revisará el diseño objetivo de la red, sus componentes y configuraciones a aplicar.

Adicional a ello se presentará [JF1]el esquema de interconexión entre los Datacenters lo que permitirá mantener una comunicación entre el Centro de Datos Principal y Alterno, con el objetivo primordial de mantener una réplica de sus aplicativos en el Datacenter secundario pensando en una alta disponibilidad de sus operaciones y a su vez en un centro de recuperación ante desastres.

Al final de este caso de estudio se desarrollará [JF2]un documento que presentará de forma general los parámetros de un plan de recuperación de desastres en infraestructura IT.

## 2. JUSTIFICACIÓN

Un Datacenter es un localidad ya sea física o virtual creada para mantener la infraestructura de comunicaciones de una empresa, almacenando gran cantidad de datos con el objeto de tener acceso a la información necesaria para sus operaciones en todo momento. En general la mayoría de las empresas, de gran o mediano tamaño, tienen algún tipo de centro de Datos. (Galván Víctor Gabriel, 2013). Entre los elementos más importantes para su construcción se puede destacar el garantizar la continuidad del servicio a clientes, empleados, ciudadanos, proveedores y empresas filiales, así como a servidores de bases de datos que puedan contener información crítica o a programas que sean vitales para el funcionamiento del negocio.

Empresas Nacionales o Internacionales relacionadas con organismos públicos y privados, necesitan asegurar que su información se mantendrá intacta y sus operaciones no cesarán frente a posibles daños que pueden ocurrir en su Centro de Datos. Fenómenos naturales como terremotos, inundaciones, incendios o ataques a las instalaciones pueden no ser frecuentes, pero tampoco algo imposible, por este motivo, y otros se ve la necesidad de implementar un Datacenter Alterno.

Debido a lo indicado con anterioridad, el objetivo de la entidad es implementar un sitio de recuperación de desastres (sitio de DR) o Data Center Alterno (DCA), de todo el entorno de TI alojado en el Data Center de producción (o Data Center Principal - DCP). Con ello se requiere garantizar que puede recuperar sus procesos de negocio, incluyendo sistemas de TI e infraestructura rápidamente y con una mínima interrupción en una situación de desastre.

# 3. ANTECEDENTES

Debido a la alta demanda y a los procesos críticos que se deben manejar a diario, la institución vio la necesidad de realizar un análisis de los sistemas críticos de TI, con el fin de proveer alta disponibilidad y una solución de continuidad de negocio. Para ello surgió el compromiso de analizar el panorama de TI existente y proporcionar un diseño de alto nivel con alta disponibilidad y una solución de recuperación de desastres.

Para solventar la necesidad de la institución se ha diseñado un plan para la implementación de un sitio de recuperación ante desastres para la empresa el mismo que se ha planificado implementarlo geográficamente en Guayaquil para todo el entorno de TI que actualmente se encuentra alojado en el Data Center de producción en Quito.

Los objetivos que se persiguen satisfacer con el diseño de un Datacenter Alterno son:

- Asegurar la disponibilidad de los sistemas de TI y operaciones críticas de la institución ante eventos de interrupción causados por fuerzas naturales o eventos provocados por el hombre, de manera que las Operaciones de Negocio de la empresa pueda mantenerse o restablecerse en el menor tiempo posible.
- Asegurar la implementación exitosa del entorno de infraestructura en el DCA (Datacenter Alterno) y su interoperabilidad con el DCP (Datacenter Principal).
- Asegurar la implementación exitosa de las aplicaciones de producción en el DCA.
- Reducir el riesgo operacional mediante la creación, implementación y pruebas de la Continuidad de Negocios y Recuperación ante Desastres (BC-DR) y definir los procesos generales de Recuperación ante Desastre para la mejora continua.

Para alcanzar los objetivos plantados, se requiere realizar el análisis, diseño e implementación de la infraestructura de red a implementar en el Datacenter Alterno.

El presente caso de estudio se enfocará en el diseño de la infraestructura de red que se requiere implementar.  Adicional se tendrá  una hoja de ruta para implementar alta disponibilidad y recuperación ante desastres en el ambiente de TI.

# 4. OBJETIVOS

**Objetivo General:**

Diseñar e implementar la infraestructura de red para un Datacenter Alterno como sitio de Recuperación ante Desastres, para una entidad financiera.

**Objetivos Específicos:**

1. Realizar el análisis de la infraestructura actual del Datacenter Principal con el que cuenta la institución, proveyendo información general del diseño actual con el fin de determinar la tecnología a utilizar en el Datacenter Alterno.
2. Diseñar y concluir con un modelo de red a implementar en el Datacenter Alterno, identificando las zonas e infraestructura para su implementación.
3. Identificar las principales configuraciones correspondientes a los equipos de red para brindar conectividad de la red del Datacenter Alterno.
4. Diseñar e implementar la interconexión entre los Datacenter Principal y Datacenter Alterno necesaria para la replicación de datos entre las dos localidades.
5. Presentar un plan general para la recuperación de red ante un desastre de IT

# 5. DESARROLLO CASO DE ESTUDIO

## 5.1. Análisis de la infraestructura actual del Datacenter Principal

En este apartado se realiza el análisis de la infraestructura de red de la Institución así como de los elementos involucrados en la misma. Este análisis se lo elabora a través de varios parámetros a tomar en cuenta, los cuales ayudan a presentar la situación actual en la que se encuentra la red de datos de la empresa.

### 5.1.1. Desafíos en la Red

Los negocios de hoy en día necesitan de un nivel muy distinto de sofisticación de red que el que se aceptaba anteriormente. Las redes comerciales en la era de hoy deben soportar una interacción constante e inmediata, lo cual se ha convertido en una prioridad para la productividad de los empleados. A medida que las aplicaciones evolucionan de centralizadas a interactivas, estas redes deben soportar un tráfico multidireccional. El cambio demanda una infraestructura de red en tiempo real y una restructuración de la red para convertirla en una plataforma comercial estratégica.

A medida que las aplicaciones en tiempo real se vuelven cada vez más vitales para los negocios, los usuarios corporativos necesitan de un acceso ininterrumpido a las redes y una respuesta rápida de las aplicaciones. Además, las nuevas aplicaciones interactivas generan un patrón de tráfico multidireccional que desafía a las antiguas redes estructuradas para aplicaciones cliente-servidor. Como complemento a estos nuevos desarrollos en el panorama corporativo, se están dando a lugar algunos otros cambios:

- *Tiempo de trabajo:* El trabajo se ha redefinido como lo que un empleado hace, en lugar de lo que un empleado es.

- *Toma de decisiones colectivas:* Los negocios deben utilizar todo el conocimiento e información disponibles para tomar las mejores decisiones; el proceso debe ser descentralizado.
- *Uniformidad de ancho de banda entre conexión cableada e inalámbrica*; La institución sigue necesitando una interacción uniforme y multimedia, tanto en su red cableada como inalámbrica para evitar cuellos de botella.
- *Compatible, seguro y "amigable al medioambiente":* En el siglo 21 los negocios deben pensar y actuar globalmente, cumpliendo con las nuevas regulaciones, defendiéndose contra amenazas y sujetándose a normas emergentes de responsabilidad social.
- *Uso óptimo de recursos:* Todos los negocios enfrentan escases de recursos: financieros, de información, de personal, de instalaciones, de distribución y de recursos naturales, o todos los anteriores, y es una prioridad optimizar estos recursos.

El análisis de red se realiza considerando las varias dimensiones de las últimas tendencias, desafíos y vacíos. Se espera que el resultado brinde a la empresa los siguientes beneficios clave:

- Una red totalmente interconectada y a prueba de fallos.
- Red multiservicios altamente disponible, resiliente[1] y escalable.
- Potenciar un negocio fluido las 24 horas del día los 7 días de la semana y las operaciones administrativas en un entorno de red completo y seguro administrado centralmente.

Los puntos destacados clave de la arquitectura de red objetivo recomendada son:

---

[1] Resiliencia: capacidad que se tiene de recuperarse frente a la adversidad

- Resiliencia de red, dispositivo y operacional para una alta disponibilidad en el diseño de la red.
- Infraestructura de red robusta y segura
- Administración y supervisión centralizada de red
- Orientada al futuro para adoptar nuevas tecnologías a medida que se vuelvan necesarias para el negocio

### 5.1.2. Marco de Evaluación de la Infraestructura de Red

La red LAN de la institución tiene un esquema de red mixto en el cual se involucran varios elementos de conectividad, seguridades y elementos de punto final como servidores. Este análisis se ha realizado tomando en cuenta componentes claves que se relacionan con el proceso de diseño de infraestructura y que son:

- *Elementos de red principales*. Los elementos de red principales que se evalúan son topología, enrutamiento, niveles jerárquicos y seguridad de red.
- *Elementos de soporte.* Los elementos de soporte son aquellos que apoyan el diseño de los elementos principales. Disponibilidad alta, conexión inalámbrica, seguridad, capacidad/escalabilidad son algunas de las áreas de elementos de soporte claves.
- *Métricas.* Las métricas son aquellas categorías de medidas que se utilizan para evaluar el desempeño de cualquier red de infraestructura. Las métricas claves son alineación del nivel de servicio (alineación de infraestructura con nivel de servicio), eficiencia operativa (uso eficiente de la infraestructura), pruebas futuras (disponibilidad para cumplir con

exigencias futuras), alineación con la industria (alineación con normas de la industria, etc.)

Del análisis de estos elementos se toma datos diversos que son relevantes al proceso de diseño de red, los cuales proveen el esquema y arquitectura objetiva para la red de infraestructura.

### 5.1.3. Estado Actual de la Red

La infraestructura IT del centro de datos de la institución consiste de varios equipamientos de red y de seguridad como Routers, Switches, firewalls, IPS, DDOS, Balanceadores de carga (F5).

La interconexión de estos equipos permite mantener las operaciones del negocio con fluidez y seguridad.  De forma general a continuación, en la figura 1, se presenta la arquitectura de red actual de la empresa, la misma que se encuentra localizada en la ciudad de Quito, Ecuador.

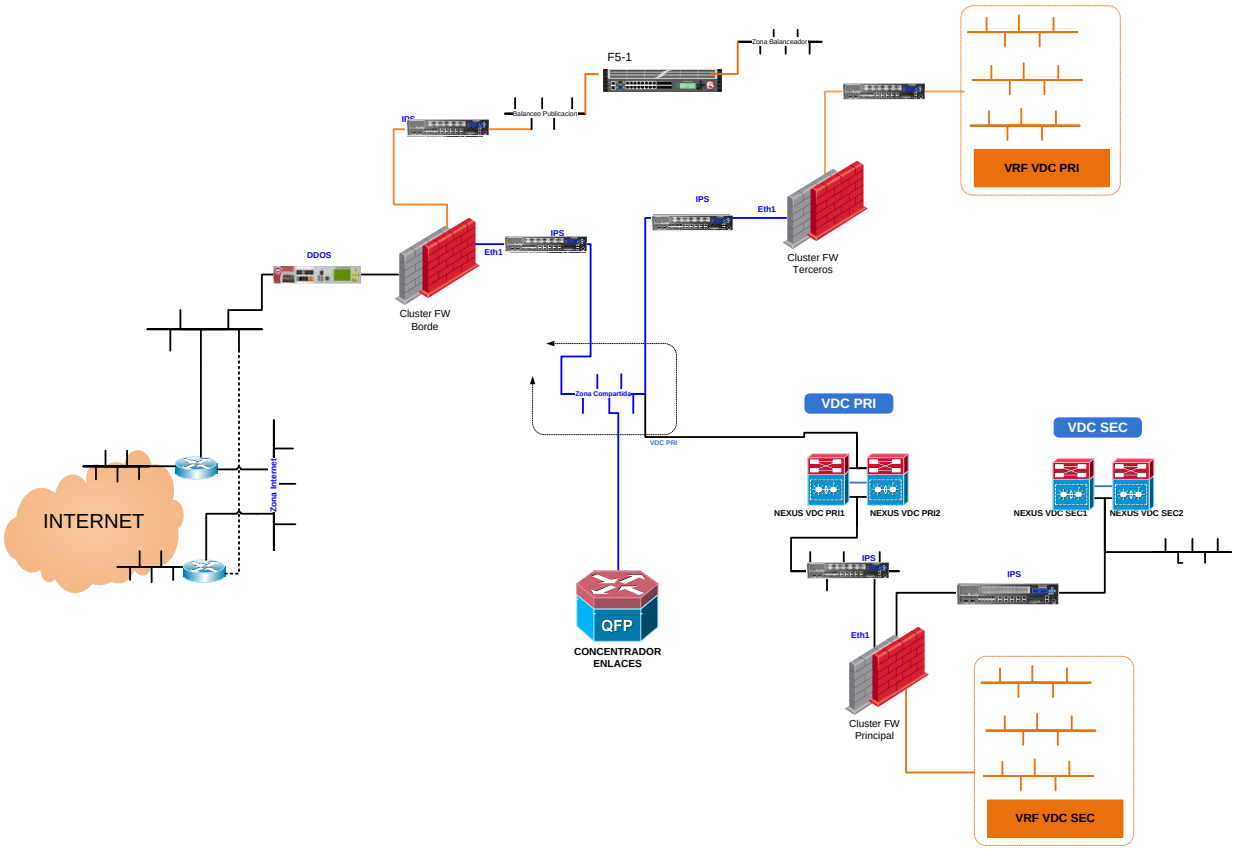


*Figura 1*. Diagrama Red Actual de la Empresa
*Fuente*: Elaboración Propia

A nivel de conectividad LAN los equipos en el DCP manejan el esquema jerárquico de 3 capas de Cisco. Teniendo como Core de la arquitectura a los SW Cisco Nexus 7000 los mismos que se encuentran conectados en un nivel inferior en la capa de agregación y acceso a los switches Cisco Nexus 5000, que estos a su vez en modo de ampliación de puerto utilizan a los Switches Nexus 2000 Extender. En la siguiente figura se representa la conexión a nivel LAN de los equipos de red.

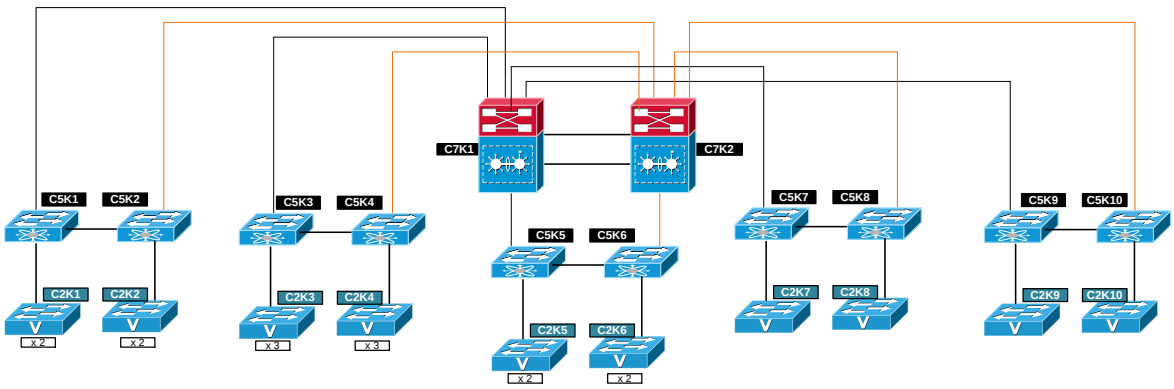


*Figura 2.* Conexión LAN DCP
*Fuente*: Elaboración Propia

En cuanto a la cantidad de componentes de red y seguridad que conforman la arquitectura de red del Datacenter Principal, se la puede observar en la siguiente tabla.

Tabla 1
*Cantidad de Dispositivos de Red, Seguridad en el DCP*

| # | Proveedor | Dispositivos | Ubicación | Cantidad |
|---|---|---|---|---|
| **1** | CISCO | Routers | Centro de Datos Quito | 3 |
| **2** | CISCO | Switch | Centro de Datos Quito | 36 |
| **3** | HP/Checkpoint | Firewall | Centro de Datos Quito | 6 |
| **4** | Radware | DDos | Centro de Datos Quito | 1 |
| **5** | HP | IPS | Centro de Datos Quito | 3 |
| **6** | F5 | Balanceador | Centro de Datos Quito | 2 |

*Fuente*: Elaboración Propia

Basados en la arquitectura de red actual se realizará el análisis de cada uno de sus componentes y tecnología utilizada.

#### 5.1.3.1. *Capa Core del Datacenter Principal*

A nivel de capa de Core, la institución utiliza dos Routers Cisco Nexus 7009, interconectados entre sí, lo que les permite brindar redundancia en las conexiones.

Estos equipos han sido divididos en dos instancias virtuales mediante la tecnología de VDCs.[2]

Un Virtual Device Context se puede utilizar para virtualizar en si el dispositivo, simulando el switch físico como múltiples dispositivos lógicos. Cada VDC puede contener su único e independiente set de VLANs y VRFs. Cada VDC puede estar asignado a interfaces físicas, permitiendo así que el hardware del plano de datos sea virtualizado de igual manera. En cada VDC, se puede gestionar un dominio de administración por separado, permitiendo que el plano de administración pueda ser también virtualizado. (Cisco, 2014, Technical Overview of Virtual Device Context).

El tener dos instancias separadas lógicamente ofrece un número de beneficios en la operación del equipo como aislamiento de fallas, lo que conduce a una mayor disponibilidad. Adicional, el aislamiento de tráfico dentro de la estructura de un VDC conduce a mantener una gran seguridad para la data de los usuarios. Numerosos contextos de Switch dentro de un dispositivo físico pueden ayudar a escalar los recursos del equipo físico a través de múltiples grupos lógicos en una organización. Esto puede guiar a una eficiencia administrativa y un costo operacional bajo.

Los VDCs creados en la infraestructura de Quito son 2: VDC PRI Y VDC SEC. El VDC PRI se creó con el objetivo de agrupar las redes donde se encuentren las aplicaciones de uso común y que soporten los procesos tecnológicos de la empresa, además de proveer una zona común para la interconexión con los dispositivos de Seguridad, específicamente los Firewalls. La VDC SEC agrupa todas las redes que brinden soporte a los procesos operativos

[2] VDC: Virtual Device Context

de la empresa, estas redes son el core de negocio de la empresa. A continuación se muestra la conectividad a nivel lógico donde se representa la separación entre las dos VDCs y su conexión con los equipos de seguridad.

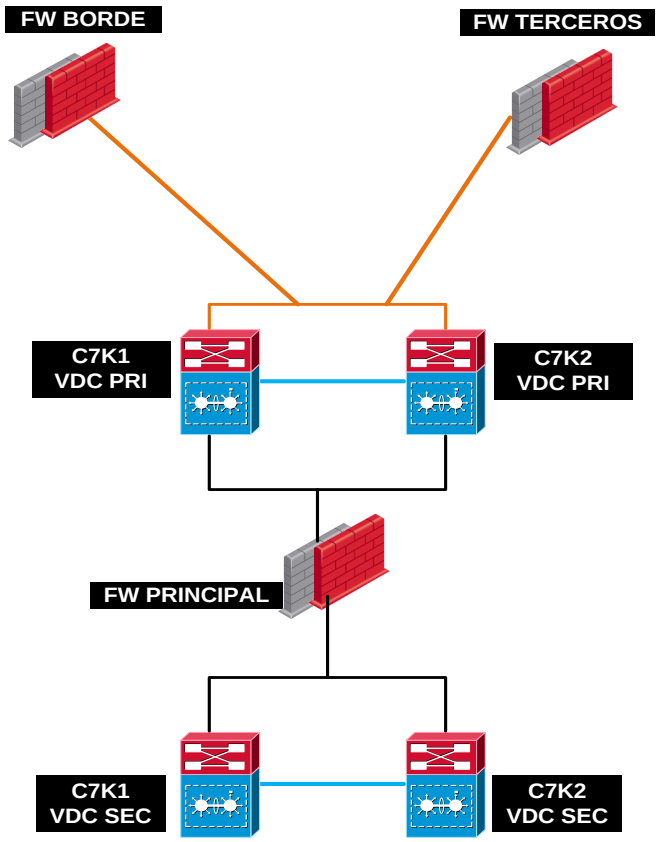


*Figura 3*. Conexión Lógica VDCs
*Fuente*: Elaboración Propia

Dentro de cada VDC se tiene adicionalmente creado segmentos de red utilizando la técnica de VRF.[3]

El Enrutamiento Virtual y Reenvío (VRF) es una tecnología incluida en Routers de red IP (Internet Protocol) que permite a varias instancias de una tabla de enrutamiento existir en un router y trabajar simultáneamente. Esto aumenta la funcionalidad al permitir que las

[3] VRF: Virtual Route Forwarding

rutas de red sean segmentadas sin usar varios dispositivos. Dado que el tráfico es automáticamente segregados, VRF también aumenta la seguridad de la red y puede eliminar la necesidad de cifrado y autenticación. (Rouse Margaret, 2012).

El objetivo de crear redes utilizando la tecnología VRF es independizar y agrupar redes con un mismo fin en un VRF autónomo del resto de redes, y así mantener el orden de acuerdo al fin de cada segmento de red.

En los Equipos de Core se define el direccionamiento de equipos, servidores, storages, appliances que se utiliza en el DCP y que están conectados en la capa de acceso. En los VDC tanto PRI como SEC se crean las VLANs Capa 3 con su direccionamiento respectivo, de igual manera en estos equipos se maneja el enrutamiento para la comunicación con los diferentes segmentos de red. La tabla de enrutamiento está creada mediante rutas estáticas configuradas en los dispositivos Cisco 7009.

En la tabla de a continuación se muestra la cantidad de equipos en la capa Core

Tabla 2
*Cantidad Equipos Core DCP*

| # | Proveedor | Dispositivos | Modelo | Cantidad |
|---|---|---|---|---|
| **1** | CISCO | Routers | Nexus 7009 | 2 |

*Fuente*: Elaboración Propia

#### *5.1.3.1.1. Características Nexus 7009.*

Los Switches Cisco Nexus 7000 son una línea de productos modulares utilizados para centro de datos con redes Gigabit Ethernet 1/10/40/100 altamente escalables con una arquitectura que puede soportar más allá de los 17 terabits por segundo (Tbps).

La serie Cisco Nexus 7000 se basa en el probado sistema operativo del software Cisco NX-OS, con funciones mejoradas para ofrecer actualizaciones del sistema en tiempo real con una manejabilidad y facilidad de servicio.

*Figura 4.* Cisco Nexus 7000 Series
*Fuente: (*Cisco, 2017. Cisco Nexus 7000 Series Switches Data Sheet)

Las características principales de estos equipos es que cuenta con nueve slots de hasta 9 ranuras de módulo accesibles desde la parte frontal. Mantiene una arquitectura de estructura escalable y totalmente distribuida compuesta por hasta cinco módulos de estructura combinados con el plano medio del chasis que entrega hasta 550 Gbps por ranura.

El chasis del Cisco Nexus 7000 puede tener hasta siete módulos de E/S que soporta hasta 336 puertos de 1 y 10 Gigabit Ethernet, 42 puertos de 40 Gigabit Ethernet y 14 puertos de 100 Gigabit Ethernet. Tiene dos ranuras de supervisor dedicadas para proporcionar redundancia completa. Las especificaciones técnicas más relevantes se muestran en la tabla a continuación:

Tabla 3
*Especificaciones Técnicas Cisco Nexus 7009*

| **Equipo** | **Cisco Nexus 7000 9-Slot Switch** |
|---|---|
| **Capacidad Max Local de Switching** | 600 Gbps |
| **Capacidad Max Inter-Slot de Switching** | 550 Gbps |
| **Compatibilidad de Software** | Cisco NX-OS Software Release 5.2 |

| | |
|---|---|
| **Performance** | 5.04 bpps (billones de paquetes por segundo) en combinación con supervisor |
| **Confiabilidad y disponibilidad** | OIR (Online Inserción y remoción) de todos los componentes redundantes: supervisor módulos estructurales, fuentes de poder, bandeja de ventiladores |
| **MIBs** | Soporta SNMPv3, v2c y v1 |
| **Especificaciones Físicas** | • Espacio de Rack Usable: 14u<br>• Chasis de 9 ranuras: 2 Módulos de supervisor dedicados y 7 módulos de E/S<br>• 5 slots de estructura modular<br>• 2 slots de fuentes de poder<br>• Dimensiones (Alto x Ancho x profundidad): 62.2 x 43.9 x 61 cm<br>• Peso: Solo Chasis 45 Kg<br>• Soporta Fuentes de Alimentación AC y DC de 6-kW y 7.5 kW |
| **Especificaciones Ambientales** | • Dirección del Flujo de Aire: Lado a Lado<br>• Temperatura de Operación: 0 to 40°C<br>• Disipación de calor: Máximo 7500 W por Chasis |

*Fuente: (*Cisco, 2017. Cisco Nexus 7000 Series Switches Data Sheet)

#### *5.1.3.1.2. Análisis consumo CPU, Memoria.*

Un dato importante a tomar en cuenta a la hora de plantear la línea base del diseño objetivo es la recolección de datos de consumo CPU y Memoria, que presentan los dispositivos, para determinar la carga con la que trabajan actualmente y si soportan las funciones de red que implica las operaciones del negocio. La validación de estos datos se realiza con la herramienta Cisco Prime que se utiliza para la supervisión de la red LAN del DCP. Los detalles de uso de CPU y memoria se los toma como muestra durante dos semanas para tener un promedio de los mismos. Los detalles mencionados se muestran en la siguiente tabla:

Tabla 4

*Consumo Promedio de CPU y Memoria, Equipos Core*

| Modelo | Nombre | Consumo CPU | Consumo Memoria |
|---|---|---|---|
| **N7K-C7009** | C7K1 | 10% | 31% |
| **N7K-C7009** | C7K2 | 10% | 31% |

*Fuente*: Elaboración Propia

Con los datos obtenidos se evidencia que en cuanto a consumo de CPU y Memoria los equipos de la capa de Core no tienen problemas para soportar la carga diaria de trabajo, un dato que se considerará para el diseño.

#### *5.1.3.2. Capa Agregación y Acceso del Datacenter Principal.*

La institución no realiza una diferencia clara a nivel de capa de agregación y acceso, ya que los servidores de aplicaciones, dispositivos de seguridad entre otros equipos se conectan directamente a los dispositivos de red que se encuentran en este único nivel. Los equipos utilizados para estas conexiones son Switches Cisco Nexus 5548, adicionalmente se utiliza la serie de switches Cisco 2000 para extender la cantidad de puertos necesarios para la conexión de equipos de punto final.

En esta capa los switches mantienen conexiones redundantes con los Switches Cisco 7009 de la capa de Core, con el fin de mantener alta disponibilidad en las conexiones, sin embargo para la conexión con los equipos Cisco Extender 2000 se tiene una sola conexión sin tener una redundancia a nivel de la capa de acceso.  Como se muestra en la siguiente ilustración:

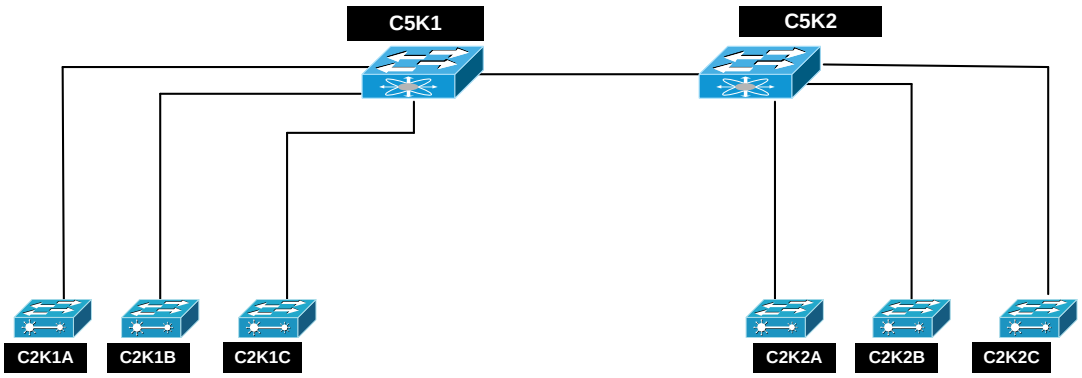


*Figura 5*. Conexiones Capa Agregación - Acceso (Cisco 5548 y Cisco 2000)
*Fuente*: Elaboración Propia

En los equipos Cisco 5548 se definen las VLAN capa 2 en las interfaces donde se conectan los dispositivos finales, el direccionamiento y enrutamiento está definido en la capa de Core.

De esta forma la capa de Agregación – Acceso se tiene 2 Switches Cisco 5548 los mismos que son utilizados para definir la Zona de DMZ, donde se encuentran los servers que brindan los servicios expuestos al internet. Estos equipos están protegidos por los Firewalls de Terceros y Borde, y de sus respectivos IPS como se muestra en la figura 6.

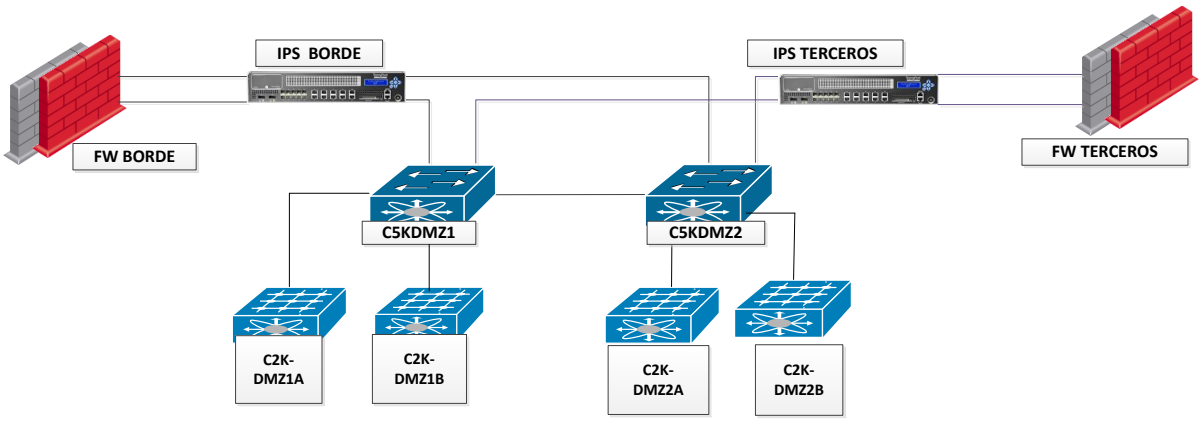


*Figura 6*. Conexiones DMZ
*Fuente*: Elaboración Propia

Para la Zona DMZ el enrutamiento lo realiza los firewalls, ya que el default Gateway de los segmentos de red de la DMZ está definido en estos equipos de seguridad.

En la tabla a continuación se muestra la cantidad de equipos en la capa de Agregación y Acceso, tanto para producción como DMZ.

Tabla 5
*Cantidad Equipos Capa Agregacion, Acceso y DMZ*

| # | Proveedor | Dispositivos | Modelo | Cantidad |
|---|---|---|---|---|
| **1** | Cisco | Switch | Nexus 5548 | 12 |
| **2** | Cisco | Switch | Extender 2000 | 24 |

*Fuente*: Elaboración Propia

#### *5.1.3.2.1. Características Nexus 5548*

Los equipos Cisco Nexus 5548 están diseñados para una amplia gama de accesos físico, virtual, acceso de storage, y entornos de computación de alto rendimiento, dando así flexibilidad para satisfacer y escalar los requisitos de los centro de datos de forma gradual y en un ritmo que se alinea con sus objetivos de negocio.

El Switch Cisco Nexus 5548UP es un dispositivo con un tamaño de 1 UR, con puertos de 10 Gigabit Ethernet, Fibre Channel, and FCoE, ofreciendo hasta 960 Gbps de throughput, con capacidad de hasta 48 puertos.

*Figura 7*. Cisco Nexus 5548UP Switch
*Fuente*: (Cisco, 2016. Cisco Nexus 5548P, 5548UP, 5596UP, and 5596T Switches Data Sheet)

Entre las características principales de este equipo se encuentran las siguientes:

Tabla 6
*Características técnicas equipos Cisco Nexus 5548*

| **Equipo** | **Cisco Nexus 5548UP** |
|---|---|
| **Hardware Performance Capa 2** | 960 Gbps o 714.24 mpps |
| **Performance Capa 3** | Hasta 160 Gbps o 240 mpps |

| | |
|---|---|
| **Interfaces** | • 32 puertos fijos de 1 0 10 Gigabit Ethernet y FCoE o Interfaces Fiber Channel de 8/4/2/1-Gbps Interfaces adicionales a través de módulo de expansión |
| **Características Capa 2** | • Encapsulación IEEE 802.1Q VLAN<br>• Rapid Per-VLAN Spanning Tree Plus (PVRST+)<br>• Multiple Spanning Tree Protocol (MSTP)<br>• Tecnología Cisco vPC<br>• Link Aggregation Control Protocol (LACP): IEEE 802.3ad |
| **Características Capa 3** | • Switch virtual interface (SVI), port channels, subinterfaces, y port channel<br>• Soporte para 1000 entradas VRF<br>• Soporte para 1664 entradas de ingreso y 2048 entradas de egreso en una listas de control de Acceso (ACL).<br>• Protocolos de enrutamiento: Estáticos, Routing Information Protocol Version2 (RIPv2), Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First Version 2 (OSPFv2), y Border Gateway Protocol (BGP)<br>• Protocolo Hot-Standby Router (HSRP) y Virtual Router Redundancy Protocol (VRRP)<br>• Virtual Route Forwarding (VRF) |
| **QoS** | • Capa 2 IEEE 802.1p (CoS)<br>• Configuración Per-port QoS<br>• Encolamiento Per-port virtual output<br>• Programación basada en puertos de salida : Weighted Round-Robin (WRR)<br>• Control Plan Policing (CoPP) - IPv4 |
| **MIBs** | Soporta SNMP v3, v2c y v1 |
| **Especificaciones Físicas** | • Soporta Cables Twinax de cobre SFP+ de 10 Gigabit Ethernet para distancias cortas<br>• SFP+ ópticos (10GBASE-SR, 10GBASE-LR, 10GBASE-ER, GLC-ZX-SM y Transceiver Fabric Extender de Nexus 2000 Series[FET-10G]) para largas distancias<br>• Espacio de Rack Usable: 1U<br>• Dimensiones (Alto x Ancho x profundidad): 4.4 x 43.9 x 74.9 cm<br>• Peso: 15.88 kg<br>• Soporta Fuentes de Alimentación AC y |

| | |
|---|---|
| | DC de 390W. |
| **Especificaciones Ambientales** | • Dirección del Flujo de Aire: De adelante hacia atrás y viceversa<br>• Temperatura de Operación: 0 to 40°C<br>• Disipación de calor: 2252 BTU/hr |

*Fuente*: (Cisco, 2016. Cisco Nexus 5548P, 5548UP, 5596UP, and 5596T Switches Data Sheet)

#### *5.1.3.2.2. Características Extensores Nexus 2000*

Los Extensores de la Serie Cisco Nexus 2000 comprenden una categoría de productos de centros de datos que proporcionan una plataforma universal de acceso, que se escala a través de una multitud de entornos de 1 Gigabit Ethernet, 10 Gigabit Ethernet. Al trabajar en conjunto con los Switches Cisco Nexus, la serie cisco 2000 ofrece una forma efectiva y eficiente de soportar los entornos Gigabit Ethernet de hoy en día, al tiempo que permite una fácil migración a tecnologías unificadas de Cisco de 10 Gigabit Ethernet.

La serie Cisco Nexus 2000 está diseñada para funcionar sin interrupciones, con fuentes de alimentación redundante e intercambiable en caliente y una bandeja intercambiable en caliente con ventiladores redundantes. Su compacto formato de 1UR ocupa poco espacio, facilitando la incorporación en los diseños de los racks (Figura 8). Los Cisco Nexus 2000 Series proporciona dos tipos de puertos: puertos para el host final (interfaces de host) y puertos de uplink (fabric interfaces).

*Figura 8*. Cisco Nexus 2000 Series
*Fuente*: (Cisco, 2016, Cisco Nexus 2000 Series Fabric Extenders Data Sheet)

#### *5.1.3.2.3. Análisis consumo CPU, Memoria*

Al igual que los dispositivos que conforman la capa de Core, el análisis de consumo de CPU y Memoria en los dispositivos de la capa de Agregación y Acceso es importante para validar la carga con la que trabajan actualmente y conocer si soportan las conexiones realizadas a diario en la empresa. La extracción de estos datos se ha realizado con la herramienta Cisco Prime que se utiliza para la supervisión de la red LAN del DCP. Los detalles de utilización de CPU y memoria se los ha tomado como muestra durante dos semanas para tener un promedio de los mismos. Estos detalles de uso se muestran en la siguiente tabla:

Tabla 7
*Consumo Promedio de CPU y Memoria, Equipos Agregación - Acceso*

| Modelo | Nombre | Consumo CPU | Consumo Memoria |
|---|---|---|---|
| **N5K-C5548UP** | C5K1 | 10% | 19% |
| **N5K-C5548UP** | C5K2 | 10% | 19% |
| **N5K-C5548UP** | C5K3 | 10% | 19% |
| **N5K-C5548UP** | C5K4 | 10% | 20% |
| **N5K-C5548UP** | C5K5 | 40% | 20% |
| **N5K-C5548UP** | C5K6 | 10% | 19% |
| **N5K-C5548UP** | C5K7 | 10% | 20% |
| **N5K-C5548UP** | C5K8 | 10% | 20% |
| **N5K-C5548UP** | C5K9 | 10% | 19% |
| **N5K-C5548UP** | C5K10 | 10% | 19% |
| **N5K-C5548UP** | C5KDMZ1 | 10% | 17% |
| **N5K-C5548UP** | C5KDMZ2 | 10% | 17% |

*Fuente*: Elaboración Propia

Es así que se puede determinar que el consumo actual de Memoria y CPU de los equipos se encuentran dentro de los parámetros normales de trabajo para las operaciones de la empresa.

Tomando en cuenta estos datos se podrá determinar los equipos a implementar en el Datacenter Alterno y que eventualmente puedan soportar en Memoria como CPU el tráfico de las conexiones del Datacenter Principal.

#### *5.1.3.3. Componentes de Seguridad de la Red del DCP.*

En una organización, los activos más valiosos son los datos que se manejan para el giro de negocio, los mismos que deben asegurar
su confidencialidad, integridad y disponibilidad. Para conseguir este fin se utilizan mecanismos de seguridad de la información. Dentro de este campo la empresa ha implementado appliances de Seguridad para garantizar su data. Algunos de estos equipos son los Firewall, IPS y Equipos contra DDoS[4]

##### *5.1.3.3.1. Características Firewall.*

La empresa cuenta con 6 Firewalls configurados en parejas para formar un Cluster con el objetivo de brindar redundancia y balanceo de las conexiones. En total se cuenta con 3 Cluster de Firewall que son: Cluster FW Borde, Cluster FW Terceros y Cluster FW Principal.

Estas 3 parejas de firewall brindan protección específica a 3 zonas las cuales son:

- Borde: Protección de las conexiones desde y hacia internet en esta zona se encuentran los servidores de publicación.
- Terceros: Protección de las conexiones desde y hacia empresas filiales o terceros con los que se cuentan con enlaces de comunicación directos.
- Principal: Protección de las conexiones desde y hacia servidores de la zona principal donde se maneja el core del negocio.

[4] DDoS: Distributed Denial-of-service (Denegación de Servicio Distribuida)

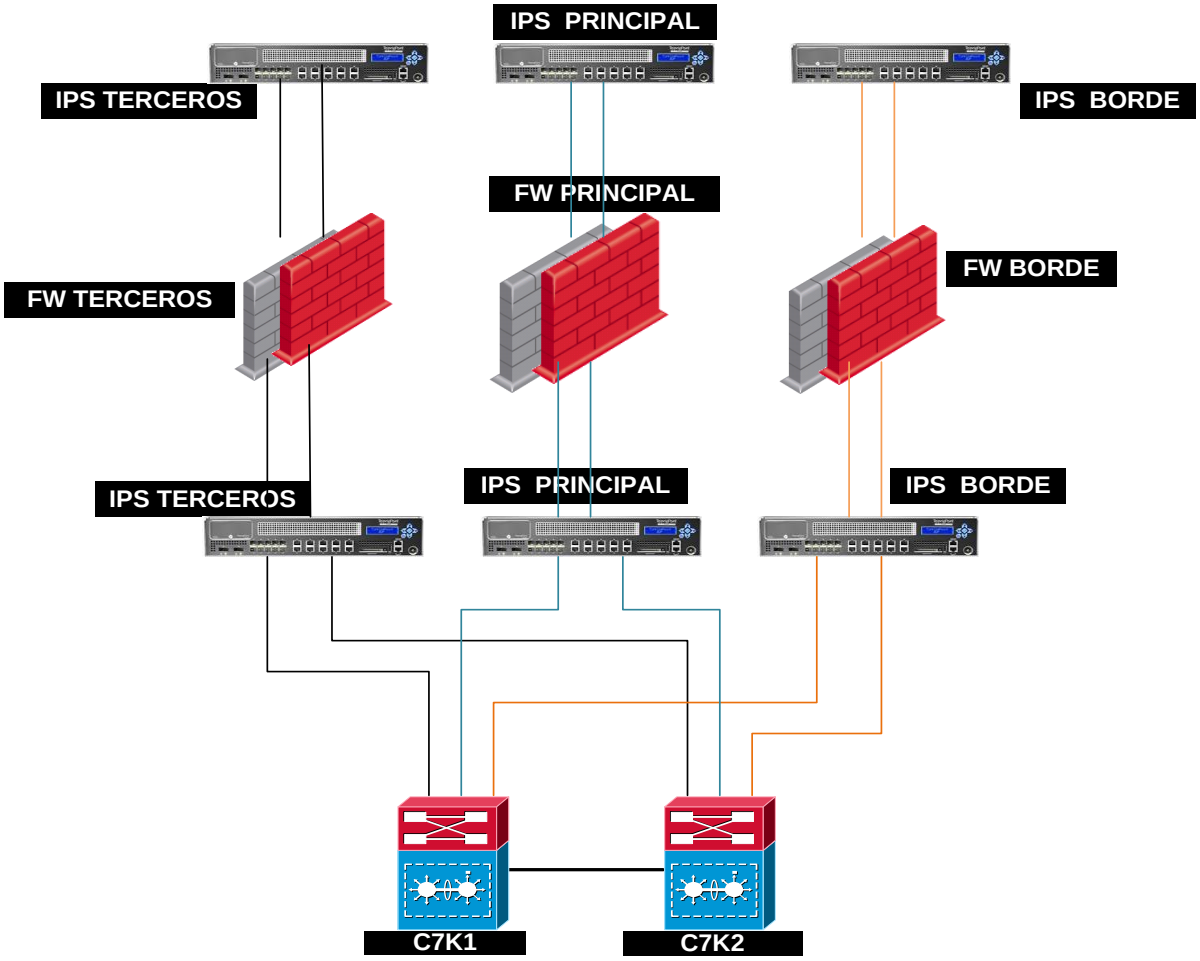


*Figura 9.* Conexiones de las 3 zonas de Firewall
*Fuente*: Elaboración Propia

Los Firewalls se encuentran implementados con la plataforma Check Point. Check Point Software Technologie, un proveedor global de soluciones de seguridad IT, conocido por sus productos Firewall y VPN. Check Point fue el pionero en la industria con el FireWall-1 y su tecnología patentada de inspección de estado. (Wikipedia, 2017).

En la tabla a continuación se muestra la cantidad de equipos Firewall usando la plataforma checkpoint.

Tabla 8
*Cantidad Equipos Firewall en DCP*

| # | Proveedor | Dispositivos | Modelo | Cantidad |
|---|---|---|---|---|
| 1 | CheckPoint | Firewall | Gaia R77.30 | 6 |

*Fuente*: Elaboración Propia

CheckPoint provee a los clientes una protección inflexible contra todo tipo de amenazas, reduciendo la complejidad de la seguridad y baja el costo total de propiedad. Ofrece Seguridad Total para redes, datos y terminales de punto final, unificadas bajo un solo marco administrativo. Algunas de sus características se enlistan a continuación:

- Hace frente a riesgos de hackers, Worms, Spyware y otros peligros relacionados con el acceso de PCs internos y remotos a sus redes.
- Las soluciones de gestión de CheckPoint están diseñadas como un sistema interoperable basado sobre una arquitectura de seguridad unificada que permite controlar de manera centralizada las políticas de seguridad a través de múltiples capas de la infraestructura.
- Los firewall de CheckPoint ofrecen características de seguridad avanzadas tales como prevención de intrusos, virtualización, Gateway antivirus, Anti-spam, Filtrados de contenidos web, así como IPsec y accesos remoto SSL VPN para PCs y dispositivos móviles. (Etic Solutions. Protección Perimetral & Firewalls)

En la siguiente tabla se señalan las características técnicas de esta plataforma.

Tabla 9
*Características Técnicas Firewall Checkpoint*

| **Equipo** | **CheckPoint** |
|---|---|
| **Edición de Software** | R65, R70 |
| **Puertos 10/100/1000** | 4/16 |
| **Puertos 10 GbE** | 6 |
| **Firewall Throughput** | 7.2/11.7 Gbps |
| **VPN Throughput** | 1.4/3.3 Gbps |
| **Sesiones concurrentes** | 1.1 Millones |
| **IPS Throughput** | 4 Gbps |
| **VLANs** | 1024 |
| **Módulos ADP** | Opcionales |
| **VPN Module** | Incluida |
| **Storage** | 80 GB |
| **Flash o Basado en Disco** | Disco o Flash |
| **Enclosure** | 1U |
| **Dimensiones** | 436 x 610 x 44 mm |
| **Peso** | 12.38 Kg |
| **Operación Ambiental** | Temperatura: 5 a 50 grados C |

| | |
|---|---|
| **Potencia de Entrada** | 100/240 V |

*Fuente*: (Etek Reycom. CheckPoint)

#### *5.1.3.3.2. Características IPS*

Es la implementación de esta solución se cuenta con los dispositivos IPS, la marca actualmente utilizada es HP TippingPoint. El objetivo de este dispositivo es realizar el monitoreo permanente del tráfico que cruza por la red LAN del DCP de la empresa para minimizar el riesgo de explotación de vulnerabilidades y accesos no autorizados. A través del IPS se gestiona de manera oportuna los eventos o incidentes de seguridad detectados en la solución de prevención de intrusos. Con este equipo se puede disponer de reportes periódicos y métricas mensuales que permitan conocer el nivel de ataques protegidos por la solución.

Actualmente se cuenta con 3 equipos IPS que sirven para proteger las 3 zonas principales de la infraestructura del Datacenter, IPS Borde, IPS Terceros e IPS Principal. Cuentan con una conexión lógica antes y después de la infraestructura de sus respectivos Firewall, logrando que todo el tráfico de red que cruza desde y hacia los servidores del Datacenter sean inspeccionados por estos dispositivos de seguridad. Sus conexiones lógicas se representan en la figura 9.

En la siguiente tabla se encuentra la cantidad de este equipamiento.

Tabla 10
*Cantidad de equipos IPS*

| # | Proveedor | Dispositivos | Modelo | Cantidad |
|---|---|---|---|---|
| **1** | HP Tipping Point | IPS | 5200NX | 3 |

*Fuente*: Elaboración Propia

Dentro de las características de este equipo tenemos las siguientes más importantes:

Tabla 11
*Características Técnicas IPS Tipping Point*

| **Equipo** | **HP Tipping Point** |
|---|---|
| **Performance del Equipo** | • Filtrado de ataques de multigigabits por |

| | |
|---|---|
| | segundo<br>• Latencia < 84 µs<br>• Mezcla de tráfico TCP/UDP en condiciones reales<br>• Más de dos millones de sesiones simultáneas<br>• TCP/UDP/ICMP<br>• Más de un millón de conexiones por segundo |
| **Protección frente a amenazas** | • VoIP<br>• Phishing<br>• Gusanos<br>• Cuarentena<br>• Vulnerabilidades de sistemas operativos<br>• DDoS<br>• P2P<br>• Spyware<br>• Virus<br>• ZDI |
| **Protección de cliente y servidor** | • Previene los ataques de sistemas operativos y aplicaciones vulnerables<br>• Elimina los costosos parches especiales<br>• Varios métodos de filtrado |
| **Protección de la infraestructura de red** | • Protege las unidades Cisco IOS, DNS y demás infraestructura.<br>• Protege frente a anomalías de tráfico, DDoS, inundaciones de SYN, inundaciones de tablas de procesos.<br>• Listas de control de acceso |
| **Protección del desempeño de las aplicaciones** | • Aumenta el ancho de banda y la capacidad de los servidores<br>• Limita la velocidad de transmisión o bloquea el tráfico no deseado (P2P/IM)<br>• Ancho de banda garantizado para aplicaciones críticas |
| **Alta disponibilidad y redundancia adaptativa de red (Stateful)** | • Dos fuentes de alimentación<br>• Repliegue a capa 2<br>• Redundancia adaptativa (Stateful) activa/activa o activa/pasiva (IPS y SMS)<br>• Alta disponibilidad en caso de apagones (ZPHA) |

*Fuente*: (Techno Partners. Especificaciones técnicas IPS)

#### *5.1.3.3.3. Características DDoS*

Otro appliance implementado dentro de la infraestructura de seguridad de la empresa es el dispositivo contra ataques DDoS, de la marca comercial Radware DefensePro.

Radware DefensePro es un detector de intrusiones de múltiple capa, que provee protección contra DoS, detección de anomalías y una gran variedad de ataques conocidos y desconocidos del día cero. Es fácil de usar y es una solución escalable para la protección contra virus y gusanos. La pro-actividad previene ataques a servidores o redes, mientras asegura un alto rendimiento para el tráfico legítimo, bajo condiciones de ataque. Como detector y prevención en línea, protector de DoS y conformador de tráfico, DefensePro está diseñado para la protección integral de las empresas e implementación en perímetros, integrando varios niveles de defensa, entre los que se incluye: Protección basado en firmas. Protección de irrupciones en servidores Mitigación de inundaciones DoS/DDoS Protección para ataques Encriptados SSL, Control de acceso, Administración de ancho de banda.

DefensePro provee una seguridad sin precedentes integra capacidades de protección basado en comportamiento adaptivo tanto a nivel de red y nivel de aplicación sin intervención de un operador. DefensePro está realizado con una arquitectura de hardware basado en ASIC (application specific integrated circuit - Circuito integrado para aplicaciones específicas), que asegura el más alto nivel de seguridad disponibilidad y rendimiento. Puede monitorizar múltiples segmentos de red de core y perímetro en ambientes de tráfico de hasta 6 Gbps. (Britos José Daniel, 2010).

El dispositivo contra Ataques DDoS se lo utiliza en la infraestructura de la empresa para la protección de los servicios expuestos a internet. La gestión y el control de la solución contienen las siguientes tareas:

- Validación de funcionamiento de los dispositivos que componen la solución de DDoS.
- Monitoreo del DefensePro.
- Actualización centralizada de firmas en DDoS para protección de ataques por denegación de servicios.

- Actualización de políticas de protección para DDoS
- Análisis de gestión de eventos de seguridad
- Administración de parches y firmware
- Actualización IPs públicas a proteger de la empresa

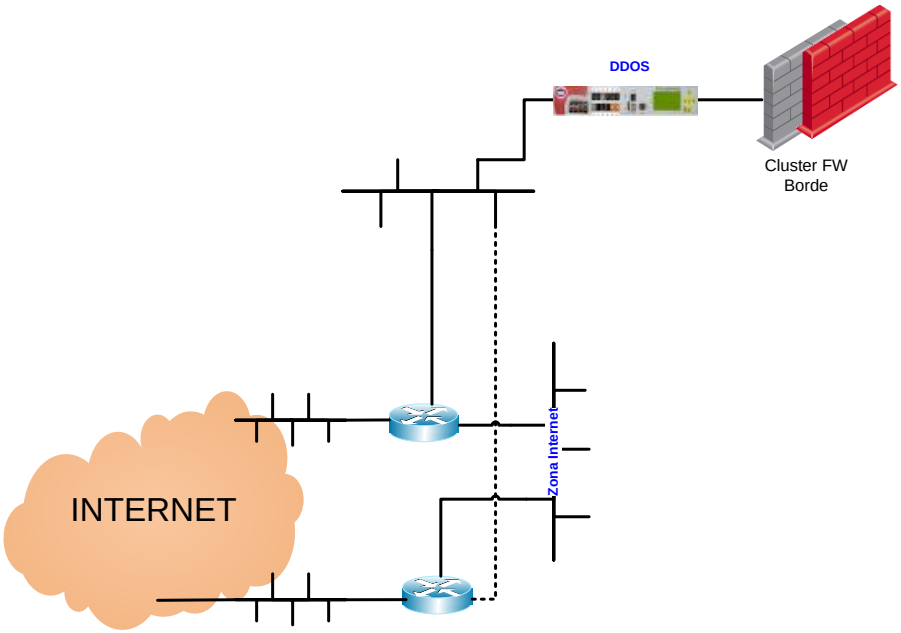


*Figura 10.* Conexiones Equipo Anti-DDoS
*Fuente*: Elaboración Propia

Como se indica en la Figura 10 el equipo anti-DDoS se encuentra a la entrada/salida de las conexiones de Internet, lo cual permite bloquear el tráfico de denegación de servicio antes que ingrese a la infraestructura de la empresa, lo que permite que los ataques sean controlados antes de llegar a cualquier servicio que se publica al exterior.

Tabla 12
*Cantidad de equipos IPS*

| # | Proveedor | Dispositivos | Modelo | Cantidad |
|---|---|---|---|---|
| **1** | Radware | DDoS | DefensePro x42 | 1 |

*Fuente*: Elaboración Propia

Dentro de las características de este equipo tenemos las siguientes:

Tabla 13
*Características Técnicas Anti DDoS*

| **Equipo** | DefenseProx42 Series |
|---|---|
| **Throughput de Inspección (Max)** | 10Gbps (10420)<br>20Gbps (20420)<br>30Gbps (30420)<br>40Gbps (40420) |
| **Latencia** | <60 µs |
| **Tasa de Protección de inundaciones (Max)** | 25M pps |
| **Interfaces** | 20 - 1/10Gb SFP+<br>4 - 40Gb QSFP+ |
| **Modos de Operación** | En-línea, Monitoreo de Puerto (SPAN), Copia de monitoreo de puerto, Out-of-Path (local), Out-of-Path (Scrubbing Center) |
| **Tamaño de Chasis** | 2U |

*Fuente*: (Sean Wilkins, 2017)

#### *5.1.3.3.4. Análisis de la infraestructura de Seguridad*

Dentro de la infraestructura de seguridad de la empresa se evidencia que algunos parámetros o configuraciones necesitan ser revisadas. Las observaciones de la infraestructura son:

- Hay demasiadas zonas DMZ creadas y configuradas dentro de los Firewall Borde y Terceros. Se observa que se han configurado 23 zonas DMZ para cada aplicación que tiene una zona DMZ separada, utilizando el puerto físico del firewall. Esta no es la mejor práctica normativa en la industria.
- Se han configurado muchas ACL (Listas de acceso por sus siglas en inglés) en el Firewall. El conteo en la lista de acceso actual es el siguiente:
    - FW Principal – 1347
    - FW Terceros - 1118
    - FW Borde – 760

- Todos los Firewall Principal, Borde, como Terceros utilizan un servidor HP (ProLiant DL 380 G7) el cual se declara como End of Live.
- La subred "Zona Compartida" no es parte del Firewall. La intercomunicación VLAN no atraviesa ningún Firewall.
- El DDoS utilizado actualmente tiene un punto de fallo único.
- El dispositivo IPS actual se encuentra operando en modo de Escucha. Esto significa que se crean registros, pero el IPS no aplicaría ninguna acción contra los ataques. Es un gran problema de seguridad.
- No se ha configurado una Alta Disponibilidad (HA) para el dispositivo IPS.

En este contexto se tendrá una línea base del diseño objetivo de seguridad para el Datacenter Alterno, tomando en cuenta las vulnerabilidades del Datacenter Actual se realizará mejoras para la implementación del DCA.

#### *5.1.3.3.5. Características Balanceador de Carga F5*

Dentro de la infraestructura de red existe actualmente un equipo Balanceador de carga de la Marca F5, modelo BIG-IP, como su nombre lo indica este dispositivo se lo utiliza para balancear las peticiones de los usuarios hacia una granja de servidores que responderá estas solicitudes.

Los dispositivos F5 BIG-IP funcionan en un sistema modular, por lo que puede agregar nuevas funciones como sean necesarias para adaptarse rápidamente a las necesidades cambiantes de las aplicaciones y los negocios.

El principal módulo utilizado en el equipo F5 es el de Administrador de Tráfico Local (LTM) BIG-IP este módulo permite entregar los servicios de aplicaciones a los usuarios de una manera confiable, segura y optimizada. Tomando decisiones de tráfico inteligentes que se adaptan a los cambios demandados por las aplicaciones, BIG-IP LTM garantiza la

consistencia, disponibilidad y escalabilidad de las aplicaciones. BIG-IP LTM, tiene la capacidad de simplificar, automatizar y personalizar aplicaciones de forma más rápida y más previsible. (F5, 2013. BIG-IP Modules DATASHEET)

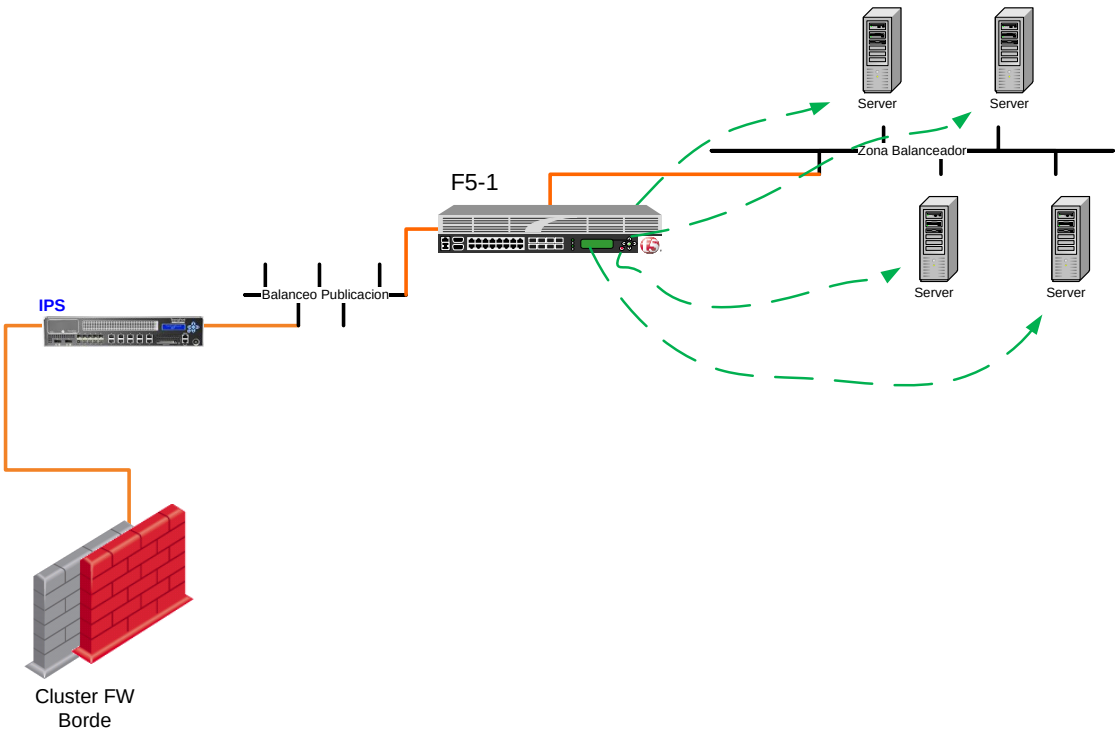


*Figura 11*. Conexiones Equipo F5
*Fuente*: Elaboración Propia

Tabla 14
*Cantidad de Equipo F5 en DCP*

| # | Proveedor | Dispositivos | Modelo | Cantidad |
|---|---|---|---|---|
| **1** | F5 | Balanceador de Carga | F5 – Big IP - LTM | 1 |

*Fuente*: Elaboración Propia

Dentro de las principales características de estos equipos tenemos:

Tabla 15
*Características F5 - LTM*

| Equipo | F5 – Big IP LTM |
|---|---|
| **Gestión del tráfico de aplicaciones** | • Balanceo de carga inteligente<br>• Soporte de protocolo de aplicación (TCP, HTTP 2.0, SPDY 3.1, SSL, SIP, FIX, MS SQL, etc.)<br>• Seguimiento de la salud de las aplicaciones y gestión del estado de la conexión<br>• Análisis F5 |
| **Optimización de la entrega de aplicaciones** | • Compresión adaptativa simétrica<br>• Caché de RAM y compresión<br>• Controlador de ancho de banda<br>• Optimización TCP<br>• Puerta de enlace SPDY y HTTP 2.0 |
| **Entrega Segura de Aplicaciones** | • Conexión SSL y mirror de sesiones<br>• Descarga SSL cyrpto para implementaciones híbridas<br>• Descarga de cifrado SSL / TLS<br>• Agilidad del algoritmo (PFS, GCM, ECC, DSA, RSA, Suite B)<br>• HSM interno / de red / en la nube (FIPS 140-2)<br>• Visibilidad SSL (entrante / saliente) |
| **Infraestructura escalable** | • Aplicación bajo demanda y totalmente activa<br>• Agrupación<br>• Escalamiento operacional (multi-tenant y Virtualización)<br>• Enrutamiento avanzado (BGP, RIP, OSPF, ISIS, BFD)<br>• Licencia de Servicios SDN (VXLAN, NVGRE) |

*Fuente*: (F5, 2014. BIG-IP Local Traffic Manager)

## 5.2. Diseño del modelo de red a implementar en el Datacenter Alterno

A continuación se menciona el diseño de red que se ha propuesto para el Datacenter Alterno de la empresa, basado en la infraestructura actual, el análisis de los equipos que la conforman y los requerimientos por parte de la empresa. A partir de estos parámetros se selecciona los equipos, topología y tecnología apropiada, para crear esta arquitectura.

En el diseño del Datacenter Alterno de la empresa se considera la arquitectura jerárquica de capas más común con ajustes en su diseño para adaptarse al modelo del centro de Datos Principal, manteniendo la simplicidad sin comprometer la seguridad. Este diseño se basa principalmente en las 3 Capas Jerárquicas del Modelo Cisco: Capa Core, Capa Agregación y Capa Acceso, dentro de la cual confluyen servicios Web, Aplicaciones y servidores de bases de datos que se ejecutan en varias plataformas, incluidos servidores blades, servidores empresariales y entornos SAN. En estas capas se incluyen de igual manera equipos de seguridad para proteger los datos que se manejen dentro del Datacenter.

De manera general se ha propuesto el siguiente diseño jerárquico para la infraestructura de red del Datacenter Alterno:

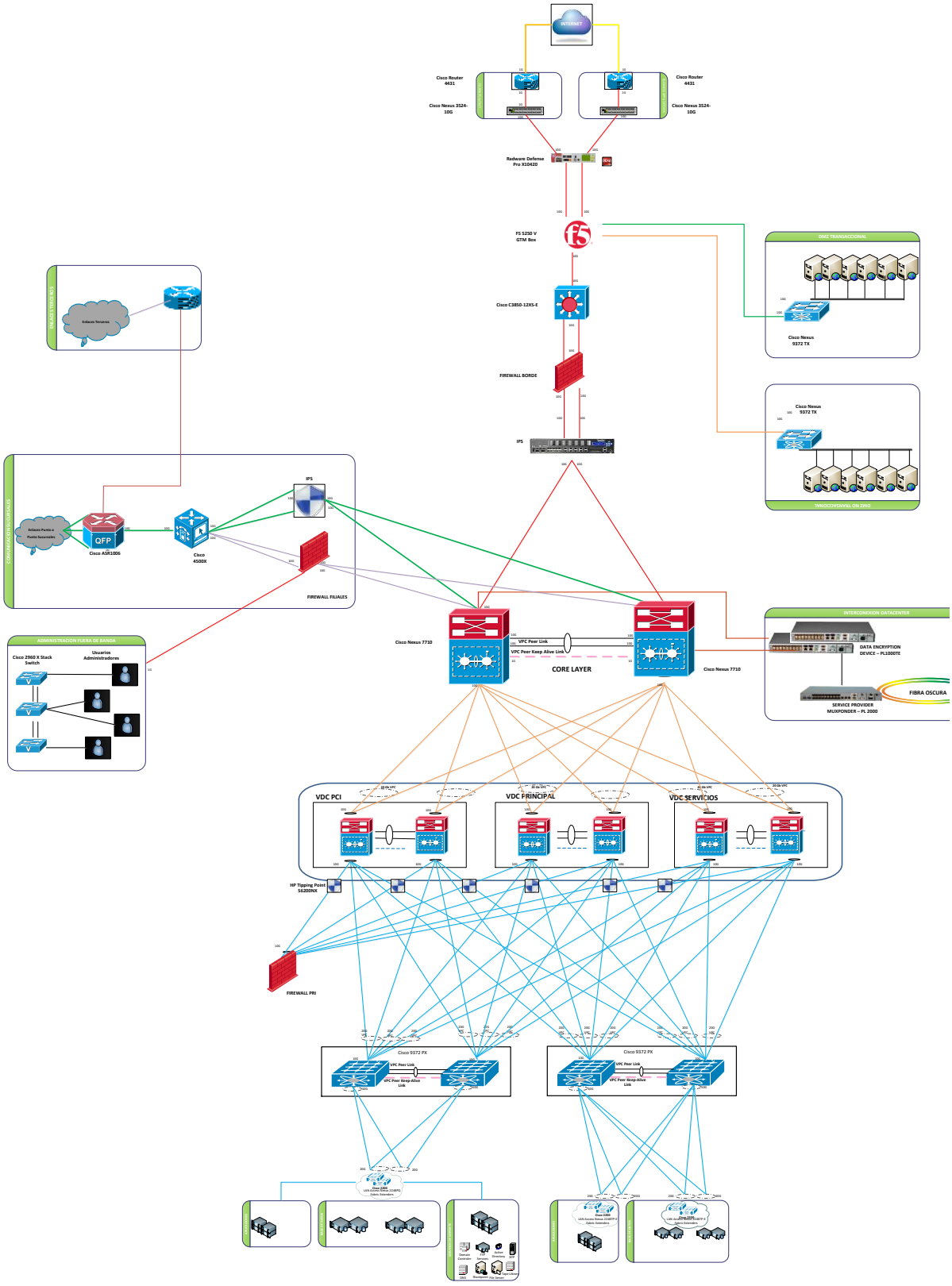


*Figura 12*. Arquitectura de Red Propuesta para DCA
*Fuente*: Elaboración Propia

El diseño de la arquitectura de red ha tratado de no realizar demasiados cambios de lo que se tiene actualmente en el Datacenter Principal, sin embargo se ha tomado las mejores prácticas para plasmarlas en el DCA. La composición de esta estructura de red se explicará más a detalle en los siguientes apartados.

### 5.2.1. Capa Core DCA

La capa Core del centro de Datos Alterno proporciona una estructura de conmutación de paquetes a alta velocidad entre varios módulos de agregación. Esta capa sirve como puerta de enlace al Core del Datacenter donde se conectan otros módulos, incluyendo, por ejemplo, la extranet, la WAN y salida hacia Internet. Todos los enlaces que conectan el Core del centro de Datos Alterno terminan en capa 3 y normalmente utilizan interfaces 1 GigE para soportar un alto nivel de rendimiento y escalabilidad.

La Capa de Core ha sido delineada similar al Data Center Primario teniendo como objetivo crear un diseño que tenga una desviación mínima del centro de datos principal, incluidos los componentes de Infraestructura, por lo cual el diseño de Core propuesto está alineado con el diseño del centro de datos primario que tiene 2 Routers de Core conectados entre sí para brindar redundancia. En estos equipos se realizará una partición lógica para crear la VDC de Core.

Los Routers de Core tienen la función de enrutar el tráfico proveniente de los equipos finales así como tráfico externo de la red. Para lograr este objetivo se tiene configurado rutas estáticas que de acuerdo al destino se envía los paquetes a su siguiente salto.

Las conexiones hacia los VDCs de la capa agregación, equipos de seguridad como IPS, Firewall se lo realiza mediante una configuración de VLAN capa 3 en los Routers 7700, que sirve de interconexión entre los equipos.

Las conexiones físicas se lo realiza mediante puertos de fibra a 10 Gb, los SFP utilizados son 10Gbase-SR (Laser de 850 nm).

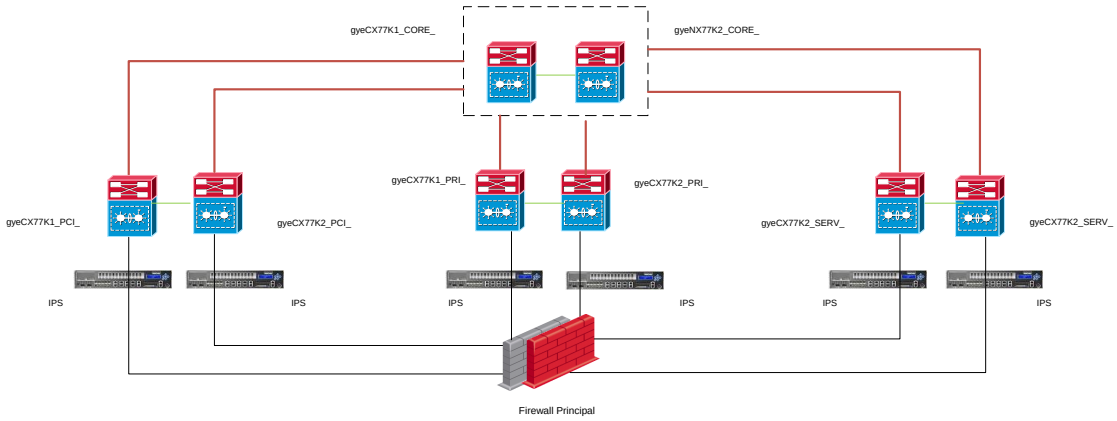


*Figura 13.* Conexiones Capa Core DCA
*Fuente*: Elaboración Propia

Los equipos seleccionados como Core del Datacenter han sido los Cisco Nexus 7700, los cuales son la siguiente generación de la serie Cisco Nexus 7000, que actualmente se tienen en el Datacenter Principal.

En la tabla de a continuación se muestra la cantidad de equipos en la capa Core

Tabla 16
*Cantidad Equipos Capa Core*

| # | Proveedor | Dispositivos | Modelo | Cantidad |
|---|---|---|---|---|
| 1 | CISCO | Switches | Nexus 7710 | 2 |

*Fuente*: Elaboración Propia

#### *5.2.1.1. Características Cisco Nexus 7700*

Los switches Cisco Nexus 7700 son la última extensión de los Switches de la serie Cisco Nexus 7000, tienen una capacidad de Switching de más de 83 terabits por segundo (Tbps), adicional los Switches Cisco Nexus 7700 ofrece puertos de 10, 40 y 100 Gigabit

Ethernet, con hasta 768 puertos nativos de 10 Gbps, 384 de 40 Gbps, o 192 puertos de 100 Gbps.

Los Switches Cisco Nexus 7700 tienen una consistencia operativa y funcional con los Switches Cisco Nexus 7000, utilizando una arquitectura común, la misma tecnología de circuito integrado de aplicación específica (ASIC) y las mismas versiones de software probadas de Cisco NX-OS. (Cisco, 2017. Cisco Nexus 7700 Switches Data Sheet)

*Figura 14*. Cisco Nexus 7700
*Fuente*: (Cisco, 2017. Cisco Nexus 7700 Switches Data Sheet)

El sistema utiliza tres bandejas de ventilador redundantes para refrigeración. Cada bandeja de ventilador está compuesta por ventiladores independientes de velocidad variable que se ajustan automáticamente a la temperatura ambiente, para ayudar a reducir el consumo de energía en instalaciones, al mismo tiempo que ayudan a optimizar el funcionamiento del switch. El sistema también permite el cambio en caliente de las bandejas de ventiladores sin afectar negativamente al sistema.

El Switch Cisco Nexus 7700 puede tener hasta ocho fuentes de alimentación de 3 o 3,5 (kW). La configuración de la fuente de alimentación más pequeña proporciona más flexibilidad y un mayor control en el aprovisionamiento de energía. Las ocho bahías de alimentación están diseñadas para un crecimiento futuro, y las configuraciones más comunes

no requieren el uso de todas las unidades de fuente de alimentación para configuraciones de alimentación redundantes.

Las características técnicas más importantes de este equipo se detallan a continuación

Tabla 17
*Características Técnicas Cisco Nexus 7710*

| Equipo | Cisco Nexus 7700 10-Slot Switch |
|---|---|
| **Cantidad de Puertos** | 384 x 10 Gbps, 192 x 40 Gbps, and 96 x 100 Gbps |
| **Compatibilidad** | • Soporta toda la serie de Cisco Nexus 7700 Supervisores y Módulos de Entrada /Salida<br>• Soporta la serie de Cisco Nexus 7700 de Módulos de Fabrica-2<br>• |
| **Compatibilidad Software** | Cisco NX-OS Software Release 6.2.2 o mayor |
| **Opciones** | • Puerta de Filtro de Aire<br>• Puertas de módulo frontales bloqueables<br>• |
| **Capacidad de reenvío del sistema** | 42 Tbps |
| **Capacidad Max de Local Switching** | 1.2 Tbps |
| **Capacidad Max de Inter-slot Switching** | 1.2 Tbps |
| **Confiabilidad y disponibilidad** | OIR (Online Inserción y remoción) de todos los componentes redundantes: supervisor módulos estructurales, fuentes de poder, bandeja de ventiladores |
| **MIBs** | Soporta SNMPv3, v2c, and v1 |
| **Especificaciones Físicas** | ● Espacio de rack requerido: 14RU<br>● Switch de 10-slots: 2 Módulos de supervisora dedicado y 8 módulos de Entrada/Salida<br>● 6 slots de módulos de fabrica<br>● 8 slots de Fuentes de poder<br>● Dimensiones (A x Ancho x P):61.85 x 43.9 x 86.4 cm<br>● Peso solo chassis: 72.6 kg,,<br>● Soporta 3-kW y 3.5-kW en Fuentes de poder AC/DC |
| **Especificaciones Ambientales** | ● Dirección del flujo de Aire: delante hacia atrás<br>● Temperatura de Operación: 0 to 40°C<br>● Disipación de Calor: Máximo 52,500 BTUs por hora |

*Fuente*: (Cisco, 2017. Cisco Nexus 7700 Switches Data Sheet)

### 5.2.2. Capa Agregación DCA

Cada capa cumple un rol importante dentro de la infraestructura de red del DCA. La capa Agregación es aquella donde se consolidan las comunicaciones de los servidores del Data Center, y debe tener una arquitectura de alta disponibilidad para ofrecer un rendimiento de baja latencia y una fiabilidad en el punto final de los equipos. Adicional esta capa debe ser la más segura de todas ya que es aquí donde se concentra la información del negocio; para esto se van a crear 4 VDCs para Producción. Estas VDCs son: Core, Principal, Servicios y PCI.

Estas VDCs creadas tienen como objetivo separar en 4 zonas que agruparan segmentos de red para una función específica, consiguiendo así separación de ambientes, y separación en zonas de acuerdo a la criticidad de las aplicaciones. La agrupación de redes en cada VDC se lo realizará de acuerdo al siguiente criterio de categorización:

Tabla 18
*Criterios para la Agrupación de los Aplicativos en VDCs*

| VDC | DEFINICIÓN | SUB ZONA | CRITERIO |
|---|---|---|---|
| **SERVICIOS** | Son aquellas aplicaciones que soportan los procesos tecnológicos de la empresa y que proveen seguridad y monitoreo de los componentes de la infraestructura | Seguridad | Aplicaciones y BDD de herramientas que permiten implementar controles de seguridad en la infraestructura tecnológica (Ej. Filtrado Web, DDoS, Prevención de Intrusos, etc.) |
| | | Red | Aplicaciones y BDD de herramientas que proveen servicios de red para los procesos operativos de la empresa (Ej. Directorio Activo, correo electrónico, File Server, etc.) |
| | | Monitoreo | Aplicaciones y BDD de herramientas que permiten implementar mecanismos de evaluación y seguimiento periódico a los componentes tecnológicos de la empresa. (Ej. HP OVO, NMMI, etc.). |
| **PCI** | Son aquellas aplicaciones sensitivas, que manejan | Aplicaciones Transaccionales | Aquellas que ejecuten transacciones financieras que: Involucre manejo de efectivo, o |

| | | | |
|---|---|---|---|
| | datos de clientes, tarjeta habientes (PCI) y/o Flujo de efectivo | | Estén expuesta a fraude electrónico |
| | | Base de Datos | Almacenamiento lógico de la información de las aplicaciones Sensitivas |
| | | Soporte | Plataforma de HW y SW que permite el funcionamiento de las aplicaciones Sensitivas. (Ej, soluciones de respaldo, etc.). |
| **PRINCIPAL** | Son aquellas aplicaciones no sensitivas que soportan los procesos operativos del negocio | Aplicaciones Transaccionales | Aquellas que ejecuten transacciones financieras que **NO**: Involucre manejo de efectivo, y no están expuestas a fraude electrónico. |
| | | Aplicaciones NO Transaccionales | Aquellas que automatizan los procesos de soporten que no corresponden a la cadena de valor (Ej. Elearning, etc.). |
| | | BDD | Almacenamiento lógico de la información de las aplicaciones. |
| | | Soporte | Plataforma de HW y SW que permite el funcionamiento de las aplicaciones |
| | | Externos | Aplicaciones y BDD de Terceros o Filiales |
| **CORE** | Esta zona sirve para la interconexión entre VDCs hacia el resto de la infraestructura de Red | | |

*Fuente*: Elaboración Propia

El tratamiento del tráfico a enrutar en la capa de Agregación se lo realiza mediante enrutamiento Inter-VLAN que lo hará cada una de las VDCs mediante VRFs e Interface VLANs, la comunicación entre las VDCs de Producción será efectuada por un Firewall nombrado Principal que tendrá un segmento de conexión a cada VDC, la interconexión entre las 3 VDCs con el Datacenter Principal, redes Sucursales, Redes de Terceros, DMZs e Internet la ejecutará la VDC de Core que tendrá un segmento de red conectado a cada una de las 3 VDCs.

Las conexiones físicas de las VDCs hacia los equipos de Core como hacia los Switches de acceso se lo realiza mediante puertos de fibra a 10 Gb, los SFP utilizados son 10Gbase-SR (Laser de 850 nm).

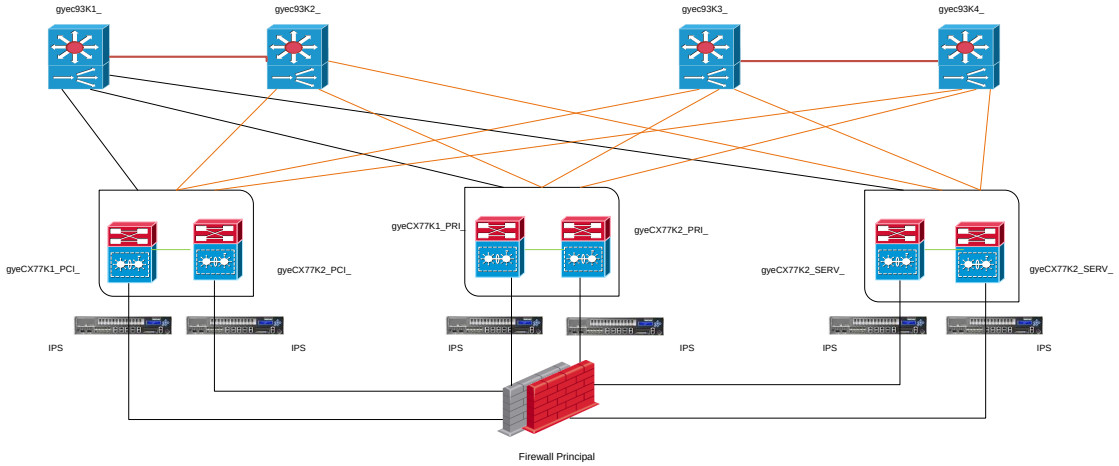


*Figura 15*. Conexiones Capa Agregación DCA
*Fuente*: Elaboración Propia

Como se indicó en apartados anteriores una VDCs puede ser usada para virtualizar el propio equipo, exponiendo el switch físico como múltiplos dispositivos lógicos. En este caso el Equipo de Core Cisco Nexus 7710 se lo particionará lógicamente en 4 VDCs, cada uno con su propia tabla de enrutamiento, recursos, administración y configuración propia. Esto con el objetivo de crear una capa de Core y una capa de Agregación con particiones lógicas que funcionan como si fueran equipos físicos independientes uno de otros.

Físicamente se asigna un grupo de interfaces del Cisco 7710 para cada VDC creada. En estas interfaces se conectan los switches de acceso para brindar la conexión a los equipos finales. La división de interfaz se muestra a continuación:

Tabla 19
*Asignación de Interfaces del Cisco 7710 a las VDCs*

| EQUIPO | RANGO INTERFACES | CANTIDAD PUERTOS |
|---|---|---|
| **C7K1-PCI** | Eth1/1 - Eth1/16 | 16 |
| **N7K2-PCI** | Eth1/1 - Eth1/16 | 16 |
| **N7K1-PRINCIPAL** | Eth1/17 - Eth1/32 | 16 |
| **N7K2- PRINCIPAL** | Eth1/17 - Eth1/32 | 16 |
| **N7K1-SERVICIOS** | Eth1/33 - Eth1/48 | 16 |
| **N7K2-SERVICIOS** | Eth1/33 - Eth1/48 | 16 |

*Fuente*: Elaboración Propia

Al ser la Capa de Agregación conformada por divisiones lógicas del equipo Cisco 7710, las características técnicas son las mismas presentadas en el aparado 5.2.1.1 Características Cisco 7700.

### 5.2.3. Capa Acceso DCA

La Capa de Acceso es la encargada de brindar conectividad a los equipos de punto final (servidores, storage, enclosure, etc) a nivel de capa 2. En esta capa se realizará la conexión de todos los equipos mediante los Switches Cisco Nexus 9372 y Cisco extender 2000.

En este nivel se configura VLANs capa 2, lo que permite segmentar a cada uno de los equipos que se conecten a las interfaces de los switches, de acuerdo a la función que deban cumplir.

Para brindar un esquema de alta redundancia en esta capa se realiza la configuración de 2 parejas de equipos redundantes uno del otro cada uno con sus propios equipos extensores de puertos.

Se debe tomar en cuenta que no realizar ninguna configuración en los equipos Cisco Nexus 2000 para la conexión de Fabric Extender contra los Cisco Nexus 9000; toda la configuración se la realiza en los Nexus 9000. En el diseño de red del DCA todos los Nexus 2000 se conectan hacia los Nexus 9000, la configuración de los puertos se la realizará en cada uno de los equipos Nexus 9000, ya que los Nexus 2000 no disponen de una interface de administración por comandos. En el siguiente Diagrama se puede observar cómo se conectan los equipos en la Capa Acceso:

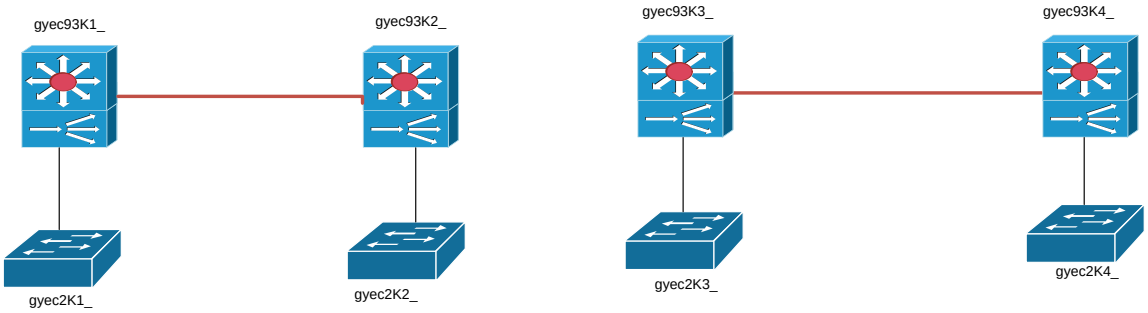


*Figura 16.* Conexiones Capa Acceso DCA
*Fuente*: Elaboración Propia

En la tabla de a continuación se muestra la cantidad de equipos en la capa Acceso

Tabla 20
*Cantidad Equipos Capa Acceso*

| # | Proveedor | Dispositivos | Modelo | Cantidad |
|---|---|---|---|---|
| **1** | CISCO | Switches | Nexus 9372 | 4 |
| **2** | CISCO | Switches | Extender 2248 | 6 |

*Fuente*: Elaboración Propia

#### *5.2.3.1. Características Cisco 9372*

La plataforma Cisco Nexus 9300 está compuesta por switches de puerto fijo diseñados para implementación de alto del rack (ToR – Top-of-Rack) y de media fila (MoR – Middle of the Row) en centros de datos que admiten aplicaciones empresariales, hosting de proveedores de servicios y entornos de cloud computing. Son switches Capa 2 y 3 con interfaces de 10 y 40 Gigabit Ethernet llegando a un ancho de banda interno de hasta 2.56 terabits por segundo (Tbps).

Específicamente los equipos Cisco Nexus 9372PX son Switches de 1RU que admiten 1,44 Tbps de ancho de banda y más de 1150 mpps en 48 puertos fijos de 10 Gbps SFP + y 6 puertos fijos de 40 Gbps QSFP +. (Cisco, 2017, Cisco Nexus 9300 Platform Switches Data Sheet)

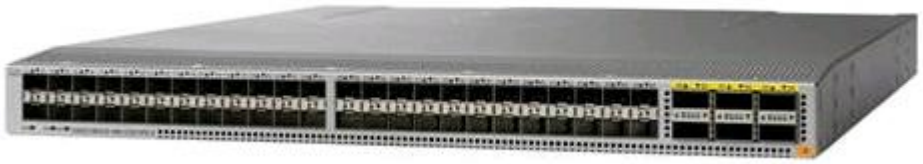

*Figura 17.* Cisco Nexus 9372PX Switch
*Fuente*: (Cisco, 2017, Cisco Nexus 9300 Platform Switches Data Sheet)

Algunas especificaciones técnicas se indican en la tabla de a continuación:

Tabla 21
*Especificaciones Técnicas Cisco Nexus 9372*

| MODELO | Cisco Nexus 9372PX |
|---|---|
| **Puertos** | 48 fijos 1/10-Gbps SFP+ y 6 puertos QSFP+ |
| **Velocidad Soportadas** | 1/10 Gigabit Ethernet |
| **Puerto Uplink 40 Gigabit Ethernet** | 6 puertos fijos QSFP+ |
| **Fuentes de Poder (hasta 2)** | 650W AC, 930W DC, o 1200W HVAC/HVDC |
| **Consumo típico (AC & DC)** | 210W |
| **Voltaje entrada (AC)** | 100 a 240V |
| **Voltaje entrada (DC)** | -40V a -72V DC (min-max)<br>-48V a -60V DC (nominal) |
| **Frecuencia (AC)** | 50 a 60 Hz |
| **Ventiladores** | 4 |
| **Dimensiones Físicas (Al x An x P)** | 4.4 x 43.9 x 57.1 cm |

*Fuente*: (Cisco, 2017, Cisco Nexus 9300 Platform Switches Data Sheet)

Adicional a las características técnicas se puede resumir otras especificaciones de estos equipos.

Tabla 22
*Especificaciones adicionales Cisco Nexus 9372*

| Especificaciones | Resumen |
|---|---|
| **Alto rendimiento previsible** | La latencia de 1 a 2 microsegundos con un ancho de banda de hasta 1,28 Tbps permite a los clientes crear una robusta estructura de conmutación de red desde sólo 200 puertos de servidor de 10 Gbps a más de 200.000 puertos de servidor de 10 Gbps. |
| **Incremento de espacio del búfer integrado** | Hasta un total de 50 MB de espacio de búfer integrado compartido permite una mejor gestión de la diferencia de velocidad entre los puertos de acceso y de uplink. |
| **Diseñado para disponibilidad** | Las fuentes de alimentación redundantes y las bandejas del ventilador removibles en caliente aumentan disponibilidad del equipo |
| **CPU, SSD, y memoria** | Las CPU x86 de 2,5 GHz de doble núcleo con unidad SSD de 64 GB y 16 GB de memoria proporcionan un rendimiento de red mejorado. |

*Fuente*: (Cisco, 2017, Cisco Nexus 9300 Platform Switches Data Sheet)

#### *5.2.3.2. Características Cisco 2248*

El equipo extensor Cisco Nexus 2248PQ de 10 Gigabit Ethernet es uno de los dispositivos más recientes en la gama de Switches extensores Cisco Nexus. Soporta entornos de 10 Gigabit Ethernet de alta densidad y cuenta con 48 puertos host SFP + de 1 y 10 Gigabit Ethernet y 4 puertos QSFP + fabric (16 puertos de 10 Gigabit Ethernet). La conectividad QSFP + simplifica el cableado mientras reduce el coste de la solución. El extensor Cisco Nexus 2248PQ 10GE soporta FCoE (Fiber Channel over Ethernet) y un conjunto de tecnologías de red conocidas como Data Center Bridging (DCB) que aumentan la confiabilidad, la eficiencia y la escalabilidad de las redes Ethernet. Estas características permiten el soporte de varias clases de tráfico sobre Ethernet sin pérdidas, permitiendo así la consolidación de entornos LAN, SAN y de clúster. (Cisco, 2016, Cisco Nexus 2000 Series Fabric Extenders Data Sheet)

*Figura 18.* Cisco Nexus N2248PQ
*Fuente*: (Cisco, 2016, Cisco Nexus 2000 Series Fabric Extenders Data Sheet)

Las especificaciones técnicas de estos equipos se indican en la tabla de a continuación:

Tabla 23
*Especificaciones Técnicas Cisco Nexus 2248*

| DESCRIPCION | Cisco Nexus 2248TP | Cisco Nexus 2248PQ |
|---|---|---|
| **Interfaces** | ● 48 | ● 48 |
| **Tipo de Interfaces** | ● Puertos 100BASE-T/1000BASE-T: Conectores RJ-45 | ● Puertos 1/10 Gigabit Ethernet SFP/SFP+ |
| **Velocidad** | ● 40 Gbps en cada dirección (80 Gbps full dúplex) | ● 160 Gbps en cada dirección (320-Gbps full dúplex) |
| **Performance** | ● Reenvío en Hardware de 176 Gbps o 131 mpps | ● Reenvío en Hardware de 1280 Gbps o 952 mpps |
| **Compatibilidad Switches Cisco** | ● Serie Cisco Nexus 5000<br>● Cisco Nexus 6000<br>● Serie Cisco Nexus 7000<br>● Serie Cisco Nexus 9000 | ● Serie Cisco Nexus 5000<br>● Cisco Nexus 6000<br>● Serie Cisco Nexus 7000<br>● Serie Cisco Nexus 9000 |
| **Dimensiones (Al x An x P)** | ● 4.37 x 43.94 x 44.96 cm | ● 4.37 x 43.94 x 44.96 cm |
| **Peso** | ● 8.0 kg | ● 8.0 kg |
| **Ambiental** | Temperatura de Operación: 0 a 40°C | Temperatura de Operación: 0 a 40°C |
| **Potencia de Entrada Típica** | ● 95W (max 110W) | ● 175W (max 234W) |
| **Corriente de Entrada** | ● 1.0A/1.2A (típica/máxima) | ● 1.46A/1.95A (típica/máxima) |
| **Corriente de Salida** | ● 8A/10A (típica/máxima) | ● 13A/20A (típica/máxima) |
| **Disipación de calor** | ● 322/403 BTU/hora (típica/máxima) | ● 597/798 BTU/hora (típica/máxima) |

*Fuente*: (Cisco, 2016, Cisco Nexus 2000 Series Fabric Extenders Data Sheet)

### 5.2.4. Diseño de la Zona de DMZ

La zona desmilitarizada sirve para asegurar la separación de la red de la empresa. Esta es la separación entre el nivel de seguridad 0 a 3 y el nivel 4 a 5. Esta separación es necesaria según estándar IACS (Industrial Automation and Control System) y las mejores prácticas para aprovechar la disponibilidad y la seguridad que se consideran requisitos críticos para el giro de negocio de la empresa. Entre las principales características de la zona Desmilitarizada se tiene las siguientes:

1. Hacer cumplir la autenticación de los usuarios que intentan acceder a datos o servicios
2. Controlar estrictamente el flujo de tráfico
3. Realizar inspección de paquetes con estado y detección / protección de intrusiones
4. Proporcionar seguridad y soporte de administración de red

La zona DMZ es creada para agrupar los servicios de la empresa que se encuentran publicados al internet, con el fin de proveer una capa adicional de seguridad a la red LAN del DCA, por lo que un usuario externo solo podrá acceder a esta zona mientras el resto de la red permanece protegida tras uno o varios dispositivos de seguridad como Firewalls.

Con el propósito de agrupar en una zona separada los servicios DMZ expuestos a Internet se considera tener equipos de red exclusivos para la conexión de los server DMZ. Adicional el diseño objetivo de la infraestructura de red considerará realizar una separación tanto lógica como física de esta zona: una para aplicaciones Transaccionales y otra para aplicaciones No Transaccionales de acuerdo al siguiente criterio de categorización:

Tabla 24
*Criterios Categorización DMZ*

| DMZ | ZONA | CRITERIO |
|---|---|---|
| DMZ1 | Servicios Transaccionales | En esta zona se agrupan los servers que brindan un servicio en el que se intercambian datos sensitivos del |

| | | |
|---|---|---|
| | | cliente (transacciones de dinero, etc.) |
| DMZ2 | Servicios No Transaccionales | En esta zona se agrupan los servers que brindan un servicio no sensitivo hacia internet (webmail, información página Web, etc.) |

*Fuente*: Elaboración Propia

Para lograr el objetivo de tener una separación lógica como física, se agrupan los server de servicios transaccionales en un Switch y los servers de servicios, no transaccionales en otro dispositivo físico. En cada uno de estos equipos se definen VLANs Capa 2. El default Gateway de las VLANs y sus respectivos segmentos de red será el equipo F5, el cual a través de su módulo LTM, balanceará el tráfico externo hacia los servidores, los mismos que estarán agrupados en una granja se servers (varios servidores que brinda un solo servicio). Más adelante se explicará sobre las funciones del equipo F5.

La arquitectura objetivo de la zona DMZ se muestra en la siguiente figura:

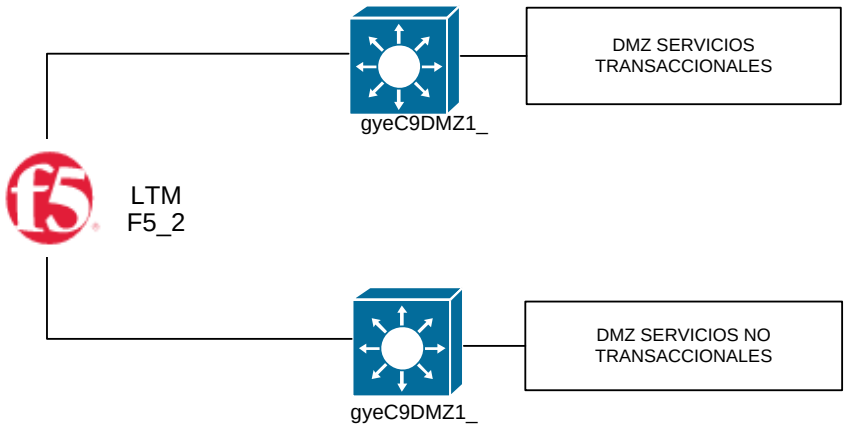


*Figura 19.* Arquitectura Zona DMZ
*Fuente*: Elaboración Propia

Para la implementación de esta zona se consideran los siguientes equipos de red:

Tabla 25
*Cantidad Equipos Capa Acceso*

| # | Proveedor | Dispositivos | Modelo | Cantidad |
|---|---|---|---|---|
| 1 | CISCO | Switches | Nexus 9372 | 2 |

*Fuente*: Elaboración Propia

Las características técnicas de los equipos utilizados en la zona DMZ son las mismas presentadas en el aparado 5.2.3.1 Características Cisco 9372.

### 5.2.5. Diseño de la Zona de Administración Fuera de Banda (Out-of-Band)

En el análisis realizado de la red LAN del DCP se evidenció que no se tiene una independencia de la red principal de datos con la red de administración, ya que a través de los mismos dispositivos de red a los cuales se conecta las interfaces de datos, se conectan también las interfaces de administración. Al evidenciar este punto de mejora, se implementa en el Datacenter Alterno el diseño de una red de administración fuera de Banda.

El propósito de la administración fuera de banda es independizar el tráfico de gestión de la red, con una solución de administración fuera de Banda se tiene un medio alternativo de acceder a dispositivos de red remotos cuando la red principal esté no disponible.

Para cumplir este objetivo en la arquitectura de red del DCA se implementa una zona para la administración fuera de banda, en esta zona todas las interfaces de administración de los dispositivos, ya sean de red (Routers, Switches), de seguridad (Firewall, IPS, DDoS) servidores (ILO - Integrated Lights-Out), storages, etc., se conectaran a los dispositivos de red que se encuentren en esta zona.

El diseño de la zona de administración de fuera de Banda incluye 3 Switches Cisco configurados en Stack (Lógicamente se ve como un solo equipo), a los cuales se conectaran todas las interfaces de administración de los equipos dentro de la infraestructura LAN del DCA, el acceso a los Switches de administración estará protegido tras el Firewall de Terceros, para permitir solo a los usuarios administradores el acceso a los mismos.

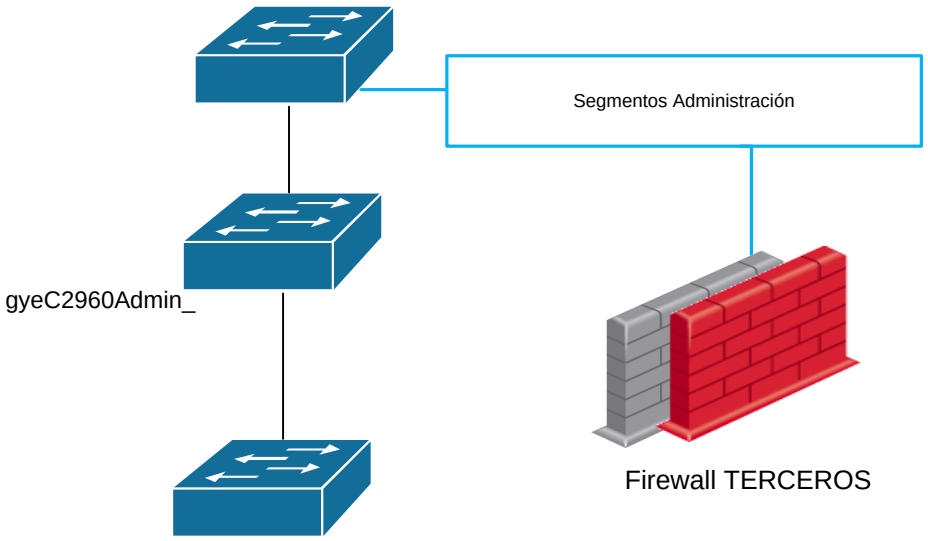


*Figura 20.* Arquitectura Zona de Administración Fuera de Banda
*Fuente*: Elaboración Propia

En los equipos Switch de administración se configura VLANs capa 2 de cada segmento de administración, el default Gateway de estos segmentos se encuentra definido en la Interfaz del Firewall de Terceros, el mismo que también maneja el enrutamiento desde y hacia los segmentos de gestión.

En la tabla de a continuación se muestra la cantidad de equipos en la zona de Administración fuera de Banda.

Tabla 26
*Cantidad Equipos zona Administración fuera de Banda.*

| # | Proveedor | Dispositivos | Modelo | Cantidad |
|---|---|---|---|---|
| 1 | CISCO | Switches | 2960X | 3 |

*Fuente*: Elaboración Propia

#### *5.2.5.1. Características Switch 2960X*

Dentro de las características principales de este equipo se encuentran las siguientes. (Cisco, 2017, Cisco Catalyst 2960-X and 2960-XR Series Switches Data Sheet):

- 24 o 48 puertos Gigabit Ethernet con rendimiento de reenvío de velocidad de línea
- Uplinks de 1 Gigabit SFP (Small Form-Factor Pluggable) o 10G SFP +
- FlexStack Plus para apilar hasta 8 switches con 80 Gbps de rendimiento de stack.
- Soporte Power over Ethernet Plus (PoE +) con hasta 740 W de consumo.
- Reducción del consumo de energía y funciones avanzadas de administración de energía
- Interfaces de gestión USB y Ethernet para operaciones simplificadas
- Características de Cisco IOS software  LAN Base o LAN Lite Cisco
- IP Lite Software Cisco IOS con enrutamiento dinámico y funciones de Capa 3

### 5.2.6. Diseño de la zona de entrada/salida hacia Internet.

La entrada/salida a Internet del centro de datos Alterno se ha diseñado para ofrecer conectividad mediante dos enlaces hacia Internet, que son usados para diferentes propósitos. El primer enlace es utilizado para las  operaciones del giro del negocio como publicación de servicios que acceden desde el exterior, y el segundo enlace es utilizado para funciones que soportan al giro de negocio como navegación de los usuarios internos.

Para realizar esta diferenciación de la utilización de Internet se maneja dos Routers Cisco que son los que se conectan directamente hacia la red del proveedor de servicios de Internet. Como dispositivo de seguridad de ataques del exterior se utiliza un equipo anti DDoS que está conectado a los Routers de internet mediante dos Switches Cisco para su interconexión.

Luego de los equipos mencionados en el párrafo anterior se encuentra conectado el Dispositivo F5-GTM el cual será el encargado de manejar la resolución DNS de los

servidores expuestos a internet del DCA. Más adelante se detallará sobre las funciones de este equipamiento.

A continuación se indica la arquitectura propuesta para la salida hacia internet del Datacenter Alterno.

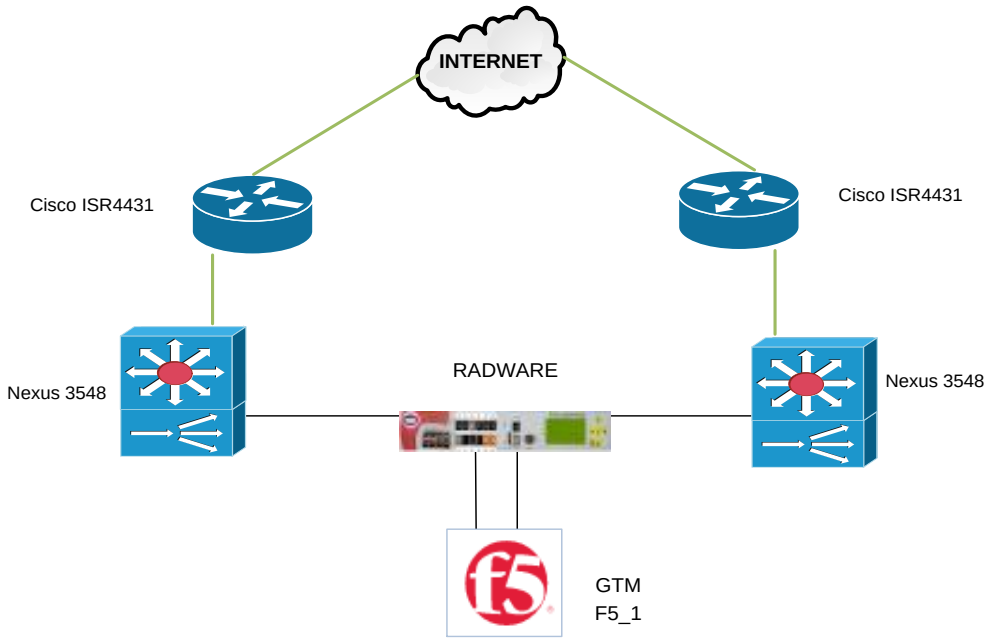


*Figura 21*. Arquitectura Zona para la Salida de Internet
*Fuente*: Elaboración Propia

Los equipos utilizados para la conexión hacia internet se indican en la siguiente tabla:

Tabla 27
*Cantidad Equipos Interconexión hacia Internet*

| # | Proveedor | Dispositivos | Modelo | Cantidad |
|---|---|---|---|---|
| **1** | CISCO | Routers | ISR 4431 | 2 |
| **2** | CISCO | Switches | Nexus 3458 | 2 |

*Fuente*: Elaboración Propia

#### *5.2.6.1. Características Routers ISR 4431*

La serie de los Routers Cisco ISR 4431 incluye varias características como las siguientes:

Tabla 28
*Especificaciones Técnicas Cisco ISR 4431*

| **EQUIPO** | Cisco ISR 4431 |
|---|---|
| **Especificaciones Generales** | • Tamaño en Rack: 1 UR<br>• Protocolos de Enrutamiento: OSPF, IS-IS, RIP-1, RIP-2, BGP, EIGRP, DVMRP, PIM-SM, IGMPv3, GRE, PIM-SSM, ruteo estático IPv4 y IPv6 , Ruteo Basado en Políticas (PBR), IPv4 |
| **Especificaciones Eléctricas** | • Voltaje: AC 120/230 V<br>• Frecuencia: 50/60 Hz<br>• Tipo: Fuente de Poder Interna |
| **Networking** | • Switch Montable en Rack<br>• Protocolo de Enlace de Datos: Ethernet, Fast Ethernet, Gigabit Ethernet<br>• Protocolos de Transporte: DHCP, IPSec, PPPoE<br>• Características: Listas de Control de Acceso (ACL), Class-Based Weighted Fair Queuing (CBWFQ), soporte VLAN, soporte VPN, Weighted Random Early Detection (WRED), protección a nivel de Firewall, VPN dinámica Multipunto (DMVPN), NetFlow, Calidad de Servicio (QoS), soporte RADIUS, soporte Syslog |
| **Interfaces Provistas** | • Ethernet 10Base-T/100Base-TX/1000Base-T<br>• Cantidad: 1,2,4<br>• Tipo Conector: 4 pin USB Tipo A, RJ-45, SFP (mini-GBIC), mini-USB Tipo B |
| **RAM** | • Tamaño máximo: 16 GB<br>• Tecnología: DDR3 SDRAM<br>• Flash Memory: Max 32 GB |
| **Parámetros Ambientales** | • Temperatura de Operación: de 0 a 40 ° C |
| **Performance** | • Throughput Agregado: 500 Mbps |
| **Dimensiones Físicas** | • Al x An x P: 4,3 x 43,6 x 50,8<br>• Peso: 8,4 Kg |

*Fuente*: CNET. Cisco ISR 4431 - Security Bundle - router - rack-mountable

#### *5.2.6.2. Características Switches Cisco 3548*

El Cisco Nexus 3548 integra la tecnología Boost en un formato compacto de 1 unidad de rack (1RU) para proporcionar un rendimiento, una visibilidad y un control notable. Ofrece switching de capa 2 y 3 a velocidad de cable con un completo conjunto de funciones El

switch es idóneo para los entornos de transacciones de alto rendimiento (High-Performance Trading, HPT) y Big Data. (Cisco. Switch Cisco Nexus 3548)

Entre las características técnicas más importante se tiene las siguientes:

Tabla 29
*Especificaciones técnicas Switch Cisco 3548*

| EQUIPO | Cisco Nexus 3548 |
|---|---|
| **Especificaciones Físicas** | • 48 puertos fijos SFP+ (1 or 10 Gbps)<br>• Fuentes de Poder removibles en caliente redundantes<br>• Cuatro ventiladores individuales removibles en caliente redundantes<br>• Dos puertos de administración 10/100/1000-Mbps<br>• Un Puerto de Consola serial RS-232<br>• Un Puerto USB |
| **Performance** | • Capacidad de Switching de 960-Gbps<br>• Tasa de transmisión de 720 millones de paquetes por segundo (mpps)<br>• Throughput de tráfico a nivel de transferencia en línea (ambos capa 2 y 3) en todos los puertos<br>• Unidades de transmisión máxima configurables (MTU) de hasta 9216 bytes (jumbo frames) |
| **Potencia Operativa Típica** | • 152 watts (W) |
| **Maxima Potencia** | • 265W |
| **Típica disipación de calor** | • 519 BTUs por hora |

*Fuente*: (Cisco, 2017. Cisco Nexus 3548x and 3524x Switches Data Sheet)

### 5.2.7. Diseño de la zona de Acceso de Terceros.

Dentro de la infraestructura del Datacenter Alterno se diseña la zona de acceso de Terceros. Esta zona sirve para la conexión de sucursales de la empresa, empresas terceras y proveedores que requieran tener una comunicación con el DCA. La conexión de esta zona se muestra en la figura siguiente.

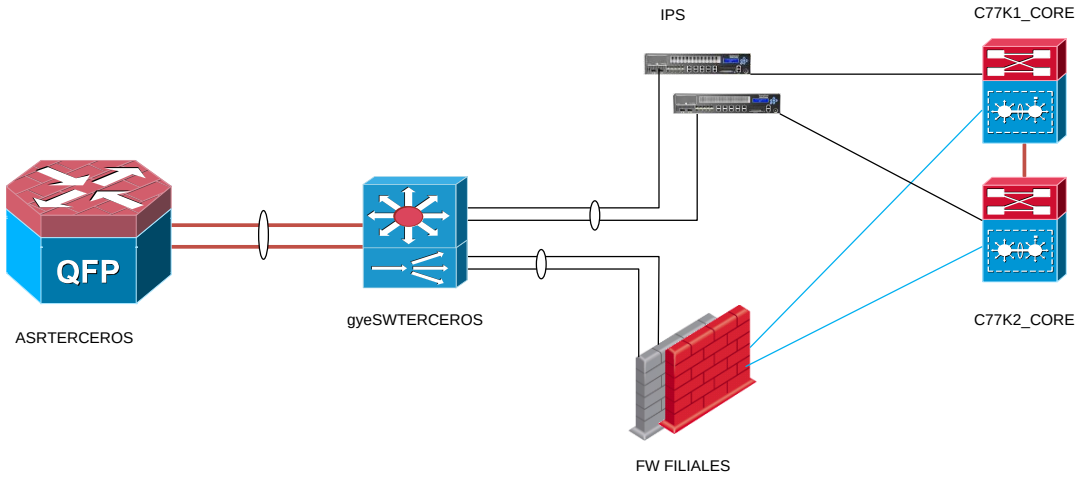


*Figura 22.* Arquitectura Zona de Acceso de Terceros
*Fuente*: Elaboración Propia

La conectividad de esta zona se realiza a través de la conexión de un router y un Switch Cisco. Los equipos utilizados son:

Tabla 30
*Cantidad Equipos Conexión Acceso Terceros*

| # | Proveedor | Dispositivos | Modelo | Cantidad |
|---|---|---|---|---|
| **1** | CISCO | Routers | ASR 1006 | 1 |
| **2** | CISCO | Switches | 4500X | 1 |

*Fuente*: Elaboración Propia

Todas las comunicaciones entrantes de la zona de terceros pasarán a través del clúster de firewall Tercero para filtrado de datos y un dispositivo IPS para la detección y prevención de intrusiones antes de que el tráfico fluya hacia la red central.

El equipo ASR1006 será el concentrador de los enlaces que se mantendrá con todas las sucursales, proveedores, empresas terceras. En este equipo se realizar la configuración de los enlaces mediantes Túneles GRE Punto a Punto.

El equipo Cisco 4500X permitirá la conexión de las sucursales, proveedores, empresas terceras hacia la red interna, mediante dos rutas: Firewall o IPS directo hacia la red de Core.

La diferenciación de estos dos caminos se realiza debido a que se requiere mantener el esquema de conectividad de las sucursales hacia la red interna que se tiene en el DCP, en el cual estas localidades no atraviesan firewall, caso contrario sucede con las empresas terceras, proveedores ya el acceso de estos últimos por temas de seguridad requieren atravesar el firewall.

Para lograr este enrutamiento diferenciado se configura una PBR (Policy Based-Routing) un enrutamiento basado en políticas. La aplicación de PBR se realiza mediante ACL que permitirá el tráfico de ciertos segmentos de red.

Con la aplicación de un PBR se determina el siguiente salto a realizar basado en la dirección de origen, en este caso para las sucursales su siguiente salto será el Switch de Core, previamente atravesando el IPS, y para empresas terceras, proveedores el siguiente salto será el Firewall de Terceros.

#### *5.2.7.1. Características Cisco ASR 1006*

La Serie Cisco ASR 1000 (Aggregation Services Routers) es una plataforma de nueva generación diseñada para ofrecer una gran variedad de servicios con un excelente desempeño (5 a 20 Gbps) y alta flexibilidad. Construida como una plataforma modular con una clara separación entre el Plano de Control y el Plano de Reenvío, posee una avanzada arquitectura de software (IOS-XE) que le otorga una alta escalabilidad y amplia variedad de servicios. (Cisco, 2017, Cisco ASR 1000 Series Aggregation Services Routers Data Sheet)

*Figura 23.* Cisco ASR1006
*Fuente*: (Cisco, 2017, Cisco ASR 1000 Series Aggregation Services Routers Data Sheet)

Entre las principales características técnicas del equipo ASR1006 se tiene las siguientes:

Tabla 31
*Especificaciones Técnicas Cisco ASR 1006*

| EQUIPO | ASR 1006 |
|---|---|
| GENERAL | |
| **Capacidad** | Rutas IPv4: 4000000<br>Rutas IPv6: 4000000<br>Reglas ACL: 16000<br>Túneles IPSec VPN: 10000<br>Entradas NAT: 1000000<br>Túneles concurrentes: L2TP VPN: 16000<br>Entradas QoS Hardware: 128000<br>Túneles concurrentes IPSec: 10000 |
| **RAM** | 6 GB |
| **Protocolo de direccionamiento** | GRE |
| DISPOSITIVO DE ALIMENTACIÓN | |
| **Voltaje nominal** | AC 120/230 V |
| **Frecuencia requerida** | 50/60 Hz |
| **Tipo** | Fuente de Poder Interna |
| REDES | |
| **Tipo** | Router |
| **Tecnología de conectividad** | Cableada |
| **Red / Protocolo de transporte** | DHCP, IPSec |
| **Características** | Soporte Access Control List (ACL), Dynamic Multipoint VPN (DMVPN), protección de firewall, balanceo de carga, |

| | |
|---|---|
| | soporte IPv6, soporte Jumbo Frames, soporte MPLS VPN, MPLS, NAT, Calidad de servicio (QoS), Stateful switchover (SSO), Soporte VPN |
| **Protocolo de direccionamiento** | GRE |
| **Protocolo de gestión remota** | CLI, SNMP, SSH, Telnet |
| | |
| CHASIS | |
| **Dispositivos instalados / N° módulos** | 3 |
| **Nº de dispositivos/módulos admitidos** | 19 |
| | |
| POTENCIA | |
| **Cantidad Instalada** | 2 (instalada) / 2 (max) |
| **Redundancia de alimentación** | Si |
| | |
| INTERFAZ PROPORCIONADA | |
| **Interfaz** | Ethernet 10Base-T/100Base-TX, auxiliar, consola |
| **Cantidad** | 1 |
| **Tipo de conector** | RJ-45 |
| | |
| RAM | |
| **Tamaño instalado** | 6 GB |
| | |
| SOFTWARE / REQUISITOS DEL SISTEMA | |
| **Tipo** | Cisco IOS Advanced Enterprise Services |
| | |
| PARÁMETROS AMBIENTALES | |
| **Temperatura mínima de funcionamiento** | 0 °C |
| **Temperatura máxima de funcionamiento** | 41 °C |
| | |
| ESPECIFICACIONES FISICAS | |
| **Ancho** | 437.4 mm |
| **Profundidad** | 461.0 mm |
| **Altura** | 266.7 mm |

*Fuente:* (CNET. Cisco ASR 1006 VPN Bundle – router)

#### *5.2.7.2. Características Cisco 4500X*

El equipo Cisco Catalyst 4500-X Series es un Switch de agregación fija que ofrece la mejor escalabilidad en su clase, virtualización de red simplificada y servicios de red integrados para entornos con limitaciones de espacio. Cumple los objetivos de crecimiento empresarial con una escalabilidad sin precedentes, simplifica la virtualización de la red con soporte para redes virtuales de uno a muchos y permite las aplicaciones emergentes mediante

la integración de muchos servicios de red. (Cisco, 2016. Cisco Catalyst 4500-X Series Fixed 10 Gigabit Ethernet Aggregation Switch Data Sheet)

*Figura 24.* Cisco 4500X**¡Error! Marcador no definido.**
*Fuente*: (Cisco, 2016. Cisco Catalyst 4500-X Series Fixed 10 Gigabit Ethernet Aggregation Switch Data Sheet)

Entre las principales características técnicas del equipo Cisco 4500x se tiene las siguientes:

Tabla 32
*Especificaciones Técnicas Cisco 4500X*

| EQUIPO | CISCO 4500X |
|---|---|
| GENERAL | |
| **Subtipo** | 10 Gigabit Ethernet |
| **Puertos** | 16 x 10 Gigabit SFP+ |
| **Capacidad** | Entradas de la tabla de reenvío IPv4: 64000<br>Entradas de la tabla de reenvío IPv6: 32000<br>Entradas NetFlow : 128000<br>Virtual interfaces (VLANs): 4094<br>Grupos IGMP: 32000<br>Entradas Multicast (IPv4): 24000<br>Entradas Multicast (IPv6): 12000<br>Entradas ARP: 47000<br>Instancias Spanning Tree Protocol: 10000<br>Colas QoS hardware: 64<br>Entradas QoS hardware: 128000<br>Entradas ACL: 131072 |
| **Admite carcasa Jumbo** | 9216 bytes |
| **RAM** | 4 GB DDR2 SDRAM |
| **Tamaño de tabla de dirección MAC** | 55K entradas |
| DISPOSITIVO DE ALIMENTACIÓN | |
| **Consumo eléctrico en funcionamiento** | 330 Watt |
| **Conexión en caliente** | hot-plug |
| **Tipo** | Fuente de Poder Interna |
| REDES | |
| **Tamaño de tabla de dirección MAC** | 55K entradas |
| **Características** | Soporte Access Control List (ACL), Quality |

| | |
|---|---|
| | of Service (QoS), Soporte VLAN, Capa 2 switching, Ventiladores redundantes hot swappable |
| **Cumplimiento de normas** | IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3, IEEE 802.3ad (LACP), IEEE 802.3ae |
| **Cantidad de puertos** | 16 |
| **Protocolo de gestión remota** | RMON 1, RMON 2 |
| **Throughput** | 125 Mpps, 250 Mpps, 800 Gbps |
| | |
| POTENCIA | |
| **Cantidad instalada** | 2 (instalada) / 2 (max) |
| **Redundancia de alimentación** | Si |
| | |
| INTERFAZ PROPORCIONADA | |
| **Interfaz** | 10Gb Ethernet / 1Gb Ethernet, Ethernet 10Base-T/100Base-TX/1000Base-T, consola |
| **Cantidad** | 16,1 |
| **Tipo de conector** | RJ-45, SFP/SFP+ |
| | |
| RAM | |
| **Tamaño instalado** | 4 GB |
| **Tecnología** | DDR2 SDRAM |
| | |
| PARÁMETROS AMBIENTALES | |
| **Temperatura mínima de funcionamiento** | 0 °C |
| **Temperatura máxima de funcionamiento** | 41 °C |
| | |
| ESPECIFICACIONES FISICAS | |
| **Ancho** | 437.4 mm |
| **Profundidad** | 461.0 mm |
| **Altura** | 266.7 mm |

*Fuente*: (CNET, Cisco Catalyst 4500-X - switch - 16 ports - rack-mountable Series)

### 5.2.8. Diseño de la arquitectura para implementación de Dispositivos de Seguridad en el DCA

Al igual que el diseño de los equipos de red es importante para el flujo correcto de las conexiones de datos dentro del Datacenter Alterno, para cumplir con las operaciones del giro de negocio de la empresa, otro factor importante a tomar en cuenta es la seguridad de estos datos es por ello que se ha contemplado en el diseño de la arquitectura de red implementar

dispositivos de seguridad que cumplan con el trabajo de proteger a la red de ataques, intrusos, etc., manteniendo la confidencialidad, integridad y disponibilidad de los datos que se manejan dentro del DCA.

Para ello se incluye en el diseño de la arquitectura de red tres dispositivos importantes para mantener la seguridad de la red del Datacenter Alterno, estos equipos son: Anti DDoS, IPS y Firewalls. En los siguientes apartados se presentara en detalle cada uno de ellos.

#### *5.2.8.1. Diseño Equipamiento de Seguridad Anti DDoS*

Un ataque distribuido de denegación de servicio (DDoS) se produce cuando varios sistemas externos inundan los recursos de la empresa, normalmente uno o más servidores web externos. Un dispositivo anti DDOS ayuda a prevenir tal ataque en los recursos de la empresa.

Al igual que en el DCP, en el Datacenter Alterno se recomienda la implementación de un equipo anti-DDoS que busca cumplir los siguientes objetivos con el diseño de su arquitectura de red:

- Implementar el equipo anti-DDoS en el Segmento de la Red_DCA (toda la red del DCA va estar protegida).
- Prevenir y detectar ataques de intrusión en los segmentos monitoreados.
    - Worms, Spyware, Virus.
    - Vulnerabilidades de sistemas operativos.
    - Vulnerabilidades de infraestructura de red.
    - DDoS.
    - HTTP Flood
    - Sync Flood.
    - Escaneo de puertos

- Garantizar una gestión unificada de las amenazas bajo una misma consola de administración.
- Alta disponibilidad del servicio de red a través bypass interno en el dispositivo.
- Alertas inmediatas en caso de detección y bloqueo de ataques o amenazas.

El dispositivo recomendado para este propósito es Radware DefensePro 10420. El cual en lugar de tener redundancia, se configurará con un Bypass para garantizar que el fallo de este dispositivo no reduzca la funcionalidad general de Internet.

A diferencia del diseño del DCP en el cual el equipo anti-DDoS protege solo a la red de publicación de servicios del DCP, en el DCA el equipo Radware DefensePro protegerá toda la red interna del Datacenter Alterno.

Como se indicó anteriormente para el diseño propuesto se plantea la adquisición de un equipo Radware DefensePro 10420 (10 segmentos fibra a 1GB o 10GB y 2 segmentos a 40GB) y un equipo de administración Radware APSolute Vision Server.

La distribución de equipos quedará de la siguiente manera:

- Radware DefensePro 10420 cubrirá los siguientes segmentos: Segmento Red_DCA (toda la red del DCA va estar protegida)
- El equipo Radware APSolute Vision será la consola de administración centralizada de los equipos DefensePro y el servidor de reportes.

Al ser un equipo que protege de Ataques externos de la red interna se lo debe ubicar lo más cercano posible a las conexiones de la red interna del DCA con el exterior, en este caso sería con la entrada/salida a Internet.

El equipo se colocará entre los Routers de conexión a Internet y el equipo F5, a través de interfaces de 10 GB a fibra, en la siguiente ilustración se muestra su conexión:

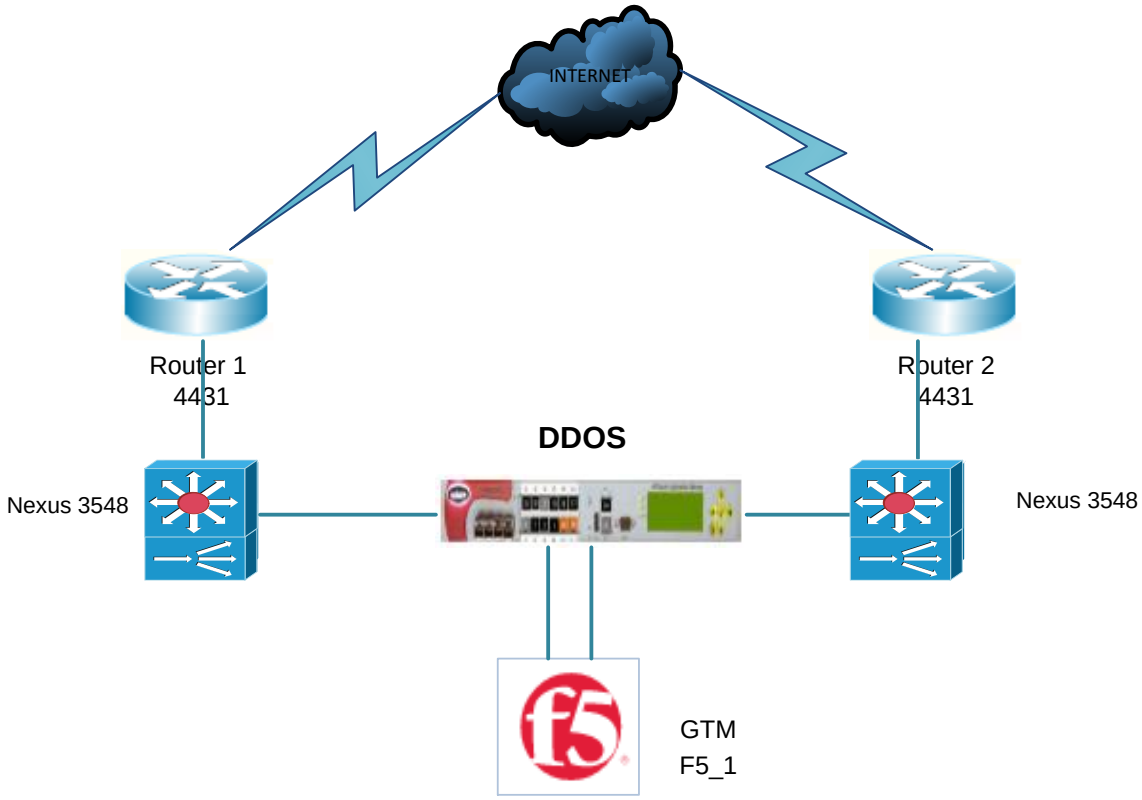


*Figura 25.* Arquitectura Equipo Anti-DDoS
*Fuente*: Elaboración Propia

Los equipos utilizados para el diseño de la protección anti-DDoS son:

Tabla 33
*Cantidad Equipos Anti-DDoS*

| # | Proveedor | Dispositivos | Modelo | Cantidad |
|---|---|---|---|---|
| **1** | RADWARE | Anti-DDoS | ProDefense x10420 | 1 |
| **2** | RADWARE | Consola Administración | APSolute Vision Server | 1 |

*Fuente*: Elaboración Propia

#### *5.2.8.1.1. Funcionamiento equipo Anti-DDoS*

Las probabilidades de tener que enfrentarse a un ataque DDoS son muy altas, y los intentos numerosos. El objetivo de un ataque DDoS es inhabilitar un servidor, un servicio o una infraestructura sobrecargando el ancho de banda del servidor o acaparando sus recursos hasta agotarlos.

Durante un ataque DDoS, se envían multitud de peticiones simultáneamente desde múltiples puntos de la Red. La intensidad de este "fuego cruzado" desestabiliza el servicio o, aún peor, lo inhabilita.

Para proteger los servicios y servidores de los ataques, los equipos anti - DDoS ofrecen una solución de mitigación, que se trata de una combinación exclusiva de técnicas destinadas a:

- Analizar en tiempo real y a alta velocidad todos los paquetes.
- Aspirar el tráfico entrante de su servidor.
- Mitigar, es decir, identificar todos los paquetes IP ilegítimos, dejando pasar los paquetes IP legítimos.(OVN, 2017)

El dispositivo Anti-DDoS supervisa el tráfico dirigido a direcciones IP especificadas en tiempo real y detecta el tráfico de acceso en los puntos de salida de la red para identificar cualquier ataque DDoS tan pronto como sea posible. A continuación, limpia el tráfico anormal de acuerdo con las políticas de defensa que el usuario ha configurado sin afectar los servicios normales.

El servicio Anti-DDoS puede defender las direcciones IP públicas de un usuario frente a los ataques de tráfico y aplicación.

Un dispositivo Anti-DDoS puede habilitarse sobre la base del tráfico máximo de acceso real y el número máximo de peticiones HTTP que un servicio de web implementado puede procesar. Todos los demás parámetros de política de defensa se establecen en un valor predeterminado por el sistema.

Si se detecta un ataque, los datos se desvían a los dispositivos de limpieza para la defensa en tiempo real. Se limpia el tráfico anormal y se envía el tráfico normal. (Telefónica, Anti DDoS)

#### *5.2.8.1.2. Características Equipo Anti-DDoS Radware*

Radware DefensePro es un sistema de protección de Intrusos y Denegación de Servicios en línea que detecta y previene amenazas en tiempo real. DefensePro inspecciona el tráfico entrante y saliente en busca de posibles ataques y limpia la red de tráfico malicioso no deseado.

Entre las especificaciones técnicas más relevantes de este equipo tenemos las siguientes:

Tabla 34
*Especificaciones técnicas equipo Anti-DDos Radware*

| EQUIPO | RADWARE PRODEFENSE 10420 |
|---|---|
| PERFORMANCE | |
| **Licencia de Throughput** | DP modelo 10420 - 10 Gbps |
| **Máx capacidad de mitigación / Rendim.** | 60Gbps |
| **Sesiones Concurrentes legítimas Max** | 6,000,000 |
| **Sesiones Concurrentes de ataques Max** | Sin limites |
| **Tasa de prevención Max para ataques de inundación DDoS** | 25,000,000 pps |
| **Latencia** | < 60 micro segundos |
| PUERTOS DE INSPECCION | |
| **1/10 GE** | 20 (SFP+) |
| **40 GE** | 4 (QSFP+) |
| MODO DE OPERACIÓN | |
| **Operación de Red** | Reenvío transparente capa 2 /Reenvío IP |
| **Modos de implementación** | En línea, Monitoreo de Puerto SPAN, Monitoreo de Puerto Copia; out-of-path local; Mitigación Out-of-path (Solución de un centro de Depuración) |
| **Protocolo de Tunneling** | VLAN Tagging, L2TP, MPLS, GRE, GTP, IPinIP |
| **Soporte IPv6** | SI |
| **Tramas Jumbo** | Soporta |
| **Acciones de Bloqueo** | Descarte de paquetes, reseteo (origen, destino, ambas) suspensión ( origen, puerto origen, destino, puerto destino, o cualquier combinación), Desafío de respuesta para trafico sospechosos de TCP, HTTP y DNS |

| | |
|---|---|
| ALTA DISPONIBILIDAD | |
| **Fallo Al Abrir/ Fallo al cerrar** | Internal fail-open / fail-close para puertos integrados de cobre; Falla al cerrar interno para los puertos de fibra o transceptores ópticos (Por ejemplo, SFP, SFP +, QSFP, QSFP28) |
| **Fuente de Poder Dual** | SI , removible en caliente |
| **Cluster Activo – Pasivo** | Si |
| | |
| ESPECIFICACIONES FÍSICAS | |
| **Dimensiones (AN x P x Al) mm** | 424 x 537 x 88 mm (2U) |
| **Peso** | 15.1 kg |
| **Potencia Consumida** | 634W |
| **Disipación de Calor** | 2162 BTU/h |
| **Temperatura de Operación** | 0-40°C |

*Fuente*: (Radware. DefensePro Overview)

#### *5.2.8.1.3. Configuraciones Equipo Anti-DDoS Radware*

Para la implementación de este equipo de seguridad se realizará las siguientes tareas en el DCA:

Configuración**:** Se realiza la configuración de políticas de protección para los servicios que tiene la Institución, es recomendable que las políticas estén en modo *Report Only*. Este modo permite visualizar todos los ataques para las protecciones que están configuradas en el DefensePro y tomar medidas al momento de cambiar el DP a modo *Block.*

Monitoreo y afinamiento**:** En esta fase se analiza los diferentes reportes para afinar las protecciones y poder cambiar la configuración de las políticas a modo *Block.*

Adicional dentro de la solución del dispositivo Anti-DDoS se cuenta con la consola de administración APSolute Vision, la cual es un sistema de gestión de última generación, que estandariza la administración de las soluciones de seguridad basadas en Radware. APSolute Vision ofrece:

- Seguimiento y control de múltiples dispositivos en una sola vista
- Generación de informes y estadísticas a nivel de dispositivo simultáneamente.
- Presentación de informes de seguridad con estándares internacionales.

- APSolute Vision también puede proporcionar informes personalizados por ejemplo tipo de ataque, duración, etc. y de nivel de red (Número de conexiones, throughput, etc).

En la parte de configuración de reglas y perfiles, el dispositivo ha sido configurado para trabajar en el modo: Report Only o modo escucha. Algunas características de la implementación de este equipo de seguridad son:

- La red se vuelve más manejable y flexible, de tal manera que es posible controlar los segmentos de red de acuerdo a políticas y criterios de administración adecuados.
- Se implementó seguridad de red perimetral de alta velocidad para garantizar la conectividad con un alto índice de disponibilidad del servicio.
- Existen tareas automáticas de actualización de base de datos de firmas, respaldo de configuración equipos y generación de reportes.
- Los respaldos de configuración serán grabados en el disco local, debido a que no se tiene un servidor dedicado para este propósito.

Dentro de la defensa contra ataques externos se ha creado políticas de protección de servidores. Estas políticas de protección protegen a los servidores contra ataques de Cracking (BruteForce) y HTTP Flood. Algunos de los Principales servicios existentes en la red que son susceptibles a ataques son:

Tabla 35
*Principales servicios dentro de la Infraestructura del DCA*

| NOMBRE DEL SERVICIO | DESCRIPCION |
|---|---|
| **Servicios WEB** | Acceso a diferentes servidores WEB de la empresa |
| **Correo electrónico** | Utilizado por todos los usuarios internos y externos como medio de comunicación. |
| **Aplicaciones WEB** | Sistemas de información utilizados por la entidad. |
| **Servicio DNS** | Servidor DNS |

*Fuente*: Elaboración Propia

**Estrategia de Implementación de Políticas**

Para aplicar dichas políticas se ha considerado armar una estrategia de implementación dividida en dos partes: Políticas de Red y Políticas de Server

Las políticas de Red se implementaran de la siguiente manera

- Definir una política global (Inbound) para todo el segmento de red destino.
    - Any → Red Internet (direccionamiento público)
    - Any → Red LAN DCA (Segmentos de red Principal, Servicios, PCI)

Las políticas de Servidores se implementaran de la siguiente manera

- Server Protections → Definir una política por servicio.
    - Server Cracking Protection – por servicio para HTTP, HTTPS, MAIL
    - HTTP Mitigator (automatic mode) – por dirección IP de los servidores Internet

Tabla 36

*Tabla de Políticas a implementar en Equipo Anti-DDoS*

| TIPO DE PROTECCION | DIRECCION | PROTECCION | RIESGO MITIGADO |
|---|---|---|---|
| **Regla Global** | Any -----> red global protegida | BDoS | DoS y Bdos |
| | | Signature Protection: Profile DoS-ALL | DoS - Herramientas y ataques conocidos |
| | | Syn-Protection | Para servicios TCP, protección ataque SYN DoS |
| | | Antiscanning | Protección contra escaneos horizontales y verticales de puertos |
| **Regla por Servicio** | Any -----> protected HTTP, MAIL, FTP Servers | BDoS | DoS y Bdos |
| | | Signature Protection: Profile Corp DMZ - Web, Mail | DoS - Herramientas y ataques conocidos |
| | Any -----> protected DNS Servers | DNS Protection | DNS query flood attacks |
| | | BDoS | DoS y Bdos |
| | | Signature protection: perfil personalizado Services = DNS y Complexity = Low | Vulnerabilidades conocidas |

*Fuente*: Elaboración Propia

**Configuración de perfiles de protección**

El detalle de los módulos habilitados en el equipo Radware ProDefense para la configuración de los perfiles de protección se indica en la tabla de a continuación:

Tabla 37
*Detalle de los módulos habilitados*

| MODULO | HABILITADO | DETALLE |
|---|---|---|
| **Signature Protection** | Si | Se habilitará las firmas de acuerdo a cada servicio que brinde cada dirección IP pública. |
| **BDos** | Si | Se habilitará únicamente protección de SYNC y TCP. |
| **Anti-Scanning** | Si | Se habilitará protección para protocolo TCP |
| **SYNC Flood Protection** | Si | Se habilitará protección para protocolo HTTP, HTTPS y SMTP |
| **HTTP Flood Protection** | Si | Se habilitará protección para protocolo HTTP |
| **Fraud Protection** | Si | Se habilitará para el tráfico de salida desde red de BG. |
| **Packet Anomaly** | Si | Se habilitará en todos los segmentos. |
| **Server Protection** | Si | Se habilitará únicamente en los servicios web con formularios y logins, FTP y SMTP. |

*Fuente*: Elaboración Propia

#### *5.2.8.2. Diseño Equipamiento de Seguridad IPS*

La institución tiene la necesidad de implementar soluciones que permitan asegurar la disponibilidad de la infraestructura en la que residen las aplicaciones que soportan los servicios críticos del negocio en el caso de presentarse un escenario de contingencia.

En la arquitectura Actual de la empresa se cuenta en su sitio principal un equipo HP Tipping Point para la protección IPS, por lo que para el sitio alterno debe contar con una infraestructura de la misma marca que permita la migración de las configuraciones y el establecimiento de esquema de contingencia entre sitios, disminuyendo el riesgo.

La solución propuesta comprende un conjunto de componentes totalmente integrables, escalables y flexibles, de tal manera, que permite responder a los diferentes retos que enfrente

la institución. Para lograr esto nos apoyamos en las características que ofrece HP Tipping Point.

El modelo definido para la empresa para la implementación en su sitio alterno es un IPS de nueva generación HP Tipping Point 2600 con una consola SMS para su administración.

En la infraestructura del Datacenter Alterno los segmentos a proteger por el IPS serán VDC PCI, VDC PRI, VDC Servicio, Terceros, Internet y DMZ.

Para los segmentos de las VDC, las conexiones que protegerá el IPS son las que están conectadas entre el Switch Nexus 7K con sus respectivos VDC y el clúster de Firewall Principal.

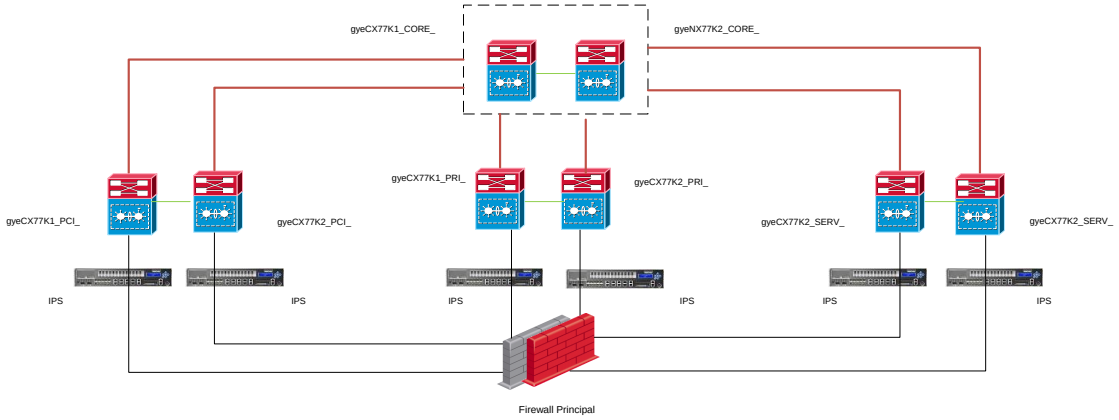


*Figura 26*. Conexión IPS – VDC
*Fuente*: Elaboración Propia

Para Internet se tendrán 2 segmentos para el PortChannel entre los Nexus 7K en la VDC de CORE y el Firewall de Borde y 1 segmento para la DMZA y otro segmento para la DMZ B. Las conexiones del IPS para la zona Zona Internet y DMZA y DMZB se muestra en la siguiente figura:

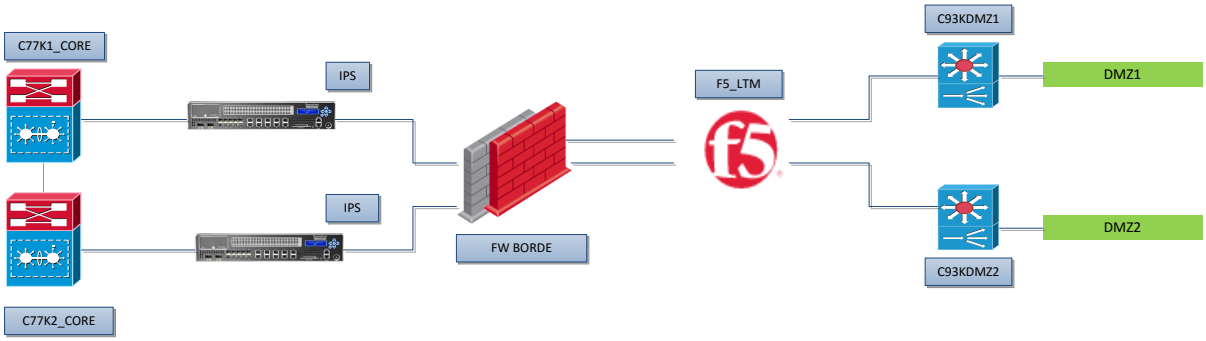


*Figura 27.* Conexión IPS Internet y DMZ
*Fuente*: Elaboración Propia

De igual manera las zonas que correspondan a Terceros tendrá 2 segmentos que interceptara el tráfico del PortChannel entre el Switch de Terceros y los Nexus 7K en la VDC de Core.

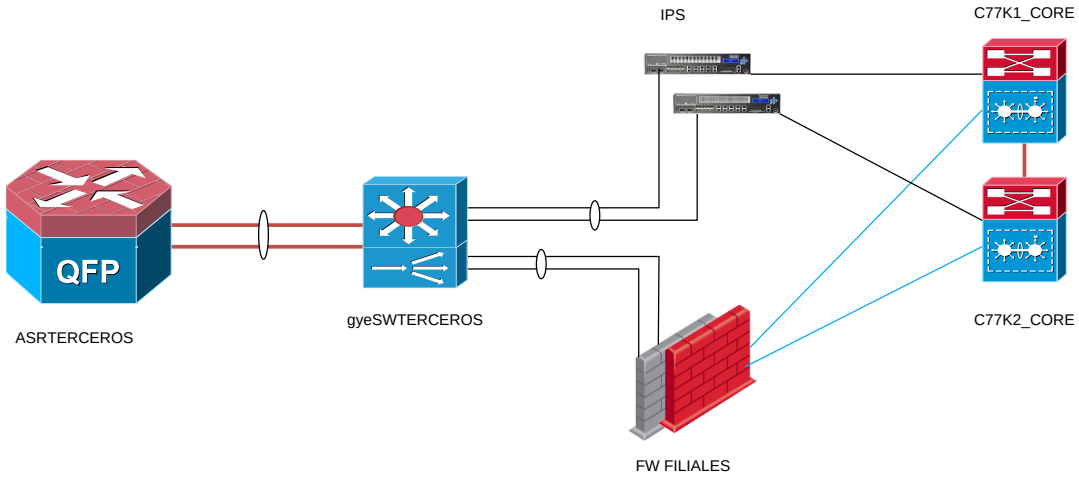


*Figura 28.* Conexión IPS – Terceros
*Fuente*: Elaboración Propia

Una vez realizadas estas configuraciones y asignaciones de segmentos, se procederá a solicitar la exportación de las políticas y reglas contenidas en el equipo Manager de Quito.

En resumen las conexiones físicas del equipo IPS se muestran en la tabla de a continuación:

Tabla 38
*Distribución Interfaces Equipos IPS*

| EQUIPO | CONEXION | INTERFACES |
|---|---|---|
| **IPS Borde** | Zona Internet | Interfaz 0 (IN)→ Hacia SW Core 7KA<br>Interfaz 0 (OUT) → Hacia FW Borde<br>Interfaz 1 (IN)→ Hacia SW Core 7KB<br>Interfaz 1 (OUT) → Hacia FW Borde |
| | Zona DMZ | Interfaz 2 (IN)→ Hacia SSL DMZA IN<br>Interfaz 2 (OUT) → Hacia SSL DMZA OUT<br>Interfaz 3 (IN)→ Hacia SSL DMZB IN<br>Interfaz 3 (OUT) → Hacia SSL DMZB OUT |
| **IPS Tercero** | Zona Terceros | Interfaz 0 (IN)→ Hacia SW Terceros<br>Interfaz 0 (OUT) → Hacia SW Core 7KA<br>Interfaz 1 (IN)→ Hacia SW Terceros<br>Interfaz 1 (OUT) → Hacia SW Core 7KA |
| **IPS Core** | Zona VDCs | Interfaz 0 (IN)→ Hacia SW 7KA – VDC PCI<br>Interfaz 0 (OUT) → Hacia FW Principal<br>Interfaz 1 (IN)→ Hacia SW 7KB – VDC PCI<br>Interfaz 1 (OUT) → Hacia FW Principal<br>Interfaz 2 (IN)→ Hacia SW 7KA – VDC PRI<br>Interfaz 2 (OUT) → Hacia FW Principal<br>Interfaz 3 (IN)→ Hacia SW 7KB – VDC PRI<br>Interfaz 3 (OUT) → Hacia FW Principal<br>Interfaz 4 (IN)→ Hacia SW 7KA – VDC Servicios<br>Interfaz 4 (OUT) → Hacia FW Principal<br>Interfaz 4 (IN)→ Hacia SW 7KB – VDC Servicios<br>Interfaz 4 (OUT) → Hacia FW Principal |

*Fuente*: Elaboración Propia

Los equipos utilizados para el diseño de la protección IPS son:

Tabla 39
*Cantidad Equipos IPS*

| # | Proveedor | Dispositivos | Modelo | Cantidad |
|---|---|---|---|---|
| **1** | HP | IPS | Tipping Point 2600 | 3 |

*Fuente*: Elaboración Propia

#### *5.2.8.2.1. Funcionamiento equipo IPS*

Un IPS (Sistema de Prevención de Intrusos) es una tecnología de seguridad de red / prevención de amenazas que examina los flujos de tráfico de red para detectar y prevenir exploits de vulnerabilidades. Los Exploits de Vulnerabilidades suelen venir en forma de entradas maliciosas a una aplicación o servicio de destino que los atacantes usan para interrumpir y obtener el control de una aplicación o máquina. Después de una explotación exitosa, el atacante puede deshabilitar la aplicación de destino (lo que da como resultado un estado de denegación de servicio) o potencialmente acceder a todos los derechos y permisos disponibles para la aplicación comprometida.(Palo Alto Networks, 2017).

Básicamente las dos funciones primordiales de un IPS son: Prevención y Detección.

*Prevención*. El IPS a menudo se localiza directamente detrás del firewall y proporciona una capa complementaria de análisis que selecciona negativamente el contenido peligroso. A diferencia de su predecesor, el Sistema de Detección de Intrusiones (IDS), el IPS se coloca en línea (en la ruta de comunicación directa entre origen y destino), analizando activamente y tomando acciones automatizadas en todos los flujos de tráfico que entran en la red. Específicamente, estas acciones incluyen:

- Enviar una alarma al administrador
- Eliminación de los paquetes maliciosos
- Bloquear el tráfico de la dirección de origen
- Restablecimiento de la conexión

Como componente de seguridad en línea, el IPS debe trabajar de manera eficiente para evitar degradar el rendimiento de la red. También debe funcionar rápido porque los exploits pueden suceder casi en tiempo real. El IPS también debe detectar y responder con precisión, a fin de eliminar las amenazas y los falsos positivos (los paquetes legítimos son mal entendidos como amenazas).

*Detección*. El IPS tiene una serie de métodos de detección para encontrar exploits, pero la detección basada en la firma y la detección basada en anomalías estadísticas son los dos mecanismos dominantes.

La detección fundamentada en la firma se basa en un diccionario de patrones (o firmas) identificables de forma única en el código de cada exploit. A medida que se descubre un exploit, su firma se registra y se almacena en un diccionario de firmas en continuo crecimiento. La detección de firmas para IPS se divide en dos tipos:

Las firmas orientadas a la exploración identifican explotaciones individuales al activarse en los patrones únicos de un intento de exploit particular. El IPS puede identificar exploits específicos encontrando una coincidencia con una firma del exploit en el flujo de tráfico

Las firmas orientadas a la vulnerabilidad son firmas más amplias que apuntan a la vulnerabilidad subyacente en el sistema que se está apuntando. Estas firmas permiten que las redes estén protegidas contra las variantes de una explotación que no se han observado directamente en la naturaleza, sino que también aumentan el riesgo de falsos positivos

La detección de anomalías estadísticas toma muestras de tráfico de red al azar y las compara con una línea base pre-calculado del nivel de rendimiento. Cuando la muestra de actividad de tráfico de red está fuera de los parámetros de rendimiento de la línea base, el IPS toma medidas para manejar la situación.

#### *5.2.8.2.2. Características Técnicas IPS HP Tipping Point*

El IPS HP Tipping Point es un dispositivo que opera en línea dentro de la red, bloqueando tráfico malicioso y no deseado mientras que permite que el tráfico benigno pase sin impedimentos. De hecho, HP Tipping Point optimiza el desempeño del tráfico limpio al

realizar una limpieza continua de la red y priorizando las aplicaciones que son de misión crítica.

Estos dispositivos realizan una inspección total del flujo de paquetes a través de la Capa 7 para limpiar continuamente el tráfico de Internet y de la Intranet de forma precisa y así erradicar los ataques (gusanos, troyanos, amenazas combinadas, phishing, virus, spyware, amenazas de VoIP, DoS, DDoS, puertas traseras) antes de que se produzcan daños. HP Tipping Point protege la infraestructura de red bloqueando ataques contra los routers, switches, DNS y otros equipos de infraestructura.

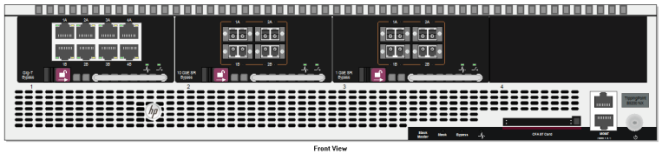

*Figura 29.* Equipo IPS HP Tipping Point
*Fuente*: (HP. Soluciones de Seguridad)

Las características técnicas del dispositivo IPS Tipping Point S2600 NX se muestran a continuación.

Tabla 40
*Especificaciones técnicas IPS Tipping Point*

| CARACTERÍSTICA | DESCRIPCION |
|---|---|
| **Desempeño** | Capacidad de inspección: 3 Gb/s Capacidad de red:<br>40 Gb/s Latencia típica: <40 microsegundos<br>Contextos de seguridad: 2,600,000<br>Conexiones por segundo: 300,000<br>Sesiones simultáneas: 30,000,000 |
| **Módulos de E/S de alta densidad** | Cada uno de los chasis NX admite hasta 4 módulos de E/S NX intercambiables en caliente. Con el chasis NX completo con 4 de los módulos de E/S SFP+ NX, puede lograr la inspección de hasta 16 segmentos de 10GbE, o una combinación de segmentos de 1GbE, 10GbE y 40GbE. |
| **Características físicas:** | Dimensiones: 55,25 cm (Prof.) x 42,78 cm (An.) x 8,89 cm (Al.)<br>Peso: 19,1 kg<br>Unidades de rack 2 Incluye hardware de montaje para 2 postes |

| | |
|---|---|
| | frontales, 2 postes medios y 4 postes de rieles deslizantes de lanzamiento rápido |
| **Entorno** | Temperatura en funcionamiento: 0 °C a 40 °C<br>Humedad relativa en funcionamiento : de 5% a 95% sin condensación<br>Temperatura durante almacenamiento/en reposo: -4°C a 70°C<br>Humedad relativa durante almacenamiento/en reposo: de 5% a 95% sin condensación<br>Altitud: Hasta 3048 metros (10.000 pies) |
| **Seguridad** | UL 60950-1;<br>IEC 60950-1;<br>EN 60950-1;<br>CSA 22.2 60950-1;<br>EN/IEC 60825-1;<br>Conformidad ROHS |
| **Características eléctricas (ca)** | Tensión: 100-240<br>Corriente Vca (alimentación máx. protegida por fusi.: 12 / 6 A<br>Frecuencia: 50–60 Hz<br>Consumo eléctrico: 750 W (2559 BTU/hora) |
| **Administración** | 1 puerto RJ-45 10/100/1000<br>Se puede gestionar mediante un servidor de gestión de seguridad (SMS), una interfaz de línea de comandos (CLI), un navegador web, o la base de información de gestión (MIB) IPS de HP TippingPoint |

*Fuente*: (HP. Soluciones de Seguridad)

En cuanto a la consola de administración HP Tipping Point SMS (Security Management System) es una plataforma de gestión de clase empresarial que provee la administración, configuración, supervisión y presentación de informes para múltiples Sistemas de Prevención de Intrusos (IPS). Este es un dispositivo montable en rack que no requiere instalación y ofrece una interfaz de usuario de última generación.

El SMS ofrece niveles de control de acceso personalizables con privilegios de operador (sólo lectura), administrador y supervisor. Permite visualizar un "panorama general" por medio de informes de tendencias, correlaciones y gráficos en tiempo real - incluidos los informes sobre estadísticas de tráfico, Filtrado de ataques, hosts, Servicios de Red e Inventarios de los IPSs HP Tipping Point.

*Figura 30.* Consola Administración HP SMS
*Fuente*:(HP. Soluciones de Seguridad)

Debido a que el HP Tipping Point SMS proporciona un modelo operativo escalable y basado en políticas, permite la gestión directa de implementaciones de IPSs a gran escala. Algunas de sus características técnicas se indican a continuación.

Tabla 41
*Especificaciones técnicas Consola Administración Tipping Point*

| CARACTERÍSTICA | DESCRIPCIÓN |
|---|---|
| **Capacidad** | Licencias para 25 dispositivos administrados; expandible a 200 millones de eventos históricos |
| **Memoria, procesador y almacenamiento** | 2 Intel® Xeon® six-core processor @ 2400 MHz, 64 GB RAM; storage 600 GB |
| **Características físicas:** | 69.85 (P) x 43.47(An) x 4.32 (Al) cm<br>(1U Altura de Rack)<br>16.78 kg |
| **Especificaciones Ambientales** | 10°C to 35°C |
| **Características eléctricas (ca)** | 100 to 120 – 200 to 240 VAC<br>2.78 a 1.15 A<br>50/60 Hz<br>Redundante 500 W Hot Swap |

*Fuente*: (HP. Soluciones de Seguridad)

#### *5.2.8.2.3. Configuraciones equipo IPS HP Tipping Point*

Se consideraron algunas tareas referentes a la implementación del equipo IPS las mismas que se detallan a continuación:

*Levantamiento de información*: Se identifica las redes, servicios, sistemas operativos a proteger por el IPS mediante la creación de un grupo de firmas.

*Configuración*: Se realiza la configuración de inspection profiles, segment group, distribución de profiles, es recomendable que las firmas se encuentren en modo *Permit + Notify*. Este modo permite visualizar todas las firmas de ataques para realizar un análisis de dichas firmas y tomar medidas al momento de cambiar las firmas a modo *Block + Notify*.

*Monitoreo y afinamiento*: En esta fase se analiza los diferentes reportes para afinar las firmas, ejecutar exclusiones y poder cambiar los inspection profiles a modo *Block + Notify*.

### 5.2.9. Diseño de la arquitectura para Firewalls

El objetivo de la implementación de los Firewall Check Point, es proveer un alto nivel de seguridad en el perímetro del Data Center Alterno, de manera tal que se proporcione protección proactiva en tiempo real a la información mediante una plataforma de seguridad, ofreciendo un alto nivel de desempeño en la red.

Para cumplir con este fin se ha identificado tres locaciones dentro de la red LAN del Datacenter Alterno a las que se brindará protección. Estas zonas son: Acceso a Terceros, Core de Datos y Salida/Entrada Internet - DMZ.

Tabla 42
*Zonas a Proteger con los Firewalls en DCA*

| ZONA | DESCRIPCIÓN |
|---|---|
| **Acceso Terceros** | Provee seguridad para las conexiones que se realicen tanto de entrada o salida hacia las empresas terceras, proveedores con el fin de permitir solo aquellas que sean legítimas, autorizadas y sean requeridas para la operación del negocios |
| **Core de Datos** | Provee seguridad para las conexiones que se realicen tanto de entrada o salida hacia los servidores de la red del DCA con el fin de permitir solo aquellas que sean legítimas, autorizadas y sean requeridas para la operación del negocios |
| **Internet - DMZ** | Provee seguridad para las conexiones que se realicen tanto de entrada o salida hacia Internet y los servidores de publicación con el fin de permitir solo aquellas que sean legítimas, autorizadas y sean requeridas para la operación del negocios |

*Fuente*: Elaboración Propia

Estos tres puntos estratégicos brindan seguridad total a la red interna del DCA cubriendo contra ataques y acceso no autorizados que se puedan dar. La cantidad de Firewalls utilizados para este propósito son 3, que se ubicaran estratégicamente para proteger los datos que atraviesan la red del Datacenter Alterno.

Al igual que en DCP, los equipos firewall en su parte Hardware serán servidores HP e IBM en los cuales se instalará el software de Checkpoint sobre un Sistema Operativo llamado Gaia que utiliza dicha compañía. Los equipos a considerar son:

Tabla 43
*Detalle de Firewalls en el DCA*

| # | Proveedor | Dispositivos | Nombre | Cantidad |
|---|---|---|---|---|
| **1** | Check Point | Firewall | Firewall Terceros | 1 |
| **2** | Check Point | Firewall | Firewall Principal | 1 |
| **3** | Check Point | Firewall | Firewall Borde | 1 |
| **4** | Check Point | Security Management | Consola de Administración | 1 |

*Fuente*: Elaboración Propia

El Appliance Smart-1 205 cumplirá la función de Security Management, Log Server y SmartReporter / SmartEvent. Esta consola servirá para la administración de las reglas de firewall a configurar en el DCA, de igual manera mediante este dispositivo se podrá obtener reportes y visualizar los logs de las conexiones en tiempo real. Se instalará en el segmento de administración designado y contará con una interfaz de administración de cobre (1 Gbps), que se conectará a los switches de la zona de administración fuera de Banda.

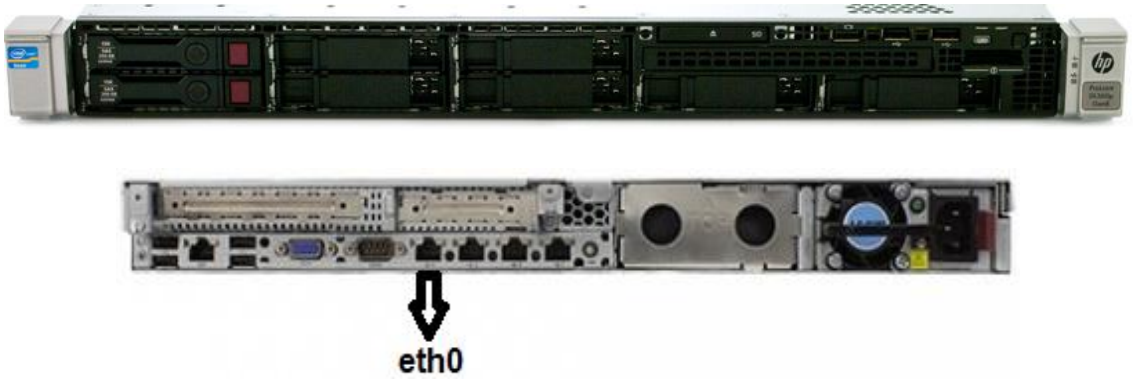


*Figura 31*. Consola Administración Firewall
*Fuente*: (HP, 2014. Reimagine the server.)

#### *5.2.9.1. Firewall Borde*

El Firewall Borde protege las conexiones desde y hacia Internet y a la DMZ donde se encuentran los servidores que se publican al exterior. Lógicamente su ubicación se muestra en la figura de a continuación:

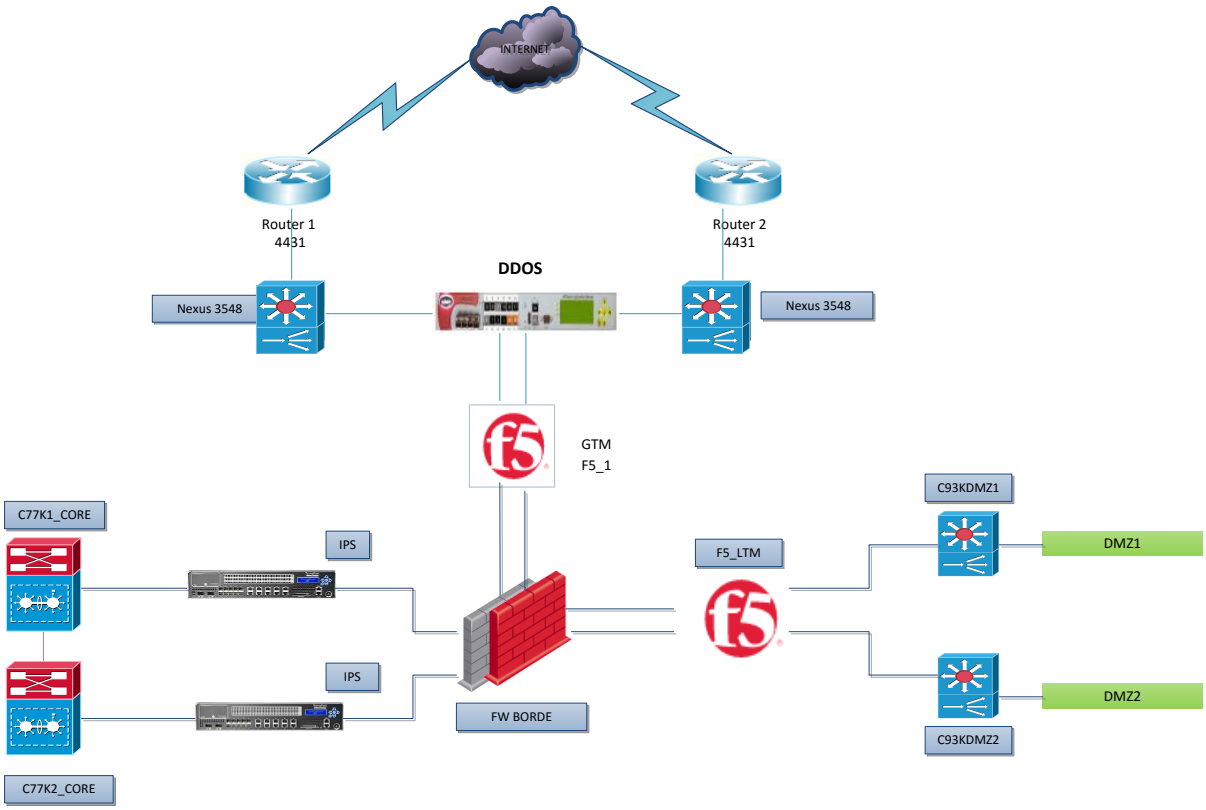


*Figura 32*. Ubicación Lógica del Firewall Borde
*Fuente*: Elaboración Propia

Todas las interfaces de red del firewall de Borde son de fibra óptica (10 Gbps), a excepción de la interfaz de Gestión que es de cobre (1 Gbps). La asignación de velocidad de las interfaces es auto negociación y el modo de operación es Full Dúplex. Las conexiones lógicas más a detalle de este equipo se muestran en el siguiente gráfico:

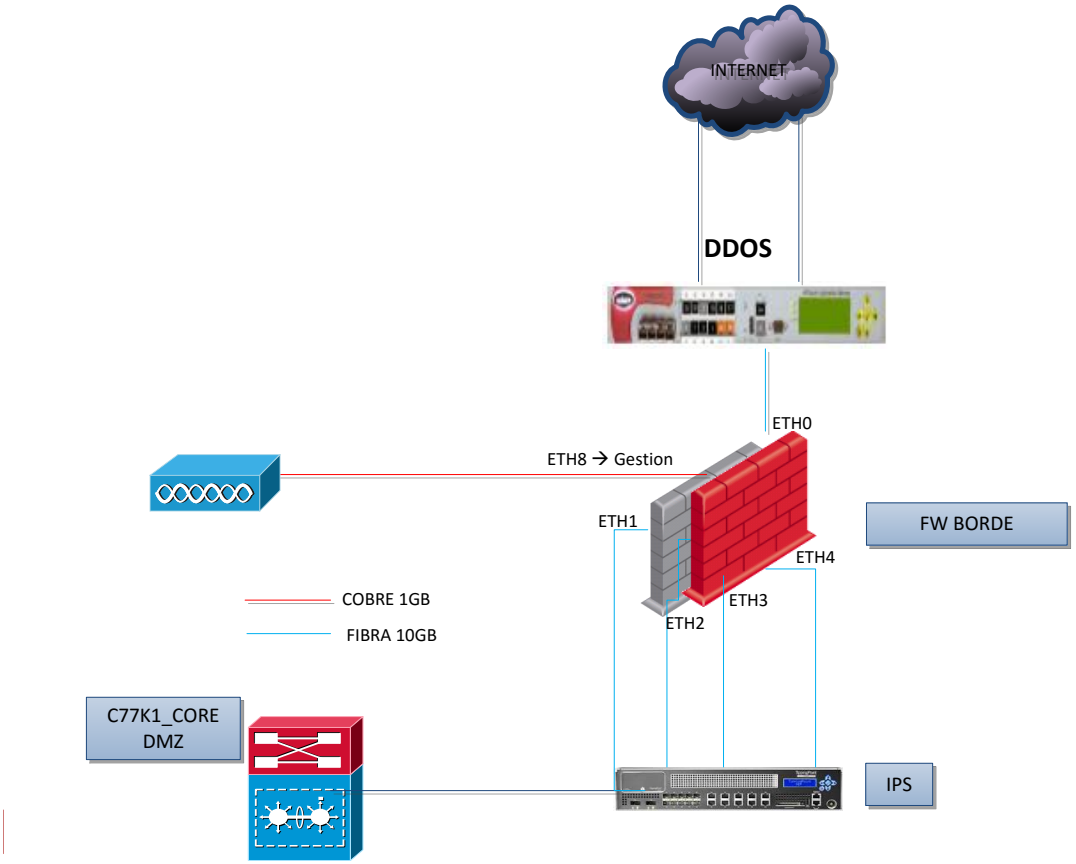


*Figura 33.* Conexiones Lógicas del Firewall Borde
*Fuente*: Elaboración Propia

Físicamente las conexiones utilizadas en el Firewall de Borde son:

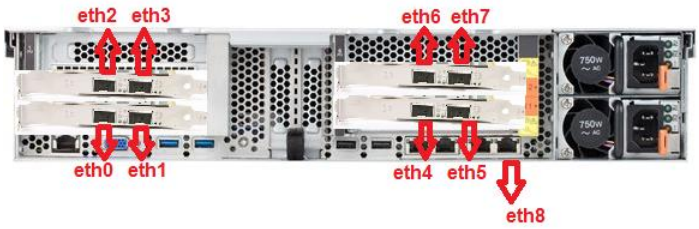


*Figura 34*. Conexiones Físicas del Firewall Borde
*Fuente*: (HP, 2014. Reimagine the server.)

Cada una de estas interfaces físicas del firewall se encuentra asociada una VLAN ID y a una dirección IP. Específicamente en el Firewall de Borde en las interfaces se configura las direcciones IP que son los default Gateway de las VLANs creadas en las DMZ, así como los segmentos de salida a Internet, la conexión en el Switch de Core y la Interfaz de Administración. En la tabla de a continuación se representa la asociación de cada interfaz

Tabla 44
*Interfaces Firewall Borde*

| Interfaz | Segmento | VLAN | Dirección IP / Netmask |
|---|---|---|---|
| **eth0** | OUTSIDE (Internet) | VLANs | - |
| **eth1** | CORE | VLANs | - |
| **eth2** | CORE Backup (contingencia eth1) | VLANs | - |
| **eth3** | VLANS DMZ A | VLANs | - |
| **eth4** | VLANS DMZ B | - | - |
| **eth5** | Deshabilitada | - | - |
| **eth6** | Deshabilitada | - | - |
| **eth7** | Deshabilitada | - | - |
| **eth8** | Gestión | - | - |

*Fuente*: Elaboración Propia

La tabla de enrutamiento de cada firewall está conformada por rutas estáticas que definen el próximo salto de acuerdo a cada destino dentro de la Red LAN del DCA.

### *5.2.9.2. Firewall Terceros*

El Firewall Terceros protege las conexiones desde y hacia la comunicación con empresas terceras, proveedores los cuales brinda o consumen algún servicio desde o hacia los servidores de la red interna del DCA. Lógicamente su ubicación se muestra en la figura de a continuación:

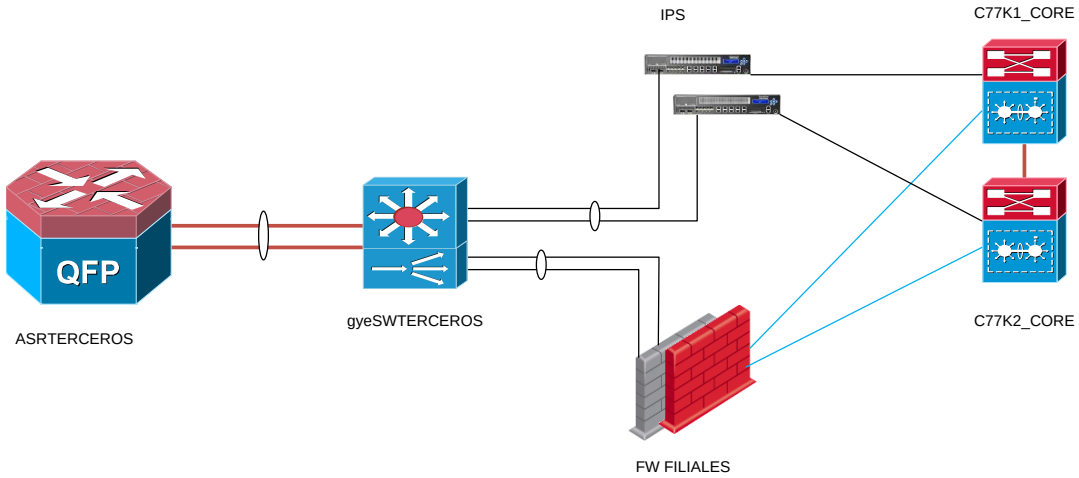


*Figura 35.* Ubicación Lógica del Firewall Terceros
*Fuente*: Elaboración Propia

Todas las interfaces de red del firewall de Terceros son de fibra óptica (10 Gbps), a excepción de la interfaz de Gestión que es de cobre (1 Gbps). La asignación de velocidad de las interfaces es auto negociación y el modo de operación es Full Dúplex. Las conexiones lógicas más a detalle de este equipo se muestran en el siguiente gráfico:

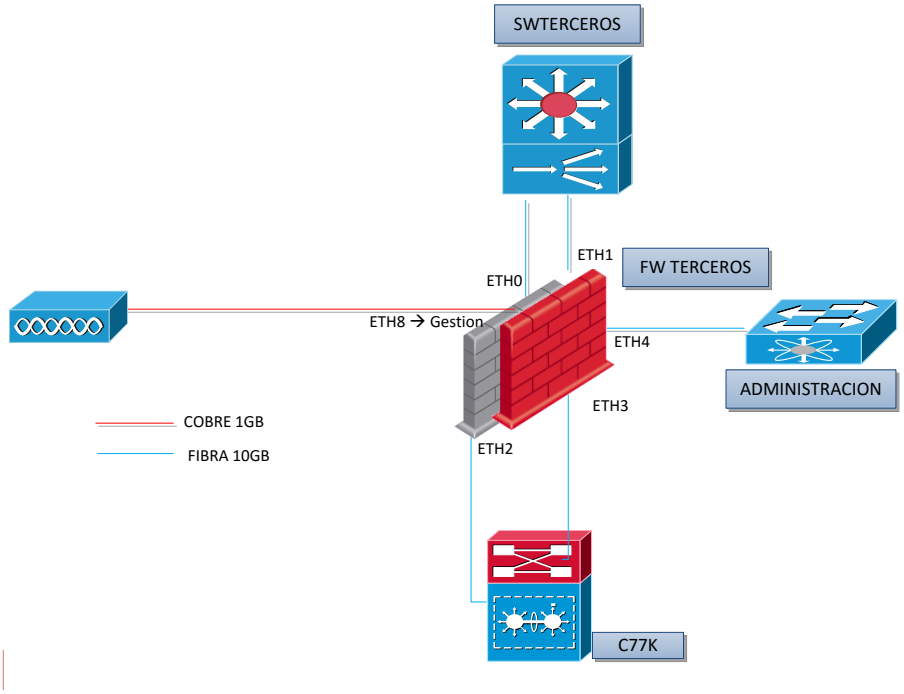


*Figura 36.* Conexiones Lógicas del Firewall Terceros
*Fuente*: Elaboración Propia

Físicamente las conexiones utilizadas en el Firewall de Terceros son:

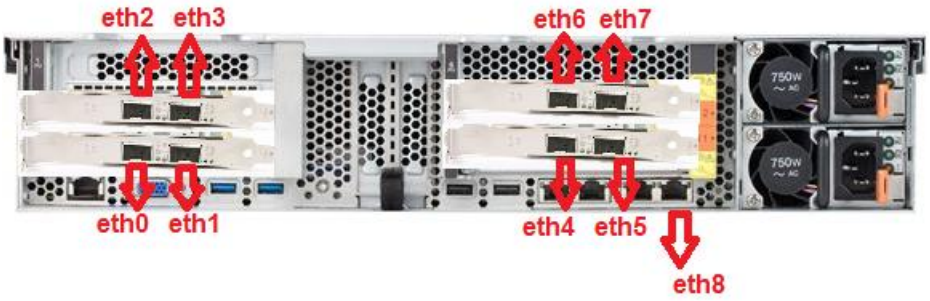


*Figura 37.* Conexiones Físicas del Firewall Terceros
*Fuente*: (HP, 2014. Reimagine the server)

Cada una de estas interfaces físicas del firewall se encuentra asociada una VLAN ID y a una dirección IP. Específicamente en el Firewall de Terceros en las interfaces se configura las direcciones IP que son los default Gateway de las VLANs creadas en los Switches de Administración, así como los segmentos de conexión con el Switch de Terceros, la conexión

en el Switch de Core y la Interfaz de Administración. En la tabla de a continuación se representa la asociación de cada interfaz

Tabla 45
*Interfaces Firewall Terceros*

| Interfaz | Segmento | VLAN | Dirección IP / Netmask |
|---|---|---|---|
| **eth0** | Terceros | VLANs | - |
| **eth1** | Terceros Backup (contingencia eth0) | VLANs | - |
| **eth2** | CORE | VLANs | - |
| **eth3** | CORE Backup (contingencia eth2) | VLANs | - |
| **eth4** | VLANS de Administración | VLANs | - |
| **eth5** | Deshabilitada | - | - |
| **eth6** | Deshabilitada | - | - |
| **eth7** | Deshabilitada | - | - |
| **eth8** | Gestión | VLAN | - |

*Fuente*: Elaboración Propia

La tabla de enrutamiento de cada firewall está conformada por rutas estáticas que definen el próximo salto de acuerdo a cada destino dentro de la Red LAN del DCA.

#### *5.2.9.3. Firewall Principal*

El Firewall Principal protegerá las conexiones que se establezcan desde y hacia los servidores que se encuentren en alguna red de las VDCs creadas, permitiendo el paso solo de aquellas que se encuentren autorizadas por la operación del negocio a interactuar con los servicios o datos alojados en los servers internos. Lógicamente su ubicación se muestra en la figura de a continuación:

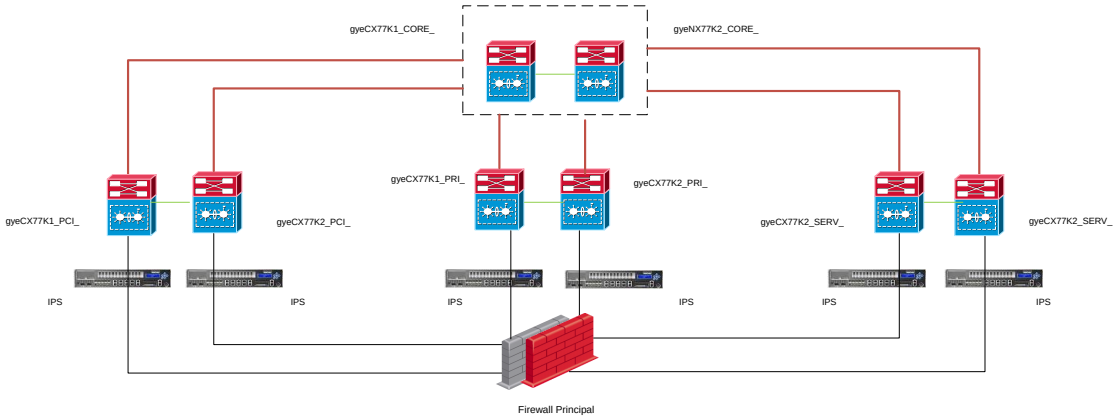


*Figura 38.* Ubicación Lógica del Firewall Principal
*Fuente*: Elaboración Propia

Todas las interfaces de red del firewall de Terceros son de fibra óptica (10 Gbps), a excepción de la interfaz de Gestión que es de cobre (1 Gbps). La asignación de velocidad de las interfaces es auto negociación y el modo de operación es Full Dúplex. Las conexiones lógicas más a detalle de este equipo se muestran en el siguiente gráfico:

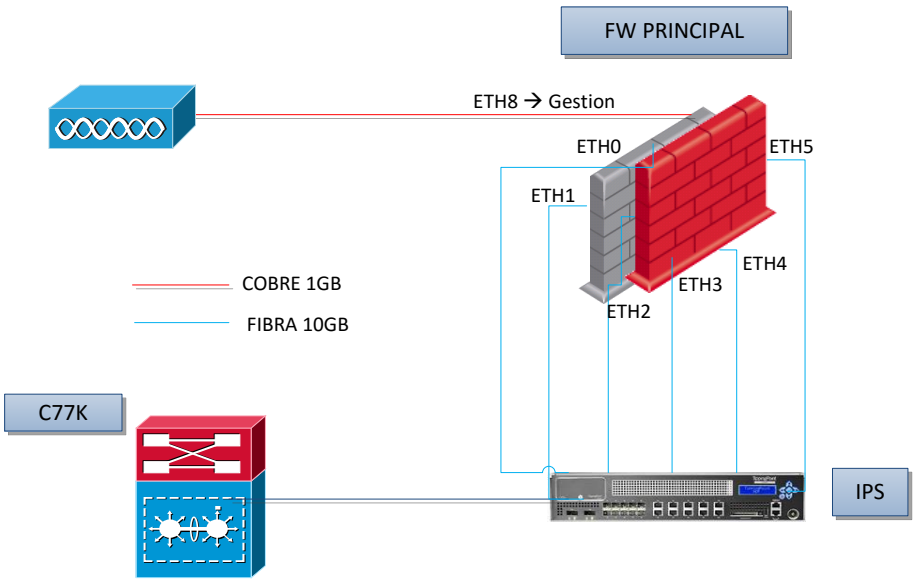


*Figura 39.* Conexiones Lógicas del Firewall Principal
*Fuente*: Elaboración Propia

Físicamente las conexiones utilizadas en el Firewall de Terceros son:

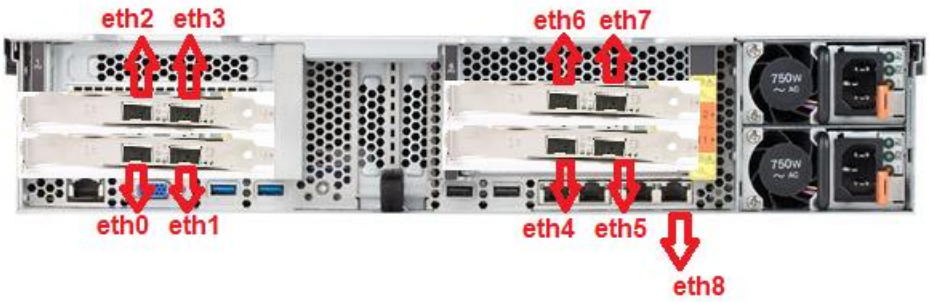


*Figura 40*. Conexiones Físicas del Firewall Principal
*Fuente*: (HP, 2014. Reimagine the server)

Cada una de estas interfaces físicas del firewall se encuentra asociada una VLAN ID y a una dirección IP. Específicamente en el Firewall Principal en las interfaces se configura las VLANs creadas para la interconexión con las 3 VDCs creadas en Core, así como el segmento de la Interfaz de Administración. En la tabla de a continuación se representa la asociación de cada interfaz.

Tabla 46
*Interfaces Firewall Principal*

| Interfaz | Segmento | VLAN | Dirección IP / Netmask |
|---|---|---|---|
| **eth0** | VLANS Interconexión VDC SERVICIO | - | - |
| **eth1** | Servicio_Backup (contingencia eth0) | - | - |
| **eth2** | VLANS Interconexión VDC PRINCIPAL | - | - |
| **eth3** | Principal_Backup (contingencia eth2) | - | - |
| **eth4** | VLANS Interconexión VDC PCI | - | - |
| **eth5** | PCI_Backup (contingencia eth4) | - | - |
| **eth8** | Gestión | - | - |

*Fuente*: Elaboración Propia

La tabla de enrutamiento de cada firewall está conformada por rutas estáticas que definen el próximo salto de acuerdo a cada destino dentro de la Red LAN del DCA.

#### *5.2.9.4. Características Firewall CheckPoint*

En la parte Hardware los equipos, sobre los cuales se montará el software de capacidades firewall, serán servidores HP e IBM con las siguientes características

Tabla 47
*Especificaciones Hardware para Servidores Firewall*

| Servidor | Función | CPU | Memoria | Disco Duro | RAID | Interfaces de Red |
|---|---|---|---|---|---|---|
| **HP DL360 g9** | Management, Log Server y Reporter | 8 cores | 16 GB | 2 discos de 300 GB en RAID1 | NA | 1 puerto de cobre de 1 GB |
| **IBM x3650 M5** | Borde | 12 cores | 64 GB | 2 discos 300 GB | 1 | 8 puertos de fibra óptica de 10 GB |
| **IBM x3650 M5** | Principal | 12 cores | 64 GB | 2 discos 300 GB | 1 | 8 puertos de fibra óptica de 10 GB |
| **IBM x3650 M5** | Terceros | 8 cores | 32 GB | 2 discos 300 GB | 1 | 8 puertos de fibra óptica de 10 GB |

*Fuente*: Elaboración Propia

Como se indicó en el apartado anterior el proveedor del software para los equipos de firewall es Checkpoint el cual utiliza el S.O. Gaia. En el DCA el Sistema Operativo a instalarse en todos los equipos CheckPoint es Gaia R77.30. Esta versión es la más actual y estable, proporcionada por el fabricante a la fecha.

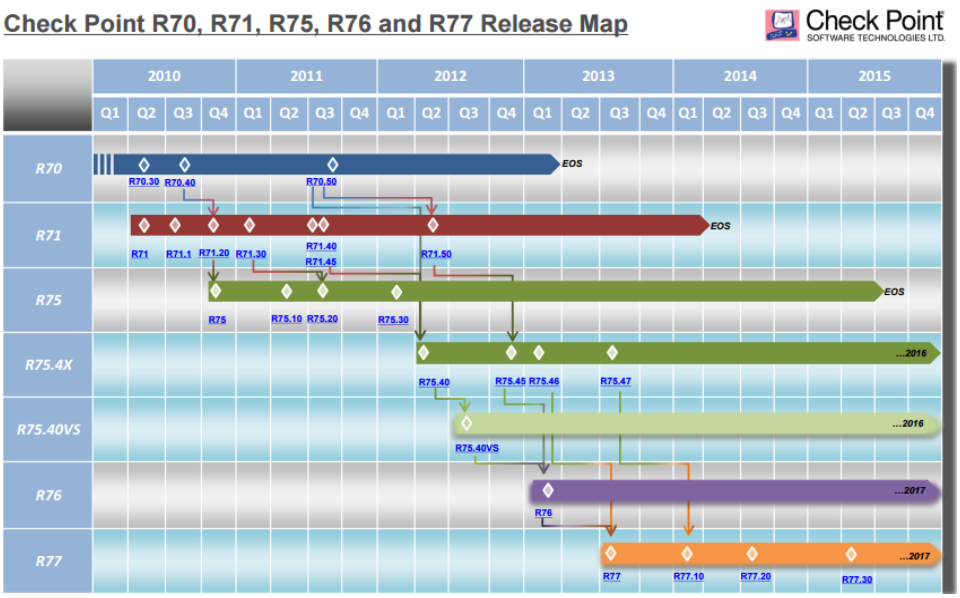


*Figura 41*. Mapa de los reléase de software para Checkpoint
*Fuente*: (Checkpoint. Firewall Software Blade)

En cuanto a las características que ofrece la plataforma Checkpoint podemos tener las siguientes:

- Mejor Seguridad: Una solución de varias capas y una plataforma consolidada de seguridad que ejerce una combinación única de red integrada y seguridad de punto final, combinado con la más completa protección anti-malware de la industria contra amenazas.
- Simplicidad: Fácil administración, una flexibilidad total y la activación de seguridad simple elimina la complejidad y hace más fácil la seguridad para operar y administrar.
- Gestión: La activación de un solo clic permite el despliegue rápido de servicios de seguridad. (Checkpoint. Firewall Software Blade)

Una amplia biblioteca de más de treinta Software Cuchillas ofrece integración sin igual para tener un nivel adecuado de seguridad en todas las capas de la red.

**Software Blade Arquitectura**

Licenciamiento Perpetuo:

- Firewall
- Identity Awareness
- VPN IPsec
- Advance networking
- ADNC

Licencias recurrentes a 3 años:

- IPS
- Application Control

**Software Blade Instalados**

Software Blade instalados perpetuos:

- Firewall:
    - Permite o bloquea el paso de datos desde un equipo a otro o desde una red interna o externa
- Identity Awareness
    - Proporciona una visibilidad granular de usuarios, grupos y equipos proporcionando acceso a través de la creación de políticas precisas basadas en la identidad.
- IPsec VPN
    - Proporciona conectividad segura a las redes corporativas para los usuarios móviles y remotos mediante la autenticación y cifrado para garantizar la seguridad en las conexiones a través de Internet.
- Advanced Networking and Clustering

- Simplifica el despliegue de seguridad de la red y la gestión dentro de las redes complejas altamente utilizadas al tiempo que maximiza el rendimiento de la red y la seguridad en entornos Multi-Gbps

**Software Blade instalados con licenciamiento a 3 años.**

- Intrusion Prevention System
  - Provee protección contra intrusiones y ataques dirigidos, Con 2 perfiles pre configurados para la protección de segmentos de red de servidores o clientes
- Applicantion Control
  - Con más de 6.000 aplicaciones Web 2.0 y 300.000 widgets de redes sociales, intuitivamente agrupados en más de 150 categorías , incluyendo la Web 2.0, IM, P2P, Voz y vídeo y de archivos compartidos

**SecurityManagement (SmartCenter) para 10 GWs.**

El Security Management (Smart Center) incorpora siete blades de administración que proporcionan la funcionalidad completa para el CheckPoint's Management Architecture (SMART) alojado en los dispositivos de hardware optimizado para un rendimiento y escalabilidad mejorada.

Para definir y supervisar las políticas de seguridad a través de las múltiples funciones incluyendo Firewall, VPN, IPS, Anti -Virus, Filtrado de URL y Control de aplicaciones, en base al licenciamiento de los Gateways. Mediante una sola consola de administración se puede aplicar políticas a todos o cada uno de los Gateways de seguridad que se encuentra a lo largo de la red, dando un control y fácil acceso para la gestión de seguridad.

**Software Blade Instalados**

Los Software Blade a continuación viene predefinidos:

- Network Policy Management: Administra y centraliza las políticas de seguridad en la red de los gateways y blades de CheckPoint a través del SmartDashboard.
- Endpoint Policy Management: Simplifica la administración de seguridad del endpoint mediante la unificación de todas las capacidades de seguridad en una única consola.
- Logging and Status: Es un analizador de registro avanzado que nos proporciona visibilidad en tiempo real de múltiples registros sobre varios períodos de tiempo y dominios.
- Monitoring: Visibilidad total del tráfico que atraviesa por el/los equipos con la posibilidad de crear filtros para un mejor manejo de la información y con la capacidad de tener un control de consumo de memoria y CPU en los diferentes Gateways
- Smart Even Intro: Software blade direccionado a la visibilidad de los eventos a nivel de IPS con la posibilidad de tomar acciones correctivas en base a las recomendaciones de la herramienta

#### *5.2.9.5. Configuración Políticas de seguridad Firewall CheckPoint*

El procedimiento para la creación de políticas de seguridad para los Firewall del Data Center Alterno se detalla en los siguientes pasos, a fin de editar las políticas de seguridad del Data Center Principal hacia el direccionamiento IP requerido para el Data Center Alterno.

- Obtener un respaldo de la base de datos del Security Management del DCP.

- Restaurar el respaldo de la base de datos en el Security Management del DCA.
- Editar los objetos de red acorde al direccionamiento IP requerido para el Data Center Alterno.
- Crear los objetos Firewall y asignar la instalación de los paquetes de políticas hacia los Firewall correspondientes.

Para identificar el direccionamiento IP existente en el DCP y en el DCA, se realizará la equivalencia de los segmentos de red con los que cuenta la empresa, esto con la finalidad de ejecutar el reemplazo del direccionamiento IP sobre los objetos de red desde la base de datos del Security Management del DCP.

Las configuraciones existentes en la base de datos del Security Management del DCP, se mantendrán para el DCA: Anti-spoofing, VPN Site-to-Site, VPN Remote Access.

### 5.2.10. Diseño de la arquitectura para Equipamiento F5

Dentro de los dispositivos de red incluidos en el diseño de la arquitectura de red del Datacenter Alterno, se ha tomado en cuenta la implementación del equipamiento F5, el cual brinda varios beneficios y funcionalidades para la operación del DCA.

Básicamente el equipo F5 tiene dos módulos dentro del mismo equipo que son los más usados y conocidos: el GTM (Global Traffic Manager) y el LTM (Local Traffic Manager).

Estos módulos tiene cada uno funciones específicas. En forma general con el módulo de GTM se pretende realizar el balanceo de la Operación entre Datacenters y Enlaces de Internet brindando seguridad y aceleración en un mismo paso, a más de garantizar su constante disponibilidad. En contraste mediante el módulo de LTM se realizará el balanceo de todas las aplicaciones y servicios que se encuentren en la zona DMZ del DCA.

Lógicamente la funcionalidad del GTM estará entre la entrada de internet y el Firewall de Borde en cambio la funcionalidad del LTM estará entre la Zona DMZ y el Firewall de Borde. Las conexiones lógicas del equipo F5 se indican a continuación:

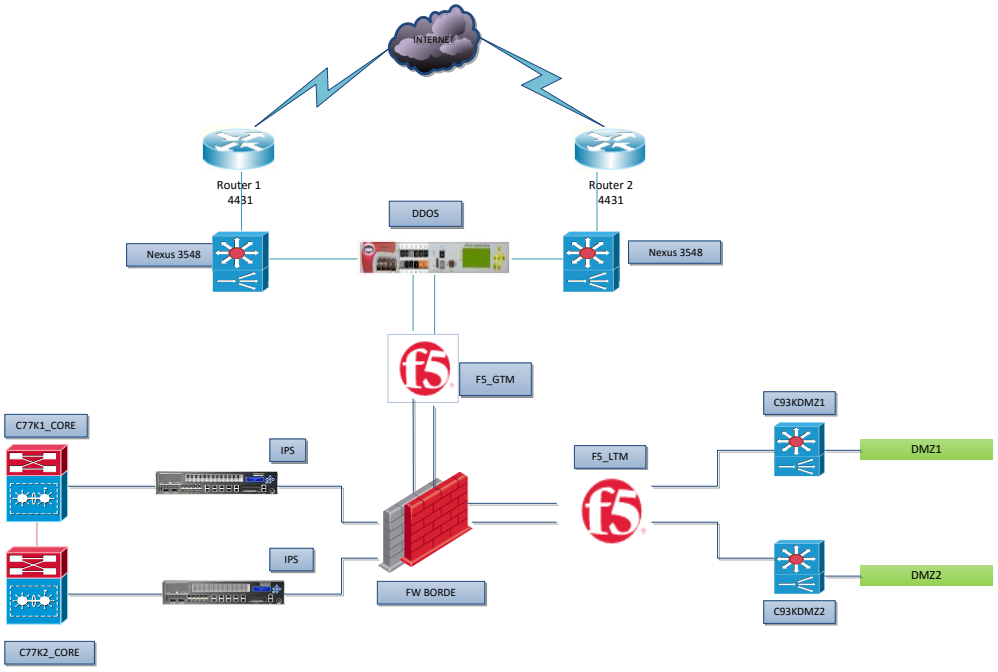


*Figura 42*. Conexiones de los Modulo GTM y LTM del F5 en el DCA
*Fuente*: Elaboración Propia

En los siguientes apartados se revisará más a detalle las funciones y capacidades de cada módulo.

El equipo utilizado para el diseño del equipamiento F5 es el siguiente:

Tabla 48
*Equipamiento F5 en el DCA*

| # | Proveedor | Dispositivos | Modelo | Cantidad |
|---|---|---|---|---|
| 1 | F5 | BIG IP F5 | 5250V | 1 |
| **Módulos Incluidos** | | | | |
| 1 | Local Traffic Manager | | | |
| 2 | SND Services | | | |
| 3 | Global Traffic Manager (GSLB, DNS Services, DNSSEC, Advanced Routing) | | | |
| 4 | Advanced Firewall Manager | | | |

*Fuente*: Elaboración Propia

#### *5.2.10.1. Características equipamiento F5*

Los dispositivos BIG-IP pueden ayudar a simplificar la red, descargando servidores y consolidando dispositivos, ahorrando costes de administración, así como de potencia, espacio y refrigeración en el centro de datos.

Con el enorme rendimiento y escalabilidad de la plataforma BIG-IP, puede reducir el número de controladores entregados en las aplicaciones más demandantes. Al descargar procesos intensos desde el punto de vista computacional, puede reducir significativamente el número de servidores de aplicaciones necesarios

El hardware de BIG-IP ofrece un gran rendimiento en las decisiones de aplicación por segundo, Procesamiento SSL y compresión de hardware para cada clase de ADC. Empresas y los proveedores de servicios pueden implementar múltiples servicios de entrega de aplicaciones, descargar procesamiento SSL, y consolidar eficientemente en una única plataforma unificada (F5, Big ip local traffic manager).

*Figura 43.* Equipo BIG IP - F5
*Fuente*: (F5, Big ip local traffic manager)

Tabla 49
*Especificaciones Técnicas equipo F5 5250v*

| EQUIPO | F5250v |
|---|---|
| **Procesamiento de tráfico Inteligente** | Peticiones por Segundo L7: 1.5M<br>Conexiones por Segundo L4: 700K<br>Máximas conexiones concurrentes L4: 24M<br>Peticiones HTTP por segundoL4: 7M<br>Throughput: 30 Gbps/15 Gbps L4/L7 |
| **Hardware SSL:** | Incluido: 21,000 TPS (2K llaves)<br>Máximo: 21,000 TPS (2K llaves) |

| | |
|---|---|
| | Encriptación masiva de 12 Gbps |
| **Protección DDoS en Hardware:** | 40M SYN cookies por segundo |
| **Compresión en Hardware** | Incluida: 12 Gbps, Máxima: 12 Gbps |
| **Arquitectura de Software** | 64-bit TMOS |
| **Virtualización (Máximo Número de Invitados vCMP)** | 8 |
| **Procesador** | 1 procesador Intel Xeon quad core (en total 8 Núcleos de procesamiento lógico hyperthreaded |
| **Memoria** | 32 GB |
| **Disco Duro** | Disco de estado solido de 400 GB |
| **Puertos Gigabit Ethernet de Cobre** | 4 |
| **Puerto Gigabit de Fibra** | Opcional SFP (SX, LX, or cobre) |
| **Puertos 10 Gigabit de Fibra (SFP+):** | 8 SR o LR |
| **Puertos 40 Gigabit de Fibra (QSFP+):** | NA |
| **Fuente de Poder** | Una de 400 W, potencia dual y opciones DC |
| **Consumo Tipico** | 165W (una fuente, 110V entrada) |
| **Voltaje Entrada** | 90-240 VAC +/- 10% auto switching, 50/60hz |
| **Disipación de calor** | 564 BTU/hora |
| **Dimensiones (Al x An x P)** | 4.45 cm x (43.18 cm x (53.34 cm<br>1 Unidad de Rack |
| **Peso** | 9.53 kg |
| **Temperatura de Operación** | 0° to 40° C |

*Fuente*: (F5, Big ip local traffic manager)

#### *5.2.10.2. Funcionalidad del LTM F5*

El gestor de tráfico local, también conocido como LTM, es el módulo más popular que se ofrece en la plataforma BiG-IP de F5 Networks. El poder real del LTM está en que es un proxy completo, lo que le permite aumentar las conexiones de cliente y servidor. Todo ello mientras se toman decisiones de balanceo de carga informadas sobre disponibilidad,

rendimiento y persistencia. Se dice Local, ya que el tráfico fluye a través del LTM a los servidores que equilibra el tráfico (Geraci Austin, 2017).

En LTM se configura una IP Virtual, la misma que está asociada a un pool de servidores internos que se utilizan para balancear la carga de tráfico de un servicio específico.

Como se ha indicado LTM es un proxy inverso completo, manejando conexiones de clientes. El F5 LTM utiliza los Servicios Virtuales (VS) y las IPs Virtuales (VIP) para definir una configuración de balanceo de carga para un servicio. Los LTMs pueden manejar el balanceo de carga de dos maneras, la primera es una configuración nPath, y la segunda es un método de traducción segura de direcciones de red (SNAT) (The JimmahKnows, 2012).

En el balanceo con nPath, el F5 hace el trabajo de balanceo de carga al decidir inteligentemente a qué punto final del servidor pasar tráfico. nPath, sin embargo, lo hace pasando por alto el F5 en la trayectoria de retorno. Por ejemplo, si se tiene dos servidores 192.168.0.10 y 192.168.0.11, y un F5 escuchando para esta configuración particular en la VIP 172.16.0.2. Ahora, cuando el tráfico de un cliente destinado a la 172.16.0.2 llega al F5, el F5 lo pasa inteligentemente a 192.168.0.10 o 192.168.0.11. La parte delicada es que cuando el tráfico sale del F5 a cualquiera de los servidores, la dirección fuente del paquete IP es la del F5. Por lo tanto, cada servidor debe tener una dirección loopback configurada que coincida con la dirección IP de origen F5s de la interfaz (en el F5) desde la que sale el paquete original. Esto evita que cada servidor final envíe directamente al F5 y obliga al servidor a utilizar su gateway de último recurso (The JimmahKnows, 2012).

Secure Network Address Translation (SNAT), es una implementación más común de BIGIP F5. En este escenario, el F5 se configura esencialmente como un servidor proxy inverso. El cliente ve una IPs virtuales de destino la misma que es el front de un pool de servidores. Sin embargo, el Cliente nunca ve detrás del VIP, para su perspectiva el VIP es el servidor que está solicitando. Por ejemplo, se tiene un VIP 192.168.0.55 que se rutea a un F5

que está escuchando peticiones destinadas a esa IP. El F5 dispone de una configuración que conoce 4 servidores que pueden contestar peticiones destinadas a esa IP, 10.0.0.5, 10.0.0.6, 10.0.0.7 ,10.0.0.8. Cuando una petición llega de un cliente al VIP, el F5 actúa como servidor para el cliente. En el back-end, el F5 actúa como un cliente que envía la petición idéntica a uno de los cuatro servidores de endpoint. La respuesta es entonces transferida desde el F5 al cliente "real"(The JimmahKnows, 2012).

Dentro del diseño de la arquitectura del DCA el módulo de LTM en F5 se lo configurará para que opere como balanceador de a las peticiones de los clientes externos hacia los servers que publican sus servicios a Internet y que se encuentran en la zona de la DMZ. La conexión física de los equipos hacia los Switches de la DMZ se lo realizará mediante Fibra 10 Gb.

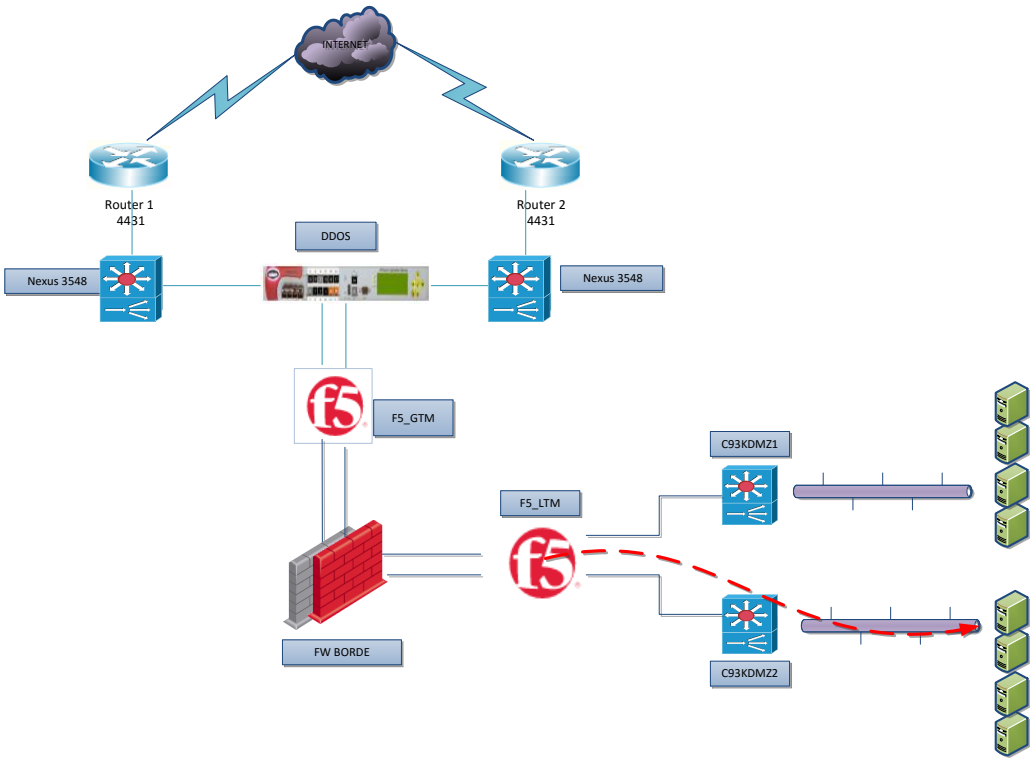


*Figura 44*. Conexiones LTM F5
*Fuente*: Elaboración Propia

#### *5.2.10.3. Funcionalidad del GTM F5*

El Global Traffic Manager, también conocido como GTM, es uno de los módulos de vanguardia que ofrece la plataforma BIG-IP de F5 Networks. Este módulo tiene la capacidad de tomar decisiones de balanceo de carga de resolución de nombres para sistemas ubicados en cualquier parte del mundo. GTM se lo puede considerar como un DNS inteligente que está orientado a la seguridad. En otras palabras, su lógica puede tomar decisiones informadas sobre la correlación de un nombre de host con una dirección IP mientras mantiene la seguridad bajo control (Geraci Austin, 2017).

El elemento de configuración principal en un GTM se llama WIP. Hay muchos elementos de configuración que funcionan en concordancia con un WIP, pero en la base de todo esto está el Wide IP. Un WIP equivale a la URL común que está balanceando la carga. Un pool o pools suelen estar conectados a un WIP que contiene las IPs que está resolviendo inteligentemente.

En el diseño del Datacenter Alterno se utiliza el dispositivo BIG-IP con el módulo GTM de F5 para realizar el balanceo de carga del servidor global el cual gestiona la Resolución de nombres de dominio (DNS) durante un desastre en el Datacenter Principal. El dispositivo F5 supervisa el estado de los servicios de aplicación en el centro de datos principal y puede configurarse para enrutar el tráfico entrante de Internet al Datacenter Alterno en caso de Falla del DCP. Para esta configuración se debe utilizar dos dispositivos BIG-IP GTM, uno en el centro de datos principal y otro en el centro de datos alterno.

En el diseño objetivo, F5 GTM se instalará después del dispositivo DDOS y del router de Internet. F5 BIG-IP DNS resolverá todas las consultas y realizará una redirección basada en IP. El centro de datos tendrá el módulo F5 BIG-IP DNS, y se sincronizará a través del enlace de interconexión entre Datacenters.

Cada URL basada en DNS tendrá dos IPs asociadas, una IP del DCP, Quito y otra IP de DCA, Guayaquil, con el objetivo de si la IP principal no responde, por el caso que fuere, las peticiones de los clientes externos se re enrutaran al Datacenter Alterno, manteniendo la disponibilidad del servicio.

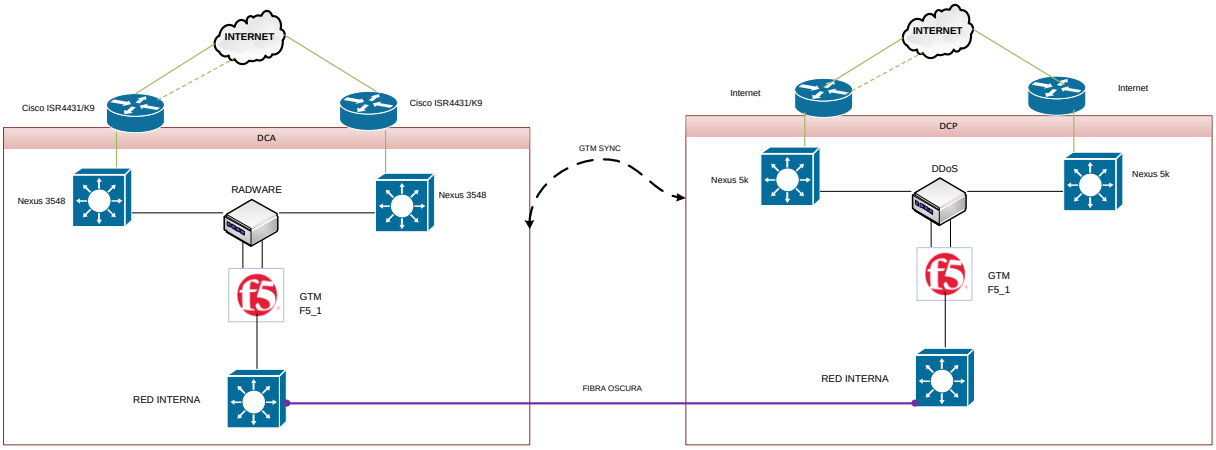


*Figura 45.* Esquema de Conexión de GTM para redundancia de Datacenters
*Fuente*: Elaboración Propia

### 5.2.11. Dispositivos de Red considerados en el Diseño del Datacenter Alterno

Luego de revisar el diseño de la infraestructura de red a implementar en el Datacenter Alterno, a forma de resumen se indican los equipos de Red a implementar en la Red LAN del DCA, su nomenclatura y su posición en el los Racks del DCA.

Tabla 50
*Nomenclatura, Posición de Equipos de Red a implementar en el DCA*

| NOMBRE | EQUIPO | MODELO | RACK |
|---|---|---|---|
| **gyeINTERNET_** | CiscoRouter4431 | ISR4431 | A9 |
| **gyeSERVICIOS_** | CiscoRouter4431 | ISR4431 | A12 |
| **gyeSWINTERNET_** | CiscoNexus3548-10G | N3K-C3548P | A9 |
| **gyeSWSERVICIOS_** | CiscoNexus3548-10G | N3K-C3548P | A12 |
| **gyeSWINTERCONEXION_** | Cisco3850-12XS-E | C3850-12XS | A12 |
| **GyeSWDMZ1_** | CiscoNexus9372TX | N9K-C9372TX | A2 |
| **GyeSWDMZ2_** | CiscoNexus9372TX | N9K-C9372TX | A2 |
| **GyeCASR_TERCEROS_** | CiscoASR1006 | ASR1006 | A9 |
| **gyeSWTERCEROS_** | Cisco4500X | C4500X | A9 |
| **gyeSWMGMT_1** | Cisco2960X | C2960X | A20 |
| | Cisco2960X | C2960X | A20 |

| | | | |
|---|---|---|---|
| | Cisco2960X | C2960X | A20 |
| **gyeC7K1-CORE** | CiscoNexus7710 | N77-C7710 | A10 |
| **gyeC7K2-CORE** | CiscoNexus7710 | N77-C7710 | A11 |
| **gyeCX7K1_PCI_** | CiscoNexus7710 | N77-C7710 | A10 |
| **gyeCX7K2_PCI_** | CiscoNexus7710 | N77-C7710 | A11 |
| **gyeCX7K1_PRI_** | CiscoNexus7710 | N77-C7710 | A10 |
| **gyeCX7K2_PRI_** | CiscoNexus7710 | N77-C7710 | A11 |
| **gyeC7K1_SERV_** | CiscoNexus7710 | N77-C7710 | A10 |
| **gyeC7K2_SERV_** | CiscoNexus7710 | N77-C7710 | A11 |
| **gyeC93K1_** | CiscoNexus9372PX | N9K-C9372PX | B1 |
| **gyeC93K2_** | CiscoNexus9372PX | N9K-C9372PX | B20 |
| **gyeC93K3_** | CiscoNexus9372PX | N9K-C9372PX | B1 |
| **gyeC93K4_** | CiscoNexus9372PX | N9K-C9372PX | B20 |
| **gyeC2K4-1** | Cisco Nexus 2248 TPE | N2K-C2248TP | B20 |
| **gyeC2K4-2** | Cisco Nexus 2248 TPE | N2K-C2248TP | B20 |
| **gyeC2K2-1** | Cisco Nexus 2248 PQ (F) | N2K-C2248PQ | B20 |
| **gyeC2K3-1** | Cisco Nexus 2248 TPE | N2K-C2248TP | B1 |
| **gyeC2K3-2** | Cisco Nexus 2248 TPE | N2K-C2248TP | B1 |
| **gyeC2K1-1** | Cisco Nexus 2248 PQ (F) | N2K-C2248PQ | B1 |
| **gyeF5_5250** | F5 BIG-IP 5250V | 5250V | A12 |

*Fuente*: Elaboración Propia

La ubicación en los racks de los equipos de red en el Datacenter se indica a continuación:

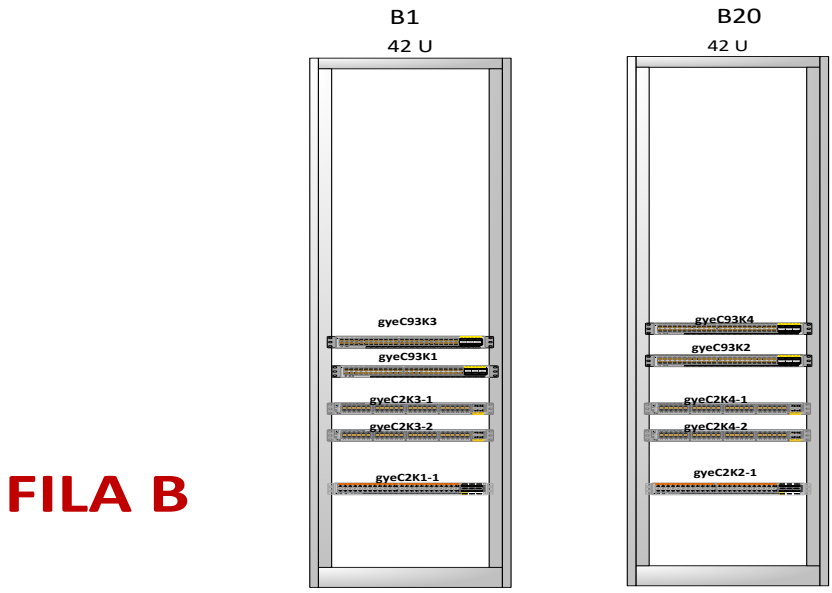


*Figura 46.* Ubicación en los Racks Equipos de Red Fila B
*Fuente*: Elaboración Propia

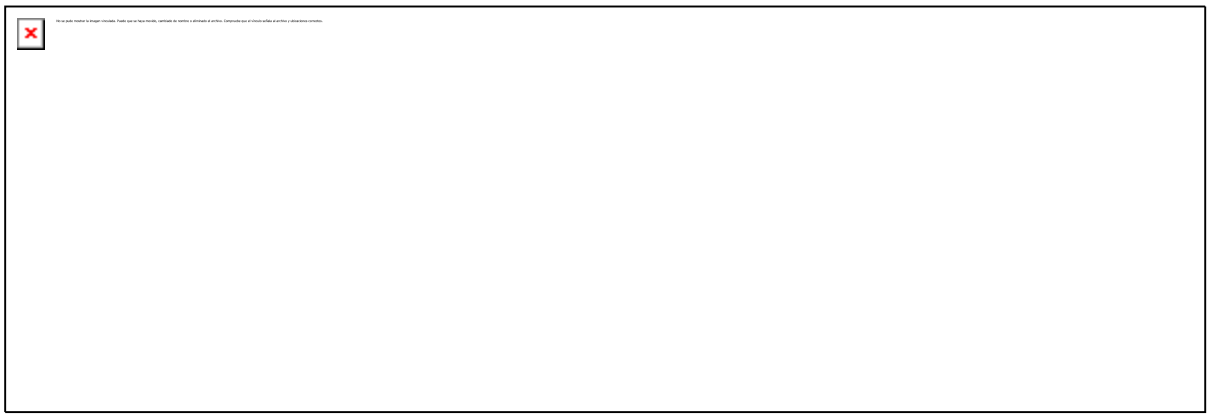

*Figura 47.* Ubicación en los Racks Equipos de Red Fila A
*Fuente*: Elaboración Propia

### 5.2.12. Cableado Requerido Equipos de Red en el Datacenter Alterno

Luego de revisar el diseño de la infraestructura de red a implementar en el Datacenter Alterno, a forma de resumen, en la tabla de a continuación se indica el cableado requerido para la conexión de los equipos de red del DCA.

Tabla 51
*Cableado Necesario Para la Conexión de los Equipos de Red en el DCA*

| EQUIPOS | | RACK | | COBRE | FIBRA OPTICA | OBSERVACIONES |
|---|---|---|---|---|---|---|
| Origen | **Destino** | **Origen** | **Destino** | **1 Gbps** | **10 Gbps** | |
| **Router Proveedor** | ISR 4431 | A1 | A9 | 1 | | Conexión de Proveedores externos Internet |
| **Router Proveedor** | ISR 4431 | A1 | A12 | 1 | | Conexión de Proveedores externos Internet |
| **Equipos Interconexión Telco** | Nexus 7710 1 | A1 | A10 | 1 | | Conexión para enlace de Fibra Oscura |
| **Equipos Interconexión Telco** | Nexus 7710 2 | A1 | A11 | 1 | | Conexión para enlace de Fibra Oscura |
| **F5** | Nexus 9372TX DMZ | A12 | A2 | | 4 | Conexión F5 - Nexus 9372TX dmz |
| **F5** | Cisco C3850X | A12 | A12 | | 2 | Conexión F5 - Cisco 3850X |

| | | | | | | |
|---|---|---|---|---|---|---|
| **F5** | Cisco 3524 | A12 | A9 | | 1 | Conexión F5 - Cisco 3524 (Rack 3D) |
| **F5** | Cisco 3524 | A12 | A12 | | 1 | Conexión F5 - Cisco 3524 (Rack 3G) |
| **Firewall Terceros** | Nexus 7710 1 | A8 | A10 | | 1 | Conexión Firewall Terceros - Nexus 7710A |
| **Firewall Terceros** | Nexus 7710 2 | A8 | A11 | | 1 | Conexión Firewall Terceros - Nexus 7710B |
| **Firewall Terceros** | Cisco 4500X | A8 | A9 | | 2 | Conexión Firewall Terceros - Cisco 4500X |
| **ASR 1006** | Router Proveedores | A9 | A1 | 6 | | Conexión AS 1006 - Acceso proveedores Terceros |
| **Nexus 7710 1** | Nexus 7710 2 | A10 | A11 | | 14 | Conexión Peer - Link |
| **Nexus 7710 1** | Nexus 7710 2 | A10 | A11 | | 12 | Conexión VDC Core - Vdc's (PRI-SERVICIOS-PCI) |
| **Nexus 7710 1** | 9372PX | A10 | B1 | | 6 | Conexión 7710A - 9372PX Contingencia |
| **Nexus 7710 2** | 9372PX | A11 | B20 | | 6 | Conexión 7710B - 9372PX Contingencia |
| **Nexus 7710 1** | 9372PX | A10 | B1 | | 6 | Conexión 7710A - 9372PX Contingencia |
| **Nexus 7710 1** | 9372PX | A11 | B20 | | 6 | Conexión 7710B - 9372PX Contingencia |
| **Firewall Borde** | 2960x | A8 | A20 | 3 | | Administración Firewall Borde |
| **Firewall Principal** | 2960x | A8 | A20 | 3 | | Administración Firewall Principal |
| **Firewall Terceros** | 2960x | A8 | A20 | 5 | | Administración Terceros |
| **Nexus 9372TX** | 2960x | A2 | A20 | 3 | | Administración Nexus 9372TX |
| **Nexus 9372TX** | 2960x | A2 | A20 | 3 | | Administración Nexus 9372TX |
| **Consola administración firewall** | 2960x | A8 | A20 | 2 | | Administración consola Checkpoint |
| **ASR1006** | 2960X | A9 | A20 | 2 | | Administración ASR1006 |
| **Nexus 3524** | 2960x | A9 | A20 | 2 | | Administración Nexus 3524 |
| **Cisco 4500x** | 2960x | A9 | A20 | 2 | | Administración Nexus 4500x |
| **Nexus 3524** | 2960x | A12 | A20 | 2 | | Administración Nexus 3524 |
| **Cisco 3850x** | 2960x | A12 | A20 | 2 | | Administración Cisco 3850x |
| **Nexus 9372PX Contingencia (1)** | 2960X | B1 | A20 | 1 | | Administración Nexus 9372PX Contingencia |

| | | | | | |
|---|---|---|---|---|---|
| **Nexus 9372PX Contingencia ( 3)** | 2960X | B1 | A20 | 1 | Administración Nexus 9372PX Contingencia |
| **Nexus 9372PX Contingencia (2)** | 2960X | B20 | A20 | 1 | Administración Nexus 9372PX Contingencia |
| **Nexus 9372PX Contingencia (4)** | 2960X | B20 | A20 | 1 | Administración Nexus 9372PX Contingencia |
| **Nexus 7710 1** | 2960X | A10 | A20 | 4 | Administración Nexus 7kA |
| **Nexus 7710 2** | 2960X | A11 | A20 | 4 | Administración Nexus 7kB |

*Fuente*: Elaboración Propia

## 5.3. Configuraciones de Equipos de Red en el Datacenter Alterno

De acuerdo al Diseño presentado para el Datacenter Alterno existen varias configuraciones que se deben realizar para lograr la conectividad total de la Red.

En esta sección se resumirá las configuraciones a realizar en los equipos de Red de la infraestructura del Datacenter Alterno. No se pretende detallar cada una de las configuraciones realizadas, el objetivo de este capítulo es dar un extracto de las configuraciones más importantes que se realiza en los equipos de Networking para tener una comunicación completa en la red.

### 5.3.1. Configuraciones Iniciales de los equipos de Red

Las configuraciones iniciales que se realizarán a los equipos se detallan resumidamente en la siguiente tabla:

Tabla 52
*Configuraciones a aplicar en los equipos de Red*

| CONFIGURACION/EQUIPO | *Nexus 7710* | *Nexus 9372* | *Nexus 2000* | *ROUTERS ASR1006 - 4431* | *Catalyst 4500x* | *Catalyst 3850* | *Catalyst 2960* |
|---|---|---|---|---|---|---|---|
| **Inicialización** | SI | SI | SI | SI | SI | SI | SI |
| **Configuración de direcciones IP de administración** | SI | SI | NO | SI | SI | SI | SI |
| **Creación de VDCs** | SI | NO | NO | NO | NO | NO | NO |
| **Configuración de Hostname** | SI | SI | NO | SI | SI | SI | SI |
| **Configuración de banner MOTD** | SI | SI | NO | SI | SI | SI | SI |
| **Configuración de SNMP** | SI | SI | NO | SI | SI | SI | SI |
| **Configuración de conexiones de acceso remoto** | SI | SI | NO | SI | SI | SI | SI |
| **Configuración de servidor NTP** | SI | SI | NO | SI | SI | SI | SI |
| **Configuración de usuarios de administración** | SI | SI | NO | SI | SI | SI | SI |
| **Activación de funcionalidades** | SI | SI | NO | NO | NO | NO | NO |
| **Configuración de Spanning-tree** | SI | SI | NO | SI | SI | SI | SI |
| **Configuración de VLANs** | SI | SI | NO | NO | NO | NO | NO |
| **Configuración de HSRP** | SI | SI | NO | NO | NO | NO | NO |
| **Configuración de PortChannels y VPCs** | SI | SI | NO | NO | NO | NO | NO |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Configuración de enlaces troncales** | SI | SI | NO | SI | SI | SI | SI |
| **Configuración de puertos de acceso** | SI | SI | NO | SI | SI | SI | SI |
| **Configuración de Direccionamiento de las capas** | SI | SI | NO | NO | NO | NO | NO |
| **Configuración de enrutamiento** | SI | SI | NO | SI | SI | NO | NO |
| **Configuración FEX** | NO | SI | NO | NO | NO | NO | NO |

*Fuente*: Elaboración Propia

Adicional a las configuraciones iniciales de los equipos se realizará la siguiente configuración de seguridad de acceso a cada uno de los equipos:

Tabla 53
*Configuraciones de acceso a los equipos de Red*

| **BANNER** | **ADVERTENCIA**<br>*****

Tabla 54
*Funcionalidades a configurar en los equipos*

| EQUIPO | FUNCIONALIDAD |
|---|---|
| **NEXUS 7710** | feature interface-vlan |
| | feature lacp |
| | feature vpc |
| | feature hsrp |
| **NEXUS 9372** | feature lacp |
| | feature vpc |
| | feature FEX |

*Fuente*: Elaboración Propia

### 5.3.2. Configuración de Spanning Tree

El protocolo a utilizar en el Data Center Alterno es Rapid Per VLAN Spanning Tree, también se habilitara en los puertos que estén en modo acceso los features de STP bpduguard y portfast. En las VDCs y Core debido a que se van a configurar VPCs se tendrá que configurar ambos equipos Nexus 7000 con la misma prioridad.

### 5.3.3. Configuración de VLANs

Cada capa dentro del nuevo Datacenter tendrá su propio esquema de VLANs. En el caso de CORE y las VDCs se configuran VLANs que sirven para el enrutamiento entre capas y se manejara HSRP como protocolo de alta disponibilidad en las VLANs, para el caso de Borde se configurarán VLANs que permiten la interacción con los proveedores, el Internet y los socios de negocio.

### 5.3.4. Configuración de PortChannels y VPCs

En el diseño de la arquitectura de red se contempla configurar PortChannels y VPCs de acuerdo a la necesidad definida en el diagrama de esquema General.

Los Virtual PortChannels (vPCs) permiten que los enlaces que están conectados físicamente a dos Switches Cisco diferentes parezcan a un tercer dispositivo como si proviniera de un solo dispositivo y como parte de un único PortChannel. El tercer dispositivo

puede ser un Switch, un servidor o cualquier otro dispositivo de red compatible con PortChannels 802.3ad de IEEE.

Para formar troncales VPC, es necesario que se conecte los dos Switchs entre sí mediante enlaces de 1/10 G, preferiblemente uno en cada una de las dos tarjetas de línea diferentes para mayor solidez, y declarando que ese enlace es un port-channel y un enlace entre pares VPC (peer link VPC). Este es un enlace especial para transportar el tráfico L2 entre los Switches VPC cuando hay un fallo de enlace. Antes de que se levante el VPC Peer Link, también se tiene que configurar las Keepalive de VPC para detectar que los dos pares estén activos cuando el enlace entre pares VPC esté caído (Welcher Peter, 2011).

### 5.3.5. Configuración de Puertos Troncales y de Acceso.

Los equipos Nexus de esta implementación tendrán una distribución de puertos en función de sus necesidades; los puertos pueden ser troncales, de acceso o FEX.

### 5.3.6. Configuración del enrutamiento

El enrutamiento dentro del Data Center Alterno será manejado por enrutamiento estático. Los Switches de acceso no forman parte del enrutamiento ya que ellos no tienen direccionamiento IP en sus configuraciones. Los Firewalls internos son aquellos que permitirán la comunicación hacia los servidores de las VDCs PRI. Servicios y PCI. La capa de Core es una capa que permite la interacción entre las VDCs y Borde.

El Firewall de Terceros tiene las redes directamente conectadas y las rutas estáticas que permitirá el paso hacia las sucursales y empresas terceras. Por último el Firewall de Borde tendrá una ruta por defecto hacia el Internet.

### 5.3.7. Configuración de Túneles

La comunicación entre el DCA y las Sucursales y empresas terceras, será manejada a través de túneles GRE, los cuales serán establecidos por medio de los diferentes enlaces directamente conectados al Router de Terceros (ASR1006). El enrutamiento que se manejará para las diferentes conexiones será manejado por enrutamiento estático y dinámico.

### 5.3.8. Configuración HSRP

La configuración de HSRP[5] se la realizará en los dos Switches de Core Cisco 7710 para brindar alta disponibilidad en las comunicaciones del Datacenter Alterno.

La implementación del protocolo HSRP dentro de la infraestructura de Core del DCA permite lograr un tiempo de funcionamiento de la red de Datacenter Alterno cercano al 100%, ya que proporciona redundancia para las redes IP, asegurando que el tráfico de usuario se recupere inmediata y transparentemente si se produce un fallo en uno de los dispositivos que conforman esta configuración.

HSRP permite compartir una dirección IP y una dirección MAC (Capa 2), con lo cual dos o más Routers/Switches pueden actuar como un solo equipo "virtual". Los miembros del grupo de dispositivos virtuales intercambian continuamente mensajes de estado. De esta manera, un equipo puede asumir la responsabilidad de enrutamiento de otro, si se sale de servicio por razones planificadas o no planificadas. Los hosts continúan reenviando los paquetes IP a una dirección IP y MAC consistente, y el cambio de dispositivo que realiza el enrutamiento es transparente.

Un único router/switch elegido del grupo es el responsable de reenviar los paquetes que los hosts envían al equipo virtual. Este elemento se conoce como router/switch activo.

---

[5] Hot Standby Router Protocol

Otro router/switch es elegido como Standby. En caso de que el router/switch activo falle, el standby asume las funciones de enrutamiento de paquetes del router/switch activo.

Para minimizar el tráfico de la red, sólo los routers/switches Activos y en standby envían mensajes HSRP periódicos una vez que el protocolo ha completado el proceso de elección (Cisco, 2006. Hot Standby Router Protocol Features and Functionality).

### 5.3.9. Configuración PBR

La configuración de PBR[6] se lo realiza en el equipo Switch de Agencias ya que a través de este equipo se podrá elegir uno de los dos caminos de entrada a la Red de Core del Datacenter Alterno.

El objetivo de esta configuración es tener un camino que atraviese firewall para aquellas conexiones no confiables (empresas terceras, proveedores) y otro camino que no atraviese firewall para conexiones fiables (sucursales) con el fin de que estas últimas no tengan problemas al conectarse a las aplicaciones de la red interna del DCA.

El enrutamiento basado en políticas (PBR) proporciona un método para reenviar paquetes al sustituir la información disponible en la tabla de enrutamiento IP. Mediante el uso de PBR, se pueden implementar políticas que hacen que los paquetes tomen diferentes caminos de forma selectiva. El enrutamiento IP tradicional reenvía paquetes basados sólo en la dirección IP de destino del paquete. El PBR puede configurarse para reenviar paquetes basándose en otros criterios, como la dirección de origen, la aplicación y la longitud del paquete.

El PBR se puede utilizar para implementar QoS clasificando y marcando paquetes con valores de precedencia IP en el campo Tipo de servicio (ToS) del encabezado IP. Los enrutadores en el core pueden entonces implementar técnicas de cola para priorizar el tráfico

[6] Policy-Based Routing

ya marcado. El PBR también se puede utilizar para enrutar los paquetes a través de rutas específicas diseñadas por ingeniería de tráfico, que proporcionan la QoS deseada a través de la red. (Cisco, 2017. How to configure PBR)

En el caso del diseño del DCA los PBR se utilizaran para definir el camino a seguir de un paquete basándose en la dirección de origen de la conexión.

## 5.4. Interconexión del Datacenter Principal con el Datacenter Alterno

En este Capítulo se abordará el diseño contemplado para lograr la interconexión de los Datacenters de la empresa.

Dentro del diseño de la arquitectura de red del DCA se considera la implementación de la conectividad entre los dos Datacenter. Esta conexión tiene como objetivo en primera instancia realizar la réplica en el DCA de los servidores y su data que se encuentra almacenada en los storage del Datacenter Principal

En el DCP existen dos clases de storage: los storage IBM y los storage HP. El tráfico de datos de estos dos equipamientos se replicará a través de la interconexión de Datacenters. Para poder enrutar el tráfico se configura una VRF para la interconexión del segmento de red entre Datacenters.

La conexión entre los Datacenters de Quito y Guayaquil se ha diseñado realizarla a través de una conexión de 2 enlaces de Fibra Oscura[7]

Como la fibra oscura es solamente un medio por el que viajan las ondas de luz, permite la transmisión de cualquier aplicación o protocolo. Puesto que no existe ningún intermediario, las redes de fibra oscura pueden operar utilizando los últimos protocolos ópticos por medio de división multiplexada de longitud de onda para añadir capacidad donde se necesita, y para proveer un camino de actualización entre tecnologías sin sacar la red de servicio (National Fiber Networks, 2012).

El proveedor ISP será también el proveedor que soporta la fibra oscura entre el centro de datos Principal y Alterno.

Para la implementación de la interconexión de Datacenters se debe considerar algunos dispositivos intermedios en los DC de Quito y Guayaquil a los cuales se conectará la

[7] Fibra a través del proveedor ISP - los circuitos de fibra óptica, que han sido desplegados por algún operador de telecomunicaciones

infraestructura de Core de cada Datacenter. Los siguientes equipos serán utilizados para proveer la interconexión de los Datacenters mediante los enlaces de fibra oscura.

Tabla 55
*Equipos de Interconexión de los Datacenters*

| DISPOSITIVO | DESCRIPCION |
|---|---|
| PL2000 | Dispositivo de Transporte; se conectará a la red Nacional del ISP |
| PL1000TE | Dispositivo usado para encripción de datos |
| CTCFRM220 | Switch óptico usado para la conversión eléctrica a Óptica |

*Fuente*: Elaboración Propia

Cada dispositivo a utilizar para la interconexión de los DC tiene una función específica como se indica en la tabla 55. La cantidad de dispositivos a utilizar en el entorno de cada Datacenter se indica a continuación:

Tabla 56
*Cantidad Equipos de Interconexión de los Datacenters*

| DISPOSITIVO | CANTIDAD |
|---|---|
| PL2000 | 2 |
| PL1000TE | 1 |
| CTCFRM220 | 2 |

*Fuente*: Elaboración Propia

El diagrama de bloque de Interconexión utilizando los equipos especificados con anterioridad quedará de la siguiente forma

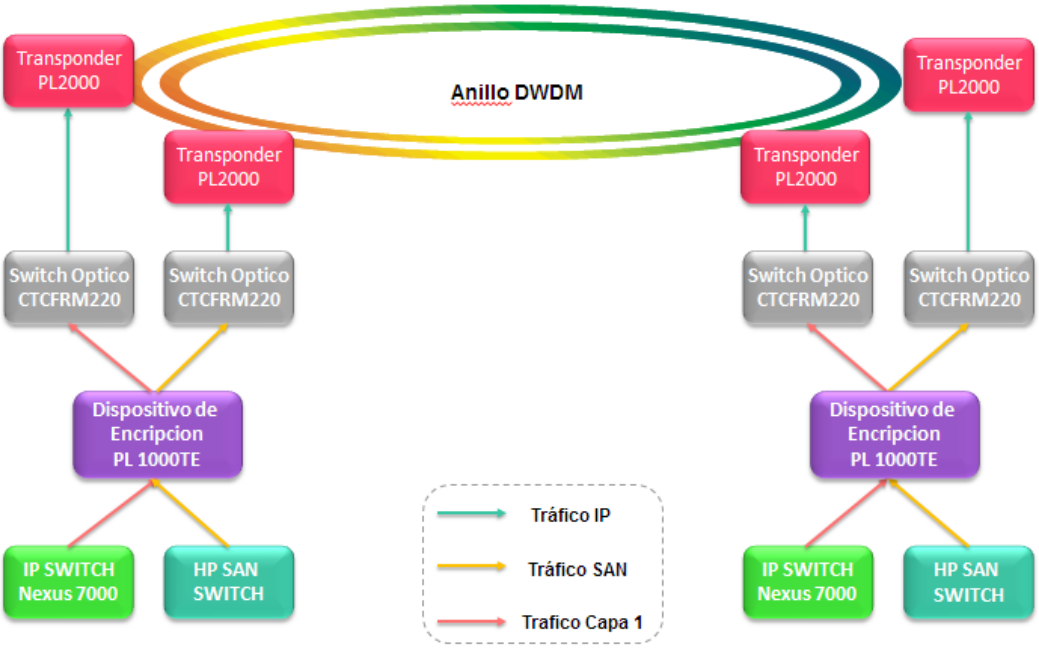


*Figura 48.* Diagrama de Bloque Interconexión Datacenters
*Fuente*: Elaboración Propia

De acuerdo a la cantidad de dispositivos de interconexión diseñados se tendrá 2 dispositivos transponder PL2000, que se configurará en estado activo-activo. De este modo, el proveedor de servicios garantiza una conmutación por error transparente en caso de fallo del enlace o del dispositivo.

Caso contrario sucede con el dispositivo de encriptación PL1000TE y el switch óptico los cuales solo se contara con una unidad en cada Datacenter por lo que no se tendrá redundancia con estos elementos.

La conexión lógica de  estos equipos se muestra en la siguiente figura:

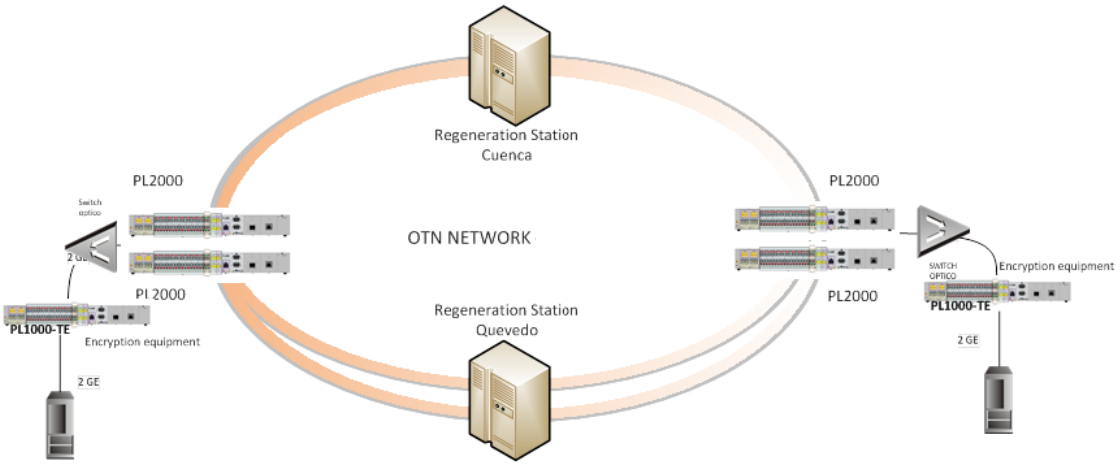


*Figura 49.* Diagrama Lógico de la Interconexión Datacenters
*Fuente*: Elaboración Propia

Físicamente las conexiones, desde la perspectiva del Datacenter Alterno, de los dispositivos involucrados en la interconexión serán:

Tabla 57
*Conexiones Físicas Equipos de Interconexión de los Datacenters*

| Dispositivo | Conexión OUT | Conexión IN |
|---|---|---|
| PL2000(Transponder) | Hacia la Fibra Oscura | Switch Óptico |
| CTCFRM220(Switch Óptico) | Transponder | Dispositivo de Encripción |
| PL1000TE(Dispositivo de Encripción) | Switch Óptico | Switch de Core |

*Fuente*: Elaboración Propia

Gráficamente estas conexiones serán de la siguiente manera:

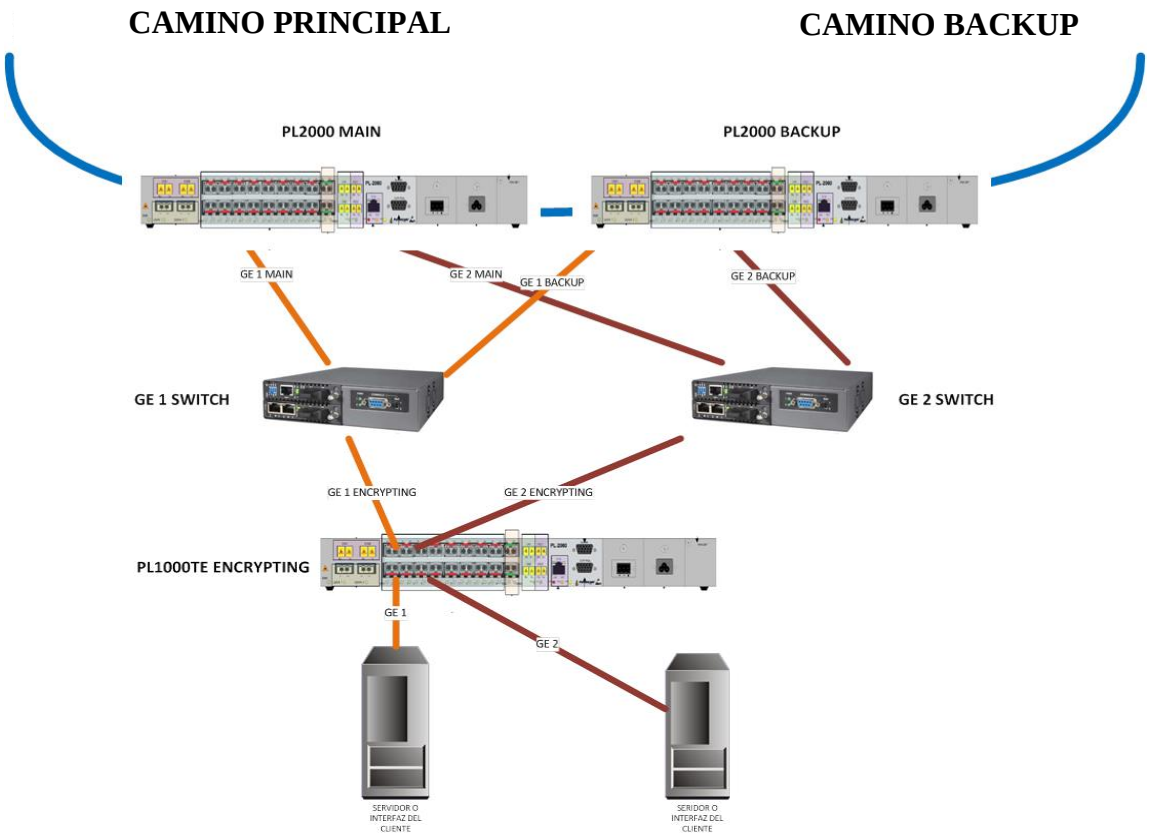


*Figura 50.* Diagrama Conexiones Físicas dispositivos de la Interconexión Datacenters
*Fuente*: Elaboración Propia

Algunas consideraciones importantes a tomar en cuenta en el diseño de la interconexión de los Datacenters son:

- Se estima que se producirá un retraso considerable cuando el tráfico del FC pase a través del cable de fibra oscura. El retardo será de aproximadamente unos 8mseg. pero al contrario, no habrá retardo en el tráfico Ethernet. Por lo general, se adquieren dispositivos especiales de Buffer intermedios para anular el retraso del tráfico de FC, pero en nuestro caso se puede aceptar un retraso de 120 ms, por lo que no es necesario adquirir estos dispositivos por separado.
- Los dispositivos que se conectarán al dispositivo de cifrado son El Switch de Core Cisco Nexus 7710, mediante conectividad de fibra a 1G que transportará tráfico IP

- No es necesaria ninguna configuración especial en los Switches de Core para soportar la infraestructura de interconexión de los Datacenters.
- El protocolo que se ejecuta entre el Datacenter Principal y el Datacenter Alterno es DWDM[8]
- El Storage ejecutará el protocolo FCIP
- Para la conectividad, Interfaces Capa3 se configurarán en los Cores de ambos Datacenters

### 5.4.1. Características equipos de Interconexión de Datacenters

Cada uno de los equipos que se involucran en la interconexión de los Datacenters mediante los 2 enlaces de fibra oscura, tiene una funcionalidad específica que permite que el tráfico del Datacenter Principal pueda ser replicado hacia el Datacenter Alterno y viceversa.

En este apartado se mencionará las características principales de cada uno de ellos.

#### *5.4.1.1. Dispositivo de Encripción PL 1000 TE*

El equipo PL 1000 TE será el dispositivo que se encontrará conectado Directamente a la red de Core de Cada Datacenter en los equipos Cisco Nexus 7710. La función de este equipo es brindar seguridad a la comunicación de los datos que viajará a través del backbone del ISP entre Datacenters, esto lo realizará a través de la encriptación de los datos.

El equipo PL1000TE proporciona un beneficio de seguridad adicional a cualquier enlace DWDM al encriptar los datos que pasan entre los sitios. La criptografía del dispositivo PL 1000TE realiza el cifrado AES a nivel de capa 1 sin ninguna degradación al ancho de

[8] DWDM (Dense Wavelength Division Multiplexing o multiplexado compacto por división en longitudes de onda) Es una técnica en donde varias señales portadoras (ópticas) se transmiten por una única fibra óptica utilizando distintas longitudes de onda de un haz de luz para cada una de ellas. Cada portadora óptica forma un canal óptico que podrá ser tratado independientemente del resto de canales que comparten el medio (fibra óptica) y contener diferente tipo de tráfico. De esta manera se puede multiplicar el ancho de banda efectivo de la fibra óptica, así como facilitar comunicaciones bidireccionales

banda completo de los servicios 1/10G y 16Gbp Fibre Channel. El servicio de cifrado proporciona una transparencia completa de extremo a extremo de los datos del servicio y con una baja latencia de menos de 12usec para 10GbE (Netways Europe, 2015).

La solución de cifrado integral de asegura tres preocupaciones principales de la seguridad óptica del enlace:

- *Confidencialidad* - prevenir la divulgación de información a partes no autorizadas
- *Integridad de los datos* - garantizar que el mensaje no se haya alterado
- *Autenticación* - validación de que ambas partes implicadas son realmente quienes afirman ser

El equipo de encriptación PL-1000TE es aplicable para los servicios de GbE, 10GbE y 4x10G PCS de 40GbE y se puede activar flexiblemente la funcionalidad de cifrado/descifrado para transpondedores específicos. Adicional es transparente para el tráfico sin degradación del rendimiento del enlace DWDM o QoS de los datos transportados.

*Figura 51.* Dispositivo de Encripción PL 1000 TE
*Fuente*: (Netways Europe, 2015).

#### *5.4.1.2. Switch Óptico CTCFRM220*

El Switch óptico realizará la conversión del medio de fibra a cobre para la conexión hacia el dispositivo de transporte PL 2000. Adicional convertirá todo el tráfico a IP para que sea manejado por el dispositivo de transporte.

*Figura 52.* Dispositivo Switch Óptico FRM220
*Fuente*: (CTC Union, 2017)

El FRM220-10/100 es un convertidor de medios de comunicación, Fast Ethernet 10/100Base-TX a 100Base-FX, stand-alone no gestionado, que ofrece las opciones para elegir entre los conectores de cableado de fibra más populares, ST, SC o FC. Están disponibles tanto los modelos de convertidores multimodo como monomodo, así como BiDi, que permiten transmisiones bidireccionales utilizando sólo un core de fibra. Cuando se selecciona la auto-negociación, estas unidades se adaptarán automáticamente para convertir tanto señales half-dúplex como señales full dúplex, de acuerdo con los estándares IEEE802.3u.[9]

La familia FRM220 de transponders 2R y 3R de CTC Union son utilizados para cambiar la longitud de onda de la señal de entrada de 850/1310/1550nm a longitudes de onda coloreadas CWDM y/o proporcionar protección óptica de las señales de entrada FE, GBE, 10GE, 16G, STM-1/4/16/64. De acuerdo a la velocidad de la señal se debe escoger entre transponders 2R o 3R, siendo estos últimos los que realizan (Re-amplificación, Re-sincronización y Re-formato de la señal. El modelo 2R no realiza la Re-sincronización. Toda la solución puede ser administrada local y remotamente a través del software de administración centralizado SmartView (Milestone. Transponders Ópticos – FRM220-Transponder).

Algunas de las funcionalidades principales del switch óptico FRM220 son:

- Convertidor de 10/100/1000Base-TX a 1000Base-FX Converter

[9] 100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet a 100 Mbit/s (12.5 MB/s) con autonegociación

- Auto-negociación o modo forzado
- Auto MDI/MDIX
- Reenvío paquetes  1600 bytes (Máx.)
- Soporta Q en Q  doble tageada transparente
- Soporta IEEE 802.1q Tag VLAN pass thru
- Soporta Control de flujo (Pausa) - Soporta el paso de falla de enlace (LFP)
- Reenviar paquetes jumbo 9K en modo convertidor

#### *5.4.1.3. Dispositivo de Transporte PL 2000*

El equipo PL2000 se utilizará en la interconexión de los Datacenters como el dispositivo encargado de transmitir el tráfico de cada Datacenter hacia la red Backbone del ISP, mediante la tecnología DWDM.

El PL-2000 es un Muxponder  Multiprotocolo/Multirate avanzado con agregación flexible de uplinks de hasta 20G de capacidad. Aumenta de la eficiencia espectral de las redes CWDM/DWDM con Muxponders 10G de baja latencia simple o dual configurables por el usuario.

*Figura 53*. Dispositivo Trasportador PL2000
*Fuente*: PacketLight. (2014).

El PL-2000 reduce significativamente el número de longitudes de onda necesarias para la red CWDM/DWDM, así como el número de filtros requeridos, lo que reduce el tamaño y el coste de los EDFA (Amplificador de fibra dopada con erbio) y la complejidad de gestión de la red.

Con su soporte multiprotocolo y multitasa, el enlace ascendente OTU2[10] de 10G puede agregar simultáneamente servicios SDH/SONET, Eth, Fibre Channel y Video, proporcionando así una plataforma de acceso perfecta para las necesidades de múltiples clientes y permitiendo la fusión de antiguos  y nuevos servicios de forma transparente.

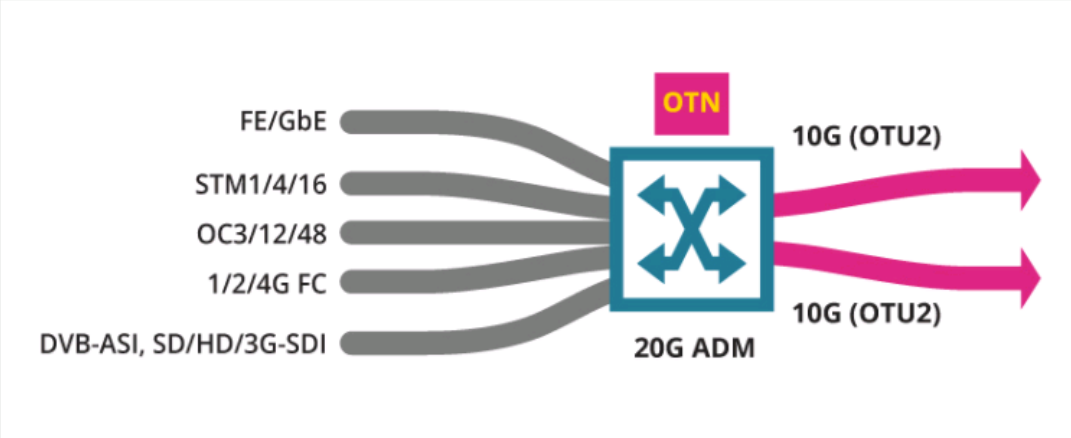


*Figura 54.* Agregación de servicios en el equipo PL 2000
*Fuente*: PacketLight. (2017).

Los equipos PL-2000 transparentemente multiplexa hasta 16 servicios de cliente en una sola o doble longitudes de onda independientes de 10G, de forma transparente en capa-1, con una latencia ultra baja a un uplink de 10G sin pérdida de paquetes y con corrección mejorada de errores de reenvío (EFEC) adecuada para redes DWDM amplificadas de larga distancia.

Las especificaciones técnicas de este equipo la podemos encontrar en la siguiente tabla:

[10] OTU: El OTUk (k=1/2/2/2e/3/3e2/4) es una estructura de información en la que se asigna otra estructura de información llamada ODUk (k=1/2/2e/3/3e2/4). La señal ODUk es la señal de capa de servidor para las señales de cliente.

Tabla 58

*Especificaciones Técnicas equipo PL 2000*

| CARACTERISTICA | DESCRIPCION |
|---|---|
| SISTEMA | |
| **Topología** | Punto a punto o Anillo |
| **Medio Red de Transporte** | Acceso/Metro CWDM/DWDM o Fibra Oscura |
| **Protección** | 1+1 Instalaciones |
| **CONFIGURACIONES DE PRODUCTO** | |
| **Muxponder Dual 10G OTU2** | Hasta 16 clientes multiservicio y tasas |
| **EDFA** | Módulo EDFA opcional |
| **Mux/Demux** | Opcional Módulo Mux/Demux/Demux |
| **AMPLIFICADOR** | |
| **Potencia de salida** | 14,17,20 o 23dBm |
| **Potencia de entrada** | -36 dBm hasta 16 dBm |
| **Ganancia** | 10 dB a 22 dB |
| **Modos de operación** | AGC (control automático de ganancia),<br>APC (Control Automático de Potencia) |
| **Seguridad ocular** | Reducción automática de la potencia del láser al cortar o desconectar la fibra |
| **MUX/DEMUX** | |
| **Canales** | 2/4/8 CWDM o DWDM Canales |
| **Separación** | 50/100GHz (para DWDM) |
| **UPINK DEL MUXPONDER** | |
| **Tasa de bits** | 10.7092G (OTU-2)* |
| **Interfaz óptica** | Transceptor XFP enchufable |
| **Tipo de servicio** | Óptica o cobre GbE<br>FC/FICON 1G, 2G o 4G<br>Fast Ethernet de cobre u óptica<br>STM1, STM4, STM16 - OC3, OC12, OC48<br>DVB-ASI, SD-SDI, HD-SDI y 3G HD-SDI |
| **Velocidad de bits** | 100 Mbps a 4.25 Gbps |
| **Interfaz óptica/cobre** | Transceptor SFP enchufable |
| **GESTIÓN DE REDES** | |
| **Puertos** | Control, LAN, OSC, alarmas externas |
| **Protocolos** | SNMP, HTTP, HTTPS, Telnet, SSH, Syslog, Radius |
| **Monitoreo de desempeño** | Intervalos de errores de Capa 1, errores actuales y del día anterior<br>Niveles de potencia óptica RX/TX |
| **Indicadores visuales** | Indicadores LED de estado para puertos ópticos<br>Alarmas Críticas, /Mayor/Menor, Amplificador, alimentación eléctrica y sistema |
| **GESTIÓN DE PUERTOS E INTERFACES FÍSICAS** | |
| **CONTROL** | RS-232, BD-9 |
| **LAN** | 10/100MBase-T, RJ-45 |
| **OSC (MNG1 & MNG2)** | 100 Base-FX, SFP |
| **FUENTE DE ALIMENTACIÓN** | |
| **AC/DC** | ~100 a ~240 VAC, -36 a -72 VDC, 68 W máx. |
| **Redundancia PSU** | Alimentación simple/doble, intercambiable en caliente |
| **Unidad de refrigeración** | Unidad de ventilador intercambiable en caliente |
| **MEDIOAMBIENTAL** | |
| **Temperatura de funcionamiento** | -5º C a 50º C |
| **Dimensiones físicas** | Tamaño 145 mm (Al) x 440mm (An) x 230 mm (P) |
| **Peso** | 5.5 Kg (Máximo) |

*Fuente*: PacketLight. (2014).

### 5.4.2. Configuración en Equipos de Core para la Interconexión DC

Para lograr la interconexión entre el Datacenter Principal y el Datacenter Alterno se requiere realizar configuraciones adicionales en los equipos de Core de cada locación.

Para ello se utilizará una interface de Fibra a 1Gb en cada equipo de Core respectivamente, con el fin de crear un port-channel que se conecte a los equipos de interconexión, para brindar disponibilidad y redundancia a las conexiones entre Quito y Guayaquil.

Todas las configuraciones se deben realizar en la VDC Core de cada NEXUS 7K1 y 7K2, tanto de UIO como de GYE. Las configuraciones a realizar serán:

- Configuración VRF
- Configuración y definición de VLAN's
- Configuración HSRP
- Configuración VPC
- Configuración enrutamiento

**Creación de VLANs en el database.**

Las VLANs se deben crear en el N7K1_CORE y en el N7K2_CORE de UIO y GYE

- Configuración de VLAN para tráfico de Storage 1

```
#vlan 2
name INTER_Replica_DCA_1
```

- Configuración de VLAN para tráfico de Storage 2

```
#vlan 3
name INTER_ Replica_DCA_2
```

- Configuración de VLAN para interconexión de los Datacenters

```
#vlan 4
 name INTER_UIO_GYE
```

**Creación de la VRF y default Gateway.**

La VRF se debe crear dentro del VDC CORE en el C7K1_CORE y en el C7K2_CORE

C7K_CORE GYE

```
vrf context INTER_VRF_UIO_GYE
  ip route 0.0.0.0/0 172.16.250.92
```

C7K_CORE UIO

```
vrf context INTER_VRF_UIO_GYE
  ip route 0.0.0.0/0 172.16.250.81
```

**Creación y asignación de SVIs**

Se creara las interfaces Virtual del Switch, para poder realizar la configuración de enrutamiento de la interconexión entre Datacenters

C7K_CORE GYE

```
interface Vlan4
  vrf member INTER_VRF_UIO_GYE
  description INTER_Replica_DCP_1
  no shutdown
  no ip redirects
  ip address 172.16.198.2/25
  hsrp 1
    preempt delay minimum 180
    priority 110
    timers  5  15
    ip 172.16.98.1

interface Vlan5
  vrf member INTER_VRF_UIO_GYE
  description INTER_Replica_DCP_2
  no shutdown
  no ip redirects
  ip address 172.16.198.130/25
  hsrp 1
    preempt delay minimum 180
    priority 110
    timers  5  15
    ip 172.16.98.129

interface Vlan6
  vrf member INTER_VRF_UIO_GYE
  description INTER_UIO_GYE
  no shutdown
```

```
no ip redirects
ip address 172.16.250.93/28
hsrp 1
  preempt delay minimum 180
  priority 110
  timers  5  15
  ip 172.16.250.92
```

C7K_CORE UIO

```
interface Vlan14
  vrf member INTER_VRF_UIO_GYE
  description INTER_Replica_DCA_1
  no shutdown
  no ip redirects
  ip address 172.17.198.2/25
  hsrp 1
    preempt delay minimum 180
    priority 110
    timers  5  15
    ip 172.17.198.1

interface Vlan15
  vrf member INTERCONEXION_VRF_UIO_GYE
  description INTER_ Replica_DCP_2
  no shutdown
  no ip redirects
  ip address 172.17.198.130/25
  hsrp 1
    preempt delay minimum 180
    priority 110
    timers  5  15
    ip 172.17.198.129

interface Vlan16
  vrf member INTERCONEXION_VRF_UIO_GYE
  description INTERCONEXION_UIO_GYE
  no shutdown
  no ip redirects
  ip address 172.17.250.82/28
  hsrp 1
    preempt delay minimum 180
    priority 110
    timers  5  15
    ip 172.17.250.81
```

**Definición de Port-Channel VPC y configuración de interfaces**

Se creará el VPC y se asignará las interfaces que lo conformarán

C7K1_CORE GYE

```
interface port-channel1
  description == FIBRA OSCURA UIO - GYE ==
```

```
  switchport
  switchport access vlan 6
  spanning-tree port type network
  speed 1000
  vpc 1

interface EthernetX/X
  description == FIBRA OSCURA UIO - GYE ==
  switchport access vlan 6
  speed 1000
  channel-group 1 mode active
  no shutdown
```

N7K2 CORE GYE

```
interface port-channel1
  description == FIBRA OSCURA UIO – GYE ==
  switchport
  switchport access vlan 6
  spanning-tree port type network
  speed 1000
  vpc 1

interface EthernetX/X
  description == FIBRA OSCURA DCP - DCA  ==
  switchport access vlan 6
  speed 1000
  channel-group 1 mode active
  no shutdown
```

**Definición de Enrutamiento**

Configuración de las políticas de enrutamiento utilizando PBR

NEXUS C7K1 Y C7K2 UIO:

```
ip access-list REPLICA-1-2
   permit ip 172.17.98.0 0.0.0.127 any
   permit ip 172.17.98.128 0.0.0.127 any

route-map PBR-INTERCONEXION-UIO-GYE permit 1
 match ip address REPLICA-1-2
 set ip next-hop 10.32.250.92

feature pbr
route-map PBR-INTERCONEXION-DCP-DCA pbr-statistics
```

Asociación de la política PBR en las interfaces VLANs

```
interface vlan 14
vrf member INTERCONEXION_VRF_UIO_GYE
ip policy route-map PBR-INTERCONEXION-UIO-GYE

interface vlan 15
vrf member INTERCONEXION_VRF_UIO_GYE
ip policy route-map PBR-INTERCONEXION-UIO-GYE
```

NEXUS 7K1 Y 7K2 GYE:

Configuración de las políticas de enrutamiento utilizando PBR

```
ip access-list REPLICA-1-2
   permit ip 172.16.98.0 0.0.0.127 any
   permit ip 172.16.98.128 0.0.0.127 any

route-map PBR-INTERCONEXION-UIO-GYE permit 1
 match ip address REPLICA-1-2
 set ip next-hop 10.32.250.81

feature pbr
route-map PBR-INTERCONEXION-DCP-DCA pbr-statistics
```

Asociación de la política PBR en las interfaces VLANs

```
interface vlan 4
vrf member INTERCONEXION_VRF_DCP_DCA
ip policy route-map PBR-INTERCONEXION-DCP-DCA

interface vlan 5
vrf member INTERCONEXION_VRF_DCP_DCA
ip policy route-map PBR-INTERCONEXION-DCP-DCA
```

### 5.4.3. Diagrama del Diseño para la Interconexión de los Datacenters

El diagrama del diseño de red de la Interconexión de los Datacenters donde se incluyen todos los dispositivos que se ha descrito previamente y su conexión con los equipos de red se muestran en la siguiente figura:

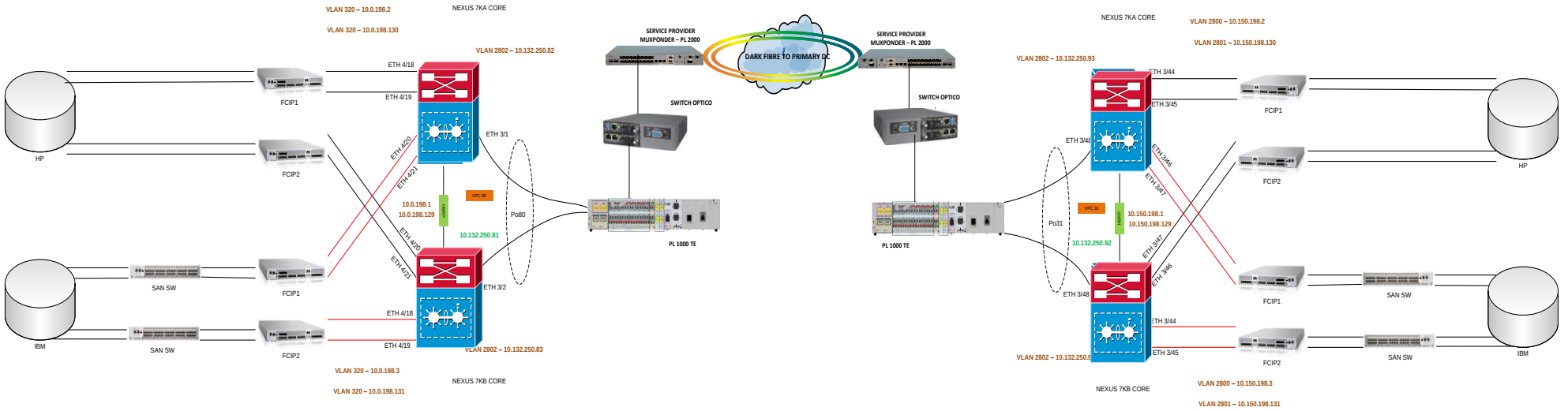


*Figura 55.* Diseño de red de la Interconexión de Datacenters
*Fuente*: Elaboración Propia

## 5.5. Plan para la recuperación de desastre de IT

En caso de desastre del Datacenter Principal y se requiera levantar la contingencia en su Datacenter Alterno, la empresa requiere de tener un plan de contingencia a aplicar para continuar con las operaciones del negocio.

En este capítulo se detallara de forma general los pasos más importantes a tomar en cuenta en un plan de recuperación de  desastre IT.

### 5.5.1. Introducción

El Plan de Recuperación de Red se prepara para que los equipos de Red TI de la empresa lo usen en caso de las interrupciones que afectan a las redes del área local corporativa (LAN), redes de área amplia (WAN), acceso al Internet y otros servicios de red debido a factores de fuerza mayor (ej., desastres naturales o eventos causados por el ser humano).  Este plan además, guiará la restauración de la integridad de la red y las operaciones normales en su mayoría en un marco de tiempo mínimo. Todas las ubicaciones de la empresa que están conectadas con WAN se espera que implementen medidas preventivas siempre que fuese posible para minimizar interrupciones operacionales y para recuperarse tan rápido como sea posible cuando ocurre un incidente.

#### *5.5.1.1. Objetivo*

El Plan de Recuperación de Desastres TI está diseñado para convertirse en un documento funcional que se pueda usar, parcial o totalmente, por los empleados que cumplen roles relacionados con el Comité BCP/gestión de crisis, de recuperación de desastres. El presente documento presenta conceptos, ideas e información relacionada con respecto a un

enfoque holístico[11] hacia la planificación, documentación, prueba, mejora continua y mantenimiento de los planes DR. A continuación se nombran objetivos importantes adicionales para este plan.

- Sirve como una guía para los equipos de recuperación de red.
- Provee procedimientos y recursos necesarios para ayudar en la recuperación de red
- Identifica a proveedores y a clientes que deben ser notificados en caso de una suspensión de la red
- Ayuda a evitar la confusión experimentada durante una interrupción de red mediante la documentación, prueba y la revisión de los procedimientos de recuperación
- Identifica fuentes alternas para los equipos de red, servicios de red, suministros de energía y otros recursos
- Almacenamiento de documentos, salvaguardias y procedimientos de recuperación para registros de red vitales y otros datos relevantes

#### *5.5.1.2. Supuestos*

Los siguientes supuestos y limitaciones deben tomarse en cuenta cuando se evalúa el uso del plan TI DR.

- Los recursos de red claves tales como un administrador líder, los administradores, los líderes de equipo, los técnicos y alternos estarán disponibles después de un desastre
- Este plan y los documentos de red críticos están almacenados en una ubicación segura fuera del sitio y no sólo sobrevivieron al desastre sino que son accesibles inmediatamente después de un desastre.

[11] Analizar los sistemas (ya sean físicos, biológicos, sociales, económicos, mentales, lingüísticos, etc.) y sus propiedades, en su conjunto.

#### *5.5.1.3. Alcance*

El alcance de este plan se limita a la recuperación de la Red en caso que el equipo de gestión de crisis convoque a un plan de continuidad Operacional.

Este es un plan de recuperación de red, no para usarse como documento de procedimientos de resolución de problemas diarios que van desde un plan de gestión de incidentes hasta problemas usuales.

#### *5.5.1.4. Responsabilidades de equipo de recuperación*

La política TI DR se alineará con la política BCM que sigue la empresa.

- Cada miembro del equipo designará un alterno/respaldo
- Todos los miembros del equipo deben conservar una lista de llamadas actualizada del trabajo de los miembros del equipo, domicilio y números celulares, esta lista deben tenerla tanta en su domicilio como en su trabajo.
- Todos los miembros del equipo deben conservar este plan para referencia en su domicilio en caso que suceda un desastre de red luego del horario normal de trabajo.
- Todos los miembros del equipo deben familiarizarse con los contenidos del presente plan.

#### *5.5.1.5. Respaldo*

- Dos veces al mes o de acuerdo a la frecuencia de cambios hechos se debe realizar una copia de la mayoría de las bases de datos de la red actual y del sistema.
- Se deben almacenar los respaldos fuera del lugar.
- El administrador líder de la red es responsable de esta actividad.

- Se debe almacenar las grabaciones, discos, y otro tipo de medios en un ambiente con instalaciones seguras.
- La rotación de las grabaciones o discos ocurre basado en una programación regular con el proveedor de almacenamiento.
- Anualmente se prueba el acceso a los respaldos de la base de datos y otro tipo de datos.

### 5.5.2. Gestión de Crisis

#### *5.5.2.1. Identificación del evento*

La activación de cualquier emergencia debe realizarse por cualquier notificación de evento recibida de parte de cualquier empleado de la empresa (una fuente externa al equipo de TI) o un mecanismo de alarma interna por los equipos de monitoreo de TI. Después de recibir una notificación de un evento por parte de cualquier fuente, el Equipo de Respuesta de Incidentes (IRT) (El líder local del sitio) evaluará la situación e informará acerca del evento al líder de la Gestión de Continuidad Comercial (BCM). El líder BCM informará de acciones adicionales a los Equipos de Gestión de Crisis (CMT) y de Gestión de Incidentes (IMT).

#### *5.5.2.2. Centro de Gestión de Crisis (CMC)*

Cuando se desarrolla una situación de emergencia en el lugar, los miembros del Equipo de Gestión de Crisis se reportarán en el CMC (si el tiempo y las circunstancias lo permiten). El equipo reunido en el CMC evaluará la situación y determinará si el lugar debe ser evacuado.

#### *5.5.2.3. Convocatoria de BCP*

CMT decidirá convocar a BCP o descartar el evento. En el caso que se convoque a BCP, IMT asumirá la dirección para llevar a cabo la recuperación aplicación/proceso por parte de los equipos TI. IMT movilizará a los equipos de recuperación TI.

#### *5.5.2.4. Roles y responsabilidades del Equipo de Recuperación*

Múltiples equipos estarán involucrados durante la recuperación, los roles y responsabilidades de las partes interesadas. Esta distribución se presenta a continuación:

**Equipo de recuperación IT – líder**

- Responsable de la comunicación entre IMT y el personal crítico
- Coordinar la información acerca de la recuperación para de esta manera asegurar que los mensajes claves han llegado a todo el equipo.
- Coordinar y monitorear la recuperación para de esta manera asegurar que se ha cumplido con la programación.
- Administrar la reubicación del personal en ubicaciones de recuperación.
- En caso que se requiera se puede realizar comunicación externa con los proveedores.
- Validar la recuperación del proceso que sea adecuado para la producción.

**Personal / Usuario Crítico**

- Recuperar el proceso crítico dentro de las actividades críticas de Rendimiento de los procesos RTO.
- Registrar el tiempo Objetivo de recuperación (RTO) alcanzado.

- Registrar el punto objetivo de recuperación alcanzado que se obtuvo la última vez en el registro de transacción (RPO).
- Escalar los problemas y los errores críticos a los equipos relevantes.
- Escalar los problemas a los líderes locales en caso que los problemas no se hayan resuelto en el tiempo correcto.
- Proveer soporte a los usuarios/personal operativo

**Instalación**

- Facilitar la administración médica y de emergencia para el personal herido en caso de ser necesario.
- Gestionar el transporte para el personal hacia la ubicación alterna (domicilio u oficina <sitio alterno>).
- Acceso físico al sitio de recuperación.
- Disponibilidad de agua potable y comida.
- Disponibilidad de abastecimiento de energía (en caso de fallo de energía, debe estar disponible un sistema de respaldo)
- Disponibilidad de líneas telefónicas, acceso a internet.
- Disponibilidad de salas de almacenamiento para conservar documentos de vital importancia, etc.
- Disposición de otro soporte administrativo.

### 5.5.3. Procedimiento de Recuperación de Desastres - Fail over.

#### 5.5.3.1. Plan de reubicación del personal

A continuación se presenta el plan de reubicación del personal dentro del cronograma:

Tabla 59
*Plan de Reubicación del Personal*

| | | | | | |
|---|---|---|---|---|---|
| Programación (posterior al desastre) | <1h | 1 a 4 Horas | 4h a 1 Día | 2do día | 1 semana |
| Reubicación del personal | | SÍ | SÍ | | |
| No. de personal a ser reubicado | | 4 | 8 | | |

*Fuente*: Elaboración Propia

El personal crítico será identificado por el equipo de Gestión de incidentes para trasladarlos a una ubicación alterna. La programación y el plan de reubicación varían de acuerdo a la decisión de CMT.

#### *5.5.3.2. Pasos de Recuperación Común*

Después de la reubicación del Equipo de Recuperación de TI, el personal crítico desempeña su operación regular con los recursos que se les entrega. Los siguientes son pasos clave involucrados para que el personal crítico desempeñe sus tareas.

1. El Equipo de Recuperación TI provee las PC/Laptop para acceder a las aplicaciones.
2. El Equipo de Recuperación de TI abre un puente de comunicación para que el equipo discuta el progreso de recuperación.

**Escenario 1: Aplica únicamente a DR (Disaster Recover – Recuperación de Desastres)**

El Datacenter Principal de Quito dejó de funcionar (Desastre).

En caso que se declare DR, El routeador de borde MPLS en Guayaquil aceptará todo el tráfico y lo trasladará hacia el dispositivo GTM en Guayaquil para comunicaciones adicionales.

**Escenario 2: No solo aplica a DR**

Quito DC está Activo pero la Red MPLS hacia Quito DC está fuera de funcionamiento.

En este caso usaremos el enlace entre Quito - Guayaquil como un respaldo para Quito DC, de manera que todo el tráfico proveniente de las Sucursales llegarán a Quito DC mediante Guayaquil.

(Nota: - En caso de un Desastre, se requiere el soporte proveniente del proveedor de Servicios para el enrutamiento o cualquier otro problema relacionado con MPLS)

- Acceso del usuario mediante DNS en base a la Aplicación / URL: El dispositivo GTM resolverá DNS dirigido a las IP asociadas en Guayaquil.
- Acceso del usuario IP en base a la Aplicación / URL

En este caso, GTM redireccionará todo el tráfico hacia el Servidor que tienen una diferente IP usando la característica de la iRule[12] de GTM.

Capa WAN (Internet):- Con el Módulo GTM para Alta Disponibilidad entre dos Centros de Datos. Existirá una IP Virtual para el grupo de GTM de Quito y Guayaquil. En una situación de tráfico normal se enrutará hacia el Datacenter Principal desde el internet

[12] iRule: - Una iRule es una característica poderosa y flexible de dispositivos BIG-IP en base a una arquitectura de Sistema Operativo de Administración de Tráfico exclusivo (TMOS). Las iRules proveen a los administradores control sin precedentes para manipular directamente y manejar cualquier tráfico de aplicación IP. Las iRules utilizan una sintaxis de escritura fácil de aprender y permite a los administradores personalizar la manera de interceptar, inspeccionar, transformar y dirigir tráfico de la aplicación de ingreso y de salida.

usando la IP virtual como IP pública asociada con el módulo GTM de Quito que se encuentra en funcionamiento. En el caso que el DC de Quito falle, se debe usar la IP Virtual, para que de esta manera se traslade hacia el Datacenter Alterno de Guayaquil como una IP Pública asociada con el Módulo GTM de Guayaquil que estará activada.

### 5.5.4. Procedimiento de Recuperación de Desastres – Retorno a la normalidad

Esta sección describe el retorno a las operaciones normales en Quito, asumiendo que esta ubicación esté lista para desempeñar todas las operaciones regulares.

1. Siguiente decisión, trabajar con administrador
2. Usar el plan de notificación común
3. Verificar las condiciones en Primario
4. Ejecutar los procedimientos "restaurar a la normalidad en Primario"
5. Verificar el área comercial con revisiones usuales

#### *5.5.4.1. Procedimiento Switch-Back*

**Cambios de Red MPLS**

Después de que el DCP esté listo para compilar toda la transaccionalidad (capa de base de datos, capa de aplicaciones, comunicaciones, etc.) posterior al desastre y que se cumplan todos los requerimientos, un procedimiento de Switch-Back debe administrarse. Switch-Back es un entorno controlado de reenrutamiento de transaccionalita en la que la solución GTM se usa y todas las conexiones desde sucursales en todas las ubicaciones están ahora redireccionadas a DCP.

Cambio de roles F5 - GTM:- Una vez que el DCP esté listo, una configuración de 2 nodos activos estarán en funcionamiento como un grupo geográfico en el F5 con el rol

principal ubicado en la ubicación DR (Por tanto redireccionará todas las transacciones a segmentos en DCA).

1.- El Primer paso en el nivel de red (capas L2 y L3), se realizará el cambio de roles entre DCA y DCP dentro del F5. Los roles IP resueltos se cambiarán entre ambas ubicaciones, esto dará como resultado la publicación de las direcciones IP reales y segmentos a trasladar a Quito.

2.- EL Datacenter Principal de Quito con el módulo GTM actualizará los detalles nuevos para que el DNS global resuelva nuevamente las URLs publicadas de la empresa.

3.- Los routers de borde en DCA necesitan configurarse de manera que que ya no publiquen los segmentos de direccionamiento público del DCA.

4.- Los routers de borde en DCP necesitan configurarse de manera que todos los cambios se añadan para poner a disposición los segmentos IP publicados en Quito.

### 5.5.5. Lista de verificación de Recuperación

A continuación se encuentra la lista de verificación de recuperación para los usuarios críticos durante la operación que se realicen con este fin. La lista de verificación de recuperación no está limitada a las consultas de a continuación, el usuario crítico debe registrar todos los problemas/éxito con la programación apropiada.

**Comunicación**

- ☐ ¿Recibió la notificación proveniente de IMT?
- ☐ ¿Se comunicó con su equipo al respecto?
- ☐ ¿Se comunicó con las partes interesadas al respecto?
- ☐ ¿Se comunicó con contactos externos?

**Instalación**

- ☐ ¿La instalación que se le suministró es similar a la oficina primaria?
- ☐ ¿Existe una cafetería disponible para comida?
- ☐ ¿Obtuvo alojamiento (si lo organizó TI)

**Laptop**

- ☐ ¿Tiene disponibilidad de usar su computadora de escritorio/laptop?
- ☐ ¿La laptop tiene todas las aplicaciones del cliente requeridas?
- ☐ ¿Sirve su identificación de ingreso desde la laptop?

**Red**

- ☐ ¿Puede conectar su laptop/computadora de escritorio a la red y al servidor?
- ☐ ¿Sus servicios tienen la conectividad similar a Producción?
- ☐ ¿Notó algún tipo de retraso al abrir sus aplicaciones?

**Servidor y Almacenamiento**

- ☐ ¿Puede acceder a sus aplicaciones?
- ☐ ¿El desempeño del servidor es similar a su producción?

**Recuperación del proceso operacional TI**

- ☐ ¿Todos sus procesos se recuperaron dentro de RPO?
- ☐ ¿Todos sus procesos se recuperaron dentro de RTO?
- ☐ ¿Todas mis dependencias internas funcionan bien según el flujo de trabajo?
- ☐ ¿Todos los proveedores externos recibieron soporte?

☐ ¿Todos los registros vitales están disponibles?

☐ ¿Registró problemas/éxito durante la operación de recuperación?

### 5.5.6. Registro de recuperación y Mejora Continua

El cuadro a continuación necesita edición durante la recuperación de los procesos durante el escenario real o ejecución de prueba, se enlista el éxito y los problemas en el cuadro para el posterior análisis para mejorar el proceso de recuperación usando el procedimiento de recuperación y, la lista de verificación en la sección anterior.

Tabla 60
*Registro de Recuperación*

| Sl.No | Descripción : Éxito/Problema | Hora | Responsabilidad |
|---|---|---|---|
| | | | |

*Fuente*: Elaboración Propia

#### *5.5.6.1. Resultado de los parámetros de recuperación archivados*

El RTO (Tiempo Objetivo de recuperación) es el tiempo que toma recuperar el proceso operacional, RPO - Punto de Recuperación Objetivo, Define la pérdida de datos máxima tolerable que se acepta ante una situación de desastre. Durante la prueba se calcula como RPO = Tiempo de desastre - Última transacción registro de hora.

Tabla 61
*Resultado de los Parámetros de Recuperación*

| SI/No | Aplicación / Proceso | RTO definido | RTO alcanzado | RPO definido | RPO alcanzado |
|---|---|---|---|---|---|
| | | | | | |

*Fuente*: Elaboración Propia

#### *5.5.6.2. Mejora continua*

El cuadro a continuación debe actualizarse con lecciones aprendidas durante el proceso de recuperación o prueba para validar el procedimiento de recuperación. Será el comentario para mejorar el procedimiento de recuperación operacional.

Tabla 62
*Cuadro de Mejora Continua*

| Sl.No | Lecciones aprendidas | Hora | Responsabilidad |
|---|---|---|---|
| | | | |

*Fuente*: Elaboración Propia

### 5.6. Conclusiones y Recomendaciones

Una vez finalizado el Caso de Estudio presentado en este trabajo se puede plantear las siguientes conclusiones.

- El análisis de la infraestructura de red actual del Datacenter Principal es un dato e insumo importante para determinar la línea base con la que se partirá para el diseño del Datacenter Alterno, ya que a través de su revisión se puede detectar puntos de falla a mejorar en el nuevo diseño.
- Con el análisis de consumo de CPU y Memoria realizado en los dispositivos de red del DCP, determina que para el DCA se podrá utilizar dispositivos de red de similares características ya que la carga podría ser soportada sin problemas, sin embargo se optó en la mayoría de los casos por tener los últimos equipos de la gama por temas de end-of-life y por proveer de mejores prestaciones al DCA.
- El modelo Jerárquico por capas de Cisco es el escogido para la implementación del Datacenter Alterno por su simplicidad de uso, escalabilidad y por la organización que permite mantener en las comunicaciones de la red.
- La implementación de la infraestructura de red del DCA con dispositivos de la marca Cisco se debe una parte para mantener lo mismo con lo que se trabaja en el DCP, y la expertis de la utilización de estos equipos y resolución de problemas y por motivos comerciales (todos los dispositivos entran en modelos de mantenimientos, actualizaciones etc. con un mismo contrato tanto en DCA y DCP y con mejores precios).
- En el diseño del DCA se considera mantener conexiones redundantes en todos los niveles de la capa Jerárquica de Cisco, a diferencia del DCP se consideró también redundancia de conexiones en los equipos que forman la capa de acceso (Switches 9372 y cisco 2000)

- Uno de las mejoras realizadas en el diseño del Datacenter Alterno es la creación de una zona exclusiva de administración, lo cual en le DCP no se tenía ya que se mezcla en un solo dispositivos las conexiones de administración y datos, lo cual no es recomendable, debido a que en caso de caída del equipo se perderá hasta su administración.
- Uno de los activos más importantes de las Empresas son los datos por lo que dentro del diseño de la red es un aspecto importante a tomar en cuenta, actualmente no es suficiente contar solo con dispositivos como firewall, ya que existe amenazas externas que este equipo no puede manejarlas a alto nivel, para ello es importante de igual manera incluir equipos especializados para otro ataques como anti-DDoS e IPS.
- Los equipos de Seguridad como IPS , anti DDoS y Firewalls implementados en el DCA han sido elegidos de la misma marca con los que se cuentan en el DCP con motivos de facilitar la exportación de sus configuraciones y mitigar temas de incompatibilidades entre plataformas.
- En el Datacenter Principal no se tiene una organización de los segmentos de red por la función que se cumple, en el Datacenter Alterno se logra esta organización mediante la creación de las VDC dentro de las cuales se ordena los segmentos de red de acuerdo a su funcionalidad y servicio que brinda.
- El direccionamiento implementado en el DCA debe der distinto al que se mantiene en el DCP con el fin de no crear inconsistencias en la red y tener una diferenciación de que aplicativos y servidores están funcionando en el Datacenter Principal y cuales están en el Datacenter Alterno.
- El LTM no hace ninguna resolución de nombre y asume que ya se ha tomado una decisión DNS. Dado que el LTM es un proxy completo, es fácil para él escuchar en

un puerto pero dirigir el tráfico a múltiples hosts escuchando en cualquier puerto especificado.

- Para la implementación de un balanceo global de Datacenters a través del módulo GTM del dispositivo F5, es necesario que se adquiera esta funcionalidad en el DCP ya que actualmente no la posee.
- El GTM es una solución que permite resolver nombres a direcciones IP de forma inteligente. Al igual que un servidor DNS normal, el GTM no proporciona ninguna información de puerto en su resolución.
- El presente caso de estudio permitió conocer las principales zonas de diseño para la infraestructura de red de un Datacenter Alterno para la empresa basándose en el diseño actual del DCP, indicando los principales elementos de red y seguridad para implementar la conexión total, así como su diseño para que exista una conexión entre estas dos localidades. El diseño presentado no pretende ser un estándar a la hora de construir la infraestructura de red de un Datacenter, sin embargo se ha tomado conceptos básicos para su arquitectura y la implementación de las mejores prácticas. Este diseño puede ser mejorado y modificado durante el transcurso del tiempo tomando en cuenta los avances en la tecnología y así mismo en las mejoras de las características de los equipos aquí implementados.

Por último se indica algunas recomendaciones:

- Se debe desarrollar un plan de actividades a la par del Datacenter Principal para mantener actualizados todos los equipos de Red del Datacenter Alterno.
- Se puede utilizar la infraestructura del Datacenter Alterno como un ambiente de laboratorio para probar nuevas aplicaciones y su conectividad hacia otros aplicativos de la red Interna o hacia Internet.

- Se recomienda realizar pruebas de la operatividad del Datacenter Alterno y de sus aplicaciones al menos dos veces por año para determinar de que en caso de que se requiere levantar la contingencia en esta localidad este en óptimas condiciones para su funcionamiento.
- Se debe escoger las herramientas adecuadas para realizar la replicación de los datos del DCP hacia el DCA para determinar si el ancho de banda de la interconexión es suficiente para la transmisión de la data entre las dos localidades.
- En el DCA el diseño de la infraestructura de Firewalls se lo ha realizado sin tomar en cuenta redundancia en estos equipos debido a los costos económicos que estos involucran. Como recomendación se debe tomar en cuenta adquirir otro equipo firewall en cada zona: Borde, Terceros, Principal, para evitar tener un punto de falla realizando la configuración en cluster de este equipamiento.

## BIBLIOGRAFÍA:


Britos José Daniel. (2010). Detección de Intrusiones en redes de datos con captura distribuida y procesamiento estadístico. (Tesis de Maestría). Universidad de la Plata, La Plata, Argentina. Recuperado de: http://postgrado.info.unlp.edu.ar/Carreras/Magisters/Redes_de_Datos/Tesis/Britos_Jose_Daniel.pdf

Checkpoint. Firewall Software Blade. Recuperado de: https://www.checkpoint.com/products/firewall-software-blade/

Cisco. (2017). Cisco Nexus 7000 Series Switches Data Sheet, recuperado de: https://www.cisco.com/c/en/us/products/collateral/switches/nexus-7000-series-switches/Data_Sheet_C78-437762.html

Cisco. (2016). Cisco Nexus 5548P, 5548UP, 5596UP, and 5596T Switches Data Sheet. Recuperado de: https://www.cisco.com/c/en/us/products/collateral/switches/nexus-5000-series-switches/data_sheet_c78-618603.html

Cisco. (2016). Cisco Nexus 2000 Series Fabric Extenders Data Sheet. Recuperado de: https://www.cisco.com/c/en/us/products/collateral/switches/nexus-2000-series-fabric-extenders/data_sheet_c78-507093.html

Cisco. (2017). Cisco Nexus 7700 Switches Data Sheet. Recuperado de: https://www.cisco.com/c/en/us/products/collateral/switches/nexus-7000-series-switches/data_sheet_c78-728187.html

Cisco. (2017) Cisco Nexus 9300 Platform Switches Data Sheet. Recuperado de: https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-736967.html

Cisco. (2016). Cisco Nexus 2000 Series Fabric Extenders Data Sheet. Recuperado de: https://www.cisco.com/c/en/us/products/collateral/switches/nexus-2000-series-fabric-extenders/data_sheet_c78-507093.html

Cisco. (2017). Cisco Catalyst 2960-X and 2960-XR Series Switches Data Sheet. Recuperado de: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/data_sheet_c78-728232.html

Cisco. (2017). Cisco Nexus 3548x and 3524x Switches Data Sheet. Recuperado de: https://www.cisco.com/c/en/us/products/collateral/switches/nexus-3548-switch/data_sheet_c78-707001.html

Cisco. (2017). Cisco ASR 1000 Series Aggregation Services Routers Data Sheet. Recuperado de: http://www.Cisco.com/en/US/prod/collateral/routers/ps9343/data_sheet_c78-447652.pdf

Cisco. (2016). Cisco Catalyst 4500-X Series Fixed 10 Gigabit Ethernet Aggregation Switch Data Sheet. Recuperado de: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-4500-x-series-switches/data_sheet_c78-696791.html

Cisco. Switch Cisco Nexus 3548. Recuperado de:

https://www.cisco.com/c/es_es/products/switches/nexus-3548-switch/index.html

Cisco. (2006). Hot Standby Router Protocol Features and Functionality. Recuperado de: https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html

Cisco. (2017). How to configure PBR. Recuperado de: https://supportforums.cisco.com/t5/network-infrastructure-documents/how-to-configure-pbr/ta-p/3122774

Cisco. (2014). Technical Overview of Virtual Device Context. Recuperado de: http://www.cisco.com/c/en/us/products/collateral/switches/nexus-7000-10-slot-switch/White_Paper_Tech_Overview_Virtual_Device_Contexts.html

CNET. Cisco ISR 4431 - Security Bundle - router - rack-mountable. Recuperado de: https://www.cnet.com/products/cisco-isr-4431-security-bundle-router-rack-mountable/specs/

CNET. Cisco ASR 1006 VPN Bundle – router. Recuperado de: https://www.cnet.com/es/analisis/cisco-asr-1006-vpn-bundle-router-desktop-with-cisco-asr-1000-series-embedded-services-processor-100gbps-route/

CNET, Cisco Catalyst 4500-X - switch - 16 ports - rack-mountable Series. Recuperado de: https://www.cnet.com/es/analisis/cisco-catalyst-4500-x-switch-16-ports-rack-mountable-series

CTC Union. (2017). FRM220A-1000EAS/X. Recuperado de: https://www.ctcu.com/en/fiber-series/iaccess-multi-service-platform/ethernet-switch-converter/frm220a-1000eas-x.html

Etek Reycom. CheckPoint. Recuperado de: http://www.etek-reycom.com.ar/tecno/proveedor/check_point.htm

Etic Solutions. Protección Perimetral & Firewalls. Recuperado de: http://www.etic-solutions.net/etic/enterprise/proteccion-perimetral-y-firewalls

F5. (2014). BIG-IP Local Traffic Manager. Recuperado de: https://www.f5.com/pdf/products/big-ip-local-traffic-manager-overview.pdf

F5. Big ip local traffic manager. Recuperado de: http://www.f5.com/pdf/products/big-ip-local-traffic-manager-ds.pdf

F5. (2013). BIG-IP Modules DATASHEET. Recuperado de: https://www.f5.com/pdf/products/big-ip-modules-ds.pdf

Galván Víctor Gabriel (2013), DATACENTER una mirada por dentro, Ediciones Índigo. Recuperado de https://www.researchgate.net/publication/282611136_ DATACENTER_-_UNA_MIRADA_POR_DENTRO

Geraci Austin. (2017). GTM vs LTM – Difference between F5 Global & Local Traffic Manager/ Recuperado de: https://worldtechit.com/gtm-vs-ltm-difference-f5-global-local-traffic-manager/

HP. Soluciones de Seguridad. Recuperado de:

http://h17007.www1.hpe.com/mx/es/solutions/security/index.aspx

HP. (2014). Reimagine the server. Think compute. Recuperado de:

http://www8.hp.com/us/en/hp-news/press-kit.html?id=1752643#.Wdmp9YxSzDd

Milestone. Transponders Ópticos – FRM220-Transponder. Recuperado de:

http://www.milestone.com.ec/site/index.php/component/jshopping/product/view/1/8?Itemid=0

National Fiber Networks. (2012). Fibra Oscura, Recuperado de:

https:// www.nfn.mx/FibraOscura.html

Netways Europe. (2015). Encrypted DWDM. Recuperado de:

http://www.netwayseurope.com/packetlight/encrypted-dwdm

OVN. (2017) La protección anti-DDoS con OVH. Recuperado de:

https://www.ovh.com/us/es/anti-ddos/principio-anti-ddos.xml

PacketLight. (2014). PL-2000 Multiprotocol / Multirate Muxponder. Recuperado de:

https://www.packetlight.com/images/Data-Sheets/PL-2000.pdf

PacketLight. (2017). 20G OTN ADM Muxponder. Recuperado de:

https://www.packetlight.com/products/1g-to-40g-services/pl-2000-10g-multirate-muxponder

Palo Alto Networks. (2017). What is an intrusion prevention system?. Recuperado de: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

Radware. DefensePro Overview. Recuperado de: https://www.radware.com/products/defensepro/

Rouse Margaret. (2012). Enrutamiento virtual y reenvío (VRF), recuperado de: http://searchdatacenter.techtarget.com/es/definicion/Enrutamiento-virtual-y-reenvio-VRF

Sean Wilkins. (2017). A Guide To DDoS Detection And Attack Mitigation Tools. Recuperado de: http://www.tomsitpro.com/articles/ddos-detection-attack-mitigation-tools,2-969-2.html

Techno Partners. Especificaciones técnicas IPS. Recuperado de: http://www.techno-partners.com/Technology/?q=content/tippingpoint-ips

Telefónica, Anti DDoS, Recuperado de: https://www.cloud.telefonica.com/es/open-cloud/products/security/anti-ddos

The JimmahKnows. (2012). What is BIGIP F5 (LTM and GTM)?. Recuperado de: http://thejimmahknows.com/whatisf5/

Welcher Peter. (2011). How vpc Works. Recuperado de: https://www.netcraftsmen.com/how-vpc-works/

Wikipedia. (2017). Check Point. Recuperado de:

https://es.wikipedia.org/wiki/Check_Point