EJECUCIÓN DE PLAN DE ACCIÓN PARA LA ORGANIZACIÓN Y ESPACIO DEL DATACENTER EN EL PUNTO CENTRAL DE UNA ENTIDAD FINANCIERA

CARLOS ARTURO BERNAL GÓMEZ
CAMILA ANDREA SALAMANCA CASTILLO

GERALD BREEK FUENMAYOR RIVADENEIRA

FACULTAD DE INGENIERIA DE TELECOMUNICACIONES
UNIVERSIDAD SANTO TOMAS
BOGOTÁ, D.C.
2015

EJECUCIÓN DE PLAN DE ACCIÓN PARA LA ORGANIZACIÓN Y ESPACIO DEL DATACENTER EN EL PUNTO CENTRAL DE UNA ENTIDAD FINANCIERA

Presentado Por:

CARLOS ARTURO BERNAL GÓMEZ
2063616
CAMILA ANDREA SALAMANCA CASTILLO
2082139

Proyecto de Pasantía para optar el Título de Ingeniero de Telecomunicaciones

(Monografía)

Dirigido por:

ING. GERALD BREEK FUENMAYOR RIVADENEIRA

UNIVERSIDAD SANTO TOMÁS

FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES

BOGOTÁ, D.C.

2014

Nota de aceptación.

_____
_____
_____
_____
_____
_____
_____

_____

Firma Director de Monografía

_____

Firma de Jurado

_____

Ciudad y Fecha (de entrega)

RESUMEN

El presente informe describe la ejecución de un plan de acción para la organización y espacio de un datacenter de una empresa catalogada como proveedor de contenido, con el fin de reunir información específica que sea de gran utilidad para procesos similares que conlleven a que el área de prevención ejecute planes de acción como área transversal a este tipo de procesos establecidos por CLARO S.A. para clientes estratégicos como lo son las entidades financieras.

ABSTRACT

This report describes the implementation of an action plan for the organization and space in a datacenter of a company listed as a content provider, in order to gather specific information that is useful for similar processes that lead to the area run prevention action plans as a cross to such processes established by CLARO SA for strategic customers as it is financial institutions.

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

TABLA DE CUADROS

TABLA DE ANEXOS

INTRODUCCIÓN

CLARO SA es una empresa multinacional que brinda conectividad mediante servicios de telecomunicaciones. Diversas compañías acuden al uso de las telecomunicaciones. De esta manera, las entidades financiera se han posicionado como proveedor de contenido, en el momento en que la compañía aumentó en la cantidad de usuarios finales, su datacenter fue creciendo, implicando instalación y puesta en marcha de nuevos equipos que en principio lograrían abastecer los servicios ofrecidos a sus cliente. Entre tanto, las condiciones ambientales no óptimas, desorganización y mal manejo de espacio, conlleva a ofrecer una baja calidad de servicio a los usuarios finales. Por lo anterior se ejecutó el “Plan de acción para la organización y espacio del datacenter en el punto central de una entidad financiera”, para replantear las condiciones físicas y ambientales de su datacenter.

No obstante, con el fin de establecer un estándar en el área de prevención para futuros planes de acción, se desarrolla el presente informe, donde se describe de manera detallada, los procesos y la explicación de cada una de las áreas que estarán implicadas en la ejecución del mismo.

En primera instancia del informe, se describe y se plantea el problema, la justificación y los objetivos del proyecto, que describirán los alcances de la ejecución del plan de acción enfocado en soluciones.

En la segunda parte del trabajo, se mencionarán aspectos teóricos y normativos, como los son los protocolos a usar, la normatividad que se debe tener en cuenta en el momento de implementar la infraestructura de un centro de datos, para así, brindar escalabilidad y a futuro prevenir inconvenientes relacionados con el manejo del espacio.

En tercer momento, se describen las fases del desarrollo del proyecto en conjunto con las áreas que tuvieron lugar, explicando funciones de las áreas transversales

y el proceso de ejecución, en el área de prevención en cada una de las fases. Por último, se analiza y se concluye con base a lo ejecutado en el plan de acción, para la organización y espacio del datacenter en el punto central de una entidad financiera.

1. ANTECEDETES.

Con el propósito de renovar y configurar tecnologías de información relacionadas con el sector financiero. Las telecomunicaciones, se consolidan como medios de solución informática, debido a su constante aplicación en servicios y alianzas que masifican el acceso al mercado financiero.

La bancarización de la economía y la imperante necesidad de recurrir a la tecnología y las telecomunicaciones como medio para afianzarse en el mercado de manera eficaz. Abre la puerta a la creatividad y eficacia en temas de la calidad aplicados a servicios de información. De esta manera, es necesario consolidar tecnologías que sean capaces de optimizar y solucionar problemas sobre áreas involucradas en la prestación de servicios financieros mediados por tecnologías de información y comunicación.

De acuerdo a lo anterior, desde la ingeniería de telecomunicaciones el diseño de infraestructura es clave en la consolidación y optimización de los servicios financieros, identificando deficiencias y potencialidades que puedan contribuir en la construcción de soluciones de comunicación. “La mejor forma de potenciar al máximo la infraestructura de TI es contar con un socio capaz de integrar soluciones de telecomunicaciones con soluciones de TI. De esta forma es posible contar con una red capaz de transportar información de forma segura, a gran velocidad y la mayor cantidad de tiempo disponible” (Montero, 2011).

Ahora bien, el manejo y uso de información representa un contexto donde el uso de la tecnología debe adecuarse de acuerdo a los fines de la información. La confidencialidad es un aspecto clave sobre este contexto, en el marco de la seguridad, administrar información que se desenvuelve sobre esquemas financieros, devela el carácter indispensable de seguridad y disponibilidad en relación a su uso.

Entonces, optimizar el servicio de información por medio de datacenter, implica un ejercicio incesante en la garantía y vigilancia del servicio, por esta razón las auditorias son un aspecto clave que garantizaría el funcionamiento de los servicios de comunicación. Abordar sistemas lógicos y físicos en la consolidación del optimo servicio en prospectiva al futuro cercano, además de la identificación de posibles problemas en el corto tiempo, representa ventajas y soluciones que puedan aplicarse dentro de un tiempo prudente “Con las auditorias es posible prevenir eventualidades posteriores no deseadas, definir las futuras líneas de actuación y eliminar riesgos de caídas del sistema. Estos últimos habrá que tenerlos muy patentes en las fases de diseño, ejecución y mantenimiento, ya que este tipo de averías pueden acarrear graves daños en el negocio” (TRC) .

2. DEFINICIÓN DEL PROBLEMA.

2.1 PLANTEAMIENTO DEL PROBLEMA

En relación a la alta gama de servicios ofrecidos en el campo de las telecomunicaciones, el internet, canales de datos (MPLS), LAN to LAN (clear channel) entre otros. Ha sido necesario que las compañías desarrollen sistemas de comunicaciones que sean capaces de convertir un proveedor de contenido de la información.

Los proveedores de contenido brindan facilidades de conectividad, que inciden sobre la adquisición de canales lógicos por parte de compañías de telecomunicaciones. Además, por medio de canales de datos (MPLS Extranet e Intranet) pueden contar con la capacidad de hacer que sus clientes finales accedan a éstas aplicaciones, servicios o productos, solo ingresando a una interface gráfica.

Las entidades bancarias ante la gran variedad de servicios financieros, han incursionado en los últimos años en servicios encaminados a proveer contenido a sus clientes finales. Según lo anterior, La entidad financiera por la cual se desarrolla este trabajo ha llevado a cabo una serie de transformaciones de espacio y desafíos en cuanto a la organización en su datacenter, relacionado con canales de datos para cubrir las necesidades de conectividad de sus clientes.

La organización y el espacio son muy importantes para los centros de datos. En esta medida es pertinente tomar en cuenta en el momento de la implementación de un nuevo servicio ofrecido por CLARO S.A, como operador de telecomunicaciones, las recomendaciones relacionadas con tomas reguladas, los racks, el cableado estructurado, entre otros.

Para cada implementación de un servicio de datos (MPLS Intranet o Extranet) ofrecido por CLARO S.A, se solicita de parte del cliente que se cuente con tomas

reguladas, espacio en el rack (según la cantidad de equipos a instalar) y con el cableado estructurado de la LAN del cliente, todo esto bajo el estándar TIA 942, de esa manera se entrega un servicio de manera ideal.

En el momento en que la entidad financiera acondicionó el datacenter, su mayor proveedor de servicio era CLARO S.A, por tal razón, se implementó la adecuación del datacenter con las recomendaciones del proveedor, adicionalmente dicha entidad hizo unas recomendaciones.

Para cada implantación de un servicio nuevo se aprovisiono de la siguiente forma:

- Se llegó con fibra óptica para cada servicio.
- Se Instaló un Router por cada servicio nuevo.
- Se Informó el tipo y modelo de router que se instaló, si es raqueable o no, en caso tal de que el equipo no fue raqueable, la bandeja fue suministrada por CLARO SA.

Durante el tiempo en que se instalaron los nuevos servicios de datos, se llegaron a implementar más de 30 enlaces (ver tabla 1).

Tabla 1. *Códigos y alias de servicios instalados por CLARO S.A.*

Código de servicio	**Nombre del cliente**
ACH0024	A.C.H. COLOMBIA S.A. BANCO DAVIVIENDA EXTRANET
BLS0049	BVC BANCO
BLS0050	BVC BANCO
BLS0166	GRANBANCO TORRE BOLIVAR
CEY0007	BOLSA ACCESO MERCADO
CIM0072	ICAP SECURITIES IHS
COP0033	COMPUTEC EXTRANET
DIL0013	DIEBOLD COLOMBIA S.A.
DVV0011	BANCO S.A
DVV0014	BANCO S.A EXTRANET
DVV0016	BANCO S.A EXTRANET
DVV0027	BANCO S.A EXTRANET
DVV0023	BANCO EXT PROCESOS Y CANJE
DVV0024	BANCO BACKUP
DVV0026	BANCO - Bloomberg

DVV0071	REDEBAN TUNEL GREP
DVV0147	BANCO GB BACKUP
DVV0375	GESTION NOC REMOTO MEZZANINE
DVV0445	BANCO INTERNET
DVV0463	EXTRANET ACH
DVV0497	BANCO EXTRANET SERVIBANCA
DVV0584	SUPERFINANCIERA EXTRANET
DVV0585	IPDP REDEBAN EXTRANET
DVV0671	BANCAFE EXTRANET BANREPUBLICA
DVV0675	BANCO EDIF PPAL PISO27 y O&M BOLIVAR VIDEOCONFERENCIA
DVV0672	BANCO EDIF PPAL PISO27 y O&M BOLIVAR VIDEOCONFERENCIA
DVV0766	BANCO INTERNACIONAL
DVV0809	BANCO BOGOTA Calle 28 # 13A-15 Mezanine – PLS
DVV0812	BANCO Calle 28 # 13A-15 Mezanine Bloomberg – PLS
UDQ0007	WINNER GROUP
DVV0994	BANCO
DVV1002	BANCO
DVV1009	COLGRABAR
FEA0023	ASSENDA S.A.
IBM0058	AT&T GLOBAL NETWORK
ISAAA06	IPDP ITAC S. A.
RRO0124	ASCREDIBANCO CL 28 EXTRANET

Tomado de: Datacenter punto central de una entidad financiera (2014)

El constante crecimiento en el datacenter de la entidad financiera estaba generando desorden debido a su limitada infraestructura, ya que por cada servicio instalado debe llegar a los rack con fibra óptica y con nuevos equipos, lo cual ocasionó que se instalaran varias cajas OB, ocupando espacio en las rejillas para el cableado estructurado de la empresa y enredo de la misma, adicional de los requerimientos de espacio en los racks y el sistema eléctrico, lo que quiere decir que para la entidad el tema del espacio está causando problemas de desorden en el Datacenter, por lo cual se realiza un plan de acción de mejora, para cambiar las condiciones propuestas por la entidad financiera.

Entre tanto, se sugirió que éste plan de acción proporcionara la capacidad de

migrar todos los servicios que estaban en las diferentes redes de acceso, así que solo se pudo pasar al nuevo esquema 27 enlaces, como se describen a continuación:

- Red de acceso metro de Cisco.
    - 11 servicios.
- Red de acceso Nortel.
    - 7 Servicios.
- Red de acceso Alcatel.
    - 9 Servicios.

En concordancia a lo anterior, el presente informe pretende dejar documentado el proceso en el que se ejecutó el plan de acción para el orden en el datacenter del punto central de una entidad financiera, de acuerdo a la entrevista realizada a Jerryt Vergara y Alberto Rodríguez funcionarios de CLARO S.A,

> "*En muchas ocasiones los trabajadores requieren el apoyo de sus compañeros para poder dar una solución a algún requerimiento, esto hace que los otros interrumpan sus labores para ayudar a dar un pronta solución a la problemática de su colega, generando así una mayor utilización de tiempo en el desarrollar una actividad, esto conlleva a la disminución en los niveles de calidad del operador. Esto se presenta frecuentemente cuando se desarrollan planes de acción y se solicita algún tipo de información al área de prevención y no se cuenta con documentación que facilite como se debe realizar dicha tarea según el proceso de las áreas involucradas"* (Vergara & Rodriguez, Entrevista a Ingeniero de Implementación y Líder área de Prevención , 2014).

2.1.1 Pregunta orientadora

¿De qué manera es posible solucionar el problema de desorganización de cableado y espacio en los racks del datacenter de una entidad financiera?

2.2 JUSTIFICACIÓN

CLARO S.A busca garantizar su servicio con las mejores condiciones físicas y lógicas dentro y fuera de la empresa, para esto, cuenta con recomendaciones que se deben tener presentes en el momento que se entrega un nuevo servicio de datos. Así, se consolidaría la adecuación del datacenter que soporte y tenga el espacio necesario para recibir el servicio y las condiciones eléctricas necesarias para conectar los equipos a instalar.

La entidad financiera a la cual se ejecuta el plan de acción es uno de los clientes más influyentes económicamente para CLARO S.A, por su gran cantidad de servicios de datos (MPLS Extranet o intranet) suministrados por el operador de comunicaciones, lo cual requiere que se tenga un datacenter que pueda soportar las recomendaciones mencionadas anteriormente.

El constante aumento de clientes finales de la entidad financiera ocasionó que el datacenter fuera quedando corto en cuanto espacio y organización, por lo cual se ve obligado a solicitar a CLARO SA que solucione el problema actual del Datacenter, sin causar mayor impacto en su operación; se hace necesario ejecutar un plan de acción que solvente el problema de espacio y desorganización del centro de datos del punto central de una entidad financiera.

Entonces, las áreas de Preventa, Implementación, NOC y Prevención de soporte corporativo ejecutan para este plan de acción diferentes actividades asignadas según las funciones de cada área. Con el fin de tener una mejora en la infraestructura interna (Cableado estructurado, organización en el rack).

De la misma manera, para el área Prevención es importante garantizar que los acuerdos comerciales de indisponibilidad de los servicios se cumplan, para esto se realizan revisiones proactivamente de las configuraciones de canales backup, así como también, se realizaran pruebas de conmutación que aseguren el correcto funcionamiento y la disponibilidad contractual.

En el desarrollo de este plan de acción, al área de Prevención se le asignaron tareas como elaboración de ingenierías de detalle (54 diagramas de detalle), verificación de configuraciones (54 enlaces) y pruebas de backup (27 pruebas de conmutación). Estas labores se encargaron a los autores del informe debido a que la carga laboral era demasiado alta, y el tiempo en que se debían realizar estas actividades no permitía que una sola persona lograra el objetivo.

Adicionalmente, se realiza este proyecto en conjunto ya que los autores se encontraban laborando en la misma área y con funciones similares, por lo cual se decidió por parte de la empresa que solo se elaborara un documento.

La elaboración de este documento es un referente para futuras ejecuciones de planes de acción, que solucionen problemas de desorganización en centros de datos de otros clientes de CLARO SA, como también puede ser un referente para otros operadores de servicio de telecomunicaciones, ya que podrían generar mejora en los tiempos de entrega, dando así a los clientes finales una seguridad de tener el servicio de manera rápida y confiable.

Este informe además de ser útil para compañías que brinden servicios de telecomunicaciones, puede ayudar en implementaciones de datacenter de empresas con la misma forma de negocio que la de una entidad financiera, que a su vez son proveedores de algún tipo de contenido, y que a futuro podrían presentar aumento en la cantidad de usuarios finales que pueden ocasionar que el centro de datos crezca y se genere desorden en éste.

Por otra parte, la realización del presente informe a nivel académico brinda a los autores grandes beneficios, ya que es necesario realizar investigaciones que traen nuevos conocimientos como las características de ciertos servicios de datos (MPLS Extranet e Intranet) y procesos metodológicos para la ejecución de un plan de acción en este caso del punto central de una entidad financiera.

2.3 OBJETIVOS

2.3.1 Objetivo general

- Ejecutar un plan de acción en conjunto con las áreas de Preventa, Implementación y NOC para la organización del datacenter del punto central de una entidad financiera.

2.3.2 Objetivos específicos

- Realizar esquemas de ingeniera de antes y después de ejecutado el plan de acción con el fin dejar documentada la topología anterior en caso de tener que realizar un rollback.
- Identificar los equipos que se implementaron sobre el plan de acción, teniendo en cuenta características como ancho de banda y protocolos que soportan, según las especificaciones del área de ingeniería de acuerdo a los estándares de CLARO SA para cada tipo de servicio de datos que se implementará.
- Verificar las configuraciones implementadas en los enlaces principales y sus respectivos backup con el fin de garantizar una mejor organización de marcación de servicios de la red de CLARO SA.
- Ejecutar pruebas de contingencia que confirme la operatividad del canal de datos y la disponibilidad del servicio al cliente.

2.4 ALCANCE

Para el desarrollo de este proyecto se tiene por tiempo y por temas de áreas, la elaboración del plan de acción y sus fases, adicional a esto los diagramas de detalles lógicos y las pruebas de BACKUP.

2.5 LIMITACIONES

- Debido a que para la ejecución del plan de acción son varias las áreas implicadas como lo son Planta externa, STI, almacén e implementación, no se tendrá accesos a las documentaciones que conlleva el proceso del aprovisionamiento del plan de acción.
- Ya que este proyecto solo tiene como enfoque las fases, diagramas técnicos y las pruebas de backup no se tendrá accesos a los procesos que conlleva cada una de las fases.
- La entidad financiera y CLARO SA no permiten por seguridad de la información, que los autores del proyecto publiquen fotos del datacenter, direccionamiento, ni antes ni después de la implementación.

3. MARCO TEORICO

3.1 PROTOCOLO HSRP (Hot Standby Router Protocol)

Hot Standby Router Protocol (HSRP) “es un protocolo propietario de cisco creado para redundancia de router en caso de fallas en la red; está diseñado para reemplazar y proteger una falla en el router principal de manera dinámica proporcionando servicios de conmutación por error en redes de difusión y multidifusión (Cole & Morton, 1998).

La finalidad de este protocolo es mantener la conectividad en la red en la que pueden participar múltiples routers, de los cuales se elige uno como predeterminado o activo, el que se encarga de enviar mensajes multicast en forma de paquetes Hello a través de la dirección 224.0.0.2 a los demás routers denominados pasivos, para que en el momento que se produzca algún problema en el activo, lo detecten y actúen como respaldo conmutando todo el tráfico de la red sin perder continuidad en esta (Scott, 2007) .

Para que no colapse la red, los routers activos y pasivos envían paquetes HSRP periódicamente después de que el protocolo complete el proceso de selección. Los equipos de respaldo adicionales, se encontrarán en estado inicial, lo que quiere decir que si el router activo falla, entrará en funcionamiento el router en espera, reemplazando al principal y en caso que este segundo falle, se entraría otro router que este en estado inicial a ser activo. Estos routers tienen una ip virtual configurada, que funciona como un router por defecto, la cual se comparte en todo el grupo HSRP para ser utilizada cuando exista un error en el router activo (Pavón, 2012).

A continuación se definirán algunos conceptos a tener en cuenta para comprender el funcionamiento de protocolo HSRP (Cole & Morton, 1998)

- Router Activo: Se encarga de enviar paquetes Hello vía multicast a la ip

virtual del router pasivo.

- Router Pasivo: Es el router de respaldo del activo.
- Grupo en espera: Son el conjunto de routers HSRP que funcionan como router virtual.
- Tiempo de Saludo: Transcurso de tiempo de los mensajes Hello de un router a otro.
- Tiempo de Espera: Intervalo de tiempo en que se recibe un mensaje hello y se detecta que el router activo fallo.

3.1.1 Formato de paquetes

El protocolo HSRP trabaja sobre UDP sobre el puerto 1985, por tanto a continuación se mostrara la trama de datos de UDP y se describirá el significado de cada campo (Aguilar & Patiño, 2012):

- Código Op (1 octeto): Es la clase de mensaje que tiene el paquete, pueden ser:
- 0 (Saludo - Hello): Se utiliza para iniciar el protocolo HSRP e indicar que es el router activo.
- 1 (Coup - Golpe): Son transmitidos cuando un router pasivo quiere ser activo.
- 2 (Resign - Retiro): Son enviados en el momento que un router no quiere ser activo.

2. Estado (1 octeto):

Este campo indica el estado actual que tiene el router que envía los mensajes. Se manejan los siguientes valore:

0 - Inicial

1 - Aprendizaje

2 - Escucha

4 - Hablar

8 - En espera

16 - Activo

3. Tiempo de saludo (1 octeto):

Indica el tiempo de duración en segundos que tienen los mensajes Hello que envía el router.

4. Tiempo de Espera (1 octeto):

El estado tiempo de espera muestra el intervalo de tiempo en que esperan los routers recibiendo el mensaje hello antes de cambiar de estado.

5. Prioridad (1 octeto):

Este campo de la trama selecciona el router activo y pasivo, elige que estado tiene cada uno de acuerdo a la prioridad de los dos routers, el que tenga la prioridad más alta quedara como activo y el de menor se denominara pasivo.

6. Grupo (1 octeto):

Determina el grupo de espera.

7. Datos de autenticación (8 octetos):

Los datos de autenticación hacen referencia a una contraseña conformada por 8 caracteres. En caso de no tener ninguna se dará un valor por defecto.

8. Dirección IP virtual (4 octetos):

Es la dirección ip que se configura en el grupo para enviar los mensajes de saludo.

3.1.2 Estado del protocolo HSRP

Todos los routers tienen proporcionado una máquina de estados simple. HSRP funciona con los siguientes estados (Cisco):

1. Inicial:

El estado inicial enuncia que el protocolo HSRP aún no se está efectuando. Es importante en el momento que se proporciona una nueva interfaz o que se desea realizar un cambio de configuración ya que es necesario aplicarlo.

2. Aprender:

Este estado indica que aún no se detecta la dirección IP virtual, ni tampoco un mensaje de saludo que envié el router activo. Por tanto el router pasivo siempre esperara poder conocer al activo.

3 Escuchar:

En este estado se identifica la IP virtual, pero aún no sabe si es el router activo o pasivo. Está a la espera de mensajes de saludo.

4. Hablar:

Cuando el router tiene estado hablar envía mensajes de saludo constantemente para elegir si es activo o pasivo. Si no se conoce la dirección IP virtual no se podrá llegar a este estado.

5. En espera:

Indica que el router es el próximo activo y está enviando mensajes de manera periódica.

6. Activo:

En el estado activo el router envía paquetes de manera constante a la dirección virtual para que cuando se presente fallas el pasivo logre activarse.

3.1.3 Temporizadores

Hot Standby Router Protocol (HSRP) maneja tres temporizadores los que permiten programar los mensajes hello. Existen los siguientes temporizadores:

- Temporizador activo: Controla el router activo desde el momento en que se recibe un mensaje de saludo y caduca según el tiempo de espera del paquete HSRP.
- Temporizador en espera: Controla el router pasivo y se activa cuando se recibe un mensaje saludo, culminando cuando se vence el tiempo de espera del mensaje.
- Temporizador de saludo: Este temporizador controla los mensajes de saludo.

3.1.4 Eventos

1. El protocolo HSRP se debe configurar en una interfaz activa.

2. Si el protocolo HSRP se configura en una interfaz inactiva se encontrara inhabilitado.

3. El temporizador activo se habilita cuando localiza el último mensaje hola del router activo.

4. El temporizador en espera finaliza se establece cuando encuentra con el último mensaje hola del router en espera.

5. El temporizador de saludo tiene un tiempo de vencimiento.

6. Ingreso de mensajes de saludo con mayor prioridad en u router que se encuentre en estado hablar.

7. Ingreso de mensaje de saludo de mayor prioridad en el router activo.

8. Recepción de un mensaje de saludo de menor prioridad desde el router activo

9. Se recibe un mensaje de retiro en el router activo.

10. Ingresa mensaje Coup desde el router con prioridad más alta.

11. Ingresa mensaje hola de alta prioridad proveniente del router de espera.

12. Ingresa mensaje hola con baja prioridad proveniente del router de espera.

3.1.5 Acciones

Son las acciones que se deben realizar en la máquina de estado (Cisco).

A. Se inicia temporizador activo.

B. Se activa temporizador en espera.

C. Finaliza el temporizador activo.

D. Finalizar el temporizador en espera.

E. Ejecutar parámetros.

F. Se transmite mensaje de saludo.

G. Se transmite mensaje Coup.

H. Se transmite mensaje de retiro.

I. Se envía mensaje ARP.

A continuación se muestra la gráfica el diagrama de cambios de estado de la máquina de estado de HSRP:

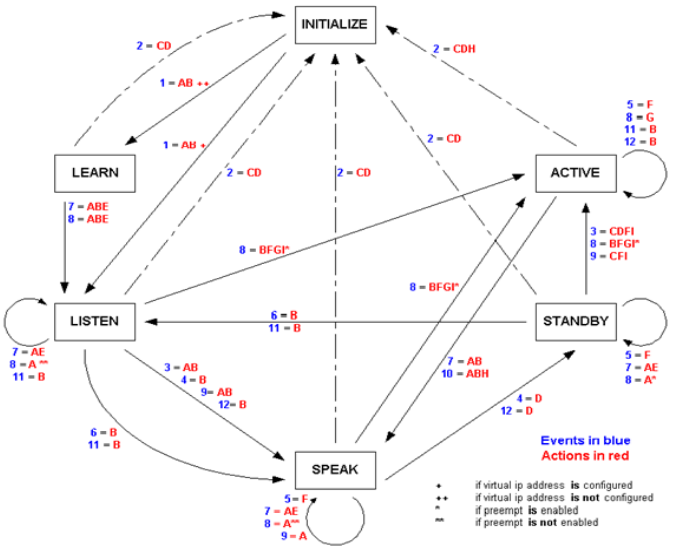


Ilustración 1. *Estados del protocolo HSRP. Tomada de: http://www.cisco.com/cisco/web/support/LA/7/73/73722_62.html#topic3.*

3.1.6 Dirección MAC

Los grupos del protocolo HSRP utilizan una dirección MAC virtual que se encarga de asociar todos los routers. El router activo recibe y envía paquetes a la dirección MAC virtual del grupo con una única tabla ARP para que al final del proceso no cambie esta y se pueda mover de un router a otro dentro del grupo (Dordogne, 2013).

3.2 DATACENTER

Es un centro de procesamiento de datos, que tiene proporcionado los recursos de servidores en los que se almacenan datos operativos de redes de una compañía. Los centros de datos garantizan disponibilidad y continuidad del negocio, lo que garantiza un porcentaje mínimo de fallas en las actividades del negocio. El datacenter es un espacio amplio en el que se encuentran diferentes dispositivos electrónicos que almacena información operacional de algún negocio (Vilar, 2003).

El diseño de un centro de procesamiento de datos se basa en la norma de implementación TIA 942 que brinda una serie de recomendaciones de infraestructuras de datacenter cuya estructura tiene cuatro subsistemas que se describen en la siguiente tabla:

Tabla 2. *Subsistemas de un datacenter.*

Telecomunicaciones	Arquitectura	Eléctrica	Mecánica
Cableado de racks	Selección del sitio	Cantidad de accesos	Sistemas de climatización
Accesos redundantes	Tipo de construcción	Putos únicos de falla	Presión positiva
Cuarto de entrada	Protección ignifuga	Cargas criticas	Cañerías y drenajes
Área de distribución	Requerimientos NFPA 75	Redundancia de UPS	Chilleras
Backbone	Barrera de vapor	Topología de	CRAC´s y

		UPS	condensadores
Cableado horizontal	Techos y pisos	PDU´s	Control de HVAC
Elementos activos redundantes	Área de oficinas	Puesta tierra	Detección de incendio
Patchpanels	Sala de UPS y baterías	Baterías	Extinción por agente limpio (NFPA 2001)
Patchcords	Sala de generador	Monitoreo	Detección por aspiración (ASD)
Documentación	Control de acceso	Generadores	Detección de líquidos

Tomado de: Association, T. I. (2005). Estándar TIA 942.

Un centro de datos debe garantizar un mínimo de parámetros en sus áreas de manera funcional:

1. Se debe tener mínimo uno o más de dos accesos a la habitación.

2. Una espacio de distribuido horizontal.

3. Área para equipos.

4. Zona de distribución.

5. Cableado estructurado.

Dentro del estándar de recomendación se encuentran cuatro niveles de Tiers que especifican los niveles de redundancia para garantizar la disponibilidad del datacenter:

1. Tier I (Datacenter Básico): Es el centro de datos más sencillo que se puede implementar. Se caracteriza por tener una estructura con un sistema de energía no tan complejo, aire acondicionado y puede presentar mayores fallas debido a que no cuenta con planes de contingencia como generadores eléctricos y UPS en casos de presentar fallas eléctrica.

Este tipo de centro de datos brinda una disponibilidad del 99.671% lo que significa que permite un tiempo de fallas de máximo 28.82 horas al año.

2. Tier II (Componentes Redundantes): Es un centro de procesamiento de datos

más complejo que el Tier I. Su estructura cuenta con elementos como UPS y generadores eléctricos que a su vez tienen equipos de respaldo, además cuentan con un piso falso y una línea de distribución eléctrica.

Este Tier ofrece un máximo de disponibilidad del 99.749 del tiempo en un centro de datos, puede interrumpir la operación durante 22.68 horas al año.

3. Tier III (Mantenimiento Concurrente): La implementación de un datacenter Tier III permite desarrollar cualquier labor definida como mantenimientos programados, mantenimientos preventivos, instalación de nuevos dispositivos, sustitución de equipos, entre otros, sobre la infraestructura sin detener los procesos de la operación ya que debe tener dos líneas de distribución para que cuando se realice alguna actividad una reemplace la otra.

Es capaz de proporcionar una tasa de disponibilidad del 99.982% del tiempo en un centro de datos. El tiempo máximo de falla que puede existir es de 1.57 horas al año.

4. Tier IV (Tolerante a Fallas): Su infraestructura es diseñado para no presentar ningún tipo de interrupción ante fallas. Posee múltiples líneas de distribución que cuentan con UPS, sistemas de redundancia y permite realizar actividades programadas sin generar daños en la operación.

Garantiza en un centro de datos una disponibilidad de tiempo del 99.995% y un tiempo máximo en caso de falla de 52.56 minutos al año.

A continuación se puede observar la tabla que especifica la disponibilidad según los tiers:

Tabla 3. *Porcentajes de disponibilidad, parada y Tiempo de parada según Tiers*

Tier	% Disponibilidad	% Parada	Tiempo parada anual
Tier I	99.671%	0.329%	28.82 horas
Tier II	99.741%	0.251%	22.68% horas
Tier III	99.982%	0.0018%	1.57 horas

Tier IV	99.995%	0.005%	52.56 minutos

Tomado de: Association, T. I. (2005). Estándar TIA 942.

3.3 PROTOCOLO BGP (Border Gateway Protocol)

Border Gateway Protocol es un protocolo de enrutamiento especialmente entre sistemas autónomos (AS) utilizado para intercambiar prefijos de rutas entre estos por medio de sesiones de BGP bajo el protocolo de control de transmisión TCP por el puerto 179 (Pantelis, & Martin, 2010).

BGP es definido por la RFC 4271 y es considerado como un protocolo vector-distancia (Path-vector) puesto que la información que transmite viaja por una serie de números de los sistemas autónomos hasta llegar a su destino. En otras definiciones se habla que es un protocolo hibrido ya que reúne características de métricas estado enlace y vector-distancia (Rekhter 2006).

El protocolo BGP tiene crea tablas de enrutamiento que a su vez almacenan rutas (prefijos, longitud y máscara) las que se definen por una serie de números de AS en donde el último número de sistema autónomo indica el destino al que se dirige la ruta. Su función principal es intercambiar información de rutas entre sistemas BGP (CISCO).

3.3.1 Términos

Sistema Autónomo (AS): Es un conjunto de routers que funcionan bajo las mismas políticas de enrutamiento. Cada sistema autónomo tiene asignado un número único AS con el que se pueda identificar proporcionado por la IANA (Internet Assigned Numbers Authority) (Traina, 2007).

EBGP (External Border Gateway Protocol): Se utiliza para conectar sistemas BGP externos.

IBGP (Internal Border Gateway Protocol): Se utiliza para conexiones internas

BGP.

IGP (Interior Gateway Protocol): Es un protocolo de enrutamiento utilizado dentro de un mismo sistema autónomo para el intercambio de información entre los routers que se encuentren en el AS.

3.3.2 Características del protocolo BGP

1. El protocolo BGP puede soportar enrutamiento entre dominios sin clase (CIDR) que consiste en simplificar las redes en una dirección ip.

2. Envía actualizaciones al iniciar sesión para poder conocer las tablas de enrutamiento de sus vecinos.

3. Emplea políticas como Access list, filterlist, router maps y prefixlist que se utilizan en las tablas de enrutamiento de entrada y salida.

4. Proporciona atributos que permiten tener administración de la red.

5. Escoge la mejor ruta.

3.3.3 Operación, rutas e información de enrutamiento

Operación:

Border Gateway Protocol (BGP) es utilizado para intercambiar información de enrutamiento entre diferentes sistemas autónomos (AS) por medio de conexiones TCP. El proceso de intercambio de información ocurre cuando dos vecinos de AS acuerdan compartir rutas o tablas de enrutamiento a lo que se denomina adquisición de vecino. El protocolo BGP mantiene las tablas de enrutamiento con las rutas actualizadas en el momento de la conexión con otros sistemas BGP, para asegurarse que la conexión permanezca establecida se envían constantemente mensajes Keepalive.

Los sistemas autónomos (AS) pueden tener múltiples routers BGP que comparten

información con otros AS, por esto es necesario utilizar un protocolo interno que garantice el correcto enrutamiento dentro del sistema autónomo. Si se requiere información de rutas del AS la indicara el protocolo interno, si por el contrario se solicita saber rutas de vecinos de otros AS dicha información la brindara el protocolo BGP.

Rutas (publicidad y almacenamiento):

Una ruta se define como "*una unidad de información que alcanza un destino con los atributos de un camino hacia ese destino" (*Rekhter 2006*).*

Las rutas son anunciadas por mensajes UPDATE entre sesiones BGP y son almacenadas en la tabla de información de enrutamiento (RIB) que proporciona un conjunto de tablas de encaminamiento llamadas Adj-RIB-In, Loc-RIB y Adj-RIB-out (*Ver ilustración 2*) (Ibíd.).

El protocolo BGP informa cuando una ruta previamente anunciada es eliminada de algún vecino BGP a través de 3 mecanismos (Castaño & Rojas, 2012):

1. A través del prefijo IP se puede etiquetar la ruta como retirada o no disponible publicándola en el campo *"rutas retiradas"* en el campo de mensaje UPDATE.

2. Con una ruta de remplazo publicada en la capa de información de red (NLRI).

3. Finalizando la sesión BGP eliminando las rutas que se habían anunciado previamente.

Información de enrutamiento:

La tabla de información de enrutamiento (RIB) es constituida por otras tablas de encaminamiento:

Adj-RIB-In: Es la tabla en la que contiene los prefijos de un vecino específico. Existe una gran cantidad de este tipo de tablas.

Loc-RIB: Tabla que almacena las mejores rutas mediante el proceso BGP ya que conoce su tabla de enrutamiento como también puede aprender por BPG (E-BGP u I-BGP). Se tiene una tabla por sistema autónomo.

Adj-RIB-out: Es una tabla que tiene los prefijos para anunciar a los vecinos. Se forma de la información que tenga la tabla Loc-RIB. Por cada par de BGP se tiene una tabla.

A continuación se muestra la gráfica de operaciones de BGP:

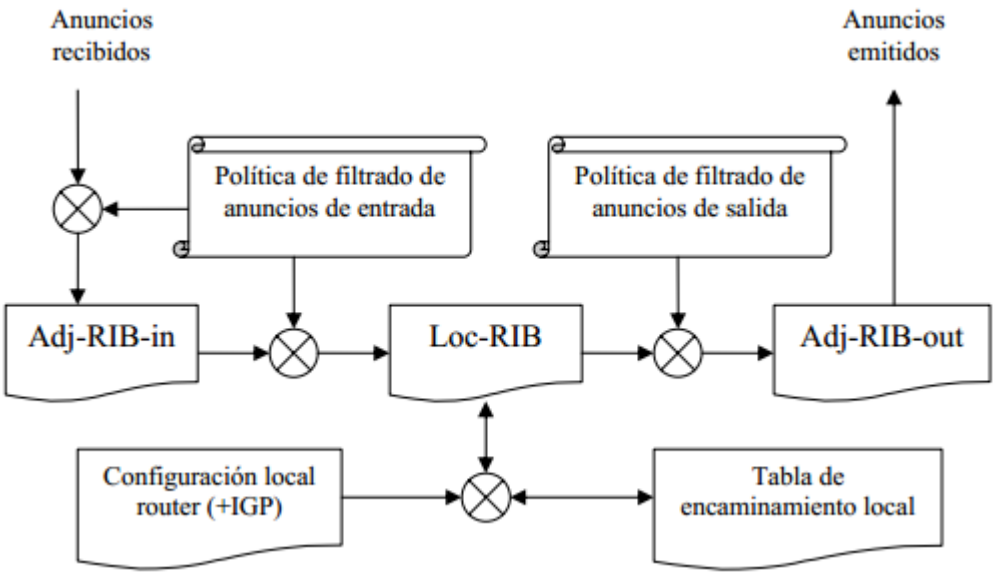


Ilustración 2. *Operaciones del protocolo BGP. Tomado de: http://bibing.us.es/proyectos/abreproy/11359/fichero/BGP%252F5.+Fundamentos+de+BGP.pdf*

3.3.4 Formato de mensajes:

El protocolo BGP utiliza mensajes para intercambiar información, parámetros o detectar errores; Estos pueden variar de tamaño desde 19 a 4096 octetos enviados a través de conexiones proporcionadas por el Protocolo de Control de Transmisión (TCP).

3.3.5 Tipos de mensaje:

A continuación se enunciaran y describirán los tipos de mensaje del protocolo BGP:

- OPEN: El mensaje OPEN es el primero en enviar después de establecer la conexión TCP. Es usado para fijar los parámetros de la sesión como: el tiempo que durara (generalmente 90 segundos), la versión del protocolo BGP y el número de AS. Cuando se recibe un mensaje OPEN se debe enviar un mensaje KEEPALIVE como respuesta.

- UPDATE: Este tipo de mensaje es el que transfiere la información de enrutamiento de las sesiones BGP como: los atributos, los prefijos, la longitud, entre otros. También puede adicionar o eliminar rutas.

- KEEPALIVE: Un mensaje KEEPALIVE es la confirmación o respuesta del mensaje OPEN. Estos son enviados constantemente cada 30 segundos, generalmente lo que indica que la sesión BGP se encuentra activa.

- NOTIFICACIÒN: Es el encargado de finalizar la sesión BGP establecida en el momento que detecta un error y a su vez finaliza la conexión TCP.

3.3.6 Estados del protocolo BGP

El protocolo BGP puede presentar 6 posibles estados que se producen en la interacción de sesiones BGP, en las que se pueden presentar varios eventos. Estos estados son los siguientes (Calleja, 2012):

1. Idle o Libre: Es el estado inicial y espera que se establezca la conexión TCP.

2. Connect (Conexión): Se encarga de establecer la conexión TCP.

3. Open Sent: Envía mensaje OPEN o de identificación y espera respuesta de su vecino.

4. Open Confirm: Respuesta de mensaje OPEN o de identificación.

5. Established: Acepta los mensajes OPEN CONFIRM garantizando que la conexión BGP se establecido completamente para poder intercambiar información.

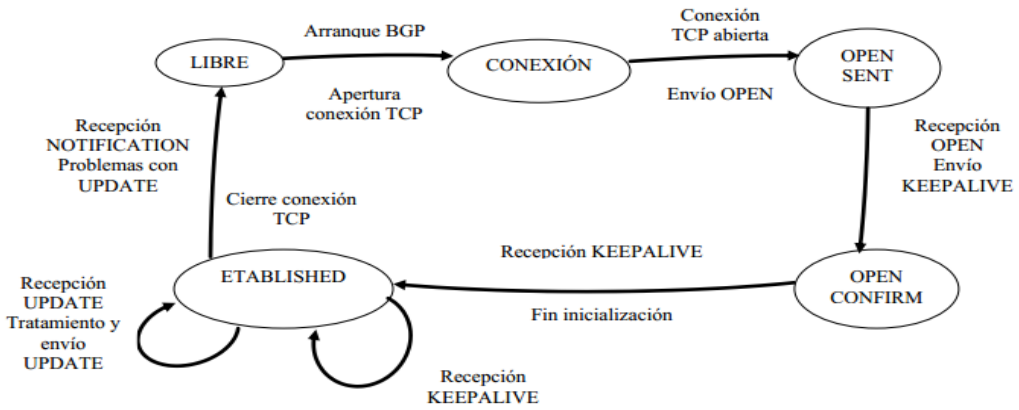


Ilustración 3. *Estados y eventos del protocolo BGP. Tomado de: http://bibing.us.es/proyectos/abreproy/11359/fichero/BGP%252F5.+Fundamentos+de+BGP.pdf*

3.3.7 Atributos del protocolo BGP

Como se definió anteriormente en el mensaje UPDATE, se conocen ciertos atributos que proporcionan características a las rutas que se van a intercambiar en la conexión BGP. Estos permiten atribuir reglas de filtrado y seleccionar la mejor ruta para llegar al destino elegido.

Los atributos del protocolo BGP se dividen en dos grupos:

1. Well-Know:

- Mandatory: Este atributo es de carácter obligatorio y debe ser conocido en todas las implementaciones del protocolo BGP.
- Discretionary: No es un atributo necesario. Si se tiene configurado se debe conocer por todos los router BGP.

2. Optional:

- Transitive: No es necesario su uso. Si se reconocen estos atributos en el mensaje no es necesario actuar de acuerdo a estos.

- Non Trasitive: Son atributos no transmitidos al peer BGP.

Estos atributos a su vez se subdividen en otros que se explicaran a continuación:

1. Origin (Well-Know): Indica cómo se aprende la ruta ya sea por el protocolo IGP, EGP o si la ruta está incompleta. Si se indica *i* quiere decir que la ruta se ha aprendido por el protocolo IGP y tendrá una mayor prioridad, si muestra *e* se aprendió con el protocolo EGP con un orden de selección secundario y si se desconoce el origen de la ruta o que no se haya aprendido mostrara ?y se dará la menos prioridad para ser seleccionada.

2. As-Path (Well-Know): Representa la secuencia de sistemas autónomos por donde paso la ruta, cada AS asigna un número ASN con el fin de indicar el camino que atravesó la ruta de sistemas autónomos para llegar a su destino.

3. Next-Hop (Well-Know): Realiza una búsqueda del próximo salto eligiendo la ruta más corta para llegar a su destino. Solo puede modificarse en rutas anunciadas por EGP. Es el siguiente salto para alcázar la red.

4. Local-Pref (Well-Know): Este atributo permite dar prioridad a las rutas mediante I-BGP dentro de un sistema autónomo AS. Elige por donde debe salir la ruta y prefiere el valor más alto.

5. Atomic-Aggregate (Well-Know): El atributo Atomic-Aggregate permite visualizar las rutas que son agregadas por otras rutas.

6. MED (Multiple Exit Discriminator) (Optional): Es la métrica externa que tiene una ruta. Indica a los routers que no se encuentren en un mismo sistema autónomo AS el camino que debe seguir para llegar y entrar al AS.

7. Community (Optional): Agrupa un conjunto de routers que comparten

propiedades similares. Etiqueta rutas que tienen características parecidas.

8. Aggregator (Optional): Cuando se agrega una nueva ruta a un router el atributo aggregator brinda información del Sistema Autónomo AS y el router ID en el que se agregó la ruta.

3.4 MPLS (MULTIPROTOCOL LABEL SWITCHING)

La tecnología MPLS (MultiProtocol Label Switching) representa un conjunto de especificaciones definidas por el IETF (*Grupo de Trabajo de Ingeniería de Internet*) y la RFC 3031, esta solución fue diseñada con el fin de unificar los servicios de datos en el momento de ser transportados sobre las redes IP y ATM, las cuales están basadas en circuitos y paquetes respectivamente. Este protocolo puede trabajar a nivel de capa 2 y capa 3, por tanto, adapta el protocolo IP a la tecnología ATM. MPLS es una tecnología innovadora en la que a los paquetes se les asignan elementos de tamaño fijo llamados etiquetas y la conmutación a través de la red se realiza de acuerdo a ellas (Garcia, 2008).

La tecnología ATM y el protocolo IP en cuestión de tratamiento de redes son bastante importantes, por un lado el Protocolo de Internet (IP) basando en el Routing de paquetes es el más utilizado para el transporte de datos en una red, por otro lado el Modo de Transferencia Asíncrona (ATM) es una tecnología de conmutación de paquetes que facilita la gestión de recursos, calidad de servicio (QoS) y ofrece una mayor velocidad a la red (A.T.M & As).

El funcionamiento de una red MPLS se basa en un conjunto de enrutadores de conmutación de etiqueta (LSR) que tienen la capacidad de conmutar y enrutar paquetes en base a la etiqueta (Label) que se la añade a cada uno, cada etiqueta determina un flujo diferente de paquetes entre los dos extremos, a este flujo se le da el nombre de FEC (Forwarding Equivalence Class) (Vicente & Martinez, 2006).

3.4.1 Terminología

A continuación se enunciaran una serie de conceptos importantes para comprender el protocolo MPLS (Gutierrez, 2012):

- P (Provider): Encargado de intercambiar paquetes entre una interfaz de entrada y una de salida, igualmente es el encargado de intercambio de labels.

- PE (Provider Edge): Recibe la conexión de clientes, realiza el intercambio y retiro de labels.

- CPE o CE (Customer Premise Equipment o Customer Edge): Equipo de cliente, No pertenece al dominio de MPLS.

- FORWARDING: Hace referencia a la secuencia o flujo de paquetes que pueden ser direccionados (forwarding) al mismo “next-hop” o a lo largo del mismo camino (Path).

- Edge: Se colocan las etiquetas por FEC para los paquetes salientes, se extraen las etiquetas para los entrantes.
- Core: Se decide la interface de salida según la etiqueta del paquete, se reemplaza la etiqueta y se envía el paquete.

La clasificación de las etiquetas está basada en:

- Destination Unicast / Multicast address
- Traffic Engineering (túnel)
- VPN
- QoS (Clase de servicio)

3.4.2 Ingeniería de tráfico

En esta parte es donde se definen las rutas de manera dinámica, asignación de recursos y optimización a la red. Los protocolos IP y OSPF permiten la gestión de ingeniería de tráfico, el primero de manera remota y el segundo con ruta más corta que da permiso a los enrutadores de los paquetes cuando se necesite balanceo de carga. Con un buen manejo de tráfico en las redes, se pueden evitar congestiones, perdidas de paquetes, reducción de latencias, entre otros aspectos, esto quiere decir que se maximiza la capacidad de la red y se minimizan los costos.

3.4.3 Soporte de redes virtuales privadas (VPN)

Una red VPN (red privada virtual) es una red privada construida dentro de una infraestructura de red pública, como por ejemplo Internet. Las empresas pueden usar una red VPN para conectar de manera segura oficinas y usuarios remotos mediante el uso de infraestructuras públicas, Los paquetes de datos de la red privada viajan por un túnel definido en la red pública.

Las VPN creadas con tecnología MPLS tienen una mayor capacidad de expansión y son más flexibles en cualquier red IP, además proveen seguridad y rapidez de transmisión de la información (Mosquera & Arboleda, 2012).

3.4.4 Soporte de calidad de servicio (QoS):

Garantiza el uso eficiente de los recursos y aplicativos (video o audio en tiempo real) que tenga asignada la red, lo que permite a su administrador un monitoreo a la red, y así mismo darle menores costos y mayores resultados al usuario final.

En el momento en que QoS provee los recursos lo primero que tiene en cuenta es el grado de prioridad de estos y así empezar a responder a los aplicativos para que puedan completar sus actividades en un tiempo prudente. La ventaja más

importante del soporte de calidad de servicio es que este disminuye los costos en la concesión de recursos con mayor eficiencia hablando del ancho de banda que estos requieran.

3.4.5 Componentes de la red mpls

LDP (Label Distribution Protocol): Protocolo a nivel de aplicación, permite el intercambio de etiquetas (labels) entre los P y los PE. LDP asocia una clase de equivalencia de reenvío (FEC) con cada LSP que crea. La distribución del protocolo LDP por la red MPLS se hace utilizando alguno de los protocolos de enrutamiento, como OSPF, BGP, IS-IS. Sin embargo existen 4 categorías de mensajes LDP.

- Mensajes de descubrimiento: se usan para anunciar y mantener la presencia de un LSR en una red.

- Mensajes de sesión: Son los encargados de establecer, mantener y terminar sesiones entre pares LDP.

- Mensajes de anuncio: Son los usados para crear cambiar y borrar mapeo de etiquetas a la FEC.

- Mensajes de notificación: proveen información de soporte e información de señal de error.

LSR (Label Switching Router): Es un tipo de un enrutador situado en el medio de la red MPLS. Es responsable de la conmutación de las etiquetas utilizadas para enrutar paquetes. Cuando un LSR recibe un paquete, se utiliza la etiqueta incluida en la cabecera como un índice para determinar el siguiente salto de la etiqueta SwitchedPath (LSP). Antes de que el paquete se enviara se retira la etiqueta antigua y se reemplaza por la nueva etiqueta.

LSP (Label Switch Path): Es una ruta sobre una red MPLS, establecida por un protocolo de señalización como LDP, La ruta es establecida basándose en los criterios definidos por la clase de equivalencia de reenvíos FEC.

Edge LSR o LER: Es el Enrutador que opera en el borde de una red MPLS, su

función es eliminar la etiqueta para entregar el paquete.

3.5 MPLS AVANZADO

Es una solución de transmisión de datos que proporciona servicios de altos estándares debido a que esta soportado por una plataforma Multiservicios de última generación, segura y privada, a través de la cual se podrá intercambiar información de manera eficiente y sencilla, permitiendo aumentar el ancho de banda de acuerdo a la necesidad de su negocio.

Con el servicio de MPLS avanzado se podrá transmitir información entre oficinas o sedes de la misma empresa lo cual establece una solución llamada INTRANET o entre oficinas o sedes de distintas empresas lo que constituye una solución llamada EXTRANET.

3.5.1 MPLS intranet

Permite la integración de redes LAN distribuidas geográficamente, conectando la oficina principal del cliente con sus sucursales remotas, en una arquitectura segura y de alta calidad, implementando los servicios de voz, video y datos en una misma conexión.

Este servicio se ofrece en las siguientes Modalidades

- MPLS Intranet Local
- MPLS Intranet Nacional

3.5.2 MPLS extranet

Admite la conexión con los proveedores de servicio y contenido para el intercambio de información, igualmente posibilita compartir aplicaciones de negocios para satisfacer sus propias necesidades de comunicación de datos, a

clientes que brinden servicios de contenido es necesario determinar una configuración especial en la red MPLS, la cual incluye enlaces de Backup, asignación de diferentes RT (Route Target) para marcar rutas que se anuncian desde el proveedor de contenido hacia los clientes y para marcar las rutas que se anuncian desde los clientes hacia el proveedor de contenido, configuración de ancho de banda por servicio, entre otros. Además para cada servicio que ofrece los proveedores de contenido se debe configurar en una interfaz lógica o física, el cual será identificado con una única VRF.

A diferencia de una Extranet habitual, la configuración con un proveedor de contenido difiere en los RT que importa y exporta el Cliente. Estas configuraciones se hacen exclusivamente en el lado del cliente, el lado del proveedor de contenido no se debe modificar.

Este servicio se ofrece en las siguientes Modalidades

- MPLS Extranet Local
- MPLS Extranet Nacional

A continuación se enunciaran algunas características de un canal MPLS avanzado:

- Manejo eficiente de tráfico
- 100% IP
- Altamente escalable, ya que se puede ofrecer altas velocidades sin cambiar el medio físico, gracias a que en el Acceso se entrega sobre interfaces Fast Ethernet/Gigabit Ethernet.
- Flexibilidad, gracias a que se cuenta con herramientas para servicios de valor agregado como la priorización del tráfico de datos sobre los canales críticos, Estadísticas MRTG, Estadísticas avanzadas y ancho de Banda por Demanda.
- Calidad de Servicio (QoS)
- Red con Estándares mundiales

- Soluciones de conectividad con disponibilidad desde 99.7% en acceso lineal en Fibra Óptica Claro, hasta 99.95% con acceso y CPE redundantes.

4. METODOLOGÍA

El presente proyecto se realizó sobre bases cualitativas, debido a su pertinencia y necesidad de sistematizar información relacionada con la ejecución del plan de acción propuesto por CLARO S.A, que permitió a esta técnica de investigación contribuir a la mejora que tuvo como finalidad la organización del datacenter de una entidad financiera.

En este contexto fue necesario orientar el contenido de los documentos relacionados con la ejecución de las fases del proyecto “Punto Central de una entidad financiera”, además de la aplicación del conocimiento de los ingenieros sobre la ejecución del proyecto quienes fueron parte activa del mismo.

Entre tanto, la investigación con enfoque cualitativo permitió la identificación, rastreo y ejecución del proyecto que es el eje transversal de la sistematización, mediante el ejercicio correctivo que se construyó sobre la deficiente organización del datacenter de una entidad financiera. De esta manera, se encuentra presente un contexto donde el ingeniero acude a su conocimiento para incidir sobre la ejecución y verificación de los procesos enfocados a la optimización del servicio, el cual se sistematizó a partir de la puesta en marcha del plan de acción. De este modo, describir de manera académica la sistematización de la experiencia implica la importancia de la metodología cualitativa como el camino idóneo para recolectar la información.

La propuesta metodológica que condujo las vías del proyecto se sustenta en la sistematización de documentos que se desarrolló en tres fases correspondientes a fuentes de información.

La primera fase correspondió a la documentación producida desde la institución para éste caso CLARO S.A. expresada en casos de seguimiento, notificaciones, ordenes de trabajo (OT), reportes técnicos, diagrama de detalle que hacen referencia a cómo está el servicio actualmente y como quedaría físicamente, éste

describe el nodo, si el servicio llega por fibra o cobre, equipo instalado (CPE) pero en él no se evidencia el direccionamiento WAN y LAN asignado al cliente ni los puertos y vlans asociadas ya que esto sería una ingeniera de detalle y no correspondía realizarlas por alcances del proyecto.

En segundo lugar, se hizo referencia a los puntos de vista de los ingenieros involucrados en la ejecución del plan de acción, como también las áreas participes en el proceso realizado, tales como implementación encargada de garantizar los requerimientos mínimos para la entrega de los servicios nuevos, el área de preventa que indica la factibilidad del proyecto a realizar, Prevención Soporte Corporativo cuya función es verificar las configuraciones de los enlaces backup para garantizar su correcto funcionamiento y la cuarta área es el NOC cuya función principal es generar, analizar, diagnosticar y solucionar los incidentes presentados sobre los enlaces de los cliente corporativos de CLARO S.A.

Por último, se tomó como referencia la observación directa de todos los procesos realizados en la ejecución del proyecto como los nuevos esquemas implementados, las configuraciones de los servicios de contingencia, las características de los equipos, entre otros, para poder concluir la ejecución del plan de acción enfocado en la organización del centro de datos de DAVIVIENDA.

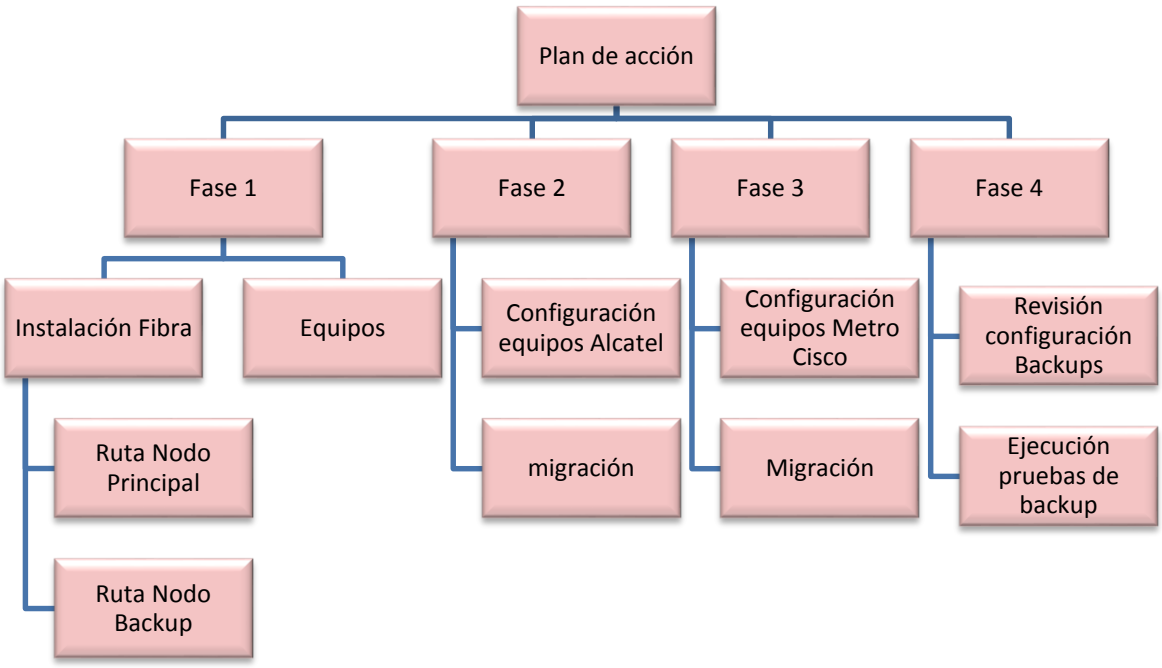
En concordancia con lo mencionado anteriormente se plantean ciertos pasos metodológicos en la ejecución de este plan de acción:

1. Se define el planteamiento del problema.
2. Se plantean los objetivos a cumplir para dar solución al problema existente.
3. Se validan las labores a realizar y se asignan las tareas a cada una de las áreas involucradas de acuerdo a sus funciones.
4. Realizar procesos del plan de acción de acuerdo a las funciones de las áreas implicadas:
    - Validación de características de equipos.

- Instalación de equipos y fibra óptica.
- Migraciones de servicios Alcatel y metro.
- Verificación de configuraciones de los servicios (MPLS Extranet o Intranet).
- Ejecución de pruebas de backup.

5. Recopilar información de lo realizado por cada una de las áreas.
6. Elaborar informe en el que se documente la ejecución del plan de acción para la organización y espacio del datacenter en el punto central Davivienda Bogotá.
7. Presentación y entrega de informe final.

A continuación se mostrara el diagrama de procesos a llevar a cabo por medio de diferentes fases:



4.1 FUENTES DE INFORMACIÒN

Para este proyecto la fuente de información es suministrada por lo aplicativos de claro.

- Fuentes primarias: Documentación en la herramienta CRM, manuales, pagina WEB (Intranet corporativa), Ordenes de trabajo, casos de seguimiento, reportes técnicos.

- Fuentes secundarias: Libros de redes cisco, páginas WEB y diccionarios.

4.2 HERRAMIENTAS INSTRUMENTALES

Las herramientas instrumentales utilizadas para este proyecto son:

- Equipos de cómputo con las aplicaciones necesarias para la documentación.

- Software (putty), aplicación que permite acceder a routers y swiches.

- CRM, herramienta de documentación interna donde se evidencia todo lo realizado con el plan de acción.

- PDSR, Pagina de registro de servicios (uso interno) en la cual se encuentra la información técnica de cada enlace.

4.3 HERRAMIENTAS METODOLOGICAS

Para este proyecto debido a que la documentación no se presenta sobre un documento escrito como tal si no que se realiza sobre las plataformas interna de claro como el CRM, se realizan una serie de métodos de aprendizajes para el grupo de prevención(área paralela de soporte corporativo CLARO SA)

- Mediante la lectura de los TKTs y OTs generadas por las áreas de implementación y soporte corporativo se realiza un cuadro en Excel que facilite el manejo de la información.

- Organizar la documentación de acuerdo a las áreas involucradas.

- Graficas de las fases relacionadas en el proyecto.
- Diagramas de detalle antes y después de la migración.

5. DESARROLLO DEL PROYECTO

5.1 DESCRIPCION DE AREAS

Lo autores del proyecto están en una de las áreas transversales a las implicadas:

- Preventa. (Gerencia).

    a. Preventa Premium. (Transversal)

- Implementación. (Gerencia)

    a. Planta externa. (Transversal)
    b. Gestión de instalaciones. (Transversal)
    c. Configuración. (Transversal)
    d. Equipos. (Transversal)
    e. Coordinación de instalaciones. (Transversal)

- NOC. (Gerencia)

    a. Aseguramiento. (Transversal)

- Soporte corporativo. (Gerencia)

    a. Ingenieros especializados. (Transversal)
    b. Prevención y proactividad. (Transversal)

De las gerencias de cada una de las áreas implicadas solo asistieron a la reunión así:

- Implementación – Gerente de proyectos
- Preventa – Coordinador activo y preventa Premium.
- NOC – Coordinador activo.
- Soporte corporativo – Coordinadores activos.

5.2 CARGOS Y FUNCIONES DE AREAS

5.2.1 Preventa

- Validar lo requerimientos físicos y técnicos de cada venta.
- Evaluar la factibilidad de cada proyecto nuevo.
- Indicar que equipos y que condiciones deben cumplirse para que el cliente reciba el servicio que contrato.
- Determinar el tipo de solución del servicio vendido por el comercial, se valida si es un servicio estándar o proyecto (pequeño, grande o especial).

5.2.2 Implementación

- Administrar la relación con el cliente para las solicitudes de Instalación y modificación de servicios de telefonía, conectividad, soluciones administradas, conectividad hacia Datacenter, de principio a fin, desde el análisis del requerimiento después de ingresada la venta hasta el cierre o entrega al cliente.

- Garantizar que se cumplan los requerimientos mínimos para entregar el servicio desde el procedimiento de Inicio o Kick Off hasta el procedimiento de entrega y aceptación del servicio por parte del cliente.

- Mantener sincronizados las solicitudes de instalación o modificación de

servicios, en tiempos, a lo largo de todo el proceso de implementación, estableciendo cronogramas y a su vez garantizando que la línea base se cumpla o que sus cambios sea justificados e informados a las partes interesadas, a través de los controles de Cambios.

- Elaborar ingenierías de detalle de las soluciones requeridas por el cliente donde se reflejan equipos, redes y factores importantes a tener en cuenta en el momento de la de la implementación del servicio y de esa manera garantizar la satisfacción de la entrega y a su vez que se cumpla con lo requerido.

- Documentar en Herramienta CRM las actividades a ejecutar durante el proceso de instalación del servicio de acuerdo al catálogo de servicios vigente y con las definiciones realizadas en el Proceso de Instalación, formalizadas en el Sistema de Gestión de Calidad de Claro Fijo Colombia, con el fin de mantener informadas a las áreas participantes del proceso de la instalación.

- Mantener un contacto eficaz y fluido con el cliente del proceso de implementación del servicio ya sea de manera verbal o escrita, estableciendo compromisos y sirviendo de negociador ante situaciones de difícil manejo hasta la entrega a satisfacción del nuevo servicio contratado.

5.2.3 Noc

- Monitorear proactivamente y diagnosticar los eventos presentados sobre la plataforma de datos de la red de CLARO S.A. para clientes corporativos; mediante las herramientas de monitoreo y gestión, y/o protocolos de verificación. Con la finalidad de cumplir los indicadores del área y los niveles de servicio acordados con los clientes internos y externos.

- Generar, analizar, diagnosticar y solucionar incidentes presentados sobre los enlaces de clientes corporativos de CLARO S.A.; Mediante el uso de herramientas de diagnóstico, conocimiento adquirido y/o documentado en las bases de datos de conocimiento y manuales de resolución de incidentes; soportado en el proceso de administración de incidentes. Con la finalidad de solucionar de forma rápida y efectiva, los incidentes reportados o detectados sobre la red de datos logrando el cumplimiento de los indicadores del área y los niveles de servicio acordados con los clientes internos y externos.

- Generar, analizar, diagnosticar y solucionar problemas proactivos o reactivos presentados sobre los servicios corporativos en la red de CLARO S.A.; Mediante el uso de herramientas de diagnóstico y técnicas de solución, utilizando el conocimiento adquirido y/o documentado en las bases de datos de conocimiento, soportado en el proceso de administración de problemas. Con la finalidad de encontrar soluciones definitivas a causas raíz, alimentado la base de conocimiento para futuros incidentes.

- Soportar actividades sobre los servicios corporativos acorde a la programación y la información consignada en la documentación del cambio generada por la administración de cambios. Para cumplir con los acuerdos de niveles de servicio con los clientes internos y externos.

- Detectar y reportar las anomalías sobre el funcionamiento o presentación de las diferentes herramientas de monitoreo y gestión. Mediante el proceso de administración de eventos para garantizar la fiabilidad de los eventos detectados por los sistemas.

5.2.4 Soporte corporativo

Es un grupo de Ingenieros altamente calificados con conocimientos sobre las diferentes plataformas tecnológicas de la red de CLARO S.A. y dispuestos atender requerimientos técnicos los 7 días de la semana, 24 horas al día, los 365 días del año

- Atención y solución de incidentes y requerimientos
- Soporte técnico de primer nivel
- Generación y entrega de informes o reportes a clientes (disponibilidad, fallas, etc.)
- Entrega de Información sobre productos y servicios. Generación de leads.

5.2.5 Prevención y Proactividad

- Controlar alarmas: Generar reportes técnicos por el servicio que se visualice alarmado, ejecutar pruebas de primer nivel y contactar al cliente para informar sobre el incidente y comunicarle el número del caso para la revisión del incidente. Escalar al centro de Gestión e informar al ingeniero especializado o líder del grupo.

- Validación de reincidencias: Hacer validación de incidentes reiterativos que se han presentado sobre el mismo código de servicio sobre el cual se observa la alarma. Al encontrar reincidencia en casos con similar resolución, se debe generar una atención tipo reporte técnico prioridad 4 al centro de gestión para que se ejecute un plan de acción con el fin de identificar la causa raíz de la incidencia y así dar una solución definitiva; las actividades a realizar serán informadas al cliente telefónicamente o por correo.

- Revisión servicios backup: Revisar y analizar configuraciones aplicadas a los servicios de backup a través del conocimiento técnico con el fin de asegurar la correcta configuración, garantizando la operatividad, funcionalidad y disponibilidad de los servicios de backup, para mantener los niveles de servicio comprometidos con el cliente.

- Crear caso para ajustes de configuración Pruebas de conmutación de tráfico: Crear casos para realizar los cambios de configuración requeridos para corregir, ajustar, estandarizar y optimizar la operación de un servicio de backup previo diagnóstico de una falla o error en la configuración. Ejecutar pruebas de conmutación de tráfico dentro de las ventanas acordadas (horarios acordados por el cliente), mediante el uso del protocolo definido para garantizar total operatividad de los servicios y aplicaciones del cliente a través de los canales de backup.

5.3 PROCESO DE PLANES DE ACCIÓN SEGÚN LAS FUNCIONES DE CADA ÀREA.

El área de preventa se encarga de evaluar la factibilidad del proyecto, donde determina que equipos se deben instalar, que PE y que nodo está en la capacidad de recibir todos los servicio a migrar, tiempo tomara la implementación del plan de acción y adicional cuantas ordenes de trabajo deben ingresar para documentar todo lo se debe realizar en el aplicativo CRM de documentación.

Implementación se encarga de recibir lo que el preventa evaluó y encarga a cada una de las áreas trasversales las tareas correspondientes, destina las tareas así:

- Planta externa: Indica los PEs y los nodos desde donde se debe realizar el tendido de la fibra externa e interna. (Planta externa puede cambiar el nodo documentado por el preventa)

- Gestión de instalaciones: debe estar pendiente de que todo lo solicitado por el gerente de proyectos se cumpla.
- Configuración: debe validar las configuraciones actuales y dejar los script listos para que se ejecuten el día de la migración.
- Equipos: validar que los equipos solicitados por el gerente de proyectos estén disponibles para el día de la migración.
- Coordinación de instalaciones: se debe encargar de tener el personal disponible para la instalación final.

NOC recibe lo implementado y se encarga de dejar lo recibido como algo estándar asignando las tareas a soporte corporativo para que en el momento dar el soporte sea de una manera organizada. Para lo cual el área transversal solicita la siguiente información.

- Aseguramiento solicita información a soporte corporativo antes de que implementación haga la entrega formal de lo que se va a instalar (ya que se trata de un plan de acción se tiene un antes y después de lo implementado), solicitando al área de prevención todas las ingenierías de detalle de cada uno de los servicio que se va a migrar. También asigna a soporte los script para las pruebas de backup después de que implementación entrega el proyecto ya terminado.

- Soporte Corporativo recibe las taras que el NOC determina, y estas las ejecuta el área transversal Prevención. Una de las tareas es realizar todos los diagramas de detalle de cada uno de los servicio que se van a migrar. En el momento que se entrega lo instalado por implementación se deben hacer los diagramas de detalle de los servicios migrados y como quedaron actualmente. También se deben generar los script de las pruebas de backup, esto lo revisa aseguramiento y corrige si es necesario, luego indica a soporte que las pruebas de backup se pueden ejecutar.

- Prevención: realiza todos los diagramas de detalle antes y después de la migración, generas los script para las pruebas de backup y las ejecuta según la ventana propuesta por los clientes finales de DAVIVIENDA.

5.4 FASE 1. INSTALACIÒN DE FIBRA Y EQUIPOS

Para esta fase los autores del proyecto debían tener conocimiento de los siguientes temas.

- Funciones básicas del área de implementación (ver descripción áreas).
- Características básicas de los equipos a implementar.

5.4.1 Instalación de fibra

En esta primera fase el área de implementación le indica a planta externa que debe realizar una visita a la sede del cliente DAVIVIENDA y validar los accesos para la fibra. Esta visita es llamada VOC (visita de obra civil) aquí se indican las proyecciones de cómo se realizará el tendido interno de la fibra y cual va ser el acceso de la fibra que viene externa, nodos de acceso más cercanos a la sede. Planta externa realiza la VOC y entrega un plano donde se evidencia los accesos al edificio y al empalme más cercano.

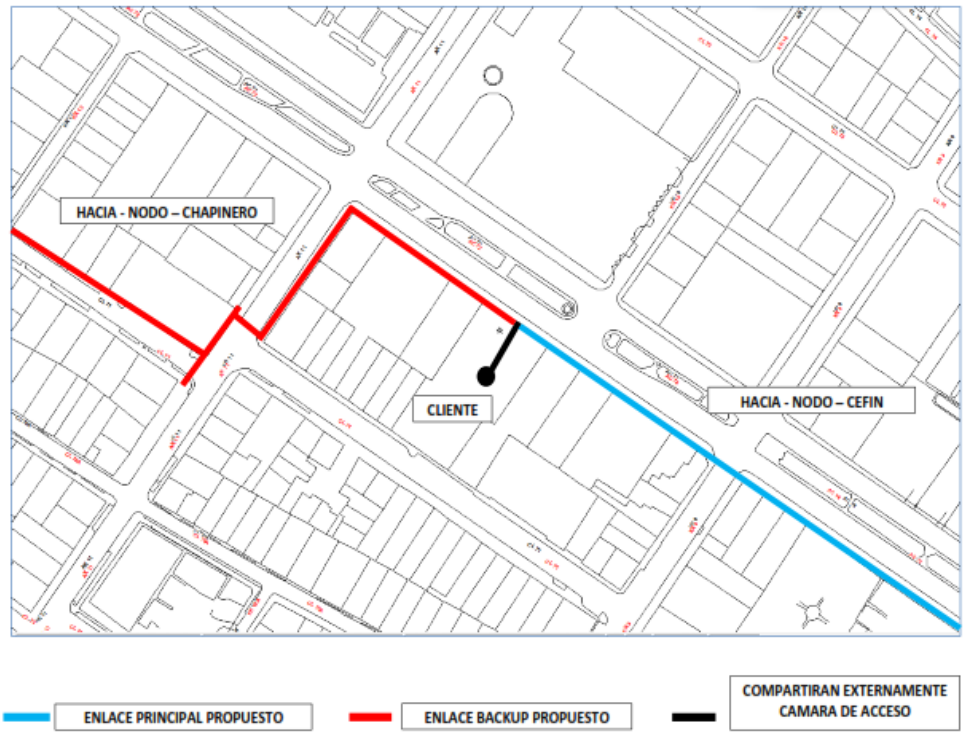


Ilustración 4. *Formato ruta externa fibra. Tomado de: Documentación área Implementación CLARO S.A.*

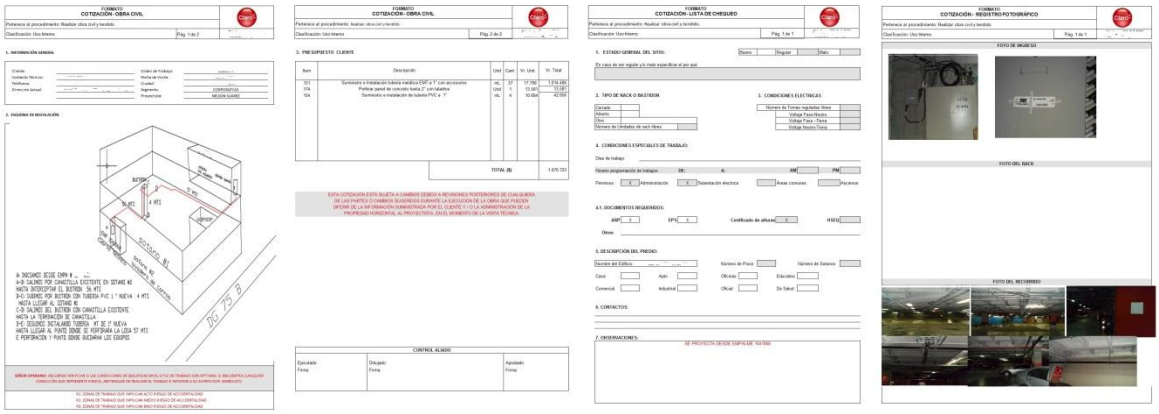


Ilustración 5. *Formato VOC y cotización de obra civil (COC). Tomado de: Documentación área Implementación CLARO S.A.*

5.4.2 Equipos

Luego de que se tienen documentados los formatos y el cliente aprueba la COC (Cotización de Obra Civil), planta externa, realiza el tendido de la fibra interna y externa- luego de que la fibra esta tendida se inicia la instalación de los equipos.

Características básicas de los equipos a implementar:

Los equipos a implementar se validaron según su ancho de banda y características básicas de acuerdo a las necesidades del cliente.

Los autores del proyecto no tienen acceso a la información de las necesidades básicas de los clientes, la información de los equipos necesarios fue enviada por el área de implementación.

Para lo cual se realizó la siguiente tabla:

Tabla 4. *Equipos instalados por servicio y ancho de banda.*

Tipo de servicio	Código de servicio	Nombre del cliente	BW DIST	Equipo
Nivel 3	ACH0024	A.C.H. COLOMBIA S.A. BANCO DAVIVIENDA EXTRANET	1M	Cisco 881
Nivel 3	BLS0049	BVC BANCO	3M	Cisco 881
Nivel 3	BLS0050	BVC BANCO	800	Cisco 881
Nivel 3	BLS0166	GRANBANCO TORRE BOLIVAR	1M	Cisco 881
Nivel 3	CEY0007	BOLSA ACCESO MERCADO	256	Cisco 881
Nivel 3	CIM0072	ICAP SECURITIES IHS	600	Cisco 881
Nivel 3	COP0033	COMPUTEC EXTRANET	2M	Cisco 881
Nivel 3	DIL0013	DIEBOLD COLOMBIA S.A.	512	Cisco 881
Nivel 3	DVV0011	BANCO S.A	1M	Cisco

				881
Nivel 3	DVV0014	BANCO S.A EXTRANET	20M	Cisco 2901
Nivel 3	DVV0016	BANCO S.A EXTRANET	20M	Cisco 2901
Nivel 3	DVV0027	BANCO S.A EXTRANET	20M	Cisco 2901
Nivel 3	DVV0023	BANCO EXT PROCESOS Y CANJE	1M	Cisco 881
Nivel 3	DVV0024	BANCO BACKUP	10M	Cisco 1905
Nivel 3	DVV0026	BANCO - Bloomberg	3M	Cisco 881
Nivel 3	DVV0071	REDEBAN TUNEL GREP	1M	Cisco 881
Nivel 3	DVV0147	BANCO GB BACKUP	100 M	Cisco 3945e
Nivel 3	DVV0375	GESTION NOC REMOTO MEZZANINE	NO	Monitor eo SW
Nivel 3	DVV0445	BANCO INTERNET	64	Cisco 881
Nivel 3	DVV0463	EXTRANET ACH	200	Cisco 881
Nivel 3	DVV0497	BANCO EXTRANET SERVIBANCA	600	Cisco 881
Nivel 3	DVV0584	SUPERFINANCIERA EXTRANET	100	Cisco 881
Nivel 3	DVV0585	IPDP REDEBAN EXTRANET	600	Cisco 881
Nivel 3	DVV0671	BANCAFE EXTRANET BANREPUBLICA	3M	Cisco 881
Nivel 3	DVV0675	BANCO EDIF PPAL PISO27 y O&M BOLIVAR VIDEOCONFERENCIA	4M	Cisco 881
Nivel 3	DVV0672	BANCO EDIF PPAL PISO27 y O&M BOLIVAR VIDEOCONFERENCIA	4M	Cisco 881
Nivel 3	DVV0766	BANCO INTERNACIONAL	2M	Cisco 881
Nivel 3	DVV0809	BANCO BOGOTA Calle 28 # 13A-15 Mezanine – PLS	3M	Cisco 881
Nivel 3	DVV0812	BANCO Calle 28 # 13A-15 Mezanine Bloomberg – PLS	3M	Cisco 881
Nivel 3	DVV0981	WINNER GROUP	600	Cisco 881
Nivel 3	UDQ0007	BANCO	1M	Cisco

				881
Nivel 3	DVV1002	BANCO	600	Cisco 881
Nivel 3	DVV1009	COLGRABAR	6M	Cisco 881
Nivel 3	FEA0023	ASSENDA S.A.	600	Cisco 881
Nivel 3	IBM0058	AT&T GLOBAL NETWORK	1M	Cisco 881
Nivel 3	ISAAA06	IPDP ITAC S. A.	600	Cisco 881
Nivel 3	RRO0124	ASCREDIBANCO CL 28 EXTRANET	600	Cisco 881

Fuente: Elaboración propia

Tabla 5. *Modelo de routers con sus características lógicas y físicas.*

Modelo	Imagen	Ancho de banda	Características básicas - lógicas	Características básicas – Físicas
Cisco 881	 Tomado de: http://www.cisco.com/c/en/us/support/routers/881-integrated-services-router-isr/model.html	15 Megas	SERVICIOS IP: • DHCP • IPv6 addressing, NAT-PT, ICMPv6, DHCP. • ACL, NAT • OSPF, BGP • Túneles GRE • HSRP, VRRP • vrf lite SWITCHING • Hasta	WAN 10/100Mbps. LAN 4Ports 10/100 switch

			ocho(8) VLANs en 8021.q • MDI-MDX GESTION: • Telnet, SSH, TACACs QoS: • Features QoS	
Cisco 1905	 Tomado de: http://www.cisco.com/c/en/us/products/routers/1905-serial-integrated-services-router-isr/index.html#)	50 Megas	SERVICIOS IP: ● NAT y ACLs ● DHCP ● IP ROUTING: BGP, OSPF, Routing Policy. ● IPv6 ● VRRP,HSRP ● vrf lite ● Túneles GRE SWITCHING ● 802.1q ● MAC address Management GESTION: ● SSH, SNMP, TACACs, Telnet QoS:	2 GE, una(1) interfaz serial integrada (SmartSerial), y un(1) slot adicional para HWIC (LAN,Serial, 3G)

			● QoS features. CoS(DSCP)	
Cisco 2901	 Tomado de: http://www.cisco.com/c/en/us/products/routers/2901-integrated-services-router-isr/index.html		SERVICIOS IP: ● NAT y ACLs ● DHCP ● IP ROUTING: BGP, OSPF, Routing Policy. ● IPv6 ● VRRP,HSRP ● vrf lite ● Túneles GRE SWITCHING ● 802.1q ● MAC address Management GESTION: ● SSH, SNMP, TACACs, Telnet QoS: ● QoS features. CoS(DSCP)	2 onboard GE(RJ45), 4 EHWIC slots
Cisco 3945		500 Megas	SERVICIOS IP: ● NAT y ACLs ● DHCP	Cisco 3945 w/SPE250 (3GE, 4EHWIC, 4DSP, 4SM, 256MBCF,1GBD

	● IP RAM,IPB) ROUTING : BGP, OSPF, Routing Policy. ● IPv6 ● VRRP,HS RP ● vrf lite ● Túneles GRE SWITCHI NG ● 802.1q ● MAC address Managem ent GESTION: ● SSH, SNMP, TACACs, Telnet QoS: ● QoS features. CoS(DSC P)	

Fuente: elaboración propia

Luego de que la fibra ha sido tendida se realiza la instalación de los equipos, esta actividad es realizada por el personal de STI (PIM) y es solicitada por el área de implementación como una actividad previa.

El personal de STI deja los equipos raqueados y marquillados en el RACK del cliente, envía registro fotográfico (Ver Ilustraciones 5, 6, 7 y 8)

FORMATO ACTA QA INTERNET		
Pertenece al procedimiento: Ejecutar instalación cliente corporativo.	Fecha: 2013-10-16	
Clasificación: Uso Interno.	Pág. **2** de 17	Código **O2.2.5-F02**

EQUIPOS INSTALADOS

TIPO DE EQUIPO	MARCA	MODELO	SERIAL	NUMERO DE PLACA
ROUTER	CISCO	881	FTX174581QC	N/A

EQUIPOS DESINSTALADOS

TIPO DE EQUIPO	MARCA	MODELO	SERIAL	NUMERO DE PLACA
ROUTER	CISCO	881	FTX173583Y6	N/A

Ilustración 6. *Acta de equipos instalados. Tomado de: Documentación área Implementación CLARO S.A.*

REGISTRO FOTOGRAFICO

1- Foto antes de la instalación (400x300 pixeles).

Ilustración 7. *Registro fotográfico antes de la instalación. Tomado de: Documentación área Implementación CLARO S.A.*

2- Foto después de la Instalación (400x300 pixeles).

Ilustración 8. *Registro fotográfico de la instalación. Tomado de: Documentación área Implementación CLARO S.A.*

3- Foto marquillas (400x300 pixeles).

4- Foto tomas eléctricas (400x300 pixeles).

Ilustración 9*. Registro fotográfico equipos marcados y tomas eléctricas. Tomado de: Documentación área Implementación CLARO S.A.*

Después de que lo equipos son marquillados y raqueados, se procede a realizar las pre configuraciones de cada uno de los servicios. Esta tarea es realizada por el área de implementación realizando el plan de trabajo para la migración, para esto los autores del proyecto deben realizar los diagramas de detalle de cada servicio de antes y después de la migración.

5.5 FASE 2. MIGRACIÒN DE SERVICIOS RED ALCATEL

En el desarrollo de la fase 2 Prevención actúa transversalmente con la elaboración de los diagramas de la topología antes de migración de los servicios y después de haber instalado los enlaces en el punto central de una entidad financiera.

5.5.1 Diagramas de detalle red Alcatel antes de migración

Para el área de implementación de servicio es muy importante dejar documentado como se encuentra un servicio y como se deben entregar los servicios. En caso tal de que se deba realizar un rollback.

A continuación se mostraran dos ingenierías de detalle elaboradas y las demás se encontraran como anexos (Ver anexo 1):

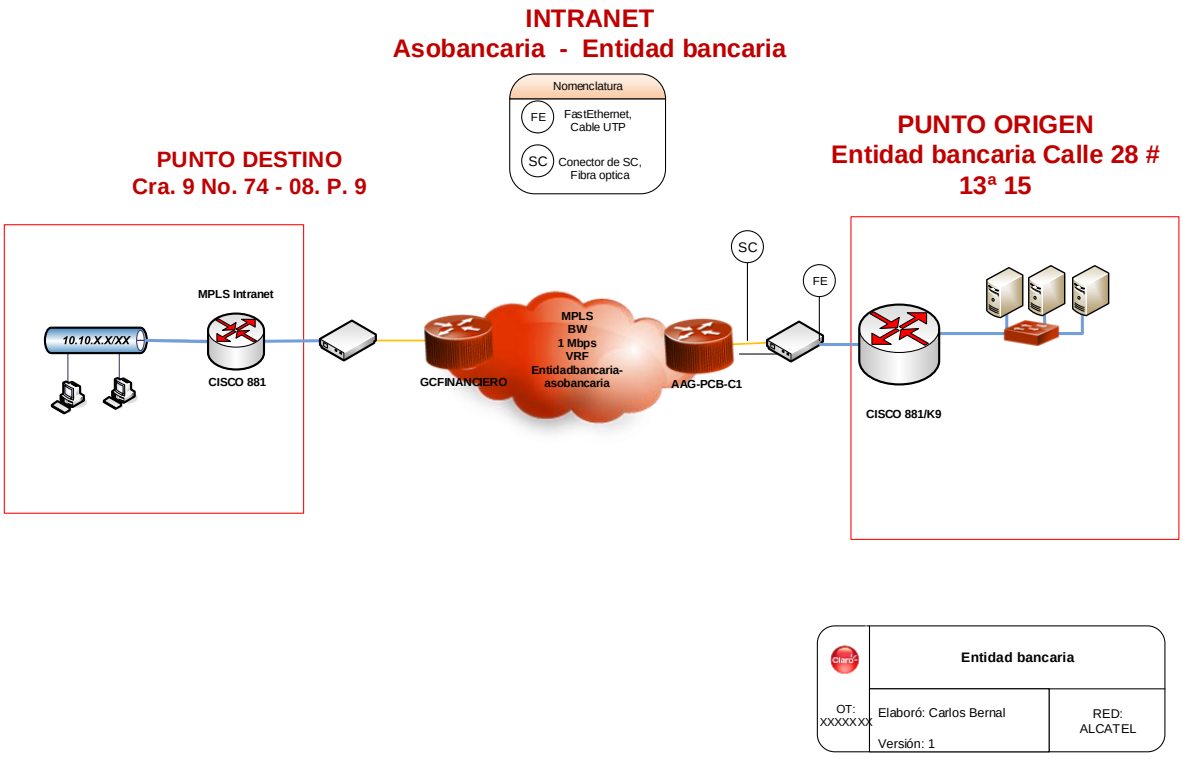


Ilustración 10. *Diagrama de ingeniería red Alcatel antes de migración Asobancaria.*

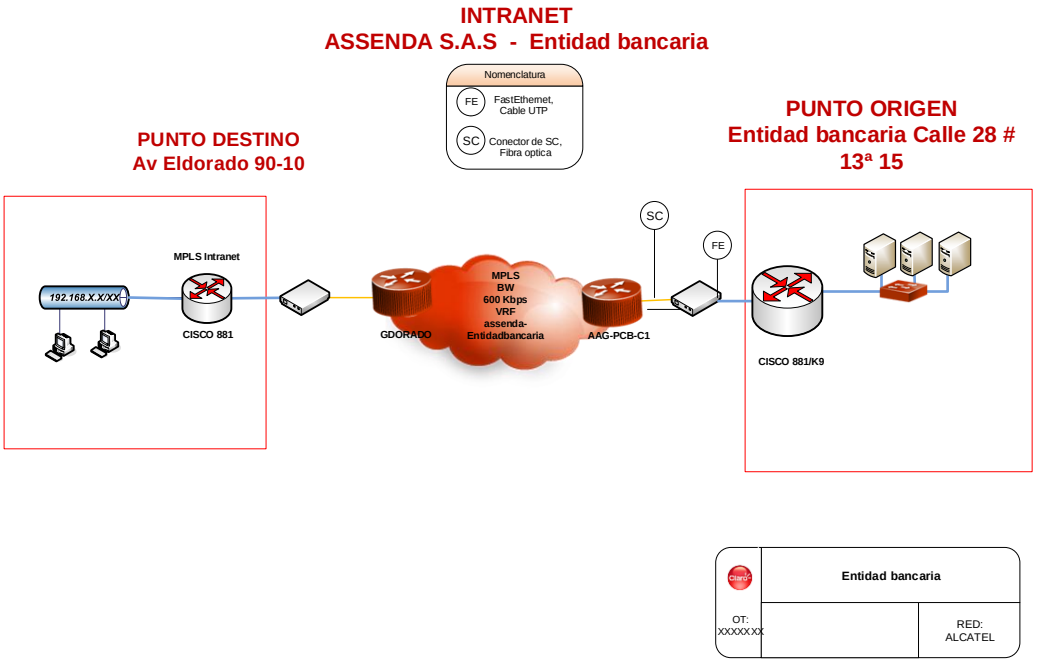


Ilustración 10. *Diagrama de ingeniería red Alcatel antes de migración Assenda S.A.S.*

5.5.2 Migración y configuración

Los permisos de red asignados a los autores del proyecto no eran lo bastante amplios para para ver la red de acceso, según lo que el NOC solicito a soporte corporativo solo realizan los esquemas de detalle de los servicio que se logran ubicar.

5.5.3 Diagramas de detalle migración de servicio Alcatel

El área de aprovisionamiento generó un diagrama de conectividad estándar para el punto central de una entidad financiera.

A continuación se mostraran dos ingenierías de detalle elaboradas y las demás se encontraran como anexos (Ver anexo 2):

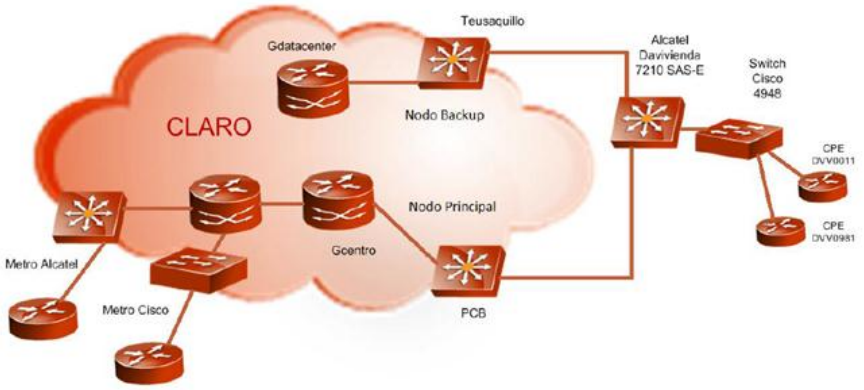


***Ilustración 11**. Diagrama de ingeniería estándar. Tomado de: Documentación área Implementación CLARO S.A.*

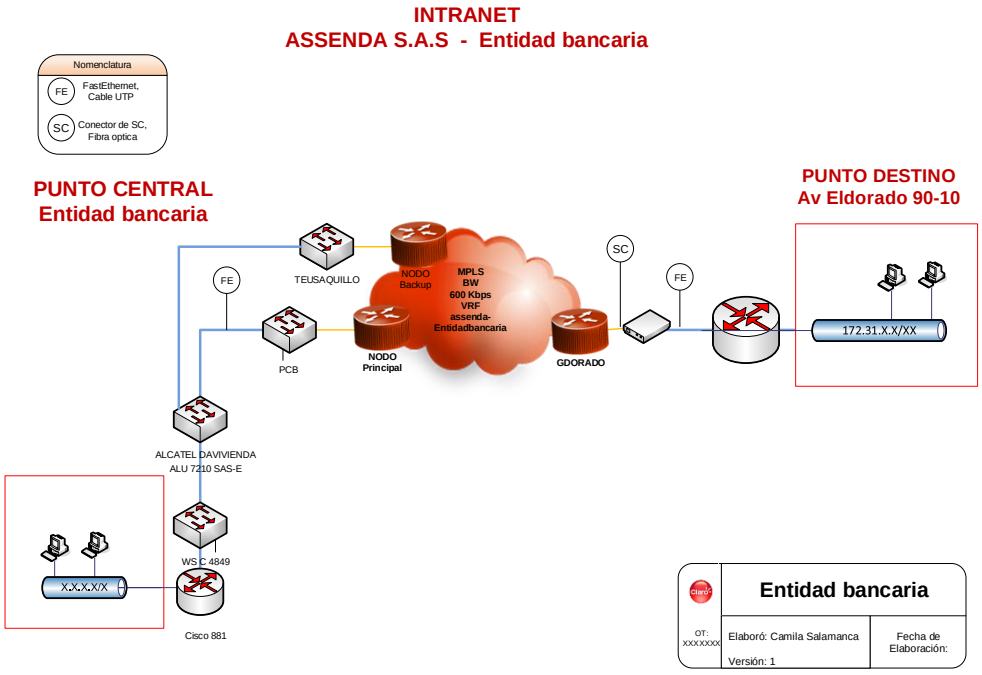


Ilustración 12. *Diagrama de ingeniería actual Assenda S.A.S.*

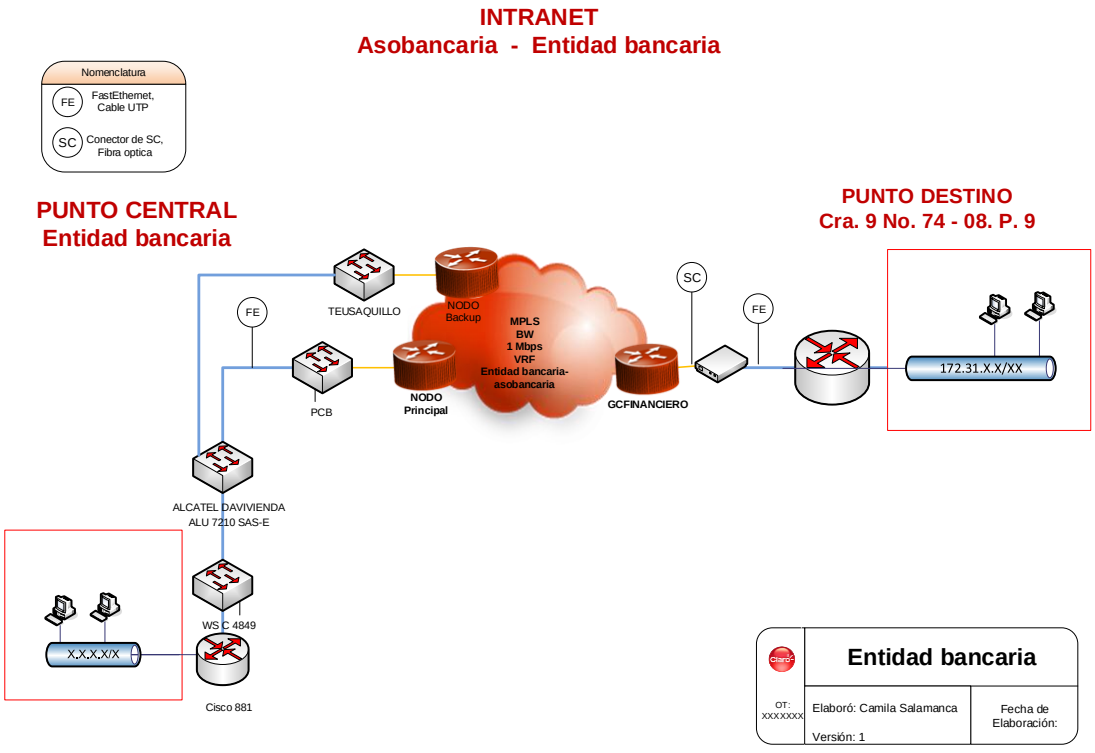


Ilustración 13. *Diagrama de ingeniería actual Asobancaria.*

5.6 FASE 3. MIGRACIÒN DE SERVICIOS RED METRO

5.6.1 Diagramas de detalle antes de migración red metro

Para el área de implementación de servicio es muy importante dejar documentado como se encuentra un servicio y como se deben entregar los servicios. En caso tal de que se deba realizar un rollback.

Los diagramas de detalles están estandarizados por el área de aprovisionamiento para un mejor entendimiento de las áreas.

Se expondrán dos esquemas de ingeniería y se podrán visualizar los restantes en la parte de anexos (ver anexo 3).

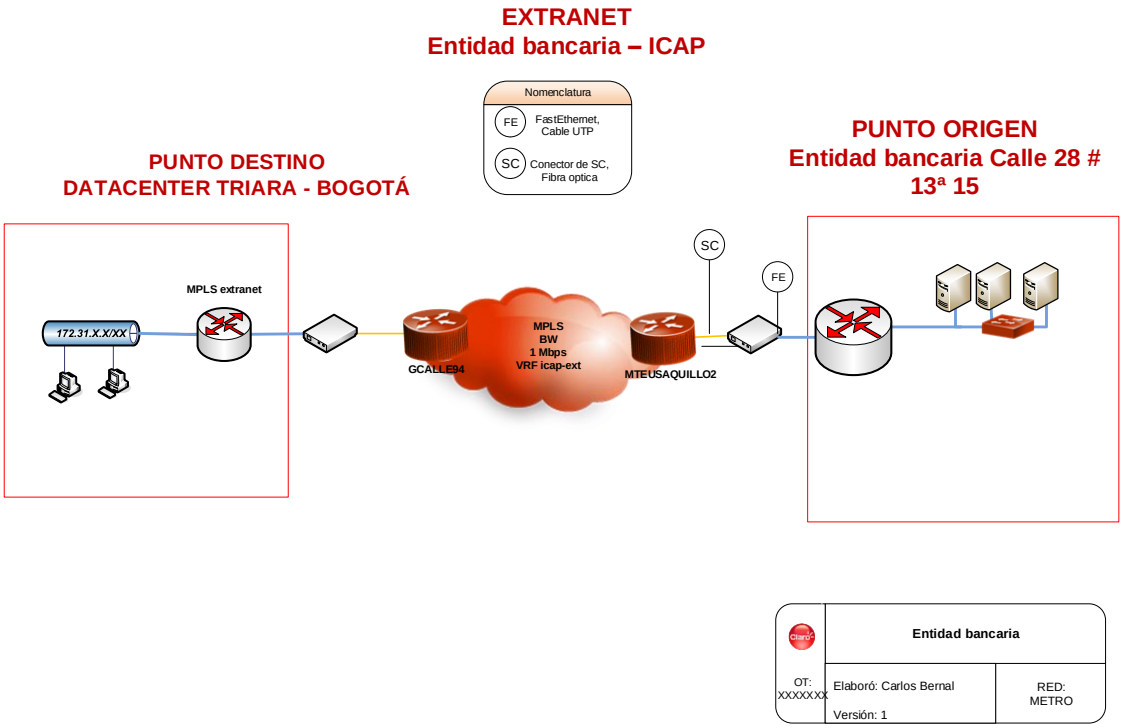


Ilustración 14. *Diagrama de ingeniería extranet entidad financiera – Icap antes.*

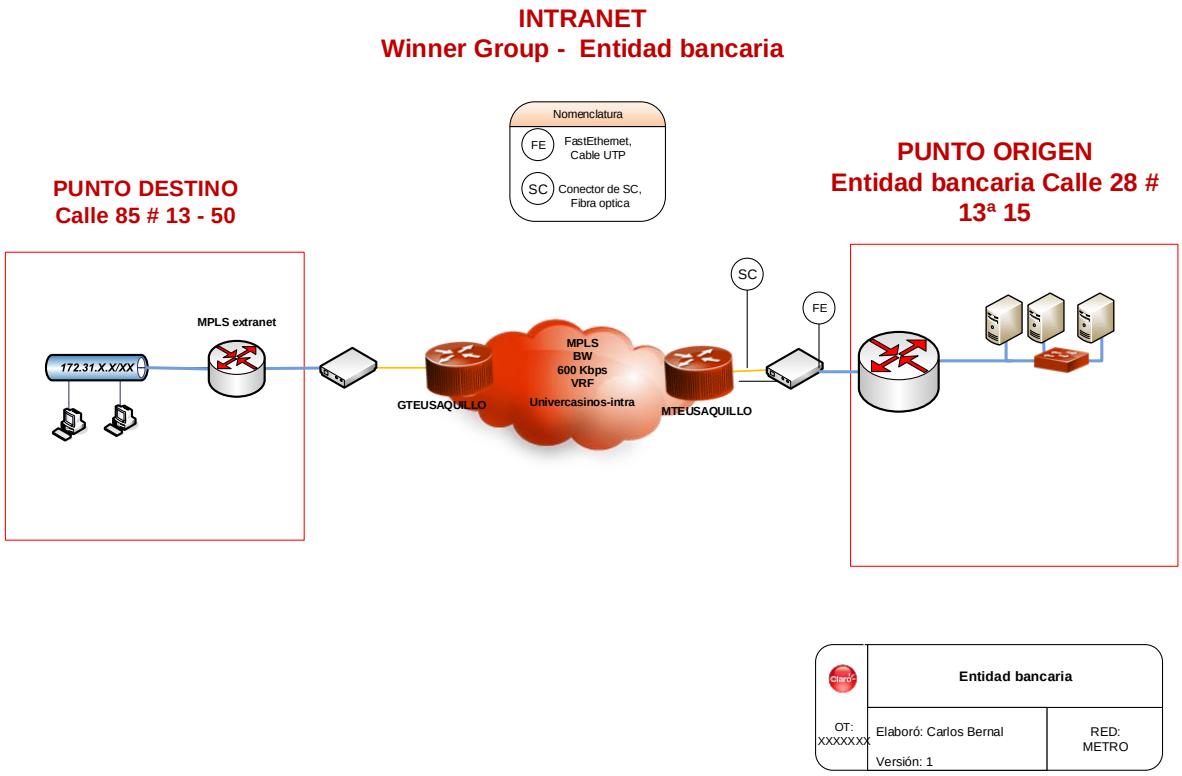


Ilustración 15. *Diagrama de ingeniería extranet entidad financiera – Winner Group antes.*

5.6.2 Migración y configuración

Los permisos de red asignados a los autores del proyecto no eran lo bastante amplios para para ver la red de acceso, según lo que el NOC solicito a soporte corporativo, solo realizan los esquemas de detalle de los servicio que se logran ubicar.

5.6.3 Diagramas de detalle migración de servicio metro

El área de aprovisionamiento ya había generado un diagrama de conectividad estándar para el punto central de una entidad financiera (Ver ilustración 11).

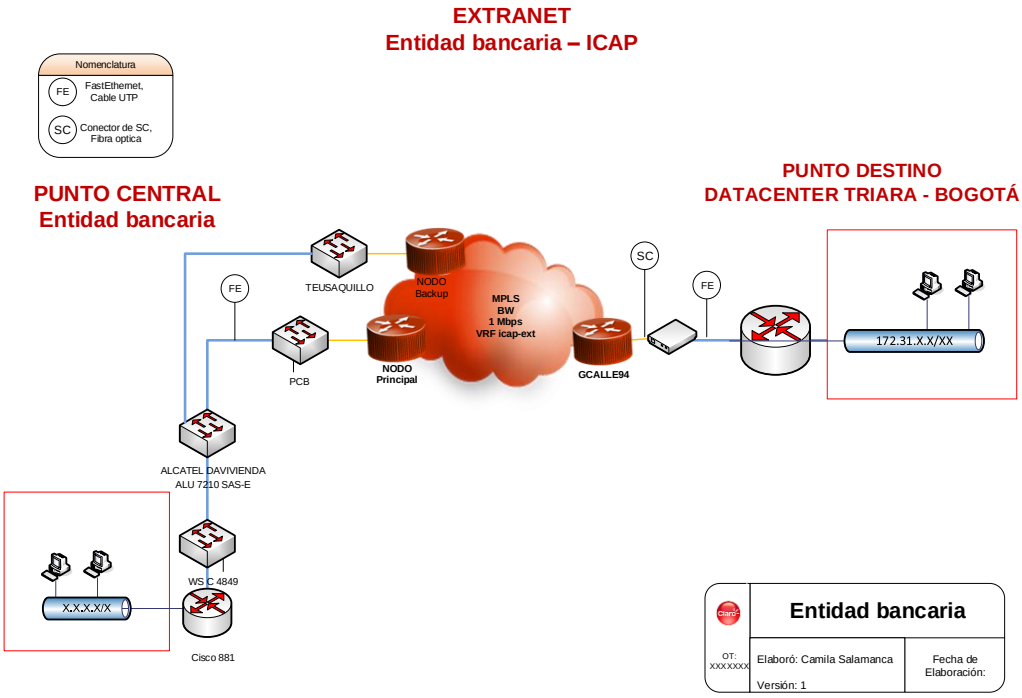


Ilustración 16. *Diagrama de ingeniería extranet actual entidad financiera – ICAP*

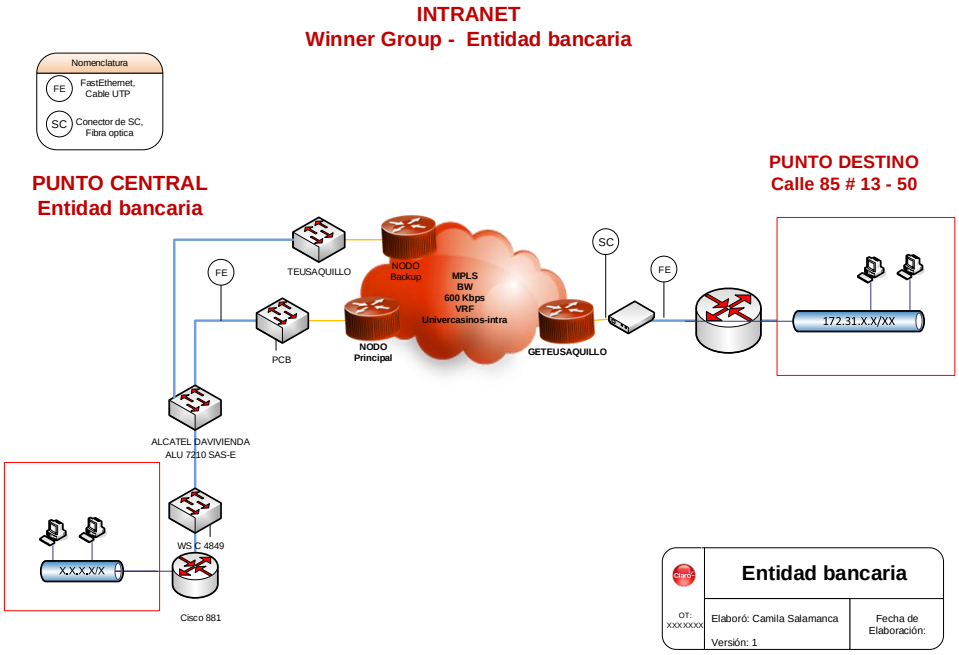


Ilustración 17*. Diagrama de ingeniería extranet actual entidad financiera – Winner Group.*

5.7 FASE 4. PRUEBAS DE BACKUP

La última fase que se realizó en el plan de acción para la organización y el orden del datacenter del punto central de una entidad financiera, fue la ejecución de pruebas de backup.

Dentro de ésta fase se elaboraron diferentes tareas como las verificaciones de las configuraciones de los canales principales y de contingencia, según los parámetros establecidos por CLARO S.A. al brindar un servicio de backup según sea la topología implementada, la creación de scripts los cuales se utilizan para documentar todo lo realizado en el desarrollo de las pruebas y la ejecución de pruebas de contingencia, en las que se comprueba con el cliente final la correcta conmutación del canal backup.

Lo anterior se explicará de acuerdo al orden en que se ejecutó esta fase y para esto, se describirá el proceso en cuatro partes en las que se expresará lo realizado:

1. Topologías de canales con redundancia.
2. Procedimiento para realizar pruebas.
3. Verificación de la configuración de los canales.
4. Ejecución de pruebas de backup.

5.7.1 Topologías de canales con redundancia

Claro S.A. ofrece a sus clientes servicios redundantes, con el fin de garantizar la continuidad del negocio y la alta disponibilidad en una empresa y prevenir en el momento que se presente algún tipo de fallas en el canal principal, tales como ruptura de fibra óptica, fallas eléctricas en la sede, daño de equipos (Transceiver o Router), saturación del servicio principal, entre otras.

Este tipo de servicios redundantes consisten en entregar al cliente dos servicios idénticos, soportados bajo la red MPLS de CLARO S.A con las mismas características y configuraciones de acuerdo a la topología implementada, para que cuando falle el enlace primario entre en funcionamiento el backup conmutando todo el tráfico saliente y entrante por este garantizando al cliente conectividad en su empresa.

Existen tres tipos de topologías que se implementan en escenarios con backup en CLARO S.A:

5.7.1.1 Dos últimas millas - un router (cpe)

Éste escenario ofrecido al cliente consiste en que se instala un único equipo router al que llegarán dos tendidos de fibras distribuidos por caminos diferentes desde el GSR (Nodo) hasta el router (llamado CPE en CLARO S.A). Se llama última milla (UM) al recorrido del tramo de fibra óptica desde el equipo de la red de acceso hasta la sede del cliente.

5.7.1.2 Dos últimas millas - dos routers (cpe)

Esta topología, se conforma con dos equipos routers conectados a dos últimas millas que llegan desde el nodo o GSR de la red de CLARO S.A.
La necesidad de colocar dos enrutadores como CPE´s, consiste en garantizar un backup tanto a nivel de última milla como de equipo GSR, por lo tanto, si el CPE principal tiene problemas, el de backup entraría a ser el default Gateway de la red LAN. Para que el default Gateway de la red LAN sea el mismo sin importar que CPE sea el que está enrutando se debe configurar HSRP entre los dos enrutadores. Adicionalmente, se debe garantizar que no se pierda enrutamiento entre ambos enrutadores para

poder alcanzar las redes destino; para este fin se utiliza el protocolo BGP tanto a nivel WAN (eBGP) como a nivel LAN (iBGP).

5.7.1.3 Un router (cpe) - una última milla (canal principal o backup con otro proveedor)

Éste escenario se conforma a través de la red de dos proveedores de telecomunicaciones (CLARO S.A y otro), uno de los dos proporcionará el canal principal por medio de su red MPLS con una última milla y un equipo router, en que tendrá configurado el protocolo HSRP o VRRP y el enrutamiento necesario para la conmutación, ya sea que funcione como canal principal o backup.

Es importante tener en cuenta que los dos proveedores deben conocerse a nivel de direccionamiento y enrutamiento, para poder garantizar la conectividad del cliente en caso de falla en el canal principal.

5.7.2 Procedimiento para realizar pruebas de backup

Con el objetivo de garantizar el correcto funcionamiento de los servicios de backup en CLARO S.A, se establecen políticas creadas para soportar solicitudes sobre servicios de backup, aplicadas desde la solicitud realizada por el cliente o la detección interna de la necesidad de programar pruebas a los servicios de backup estándar para la red MPLS[1]. A continuación se mostrara Ilustración en la que se describe el procedimiento para realizar pruebas de backup.

[1] Prevención Corporativo (2013). Políticas para soportar solicitudes pruebas de backup. Claro S.A.

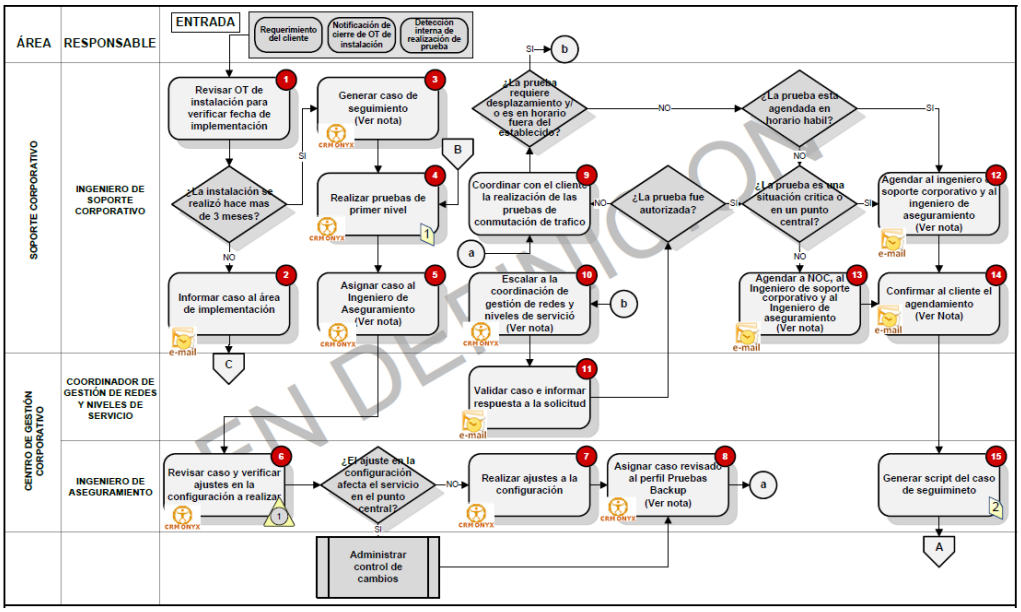


Ilustración 18. *Diagrama de políticas para realizar pruebas de backup. Tomado de: Documento políticas para soportar solicitudes pruebas de backup CLARO S.A*

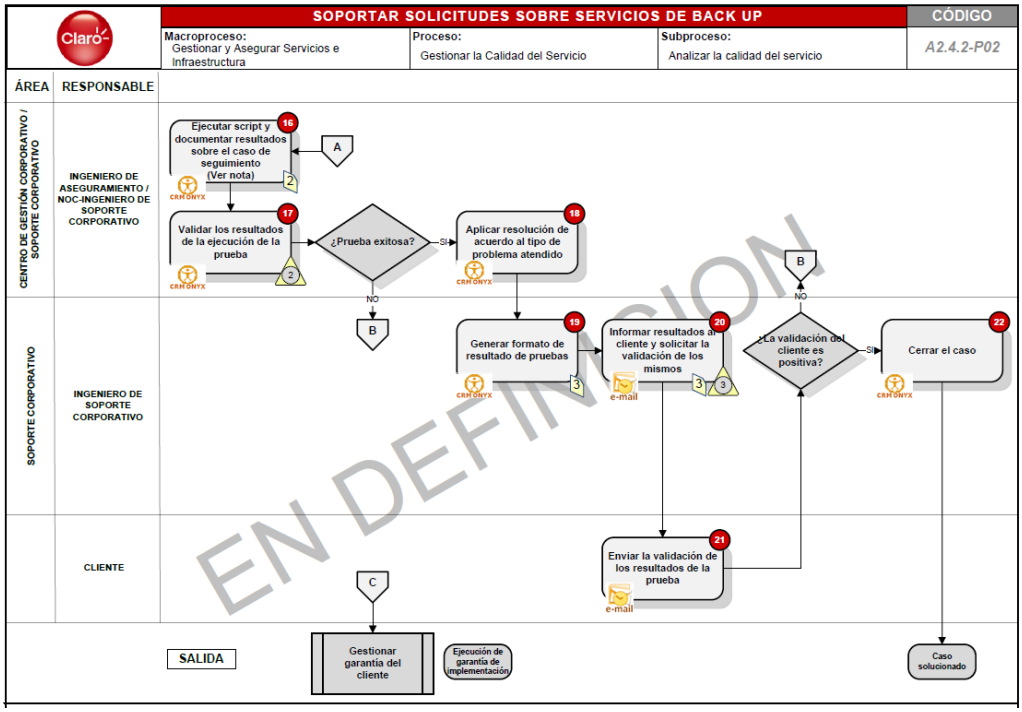


Ilustración 19. *Diagrama de políticas para realizar pruebas de backup. Tomado de: Documento políticas para soportar solicitudes pruebas de backup CLARO S.A*

En resumen a la Ilustración anterior para ejecutar una prueba de contingencia se debe realizar el siguiente proceso:

1. Se recibe solicitud para realizar pruebas de backup por el cliente ya sea por medio del área de soporte corporativo, cuidado al cliente, ingenieros de gestión de red o el área comercial.
2. Verificación de los canales principales y backup, de acuerdo a la topología que tenga el cliente para asegurar el correcto funcionamiento por parte de los ingenieros del área de prevención.
3. Crear script en el que se evidencie la revisión de los canales y procedimiento para la ejecución las pruebas.
4. Se genera Caso de Seguimiento (Reporte en el que se documenta las validaciones, correcciones y ejecución de pruebas).
5. Responder solicitud del cliente para coordinar pruebas en donde se indique fecha, hora y datos de contacto del cliente que realizará pruebas en conjunto con CLARO S.A.
6. Ejecución de pruebas de backup en la fecha y hora acordada previamente.

5.7.3 Verificación de configuración de canales

En el momento que se recibe una solicitud para ejecución de pruebas de contingencia, lo primero que se debe realizar es la verificación de la configuración de los canales principal y backup de acuerdo a la topología asignada.

Al iniciar el plan de acción del punto central de DAVIVIENDA, se evidenció que en el área de Prevención no se contaba con un estándar en el que se estipulara el proceso, al verificar las configuraciones para servicios redundantes que ofrece CLARO S.A a sus clientes. De acuerdo a esto, los autores de éste informe definieron un script con los pasos a seguir para comprobar la correcta configuración de los enlaces.

Para poder mostrar las verificaciones realizadas antes de ejecutar las pruebas, se tomó como ejemplo 2 casos de seguimiento de los 27 realizados que se explicaran a continuación:

Script 1:

Tabla 6. *Información script 1 (enlaces principal – backup, topología y protocolo).*

PRINCIPAL	BACKUP	TOPOLOGIA	PROTOCOLO
CIM0072	CIM0068	2 UM – 2 CPE	HSRP

- Verificaciones canal principal :

1. Se localiza el servicio: Para encontrar el servicio es necesario ingresar al equipo GSR (nodo) con el comando *ssh (nombre nodo)*. Al encontrarse en el GSR se debe ubicar el servicio digitando *show ip vrf | i (nombre vrf, #vlan o ip wan del servicio)*

```
GCALLE94#sh ip vrf int | i icap-ext
Gi1/0/3.105            10.161.98.157   icap-ext                        up
GCALLE94#
GCALLE94#sh run int Gi1/0/3.105
Building configuration...

Current configuration : 315 bytes
!
interface GigabitEthernet1/0/3.105
 description IPDP ICAP KR 11 EXTRANET - CIM0072,CC0029
 encapsulation dot1Q 105
 ip vrf forwarding icap-ext
 ip address 10.161.98.157 255.255.255.252
 no ip directed-broadcast
 ip accounting mac-address output
 service-policy input CAR-1024
 service-policy output CAR-1024
end
```

Ilustración 20. *Ubicación del enlace principal en el GSR (nodo) en la red de CLARO S.A.*

2. Se valida operatividad del servicio: se realiza prueba de ping hacia el router del cliente utilizando el comando *ping vrf (nombre vrf) ip WAN router.*

```
GCALLE94#ping vrf icap-ext 10.161.98.158

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.161.98.158, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Ilustración 21. *Validación de conectividad desde el GSR al equipo router del cliente.*

3. Se valida protocolo BGP y Router Target (RT): Se revisa la configuración de la vrf del servicio con el comando *Show run vrf (nombre vrf)*.
   Nota: Se deben configurar los mismos RT en el canal principal y backup.

```
GCALLE94#sh run vrf icap-ext
Building configuration...

Current configuration : 1173 bytes
ip vrf icap-ext
 rd 100:3293
 export map ARCOM-LAN-EXT
 route-target export 14080:2190000003
 route-target import 14080:207500
 route-target import 14080:337900
 route-target import 14080:2190000002
!
!
!
router bgp 14080
!
address-family ipv4 vrf icap-ext
 redistribute connected
 redistribute static
 neighbor 10.161.98.158 remote-as 65535
 neighbor 10.161.98.158 description EXTRANET_SUPERFI
 neighbor 10.161.98.158 activate
 neighbor 10.161.98.158 remove-private-as
 neighbor 10.161.98.158 maximum-prefix 50 20 restart 2
 maximum-paths import 2
 no synchronization
 exit-address-family
!
```

Ilustración 22*. Validación de Router Target (import – export).*

4. Se validan las redes que aprende el canal principal: Es necesario saber que rutas aprende el canal principal para comparar con lo que aprende el canal backup ya que debe ser lo mismo. Se utiliza el comando *Show ip bgp vpnv4 vrf (nombre vrf) neighbors (ip wan router) routes.*

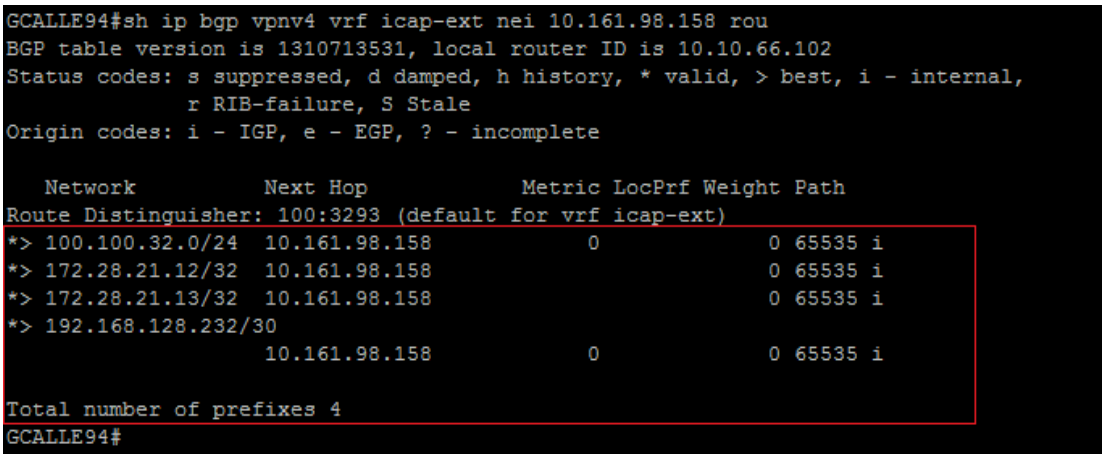


Ilustración 23. *Rutas que aprende el servicio principal.*

5. Se ingresa al router del cliente usando *telnet (ip wan router) /vrf (nombre vrf)*

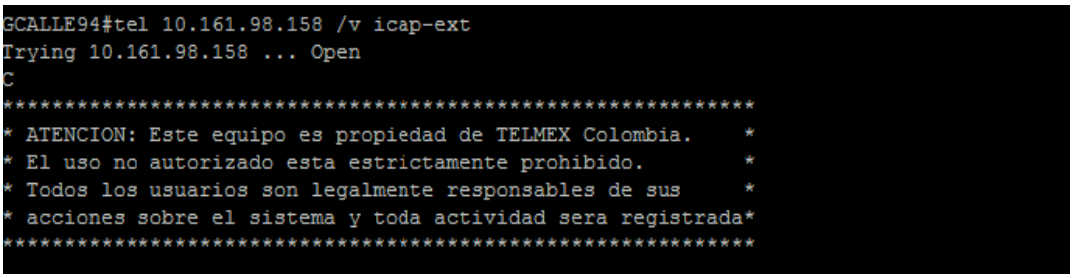


Ilustración 24. *Ingreso al router cliente.*

6. Se verifican interfaces: se valida configuración de interfaces WAN y LAN del servicio con ayuda del comando *Show run interfaz (# interfaz).*En la configuración de la interfaz LAN si se tiene configurado el protocolo HSRP se debe tener en cuenta los siguientes parámetros:

   - Se debe tener el mismo grupo configurado.
   - Se debe asignar una mayor prioridad que la configurada en el canal backup para que se identifique como router activo.
   - Se debe tener configurado el parámetro *prempt* ya que es el que determina que router es el principal.
   - Se debe configurar *track* el cual censará la interfaz WAN del canal principal con un decremento el que determine que cuando exista una

falla en el canal principal el respaldo pueda pasar a ser activo debido a que quedara con una prioridad más alta.

```
CIMD_CIMD0012,13,45,53,61,72,CC0003,15,29#sh run int Gi0/0.200
Building configuration...

Current configuration : 471 bytes
!
interface GigabitEthernet0/0.200
 description --- LAN ICAP SECURITIES ---
 encapsulation dot1Q 200
 ip vrf forwarding datos-icap
 ip address 192.168.250.1 255.255.255.0 secondary
 ip address 100.100.32.25 255.255.255.0
 ip helper-address 100.100.32.248
 ip nbar protocol-discovery
 ip flow ingress
 ip flow egress
 ip nat inside
 no ip virtual-reassembly in
 standby 10 ip 100.100.32.2
 standby 10 priority 120
 standby 10 preempt
 standby 10 track 1 decrement 30
end
```

Ilustración 25. *Configuración interfaz LAN servicio principal.*

```
CIMD_CIMD0012,13,45,53,61,72,CC0003,15,29#sh run int GigabitEthernet0/1.105
Building configuration...

Current configuration : 235 bytes
!
interface GigabitEthernet0/1.105
 description --- WAN EXTRANET PPAL - CIM0072,CC0029 ---
 encapsulation dot1Q 105
 ip vrf forwarding datos-icap
 ip address 10.161.98.158 255.255.255.252
 ip nat outside
 ip virtual-reassembly in
end
```

Ilustración 26. *Configuración interfaz WAN servicio principal.*

7. Protocolo HSRP: se verifica la configuración del protocolo de redundancia de router. Se indica *Show standby brief,* se mostrará el equipo al que se ingresa como local, se observa ip virtual, router activo y standby.

```
CIMD_CIMD0012,13,45,53,61,72,CC0003,15,29#sh stand br
                    P indicates configured to preempt.
                    |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gi0/0.66    66   100 P Standby 10.10.0.5       local           10.10.0.3
Gi0/0.200   10   120 P Active  local           100.100.32.26   100.100.32.2
Gi0/0.210   210  110 P Init    unknown         unknown         172.20.68.65
Gi0/0.300   30   120 P Active  local           192.168.10.2    192.168.10.1
V12         20   120 P Active  local           190.144.195.67  190.144.195.65
```

Ilustración 27. *Configuración protocolo HSRP canal principal.*

8. Se valida configuración BGP e IBGP en el router: Se utilizan los comandos *Show run | i sección bgp y Show ip bgp summary.* Se realiza esta verificación para evidencias que se tenga configurado IBGP en caso de que falle el protocolo HSRP.

```
 neighbor 10.161.98.157 distribute-list SUFINANCIERA out
 neighbor 100.100.32.26 remote-as 65535
 neighbor 100.100.32.26 activate
 neighbor 100.100.32.26 route-map BACKUP in
exit-address-family
```

Ilustración 28. *Configuración protocolo BGP e IBGP equipo router.*

```
CIMD_CIMD0012,13,45,53,61,72,CC0003,15,29#sh ip bgp summ
BGP router identifier 201.232.120.35, local AS number 65535
BGP table version is 14314836, main routing table version 14314836
19865 network entries using 2940020 bytes of memory
39656 path entries using 2537984 bytes of memory
1932/591 BGP path/bestpath attribute entries using 262752 bytes of memory
581 BGP AS-PATH entries using 33756 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 5774512 total bytes of memory
BGP activity 1853469/1833439 prefixes, 7182870/7142924 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.160.47.205   4        14080  676021  708254 14314836    0    0 11w1d         745
10.161.28.125   4        14080  129763  123691 14314836    0    0 11w1d         386
10.161.162.161  4        14080 2396923 2128950 14314836    0    0 33w3d       19044
190.144.195.67  4        65535 4188231 4349549 14314836    0    0 1y6w        19480
```

Ilustración 29. *Validación de estado protocolo BGP.*

9. Se observa si existen rutas estáticas: se deben tener configuradas las mismas rutas estáticas en el canal principal y el backup. Se validan con el comando *Show run | i ip route*

```
CIMD_CIMD0012,13,45,53,61,72,CC0003,15,29#sh run | i ip rou
ip route 100.100.50.0 255.255.255.0 190.144.195.74
ip route vrf autoreguladores-icap 0.0.0.0 0.0.0.0 10.161.79.117
ip route vrf autoreguladores-icap 100.100.32.250 255.255.255.255 10.0.250.4
ip route vrf autoreguladores-icap 100.100.32.252 255.255.255.255 10.0.250.4
ip route vrf datos-icap 0.0.0.0 0.0.0.0 100.100.32.58 name INTERNET_ASA
ip route vrf datos-icap 10.172.16.163 255.255.255.255 GigabitEthernet0/0.200 100.100.32.4
ip route vrf datos-icap 10.210.27.0 255.255.255.0 100.100.32.220 name CRCC_MERCADO_TELMEX
ip route vrf datos-icap 10.210.28.0 255.255.255.0 100.100.32.220 name CRCC_MERCADO_TELMEX
ip route vrf datos-icap 10.240.245.0 255.255.255.0 10.192.147.1 name Monitoreo_BVC
ip route vrf datos-icap 10.240.246.0 255.255.255.0 10.224.147.1 name SET-FX
ip route vrf datos-icap 10.240.248.0 255.255.255.0 10.192.147.1 name MEC_BackOffice
ip route vrf datos-icap 10.240.250.0 255.255.255.0 10.224.147.1 name Red_Monitoreo_BVC
ip route vrf datos-icap 10.240.251.0 255.255.255.0 10.224.147.1 name SET-FX
ip route vrf datos-icap 10.240.252.0 255.255.255.0 10.192.147.1 name MEC_BackOffice
ip route vrf datos-icap 10.240.253.0 255.255.255.0 10.192.147.1 name MEC_Plus_(SIOPEL)
ip route vrf datos-icap 10.244.138.0 255.255.255.0 10.161.7.237
ip route vrf datos-icap 10.244.170.0 255.255.255.0 10.161.7.237
ip route vrf datos-icap 10.244.171.0 255.255.255.0 10.161.7.237
ip route vrf datos-icap 172.22.16.93 255.255.255.255 10.161.7.237
ip route vrf datos-icap 172.22.71.19 255.255.255.255 10.161.7.237
ip route vrf datos-icap 172.22.71.21 255.255.255.255 10.161.7.237
ip route vrf datos-icap 172.22.88.0 255.255.255.0 10.161.7.237 name VPN_SSl
ip route vrf datos-icap 172.22.192.4 255.255.255.255 10.161.7.237 name GESTION_ACS
ip route vrf datos-icap 172.22.192.5 255.255.255.255 10.161.7.237 name GESTION_ACS
ip route vrf datos-icap 172.31.238.0 255.255.255.0 10.161.7.237 name GESTION_ASA
ip route vrf datos-icap 172.31.239.53 255.255.255.255 10.161.7.237
ip route vrf datos-icap 172.31.239.70 255.255.255.255 10.161.7.237
ip route vrf datos-icap 172.31.245.0 255.255.255.248 10.161.7.237
ip route vrf datos-icap 192.168.150.0 255.255.255.0 10.161.7.237
```

Ilustración 30. *Rutas estáticas servicio principal.*

- Verificaciones canal Backup:

En esta parte, se describirán las revisiones que se realizaron en el canal backup pero no se indicaran los comandos utilizados ya que son los mismos que se mencionaron anteriormente.

1. Se localiza el servicio:

```
GCHICO#sh ip vrf int | i icap-ext
Gi2/3.216             10.161.107.53   icap-ext                       up
GCHICO#sh run int Gi2/3.216
Building configuration...

Current configuration : 307 bytes
!
interface GigabitEthernet2/3.216
 description IPDP ICAP SECURITIES COLOMBIA S.A. EXTRANET SUPERFINANCIERA - CIM0068
 encapsulation dot1Q 216
 ip vrf forwarding icap-ext
 ip address 10.161.107.53 255.255.255.252
 no ip directed-broadcast
 service-policy input CAR-1024
 service-policy output CAR-1024
end
```

Ilustración 31. *Ubicación del enlace Backup en el GSR (nodo) en la red de CLARO S.A.*

2. Se valida operatividad del servicio:

```
GCHICO#ping vrf icap-ext 10.161.107.54

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.161.107.54, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Ilustración 32. *Validación de conectividad desde el GSR al equipo router del cliente.*

3. Se valida protocolo BGP y Router Target (RT): Se debe validar que los RT que está exportando e importando el canal backup son lo mismo que los del principal.

```
GCHICO#sh run vrf icap-ext
Building configuration...

Current configuration : 911 bytes
ip vrf icap-ext
 rd 100:3293
 export map ASP
 route-target import 14080:207500
 route-target import 14080:337900
!
!
!
router bgp 14080
!
address-family ipv4 vrf icap-ext
 neighbor 10.161.107.54 remote-as 65535
 neighbor 10.161.107.54 description SIF GARBAN COLOMBIA BACKUP
 neighbor 10.161.107.54 activate
 neighbor 10.161.107.54 route-map BACKUP in
 neighbor 10.161.107.54 maximum-prefix 40 90 restart 2
 no synchronization
 exit-address-family
!
```

Ilustración 33. *Validación de Router Target (import – export)*

4. Se validan las redes que aprende el canal principal: Se verifica que el canal backup aprenda las mismas rutas que el canal principal.

```
GCHICO#sh ip bgp vpnv4 vrf icap-ext nei 10.161.107.54 rou
BGP table version is 148651947, local router ID is 10.10.66.104
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:3293 (default for vrf icap-ext)
*> 100.100.32.0/24  10.161.107.54            0     50      0 65535 i
*> 192.168.128.232/30
                    10.161.107.54            0     50      0 65535 i

Total number of prefixes 2
```

Ilustración 34. *Rutas que aprende el servicio backup.*

5. Se ingresa al router del cliente:

```
GCHICO#telnet 10.161.107.54 /v icap-ext
Trying 10.161.107.54 ... Open
CC
**************************************************************************
* ATENCION: Este equipo es propiedad de TELMEX Colombia.                 *
* El uso no autorizado esta estrictamente prohibido.                     *
* Todos los usuarios son legalmente responsables de sus                  *
* acciones sobre el sistema y toda actividad sera registrada             *
**************************************************************************
```

Ilustración 35. *Ingreso al router cliente.*

6. Se verifican interfaces: se verifica que la prioridad del canal backup quede como activo según el decremento y la prioridad del principal en el momento que esté presente falla.
   Se debe tener configurado el parámetro prempt y la no se asume prioridad del canal de 100 por defecto.

```
ICAP_CIM0068,CC0003,15,29#sh run int GigabitEthernet0/1.216
Building configuration...

Current configuration : 207 bytes
!
interface GigabitEthernet0/1.216
 description --- WAN EXTRANET BACKUP - CIM0068,CC0029 ---
 encapsulation dot1Q 216
 ip address 10.161.107.54 255.255.255.252
 ip nat outside
 ip virtual-reassembly in
end
```

Ilustración 36. *Configuración interfaz WAN servicio principal.*

```
ICAP_CIM0068,CC0003,15,29#sh run int GigabitEthernet0/0.200
Building configuration...

Current configuration : 329 bytes
!
interface GigabitEthernet0/0.200
 description --- LAN INTRANET - CIM0068 ---
 encapsulation dot1Q 200
 ip address 192.168.250.1 255.255.255.0 secondary
 ip address 100.100.32.26 255.255.255.0
 ip flow ingress
 ip nat inside
 ip virtual-reassembly in
 standby 10 ip 100.100.32.2
 standby 10 preempt
 standby 10 name BACKUP
end
```

Ilustración 37. *Configuración interfaz LAN servicio principal.*

7. Protocolo HSRP:

```
ICAP_CIM0068,CC0003,15,29#sh stand br
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gi0/0.2     20   100 P Standby 190.144.195.66  local           190.144.195.65
Gi0/0.66    66   110 P Active  local           10.10.0.4       10.10.0.3
Gi0/0.200   10   100 P Standby 100.100.32.25   local           100.100.32.2
Gi0/0.210   210  100 P Active  local           unknown         172.20.68.65
Gi0/0.300   30   100 P Standby 192.168.10.4    local           192.168.10.1
```

Ilustración 38. *Configuración protocolo HSRP canal principal.*

8. Se valida configuración BGP e IBGP en el router: Se observa que se conoce el canal principal por IBGP.

```
 neighbor 10.161.107.53 distribute-list SUFINANCIERA out
 neighbor 100.100.32.25 remote-as 65535
 neighbor 100.100.32.25 description IBGP ROUTER PPAL
 neighbor 100.100.32.25 next-hop-self
 neighbor 100.100.32.25 distribute-list INTRANET out
 neighbor 100.100.32.25 route-map BACKUP in
 !
```

Ilustración 39. *Configuración protocolo BGP e IBGP equipo router.*

Se observa si existen rutas estáticas: se deben tener configuradas las mismas rutas estáticas en el canal principal y el backup. Se validan con el comando *Show run | i ip route*

```
ICAP_CIM0068,CC0003,15,29#sh run | i ip rou
ip route 0.0.0.0 0.0.0.0 100.100.32.58 name INTERNET_ASA
ip route 10.160.47.205 255.255.255.255 190.144.195.66
ip route 172.28.21.12 255.255.255.255 Null0
ip route 172.28.21.13 255.255.255.255 Null0
```

Ilustración 40. *Rutas estáticas servicio Backup.*

Al finalizar las verificaciones pertinentes de los canales se realiza un cuadro comparativo de los parámetros revisados de cada servicio para poder determinar que el canal conmutara de manera correcta cuando se ejecuten las pruebas de backup.

Tabla 7. *Cuadro comparativo configuraciones canal principal y backup.*

VERFICACIÒN	PRINCIPAL	BACKUP
La vrf exporta e importa lo mismo en ambos nodos	OK	OK
Se aprenden las mismas rutas en ambos nodos	OK	OK
Protocolo HSRP	OK	OK
Ip virtual	OK	OK
Hay rutas estáticas	OK	OK
Configuración interfaces	OK	OK
Prioridad y decremento	110 – 30	100

Fuente: elaboración propia

Script 2:

- Verificaciones canal principal:

Tabla 8. *Información script 2 (enlaces principal – backup, topología y protocolo).*

PRINCIPAL	BACKUP	TOPOLOGIA	PROTOCOLO
UDQ0007	UDQ0025	2 UM – 1 CPE	BGP

1. Se localiza el servicio: Para encontrar el servicio es necesario ingresar al equipo GSR (nodo) con el comando *ssh (nombre nodo)*. Al encontrarse en el GSR se debe ubicar el servicio digitando *show ip vrf | i (nombre vrf, #vlan o ip wan del servicio)*

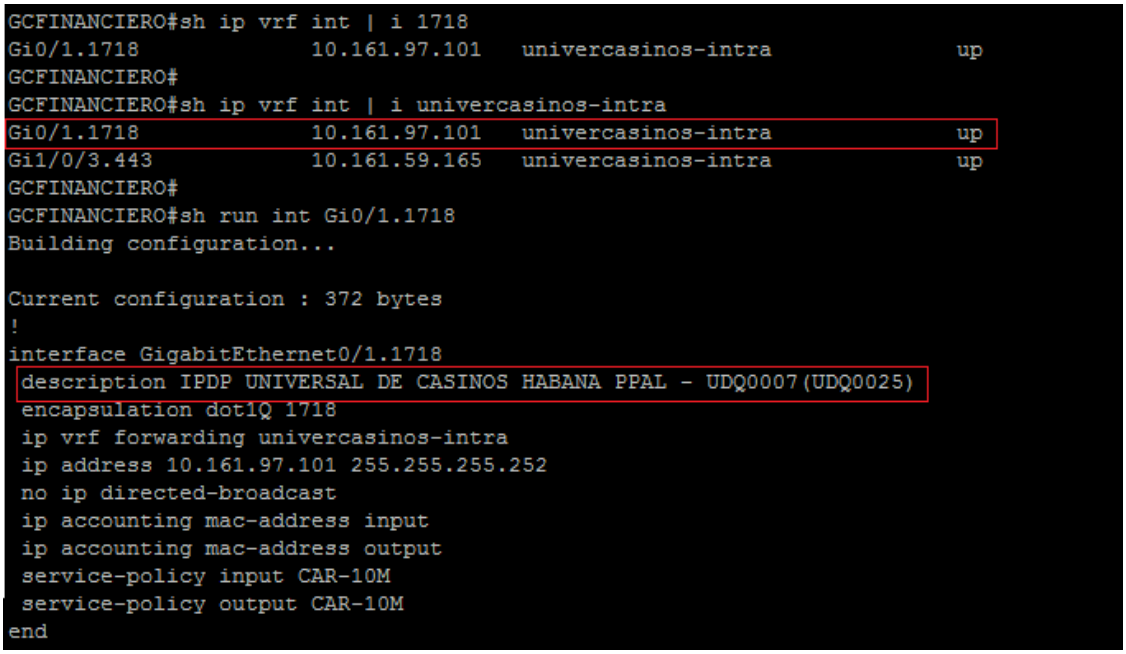


Ilustración 41. *Ubicación del enlace principal en el GSR (nodo) en la red de CLARO S.A.*

2. Se valida operatividad del servicio: se realiza prueba de ping hacia el router del cliente utilizando el comando *ping vrf (nombre vrf) ip wan router*

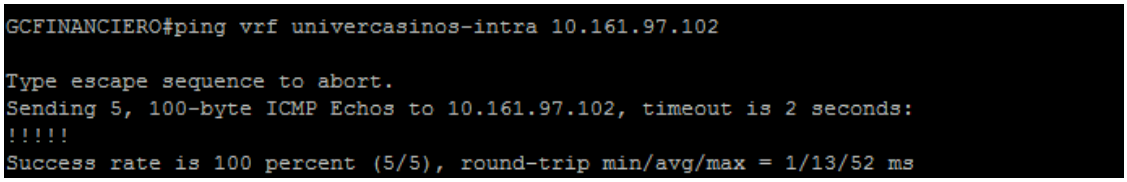


Ilustración 42. *Validación de conectividad desde el GSR al equipo router del cliente.*

3. Se valida protocolo BGP y Router Target (RT): Se revisa la configuración de la vrf del servicio con el comando *Show run vrf (nombre vrf)*.

Nota: Se deben configurar los mismos RT en el canal principal y backup ya que se tiene que importar y exporta lo mismo.

```
GCFINANCIERO#sh run vrf univercasinos-intra
Building configuration...

Current configuration : 2296 bytes
ip vrf univercasinos-intra
 rd 100:2902
 route-target export 100:2902
 route-target export 14080:2190000003
 route-target import 100:2902
 route-target import 14080:2190000002
!
```

Ilustración 43. *Validación de Router Target (import – export)*

```
GCFINANCIERO#
GCFINANCIERO#sh run vrf | i 10.161.97.102
 neighbor 10.161.97.102 remote-as 65521
 neighbor 10.161.97.102 activate
 neighbor 10.161.97.102 as-override
 neighbor 10.161.97.102 maximum-prefix 50 70 restart 2
```

Ilustración 44. *Validación de configuración protocolo BGP en GSR (nodo).*

4. Se validan las redes que aprende el canal principal: Es necesario saber que rutas aprende el canal principal para comparar con lo que aprende el canal backup ya que debe ser lo mismo. Se utiliza el comando *Show ip bgp vpnv4 vrf (nombre vrf) neighbors (ip wan router) routes.*

```
GCFINANCIERO#sh ip bgp vpnv4 vrf univercasinos-intra nei 10.161.97.102 rou
BGP table version is 1127477391, local router ID is 10.10.66.136
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:2902 (default for vrf univercasinos-intra)
*> 10.114.144.0/24  10.161.97.102            0             0 65521 i
*> 10.161.210.88/30 10.161.97.102            0             0 65521 i
*> 192.168.186.0    10.161.97.102            0             0 65521 i

Total number of prefixes 3
```

Ilustración 44. *Rutas que aprende el servicio principal.*

5. Se ingresa al router del cliente usando *telnet (ip wan router) /vrf (nombre vrf)*

```
GCFINANCIERO#tel 10.161.97.102 /v univercasinos-intra
Trying 10.161.97.102 ... Open
C
************************************************************
* ATENCION: Este equipo es propiedad de TELMEX Colombia.    *
* El uso no autorizado esta estrictamente prohibido.        *
* Todos los usuarios son legalmente responsables de sus     *
* acciones sobre el sistema y   actividad sera registrada*
************************************************************
```

Ilustración 45. *Ingreso al router cliente.*

6. Se verifican interfaces: se valida configuración de interfaces WAN y LAN del servicio con ayuda del comando *Show run interfaz (# interfaz)*

```
WINN_UDQ007#sh run int GigabitEthernet0/1.1718
Building configuration...

Current configuration : 154 bytes
!
interface GigabitEthernet0/1.1718
 description --- WAN INTRANET PPAL - UDQ0007
 encapsulation dot1Q 1718
 ip address 10.161.97.102 255.255.255.252
end

WINN_UDQ007#sh run int Vlan1
Building configuration...

Current configuration : 242 bytes
!
interface Vlan1
 description --- LAN INTRANET - UDQ0025 ---
 ip address 192.168.186.1 255.255.255.0 secondary
 ip address 10.114.144.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip verify unicast reverse-path
end
```

Ilustración 45. *Configuración de interfaces LAN y WAN servicio principal.*

7. Se valida configuración BGP e IGP en el router: Se utilizan los comandos *Show run | sección bgp y Show ip bgp summary.* En esta topología la conmutación se realiza con el atributo local-preference el cual se configuración como estándar de CLARO S.A. para el canal principal con un

peso de 100 y para el backup 50 determinando que elija la ruta con preferencia mayor.

```
WINN_UDQ007#sh run | sec bgp
router bgp 65521
 no bgp log-neighbor-changes
 network 10.114.144.0 mask 255.255.255.0
 network 10.161.210.84 mask 255.255.255.252
 network 10.161.210.88 mask 255.255.255.252
 network 192.168.186.0
 neighbor 10.161.42.177 remote-as 14080
 neighbor 10.161.42.177 description INTRANET BACKUP
 neighbor 10.161.42.177 prefix-list MONITOREO_BCKP out
 neighbor 10.161.42.177 route-map BACKUP in
 neighbor 10.161.97.101 remote-as 14080
 neighbor 10.161.97.101 description INTRANET PPAL
 neighbor 10.161.97.101 timers 10 30
 neighbor 10.161.97.101 prefix-list MONITOREO_PPAL out
WINN_UDQ007#
```

Ilustración 46. *Configuración protocolo BGP e IBGP equipo router.*

```
WINN_UDQ007#sh route-map BACKUP
route-map BACKUP, permit, sequence 10
  Match clauses:
    ip address (access-lists): 2
  Set clauses:
    local-preference 50
    weight 0
  Policy routing matches: 0 packets, 0 bytes
```

Ilustración 47. *Configuración local-preference de router-map Backup.*

8. Se observa si existen rutas estáticas: se deben tener configuradas las mismas rutas estáticas en el canal principal y el backup. Se validan con el comando *Show run | i ip route*

```
WINN_UDQ007#sh run | i ip rou
ip route 172.31.239.18 255.255.255.255 10.161.97.101
```

Ilustración 48. *Rutas estáticas servicio principal.*

- Verificaciones canal backup:

En esta parte se describirán las revisiones que se realizaron en el canal backup pero no se indicaran los comandos utilizados ya que son los mismos que se mencionaron anteriormente

1. Se localiza el servicio:

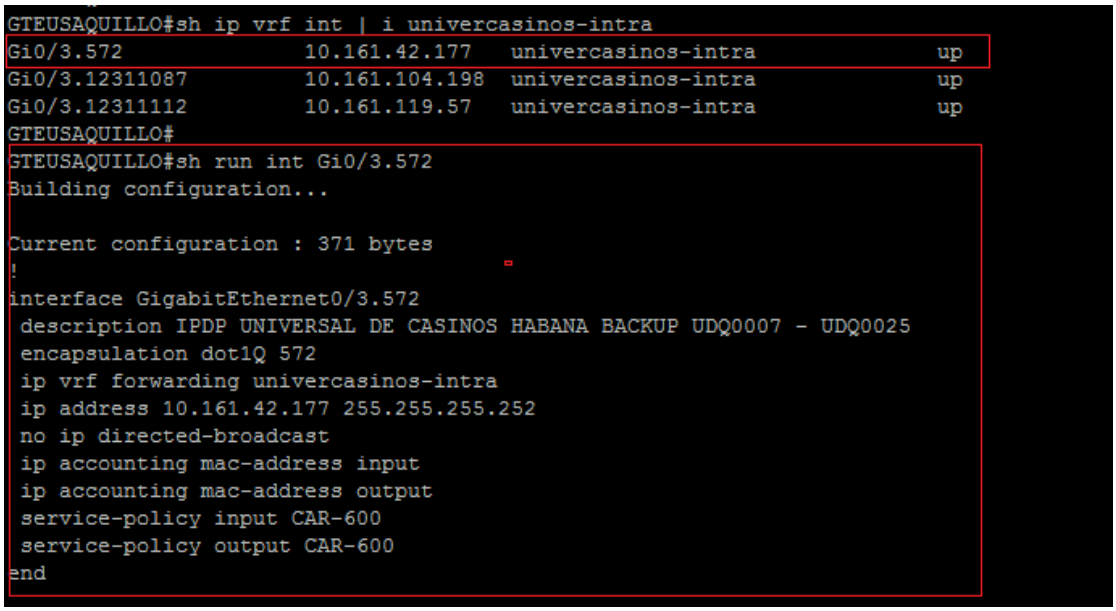


Ilustración 49. *Ubicación del enlace backup en el GSR (nodo) en la red de CLARO S.A.*

2. Se valida operatividad del servicio:

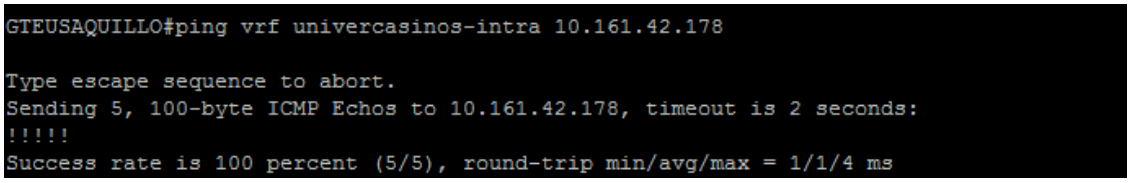


Ilustración 50. *Validación de conectividad desde el GSR al equipo router del cliente.*

3. Se valida protocolo BGP y Router Target (RT): Se debe validar que los RT que está exportando e importando el canal backup son el mismo que los del principal. Adicionalmente se debe observar configurando el atributo local-preference con un peso de 50 para el backup que indica que se prefiera el canal principal.

```
GTEUSAQUILLO#sh run vrf univercasinos-intra
Building configuration...

Current configuration : 2418 bytes
ip vrf univercasinos-intra
 rd 100:2902
 route-target export 100:2902
 route-target export 14080:2190000003
 route-target import 100:2902
 route-target import 14080:2190000002
!
```

Ilustración 51. *Validación de Router Target (import – export).*

```
router bgp 14080
!
address-family ipv4 vrf univercasinos-intra
 redistribute connected
 redistribute static route-map BACKUP
 neighbor 10.161.42.178 remote-as 65521
 neighbor 10.161.42.178 activate
 neighbor 10.161.42.178 as-override
 neighbor 10.161.42.178 route-map BACKUP in
 neighbor 10.161.42.178 maximum-prefix 50 70 restart 2
 maximum-paths import 2
 no synchronization
 exit-address-family
```

Ilustración 52. *Validación de configuración protocolo BGP servicio backup en GSR (Nodo).*

4. Se validan las redes que aprende el canal principal: Se verifica que el canal backup aprenda las mismas rutas que el canal principal.

```
GTEUSAQUILLO#sh route-map BACKUP
route-map BACKUP, permit, sequence 10
  Match clauses:
    ip address (access-lists): 2
  Set clauses:
    local-preference 50
    weight 0
  Policy routing matches: 0 packets, 0 bytes
```

Ilustración 53. *Configuración local-preference del router-map backup en GSR (nodo).*

5. Se ingresa al router del cliente:

```
GTEUSAQUILLO#telnet 10.161.42.178 /v univercasinos-intra
Trying 10.161.42.178 ... Open
C
************************************************************
* ATENCION: Este equipo es propiedad de TELMEX Colombia.    *
* El uso no autorizado esta estrictamente prohibido.        *
* Todos los usuarios son legalmente responsables de sus     *
* acciones sobre el sistema y   actividad sera registrada*
************************************************************
```

Ilustración 54. *Ingreso al router cliente.*

6. Se verifican interfaces:

```
WINN_UDQ007#sh run int Gi0/0.572
Building configuration...

Current configuration : 158 bytes
!
interface GigabitEthernet0/0.572
 description --- WAN INTRANET BACKUP - UDQ0025 ---
 encapsulation dot1Q 572
 ip address 10.161.42.178 255.255.255.252
end

WINN_UDQ007#sh run int Vl1
Building configuration...

Current configuration : 242 bytes
!
interface Vlan1
 description --- LAN INTRANET - UDQ0025 ---
 ip address 192.168.186.1 255.255.255.0 secondary
 ip address 10.114.144.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip verify unicast reverse-path
end
```

Ilustración 55. *Configuración interfaces WAN y LAN servicio backup.*

Al finalizar las verificaciones pertinentes de los canales se realiza un cuadro comparativo de los parámetros revisados de cada servicio para poder determinar que el canal conmutara de manera correcta cuando se ejecuten las pruebas de backup.

Tabla 9. *Cuadro comparativo configuraciones canal principal y backup.*

VERFICACIÒN	PRINCIPAL	BACKUP
La vrf exporta e importa lo mismo en ambos nodos	OK	OK
Se aprenden las mismas rutas en ambos nodos	OK	OK
Protocolo BGP	OK	OK

Fuente: elaboración propia

5.7.4 Ejecución de pruebas de backup

El área de Prevención después de recibir la solicitud y crear el script, genera un caso de Seguimiento, que es el radicado en el cual se guarda toda la documentación histórica de las pruebas que se ejecutan. Después de esto, se coordina con el cliente fecha y hora para realizar la actividad y ejecutar las pruebas de backup.

Las pruebas de backup se realizan bajo una metodología estipulada dentro del desarrollo de las pruebas:

1. Se valida conectividad en los servicios, entre el principal y el backup
2. Se confirman direcciones de origen y destino.
3. Se toman trazas y ping entre origen y destino.
4. Se baja el enlace principal y se espera que de manera automática el canal de backup conmute (3 y 5minutos)
5. Un vez conmute el canal de backup se valida conectividad, se toman trazas y ping nuevamente.
6. Se sube el canal principal nuevamente, se valida tomando trazas y ping.

7. Al finalizar la prueba el servicio queda operativo nuevamente por el canal principal

A continuación se describe el desarrollo de la metodología al ejecutar las pruebas de backup para los 2 scripts expuestos anteriormente:

Ejecución de pruebas de backup (CIM0072 - CIM0068):

a. Se valida conectividad antes de conmutar al canal backup:
   Se realizan pruebas de ping y traza a sedes remotas o servidores, que el cliente indique con el fin de que al momento de conmutar el canal, se puede validar nuevamente conectividad a los mismos equipos y se evidencie que el tráfico sale por el enlace backup.

Ilustración 56. *Prueba de conectividad antes de iniciar pruebas de conmutación.*

b. Con previa autorización del cliente se procede a bajar el canal principal para que de manera automática el tráfico conmute hacia el backup:

Ilustración 57. *Interfaz WAN canal principal administrativamente abajo.*

c. Se realizan pruebas de conectividad y se evidencia en traza que el tráfico conmuto hacia el canal backup:

Ilustración 58. *Prueba de conectividad después de conmutación.*

d. Se sube canal principal y se valida conectividad verificando que el primer salto es hacia la ip WAN del servicio principal:

Ilustración 59. *Rollback, canal principal arriba.*

e. Se confirma con cliente resultado de pruebas exitosas y se procede con el cierre del caso de seguimiento:

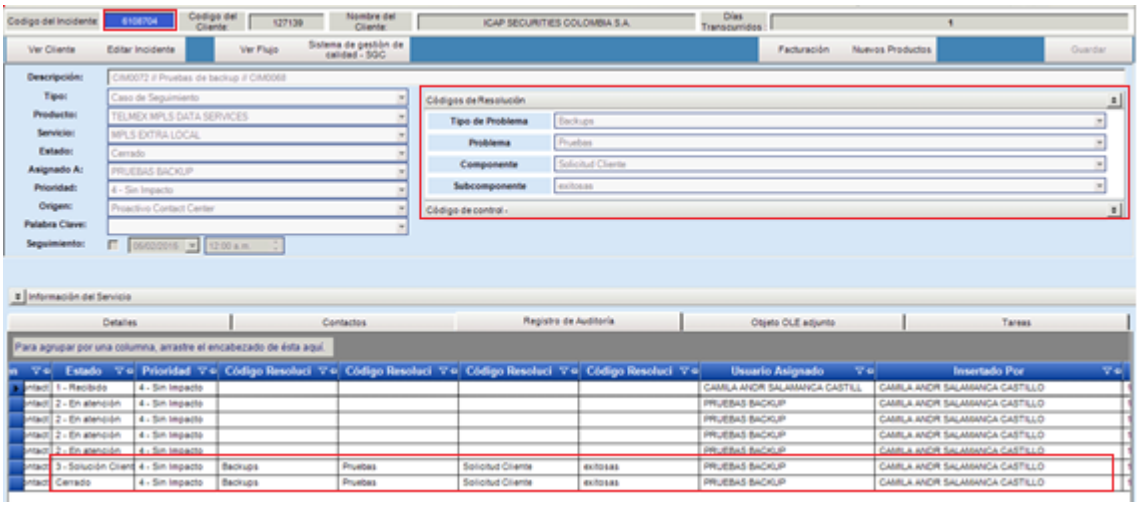


Ilustración 60. Caso de seguimiento.

En la Ilustraciòn 61 se evidencia en la parte de superior izquierda el nùmero del caso 6108704, al lado derecho se evidencias los codigos de resolucion del caso comprobando que la prueba que se realizo fue exitosa y en la parte inferiror se observa el ingeniero (a) por parte de CLARO S.A. que ejecuto las pruebas de backup.

Ejecución de pruebas de backup (UDQ0007- UDQ0025):

a. Se valida conectividad antes de conmutar al canal backup:

   Se realizan pruebas de ping y traza a sedes remotas o servidores que el cliente indique, con el fin de que al momento de conmutar el canal se puede validar nuevamente conectividad a los mismos equipos y se evidencie que el tráfico sale por el enlace backup.

Ilustración 61. *Pruebas de conectividad antes de iniciar pruebas de conmutación.*

b. Con previa autorización del cliente se procede a bajar el canal principal para que de manera automática el tráfico conmute hacia el backup:

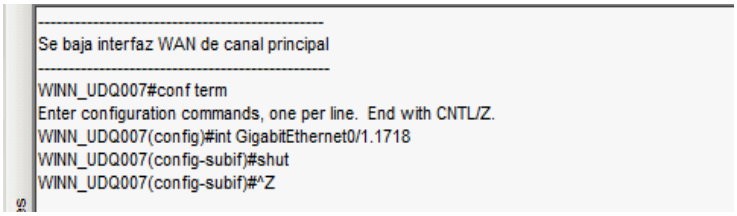


Ilustración 62. *Comando shut interfaz WAN canal principal.*

c. Se realizan pruebas de conectividad y se evidencia en traza que el tráfico conmuto hacia el canal backup:

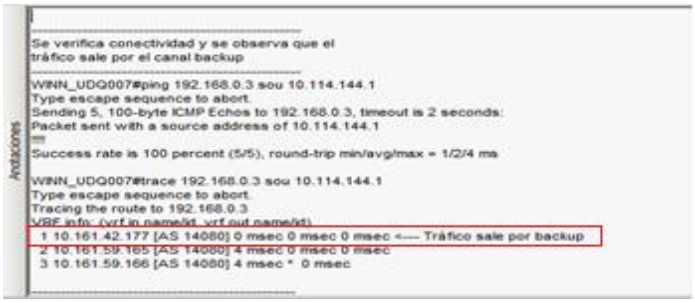


Ilustración 63. *Prueba de conectividad después de conmutación.*

d. Se sube canal principal y se valida conectividad verificando que el primer salto es hacia la ip WAN del servicio principal:

Ilustración 64. *Rollback, canal principal arriba.*

e. Se confirma con cliente resultado de pruebas exitosas y se procede con el cierre del caso de seguimiento.

6. CRONOGRAMA

A continuación se mostrará el cronograma que se llevó a cabo en la ejecución del PLAN DE ACCIÓN PUNTO CENTRAL DE UNA ENTIDAD FINANCIERA:

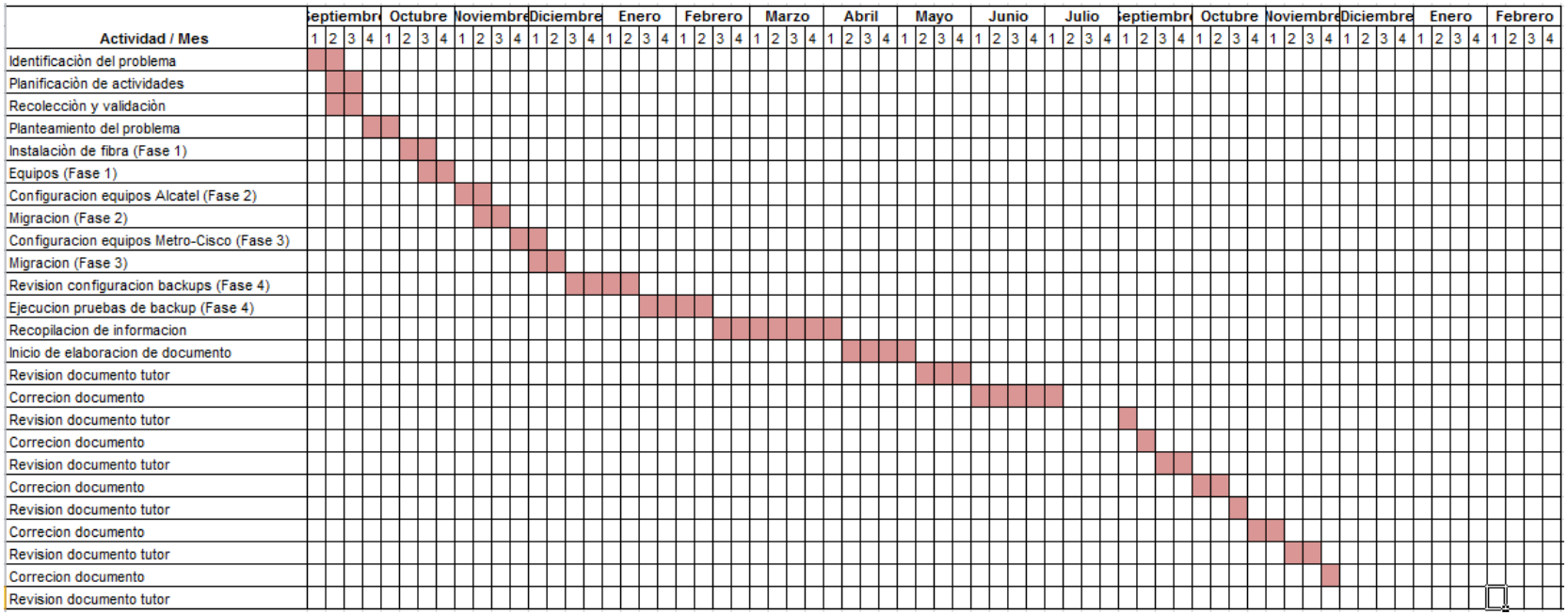


Ilustración 65. *Cronograma de actividades.*

CONCLUSIONES

- A través de la ejecución del plan de acción punto central una entidad financiera, se restructuró el centro de datos de la empresa bancaria demostrando que es importante elaborar un plan estratégico en el que se evidencian las tareas a realizar por cada una de las áreas implicadas, la duración del proyecto y los pasos a seguir en su desarrollo, de acuerdo al cronograma preestablecido para cumplir con cada objetivo planteado de manera exitosa.

- Las limitantes en la información hacen que los procesos entre áreas no dejen proporcionar una exactitud de tiempos de respuesta, por lo cual la importancia de tener documentos para poder enfrentar escenarios alternativos y lograr mejoras en los tiempos.

- En el momento de identificar los equipos a implementar es importante verificar que las características de cada uno sean predilectas según el tipo de servicio (MPLS Extranet o Intranet) que se brinda al cliente ya que se deben cumplir los estándares establecidos por CLARO S.A.

- Es importante identificar la topología implementada al cliente para las soluciones backup, de acuerdo a esta se deben verificar las configuraciones en los equipos puesto que las 3 topologías establecidas por CLARO S.A. utilizan protocolos diferentes como HSRP, BGP o IBGP, que implican validar diferentes parámetros que avalan una correcta conmutación en el momento que se presenten fallas en el canal principal proporcionando al cliente disponibilidad a su empresa.

- Realizar pruebas de backup de manera controlada, ayuda a mejorar y detectar falencias en los servicios (MPLS Extranet o Intranet) permitiendo solucionarlas en ventanas acordadas y aprobadas por el cliente que evitan que en un momento de falla real se presente algún inconveniente.

- Se debe tener en cuenta antes de realizar cualquier proyecto las ventajas y las limitantes para poder proporcionar un mejor alcance al objetivo general.

GLOSARIO

Adj-RIB-In: Es la tabla en la que contiene los prefijos de un vecino específico. Existe una gran cantidad de este tipo de tablas.

Adj-RIB-out: Es una tabla que tiene los prefijos para anunciar a los vecinos. Se forma de la información que tenga la tabla Loc-RIB.

BGP: Border Gateway Protocol es un protocolo de enrutamiento especialmente entre sistemas autónomos (AS) utilizado para intercambiar prefijos de rutas entre estos.

COC: Cotización de obra civil.

CPE (Customer Premise Equipment o Customer Edge): Equipo de cliente, No pertenece al dominio de MPLS.

Datacenter: centro de procesamiento de datos que tiene proporcionado los recursos de servidores en los que se almacenan datos operativos de redes de una compañía.

Dirección MAC virtual: se encarga de asociar todos los routers a una ip virtual.

EBGP (External Border Gateway Protocol): Se utiliza para conectar sistemas BGP externos.

Forwarding: Hace referencia a la secuencia o flujo de paquetes que pueden ser direccionados (forwarding) al mismo “next-hop” o a lo largo del mismo camino (Path).

HSRP: Hot Standby Router Protocol (HSRP) es un protocolo propietario de cisco creado para redundancia de router en caso de fallas en la red.

IBGP (Internal Border Gateway Protocol): Se utilizaa para conexiones internas BGP

IGP (Interior Gateway Protocol): Es un protocolo de enrutamiento utilizado dentro de un mismo sistema autónomo para el intercambio de información entre los routers que se encuentren en el AS.

LDP: Label Distribution Protocol.

Loc-RIB: Tabla que almacena las mejores rutas mediante el proceso BGP.

LSP: Label Switch Path

LSR: Label Switching Router.

MPLS: Multiprotocol Label Switching

MPLS Avanzado: solución de transmisión de datos que proporciona servicios de altos estándares.

MPLS INTRANET: Permite conectividad de redes LAN distribuidas geográficamente.

MPLS EXTRANET: Permite la conexión con los proveedores de servicio y contenido para el intercambio de información.

PE (Provider Edge): Recibe la conexión de clientes, realiza el intercambio y retiro de etiquetas.

Router Activo: Se encarga de enviar paquetes Hello vía multicast a la ip virtual del router pasivo.

Router Pasivo: Es el router de respaldo del activo.

Sistema Autónomo (AS): Es un conjunto de routers que funcionan bajo las mismas políticas de enrutamiento.

Tier: Nivel redundancia para garantizar la disponibilidad de un centro de datos.

Última Milla (UM): Recorrido del tramo de fibra óptica desde el equipo de la red de acceso hasta la sede del cliente.

VRF: Etiqueta virtual que define cada cliente y contiene su propia tabla de enrutamiento.

VOC: Visita de obra civil.

BIBLIOGRAFIA

A.T.M, M., & As, T. (s.f.). *Modo de Transferencia Asíncrona .*

Aguilar, D., & Patiño, V. (2012). *Analisis de los protocolos de alta disponibilidad de gateways en la interconectividad LAN/WAN aplicadas en el diseño del MAGAP Cotopaxi.* Cotopaxi: Universidad Técnica de Cotopaxi.

Association, T. I. (2005). *Estandar TIA 942.*

Calleja, J. (2012). *SEGURIDAD EN BGP, ATAQUES AL PROTOCOLO Y FALLOS DE CONFIGURACIÓN.* Madrid: ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI).

Castaño, J., & Rojas, J. (2012). *Evaluación del Desempeño del Protocolo BGP con atributos de Ingeniería de Tráfico.* Popayan: Universidad del Cauca.

CISCO. (s.f.). *CISCO.* Recuperado el 2 de Noviembre de 2014, de http://www.cisco.com/cisco/web/support/LA/7/73/73722_62.html#topic3.

Cole, B., & Morton, P. (1998). *Cisco Hot Stand by Router Protocol.* EE UU: HSRP.

Dordoigne, J. (2013). *Redes informaticas nociones fundamentales (protocolos, arquitecturas, Redes inalambricas, virtualización, Seguridad, IP V6,..) 4 edicion.* Barcelona: eni ediciones.

Empson, S. (2007). *CCNP BCMSN Portable Command Guide.* Cisco Press.

Garcia, M. (2008). *El Presente de las Redes IP.* Pereira: Universidad Tecnológica de Pereira.

Gutierrez, J. (2012). *Capacitación Técnica.* Bogotá: Claro S.A.

Inc, C. S. (2013). *Configuración de una Red BGP Básica.* http://www.cisco.com/cisco/web/support/LA/111/1116/1116297_irg-basic-net.html.

Montero, F. (2011). *Gestión del riesgo en Infraestructura y Telecomunicaciones TI, para empresa del sector financiero.* Valparaiso: Universidad Técnica Federico Santa Maria.

Mosquera, A. M., & Arboleda, C. (2012). *Asignación y Conilustración VRF, RD y RT.* Bogotá: Claro S.A.

Pantelis, P. F., Monte de Oca, V. M., & Galleguillo, J. (2010). *BGP (Border Gateway Protocol) Análisis y simulación.* Cordoba: Instituto Universitario Aeronáutico .

Pavón, C. (2012). *Diseño de una red WAN para una compañía nacional.* Barcelona: Universidad de Catalunya.

Rekhter, Y., Li, T., & Hares, S. (2006). *A Border Gateway Protocol 4 (BGP-4).* Request for Comments: 4271 .

Ruiz, A., Ros, f. J., & Pereñiguez, F. (2010). *ARQUITECTURA DE REDES .* Madrid: Universidad Complutense de Madrid.

Traina, P., McPherson, D., & Scudder, J. (2007). *Autonomous System Confederations for BGP.* Request for Comments: 5065.

TRC. (s.f.). *TRC*. Recuperado el 4 de Diciembre de 2014, de TRC: www.trc.es

Vergara, J., & Alberto, R. (5 de Agosto de 2013). Entrevista Ingeniero Implementación. (C. Bernal, & C. Salamanca, Entrevistadores)

Vergara, J., & Rodriguez, A. (5 de Noviembre de 2014). Entrevista a Ingeniero de Implementación y Líder área de Prevención . (C. Salamanca, Entrevistador)

Vicente, A., & Martinez, C. (2006). *Introducción a Redes MPLS .* Madrid: Universidad Politécnica de Madrid.

Vilar Reyes, J. (2003). *PFC: Estudio sobre la creación y explotación de un centro de procesos de datos.* Barcelona: Universitat Politècnica de Catalunya.

ANEXOS

Anexo 1. Diagramas de detalle red Alcatel antes de migración.

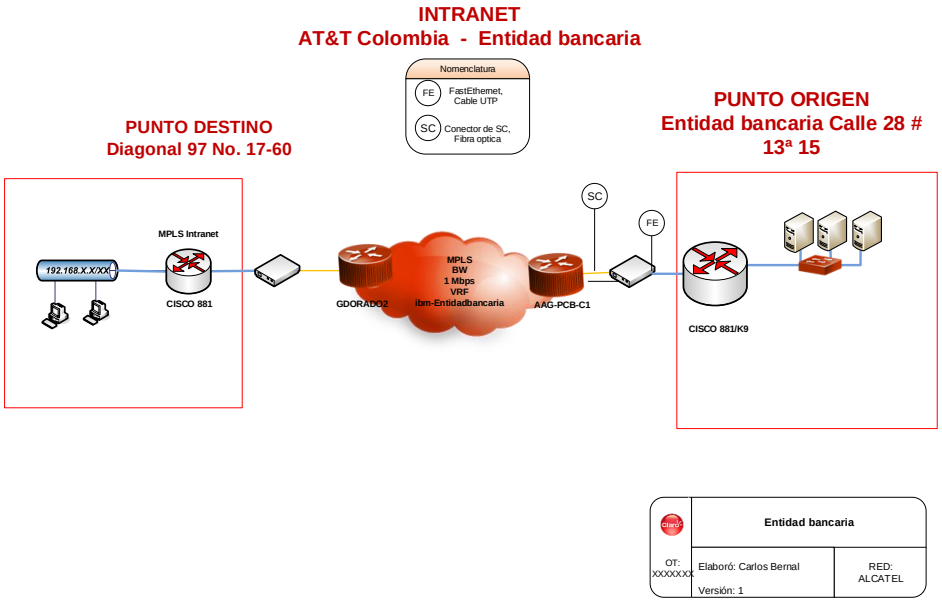


Ilustración 66. *Diagrama de ingeniería red Alcatel antes de migración AT&T Colombia S.A.S.*

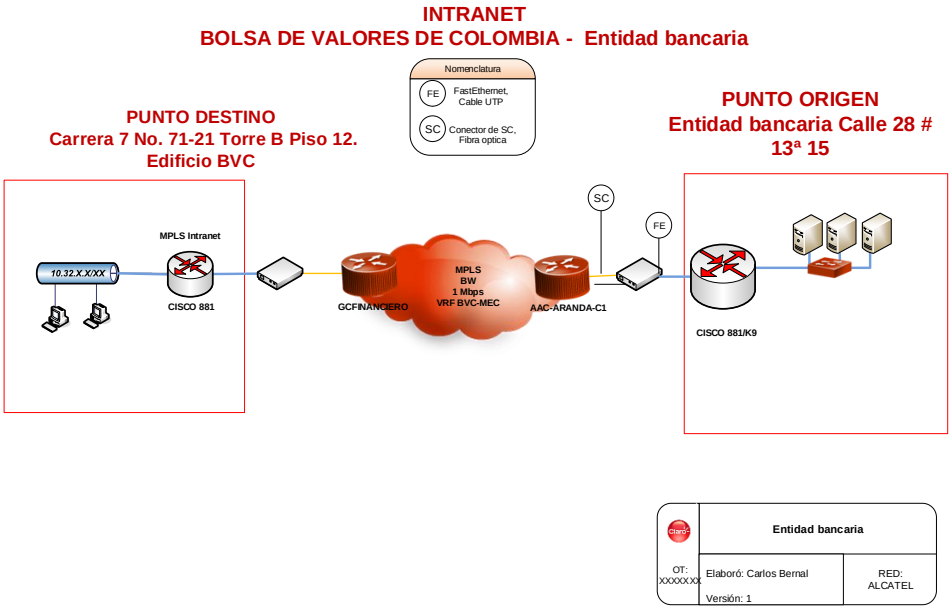


Ilustración 67. *Diagrama de ingeniería red Alcatel antes de migración Bolsa de Valores de Colombia.*

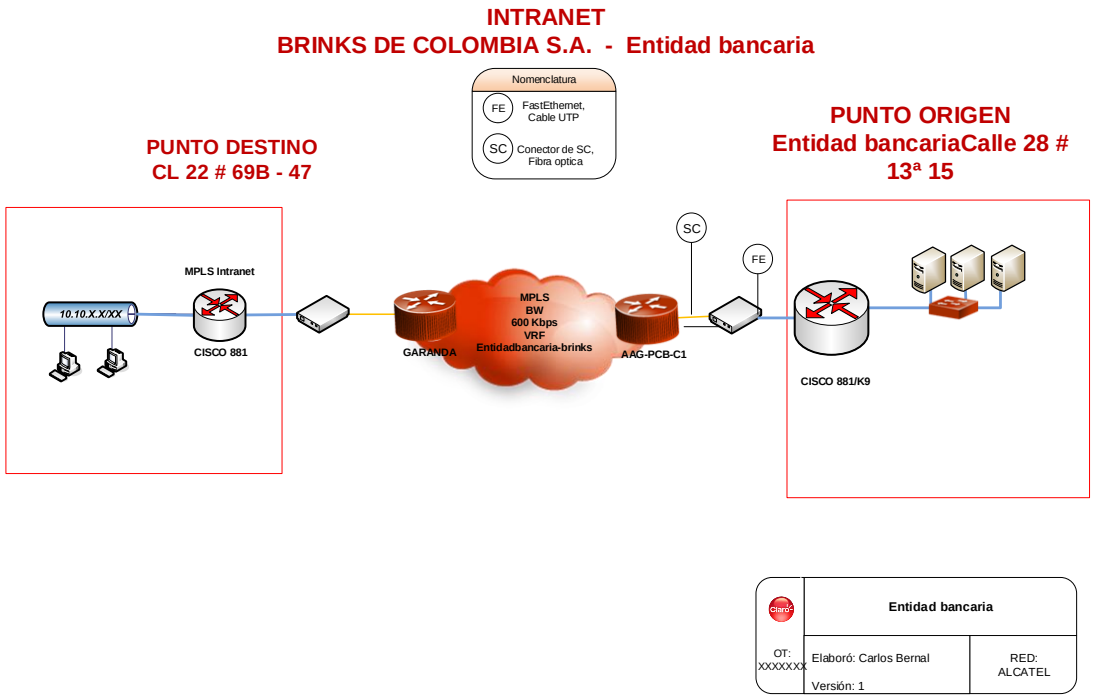


Ilustración 68. *Diagrama de ingeniería red Alcatel antes de migración Brinks de Colombia.*

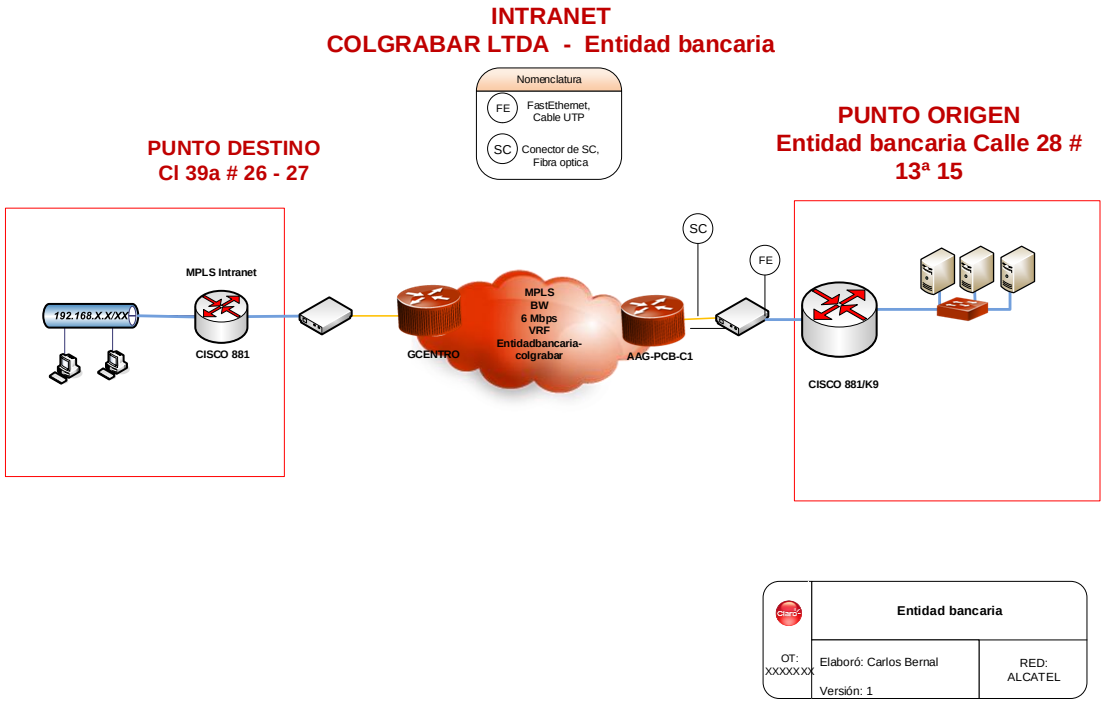


Ilustración 69. *Diagrama de ingeniería red Alcatel antes de migración Colgrabar LTDA.*

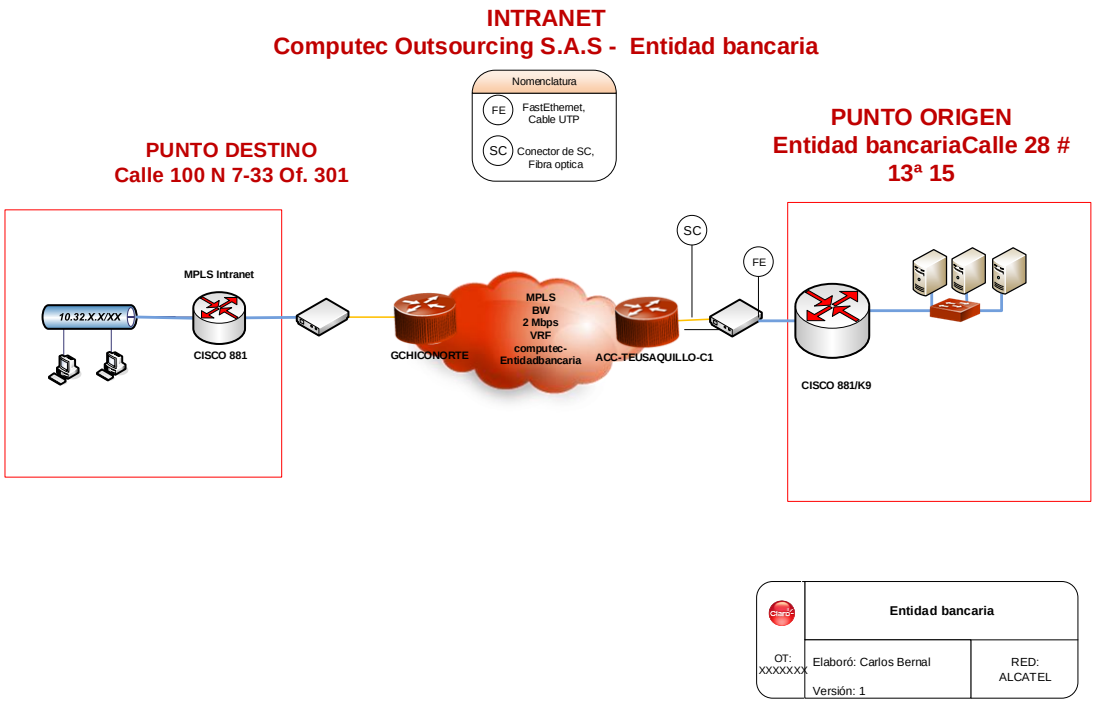


Ilustración 70. *Diagrama de ingeniería red Alcatel antes de migración Compunet Outsorcing S.A.S*

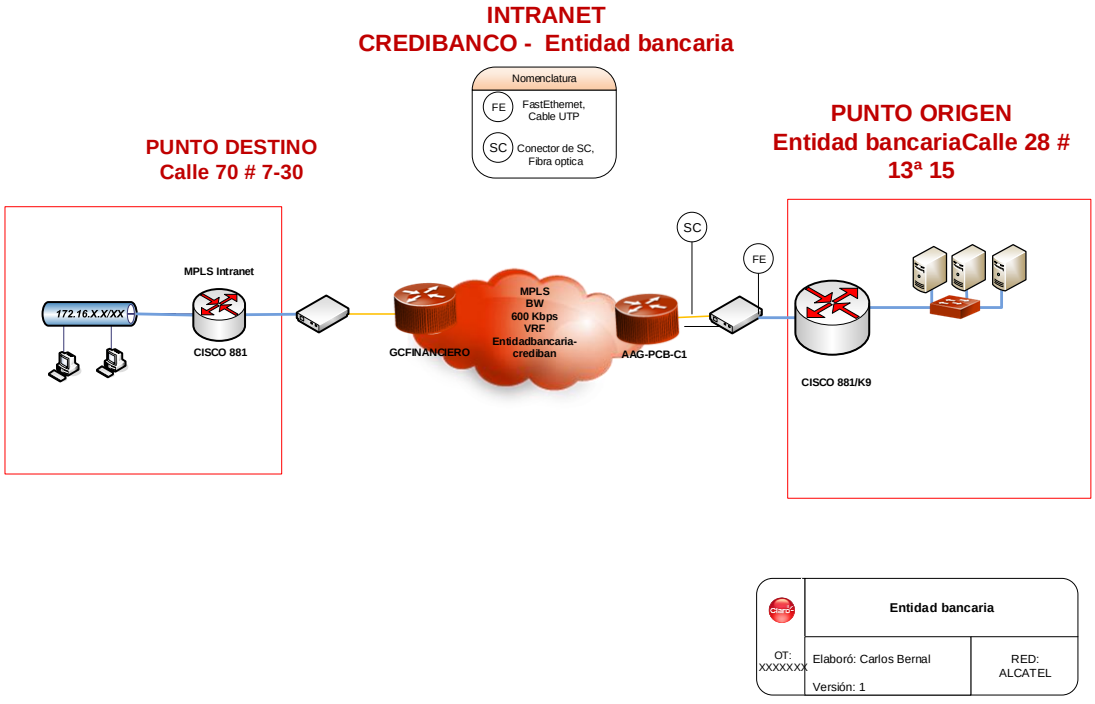


Ilustración 71. *Diagrama de ingeniería red Alcatel antes de migración Credibanco*

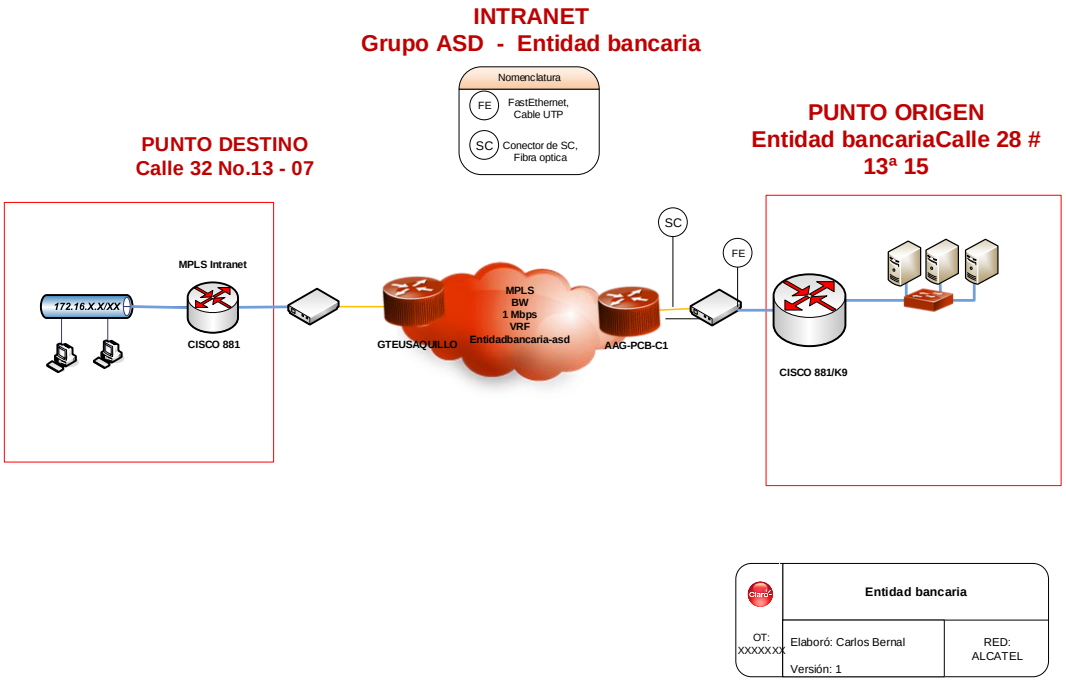


Ilustración 72. *Diagrama de ingeniería red Alcatel antes de migración Grupo ASD.*

Anexo 2. Diagramas de detalle migración de servicio Alcatel.

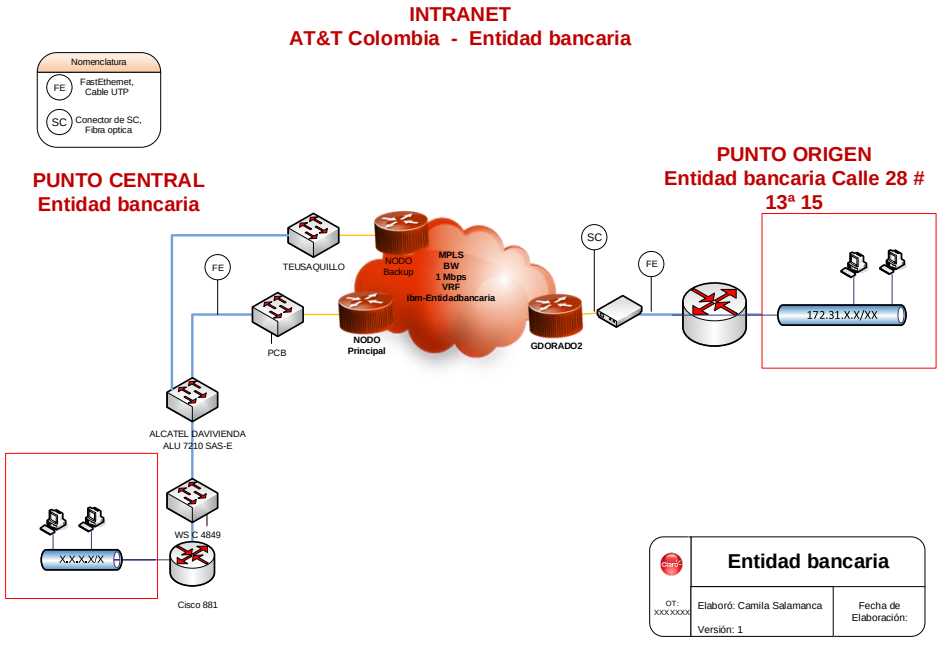


Ilustración 73. *Diagrama de ingeniería AT&T Colombia.*

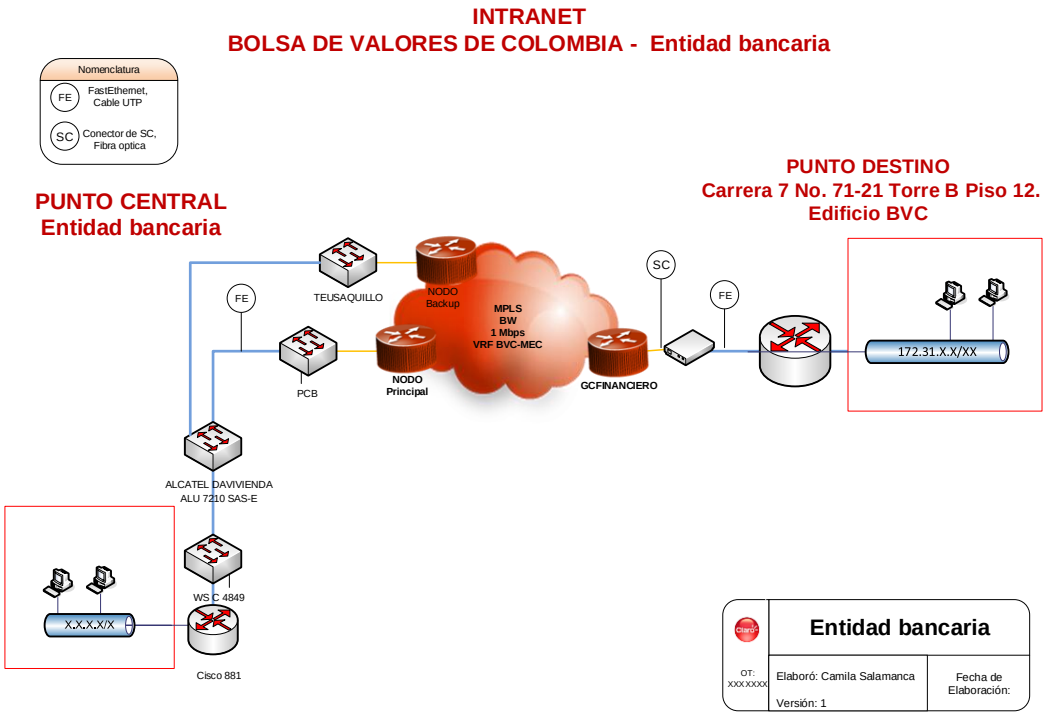


Ilustración 74. *Diagrama de ingeniería Bolsa de Valores de Colombia.*

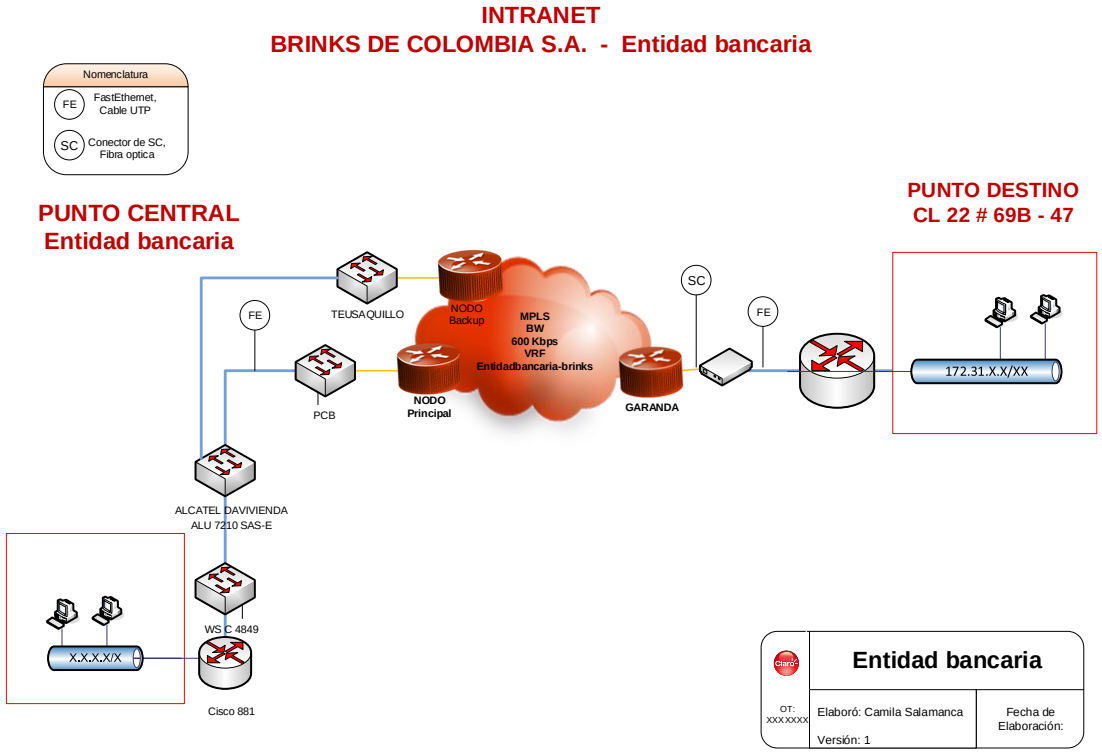


Ilustración 75. *Diagrama de ingeniería Brinks de Colombia.*

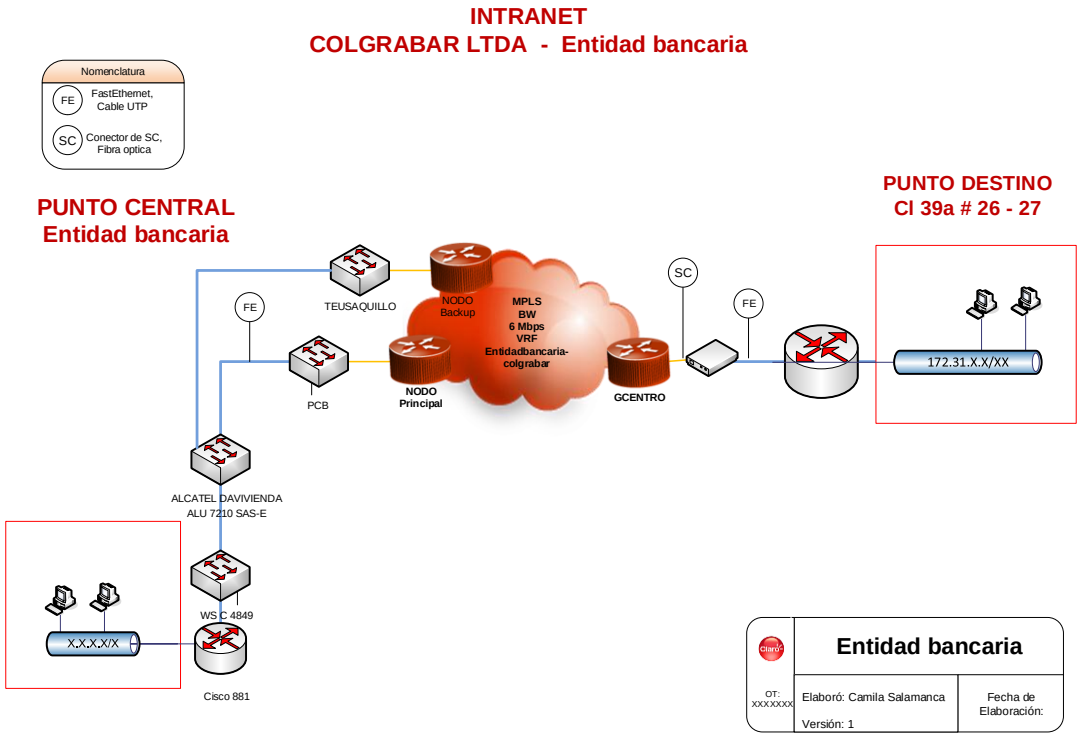


Ilustración 76. *Diagrama de ingeniería actual Colgrabrar.*

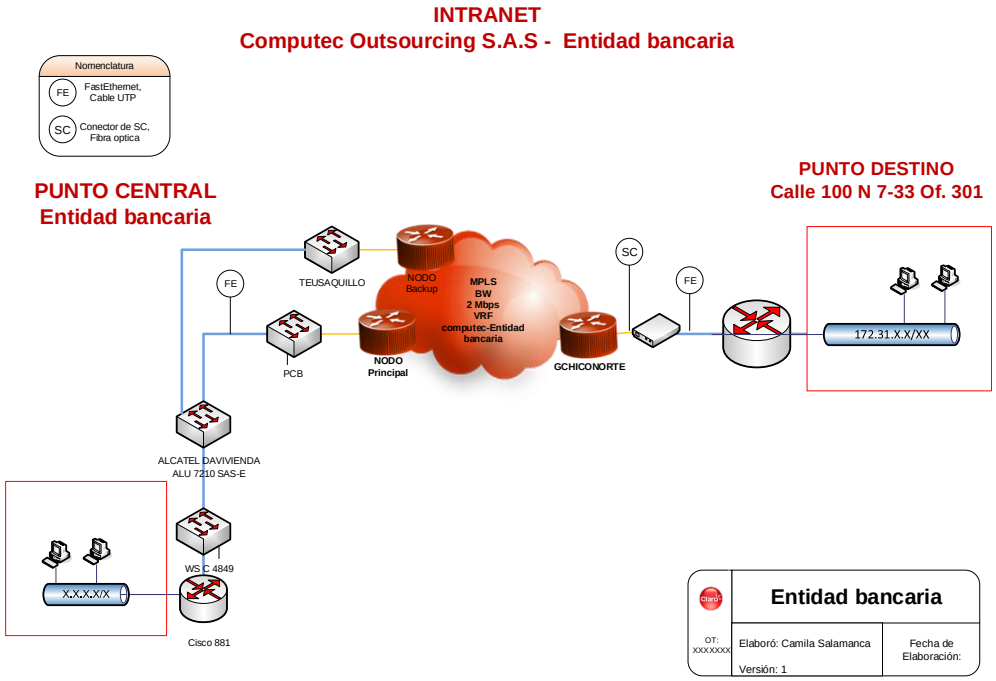


Ilustración 77. *Diagrama de ingeniería actual Compunet Outsorcing S.A.S*

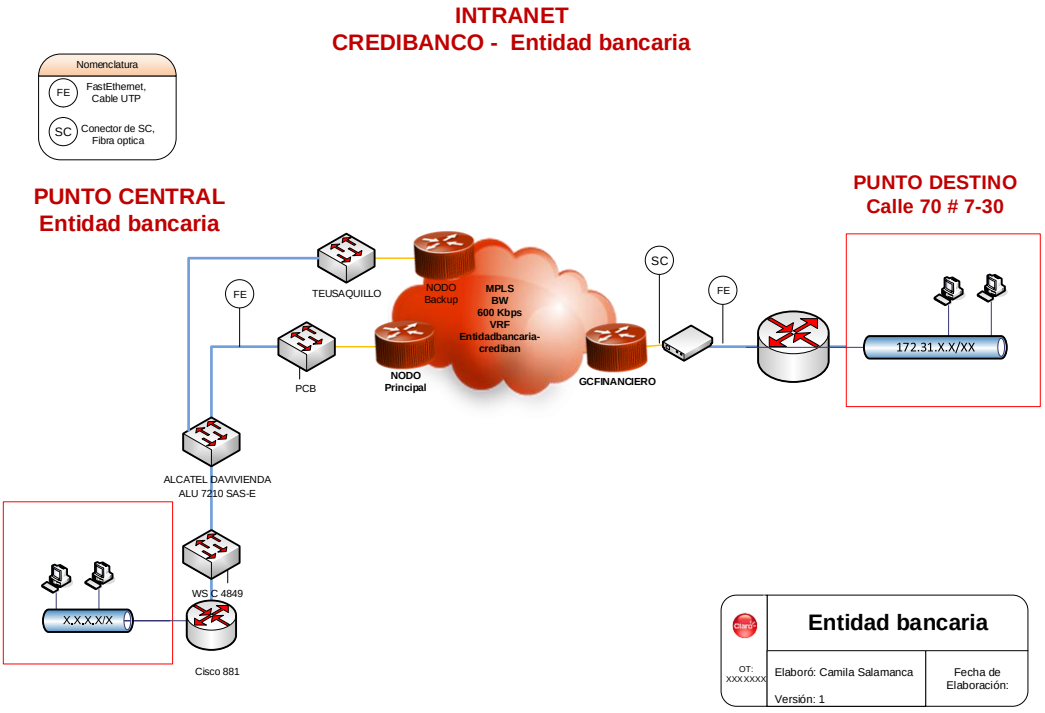


Ilustración 78. *Diagrama de ingeniería actual Credibanco.*

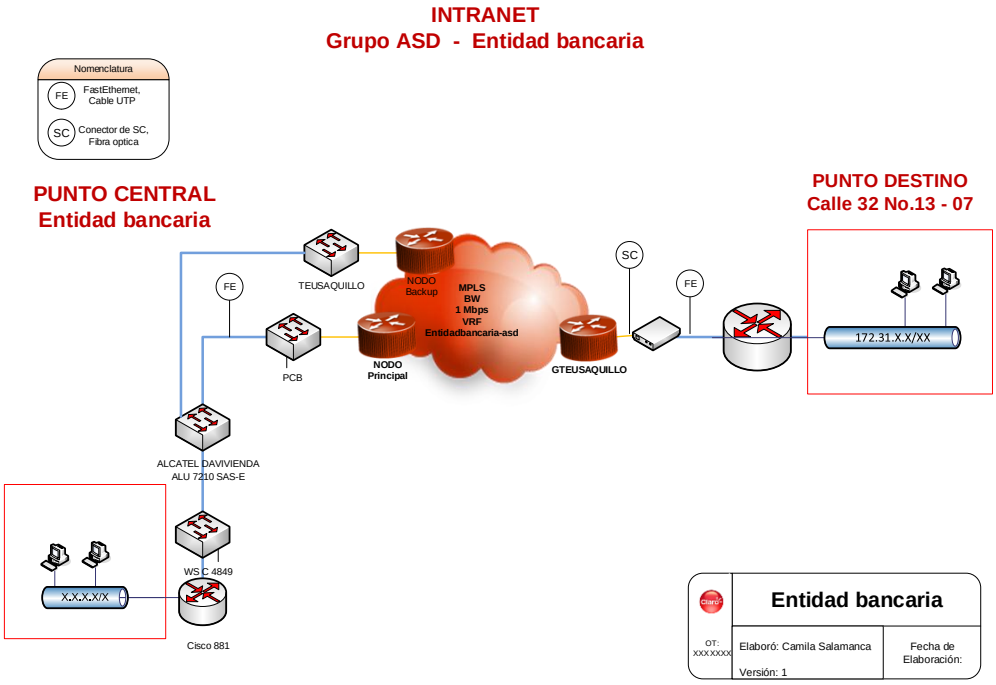


Ilustración 79. *Diagrama de ingeniería actual Grupo ASD.*

Anexo 3. Diagramas de detalle red metro antes de migración.

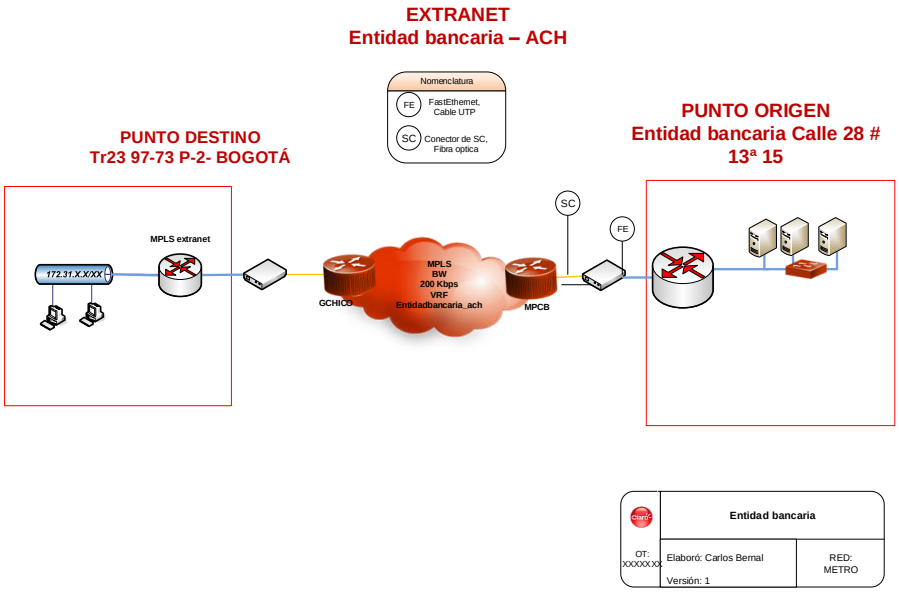


Ilustración 80. *Diagrama de ingeniería extranet entidad financiera – ACH (antes).*

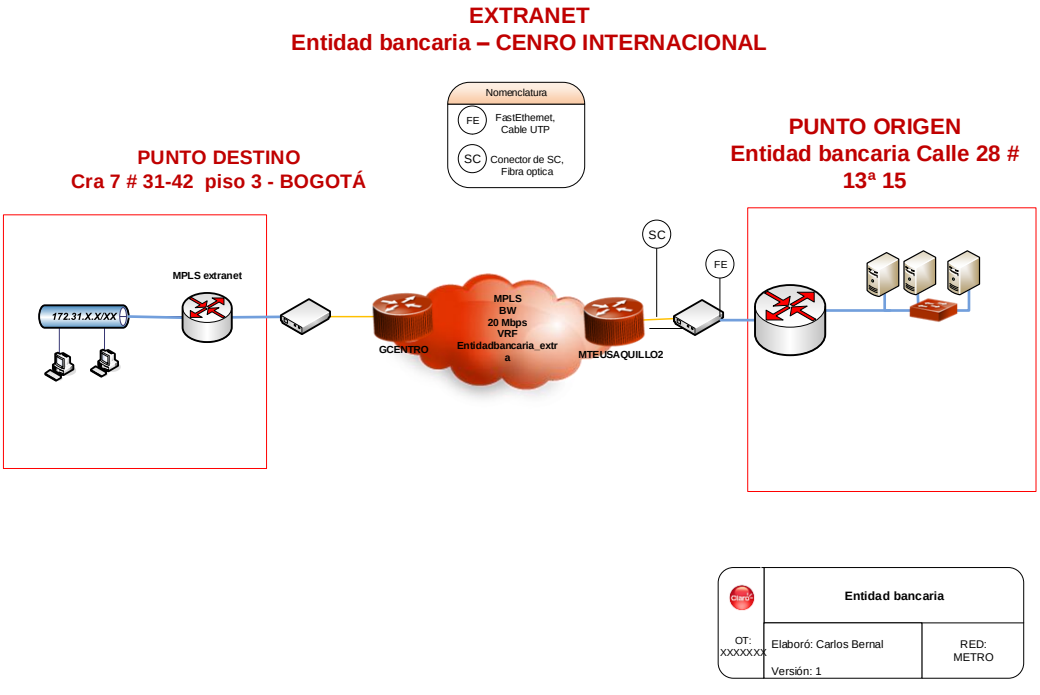


Ilustración 81*. Diagrama de ingeniería extranet entidad financiera punto origen – Sede Remota (antes).*

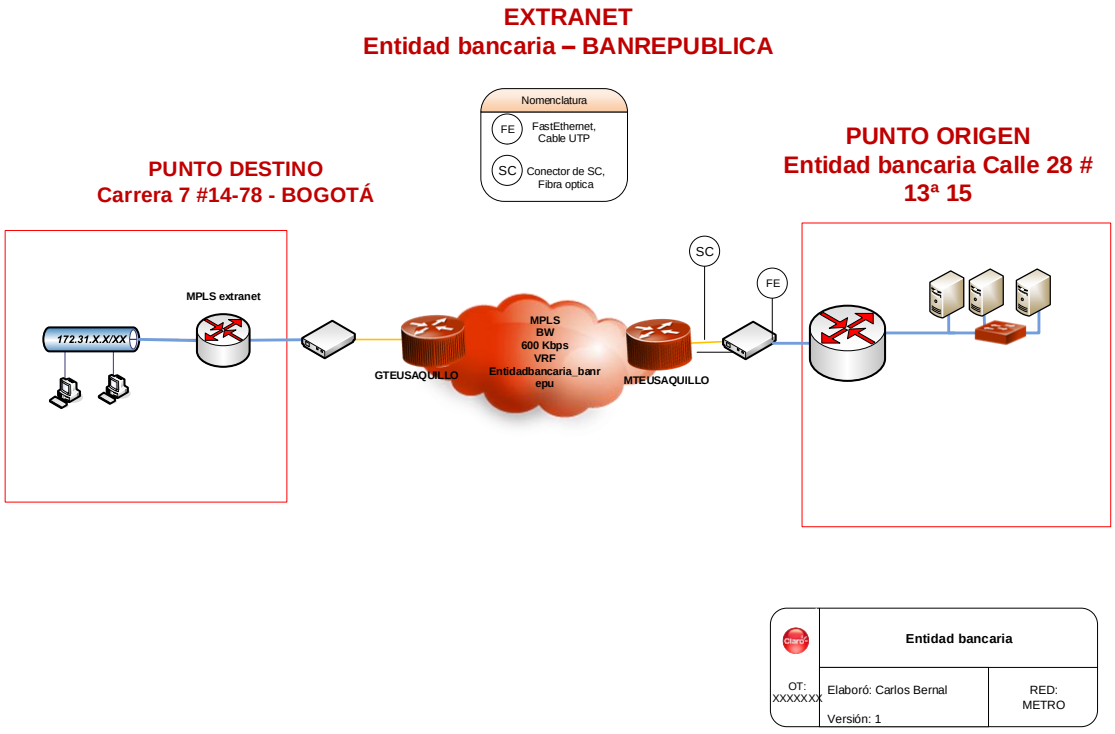


Ilustración 82. *Diagrama de ingeniería extranet entidad financiera- Banrepublica (antes).*

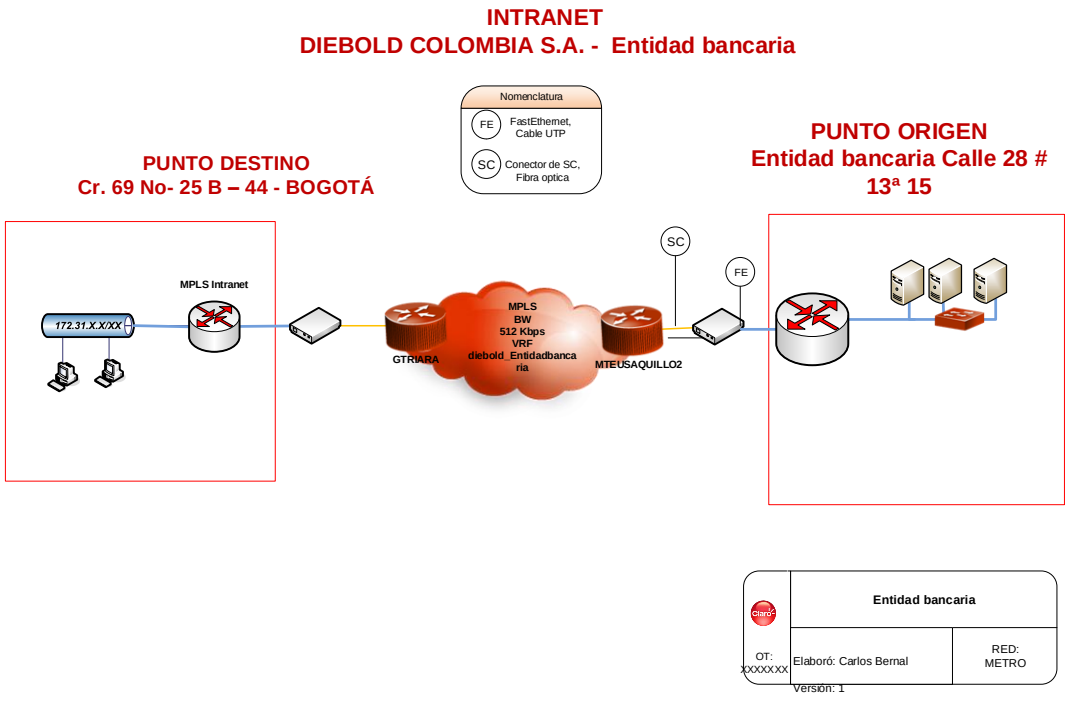


Ilustración 83. *Diagrama de ingeniería extranet entidad financiera - Diebold Colombia (antes).*

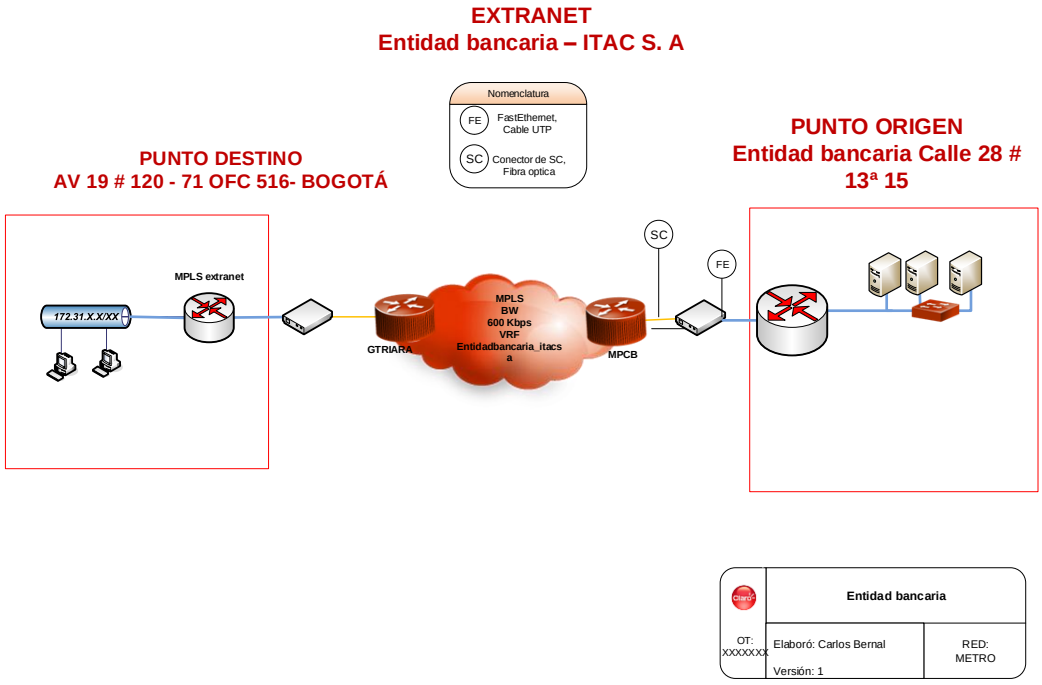


Ilustración 84. *Diagrama de ingeniería extranet entidad financiera - ITAC (antes).*

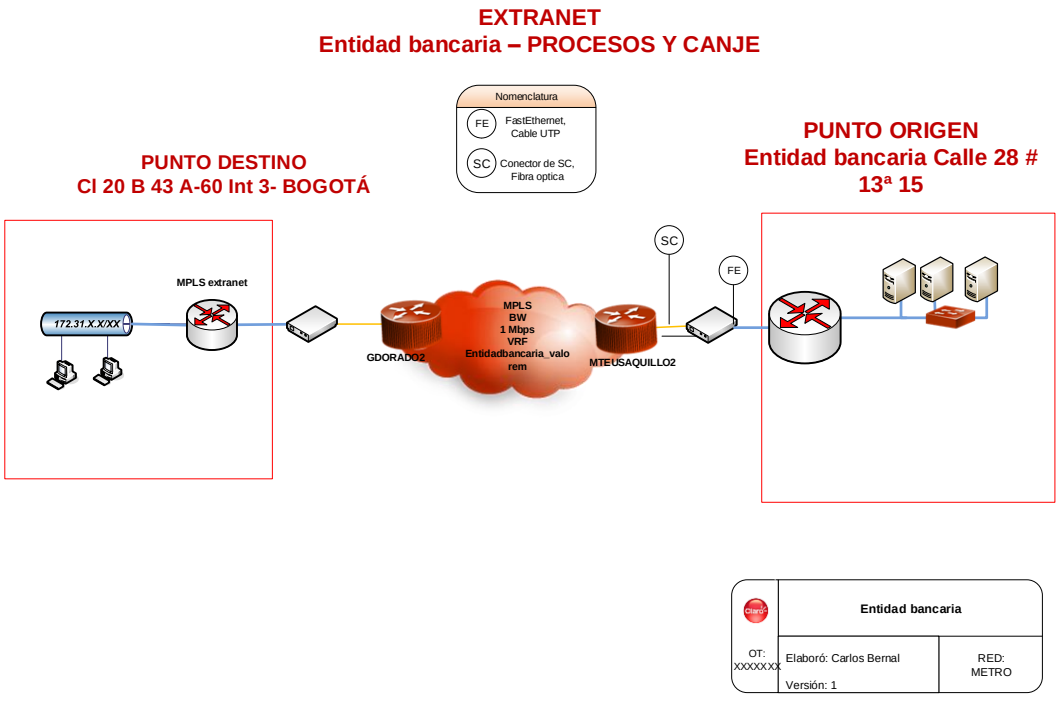


Ilustración 85. *Diagrama de ingeniería extranet entidad financiera - Procesos y Canje (antes).*

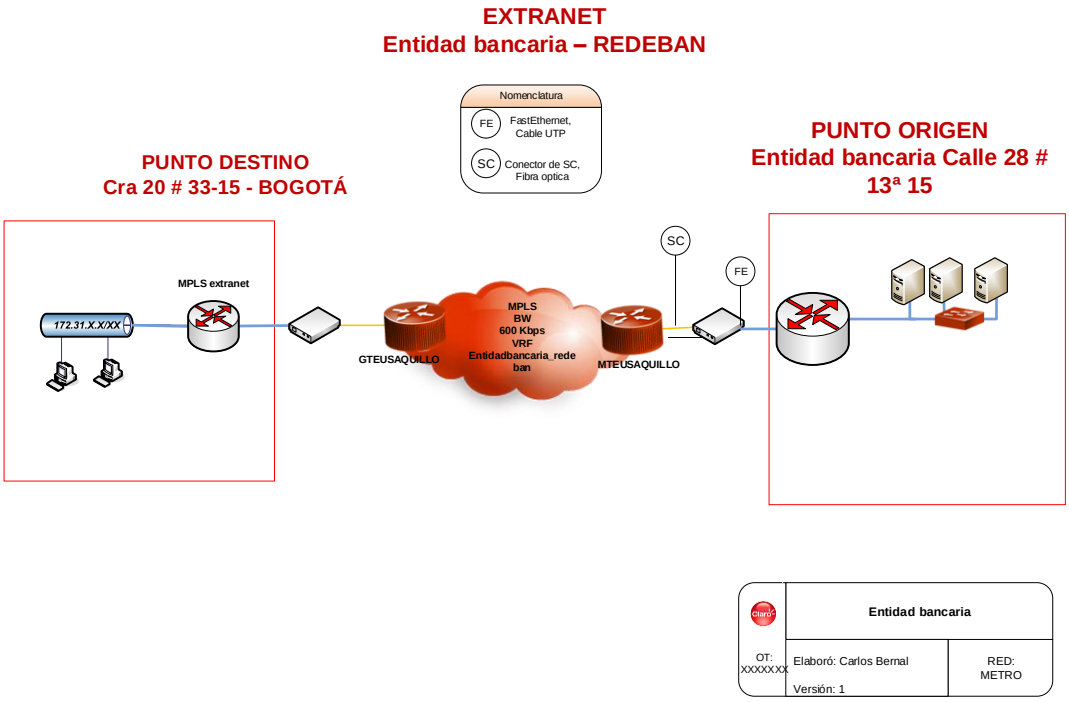


Ilustración 86. *Diagrama de ingeniería extranet entidad financiera - Redeban (antes).*

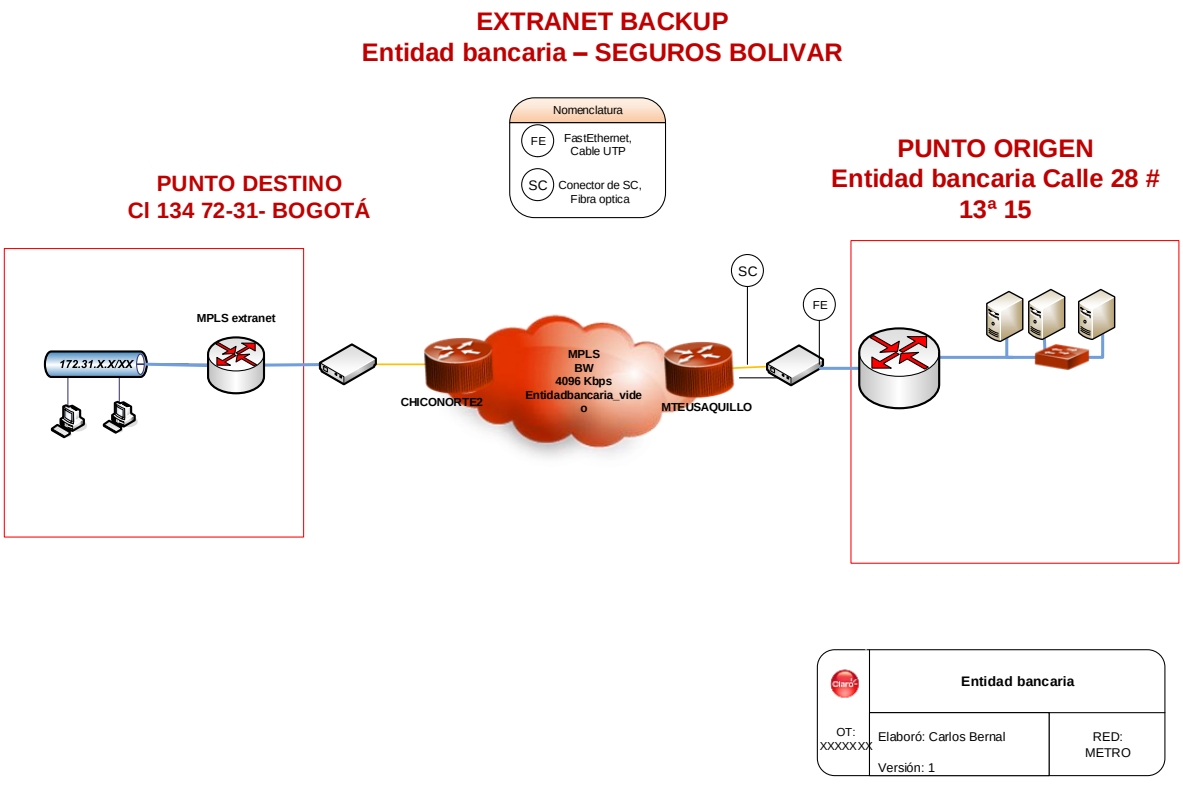


Ilustración 87. *Diagrama de ingeniería extranet entidad bancaria - Seguros Bolívar (antes).*

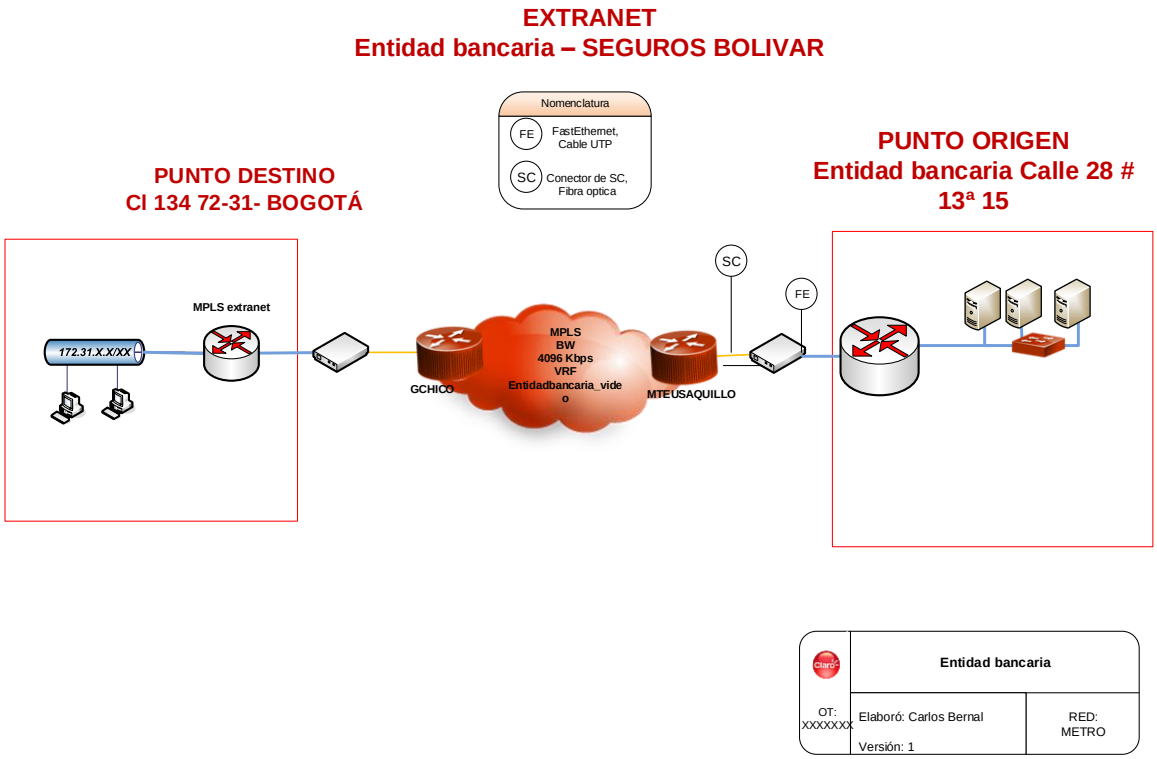


Ilustración 88. *Diagrama de ingeniería extranet entidad financiera - Seguros Bolívar (antes).*

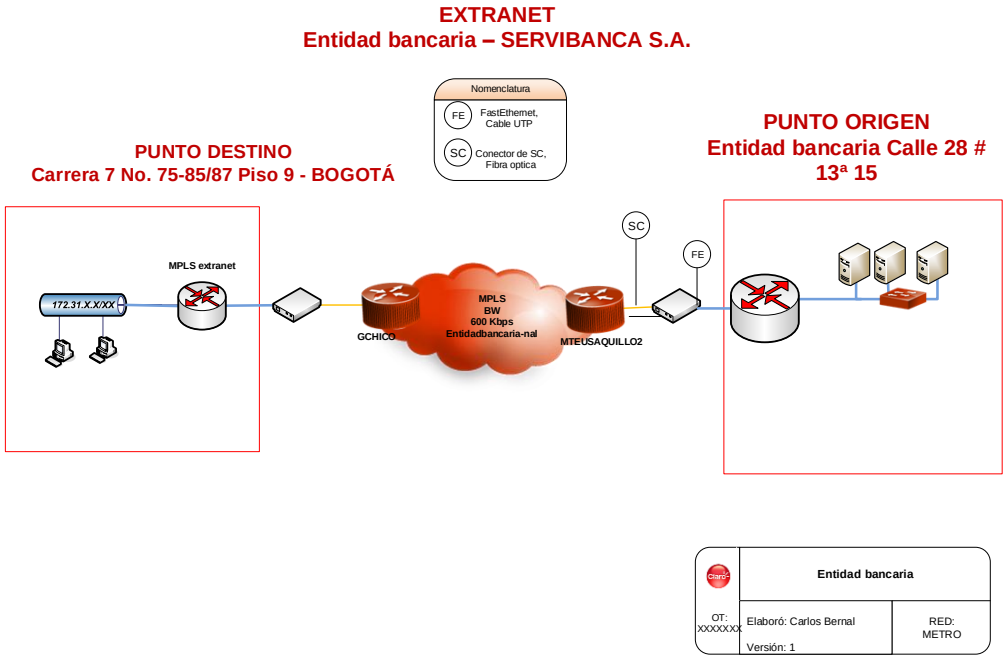


Ilustración 89. *Diagrama de ingeniería extranet entidad financiera - Servibanca (antes).*

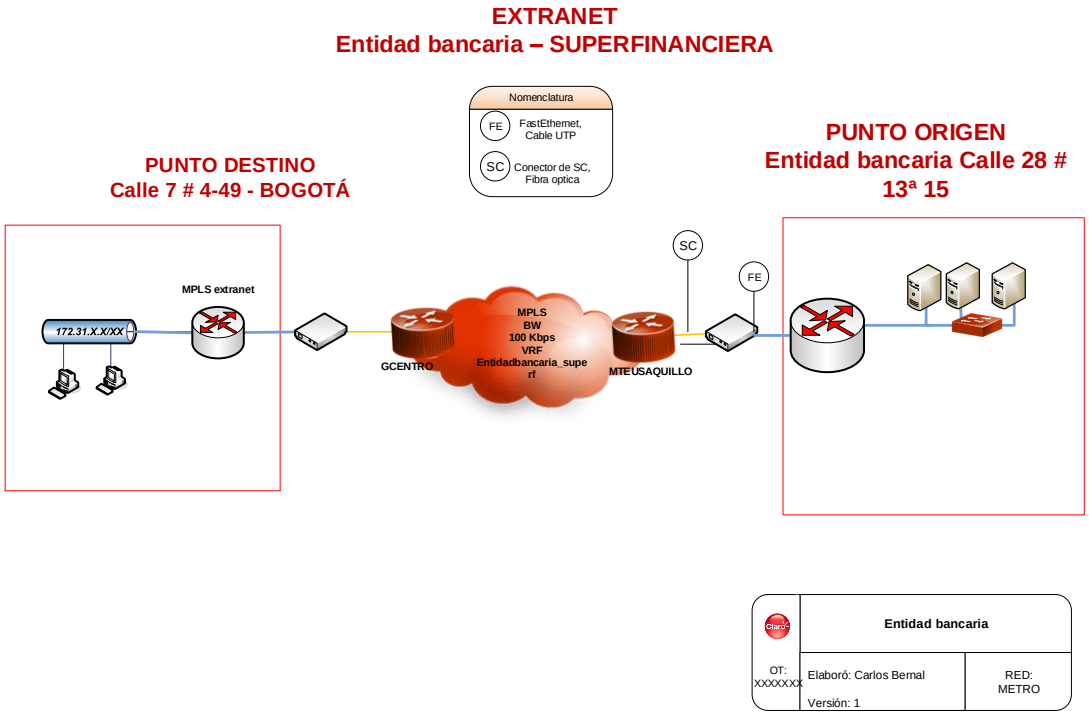


Ilustración 90. *Diagrama de ingeniería extranet entidad financiera - Superfinanciera (antes).*

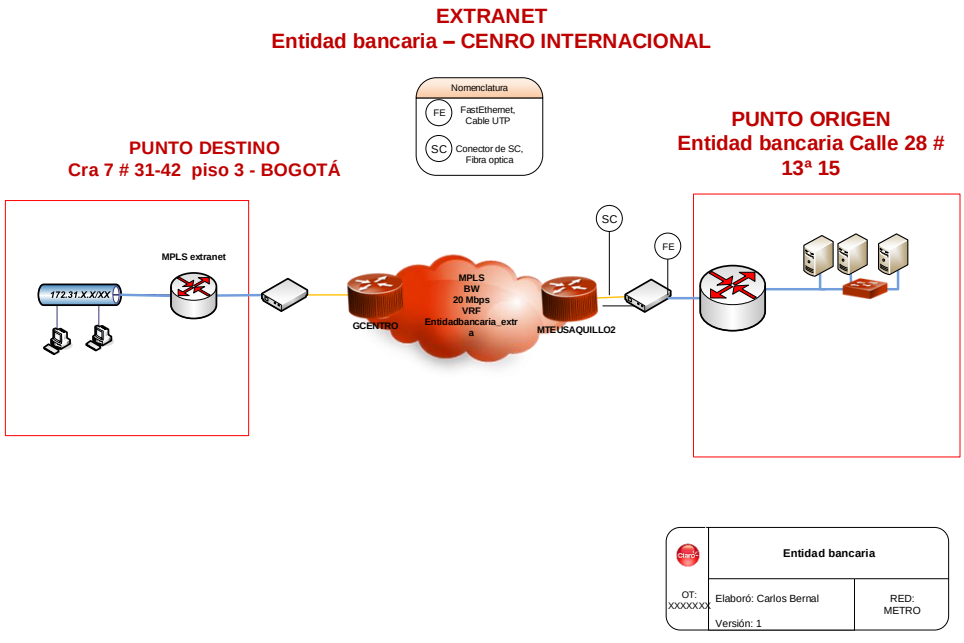


Ilustración 91. *Diagrama de ingeniería extranet entidad financiera - Centro Internacional (antes).*

Ilustración 92. *Diagrama de ingeniería extranet entidad financiera - Centro Internacional (antes).*

Anexo 4. Diagramas de detalle red metro

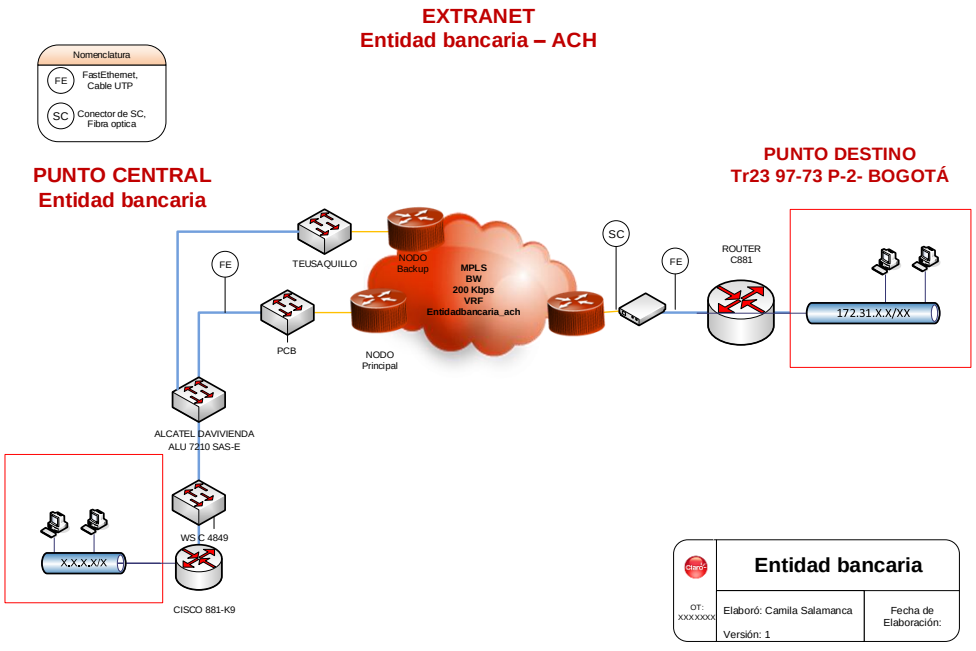


Ilustración 93. *Diagrama de ingeniería actual extranet entidad financiera – ACH.*

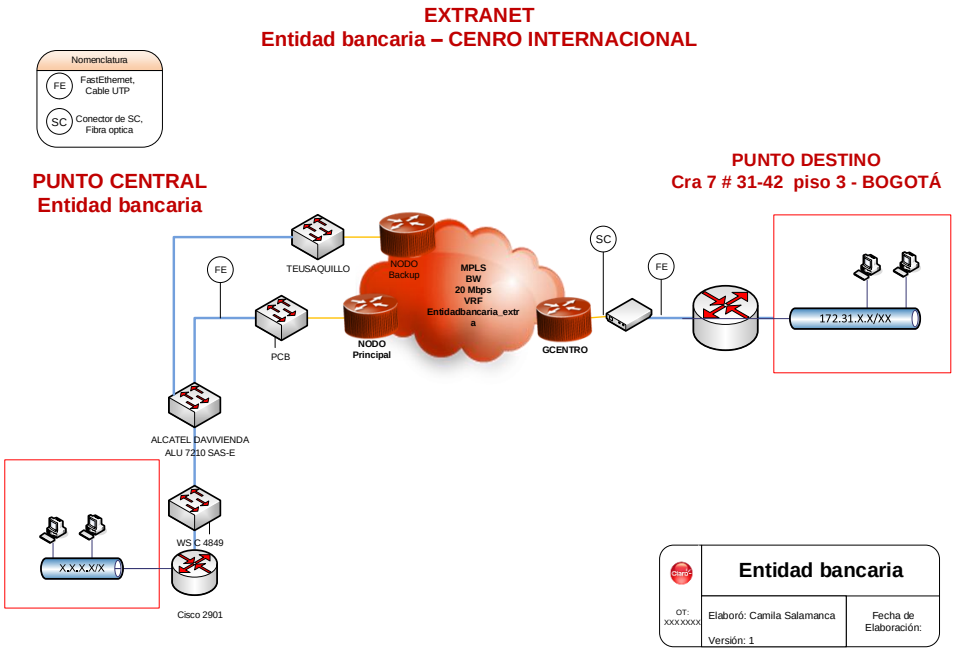


Ilustración 94. *Diagrama de ingeniería actual extranet entidad financiera – CENTRO INTERNACIONAL.*

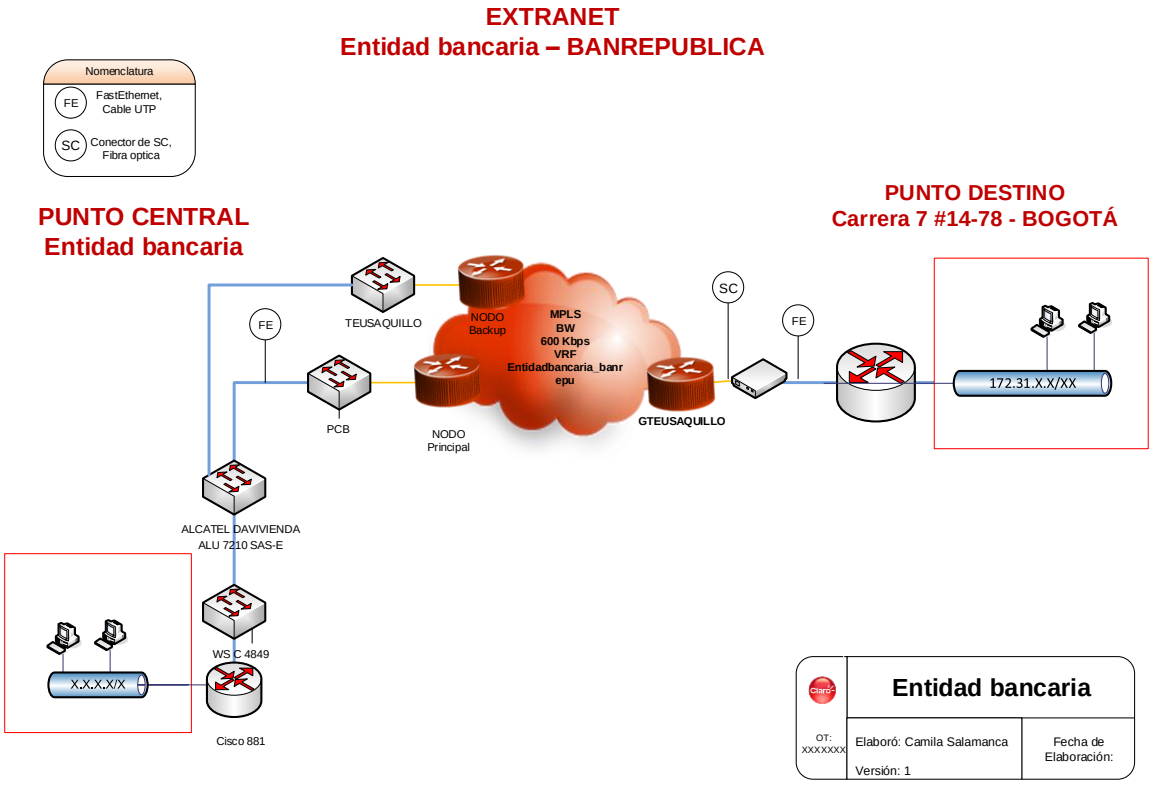


Ilustración 95. *Diagrama de ingeniería actual extranet entidad financiera– Banrepublica.*

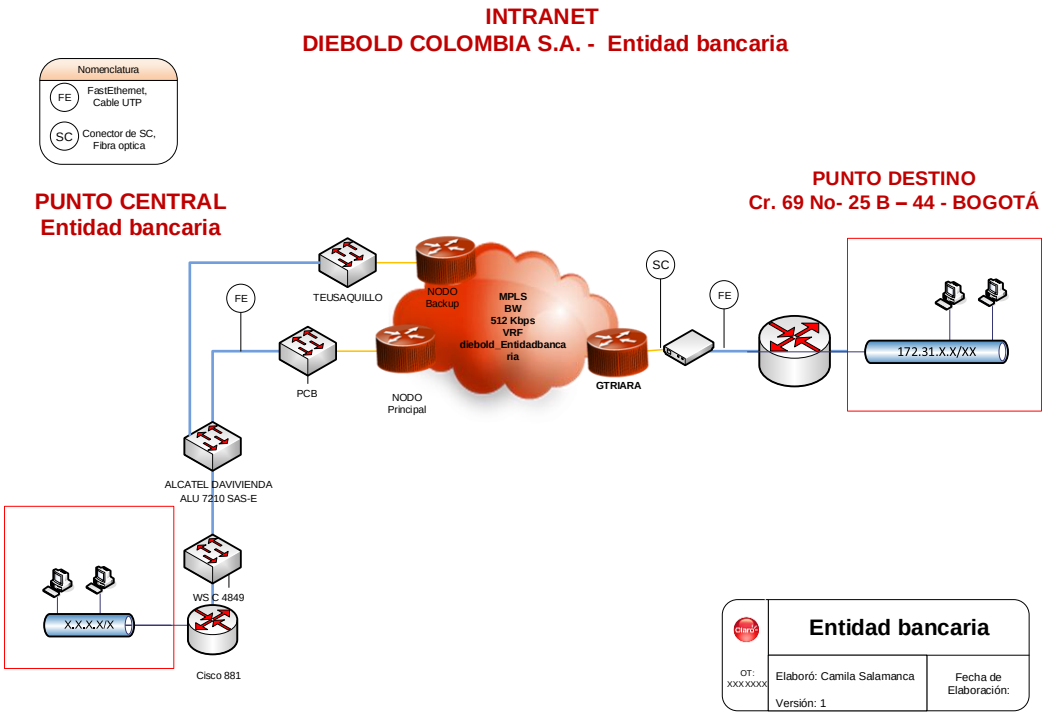


Ilustración 96. *Diagrama de ingeniería actual intranet entidad financiera – Diebold Colombia S.A.*

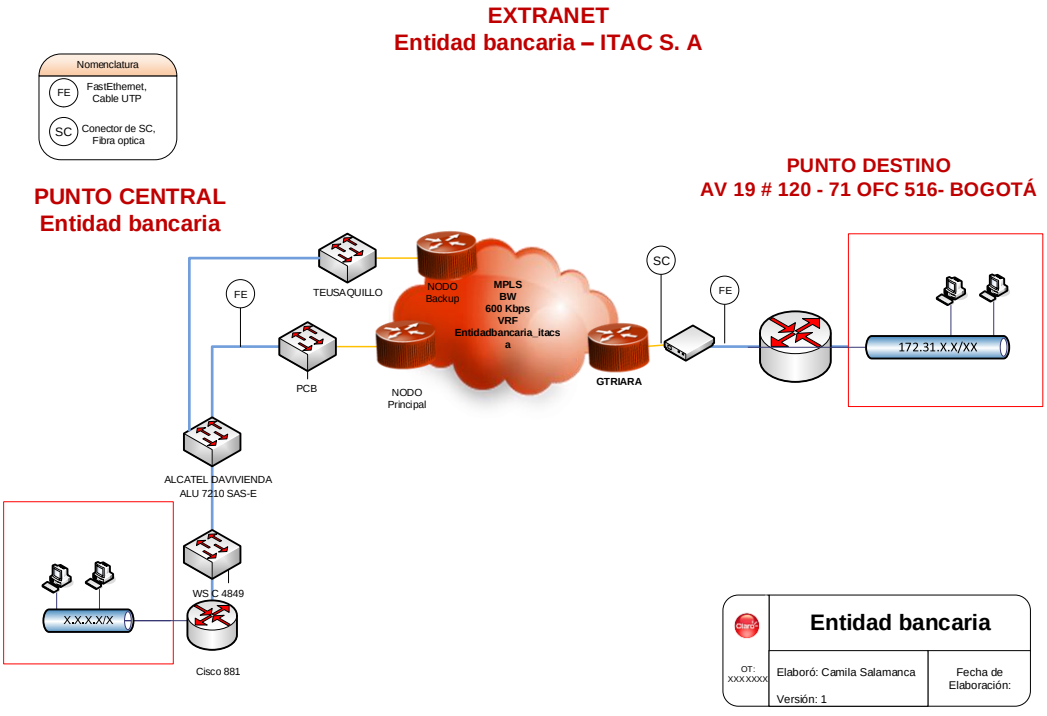


Ilustración 97. *Diagrama de ingeniería actual extranet entidad financiera – ITAC S.A.*

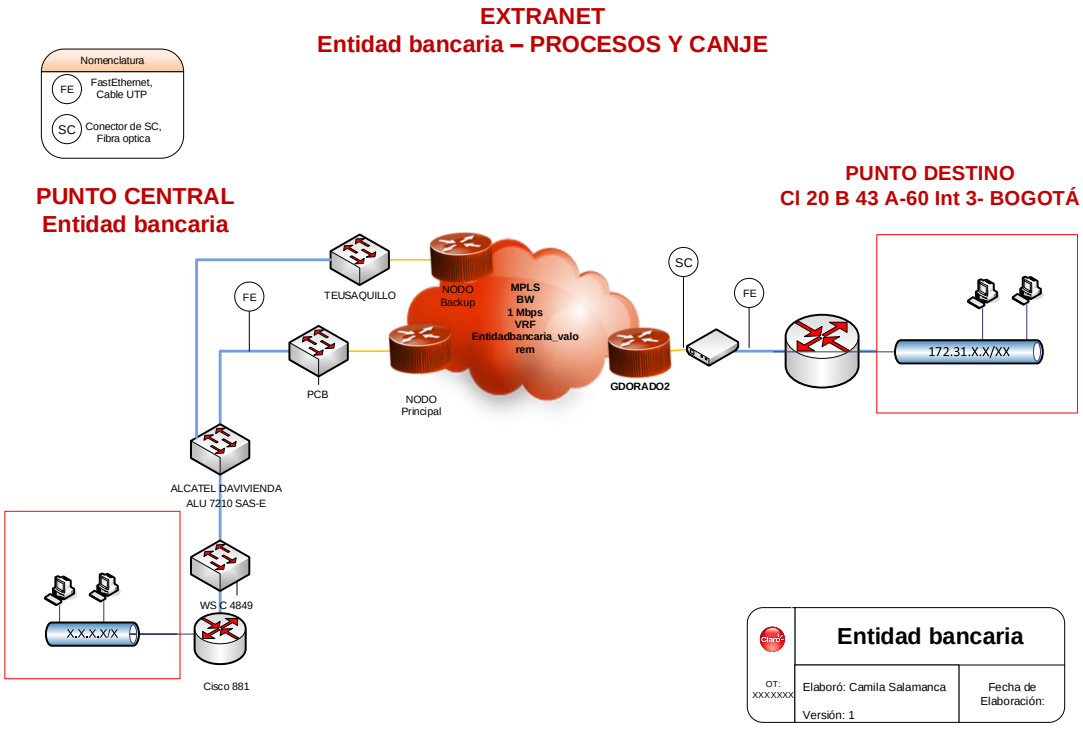


Ilustración 98. *Diagrama de ingeniería actual extranet entidad financiera – Procesos y Canje.*

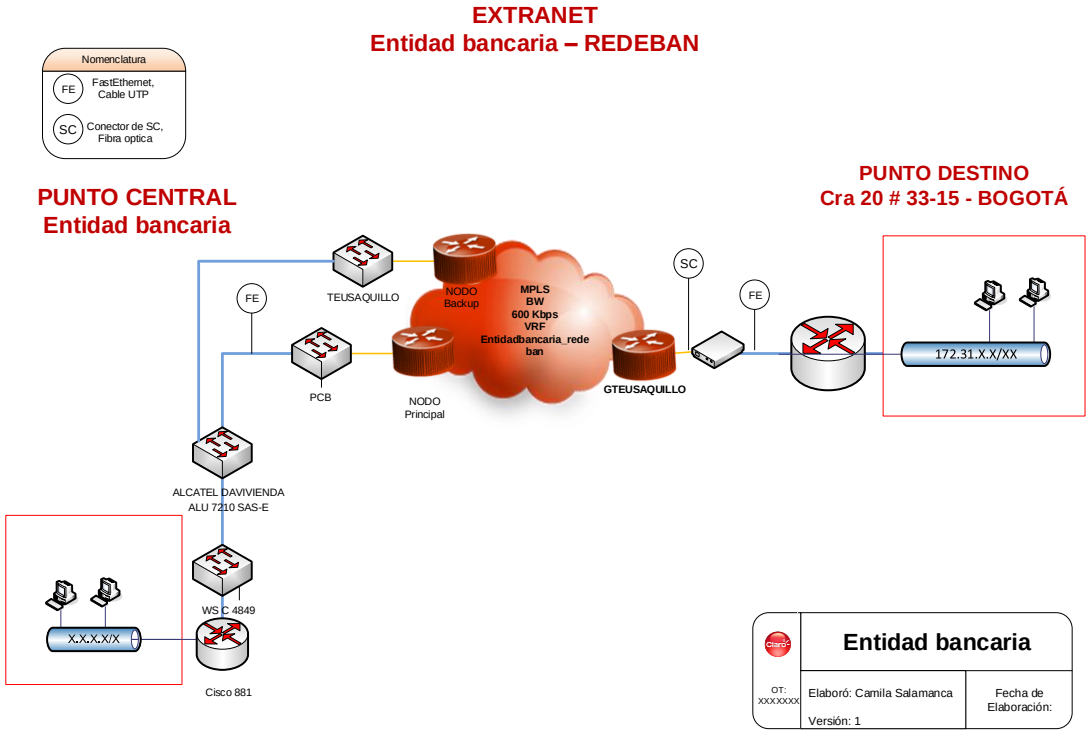


Ilustración 99. *Diagrama de ingeniería actual extranet entidad financiera – Redeban.*

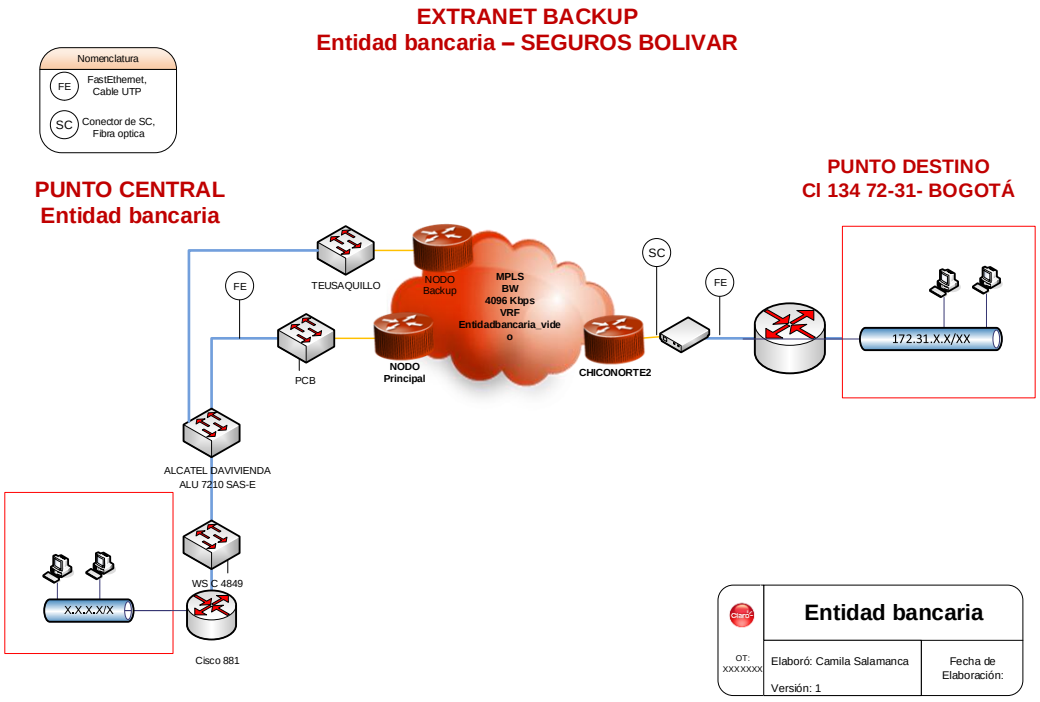


Ilustración 100. *Diagrama de ingeniería actual extranet entidad financiera– Seguros Bolívar.*

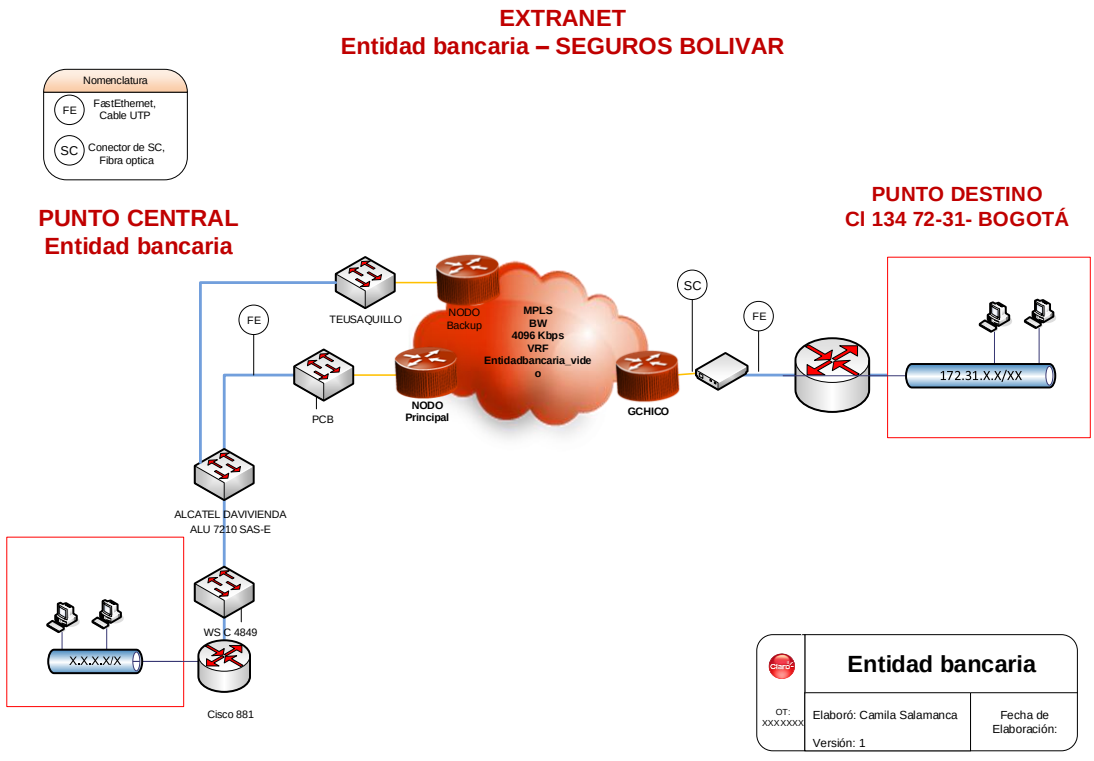


Ilustración 101. *Diagrama de ingeniería actual extranet entdad financiera – Seguros Bolívar.*

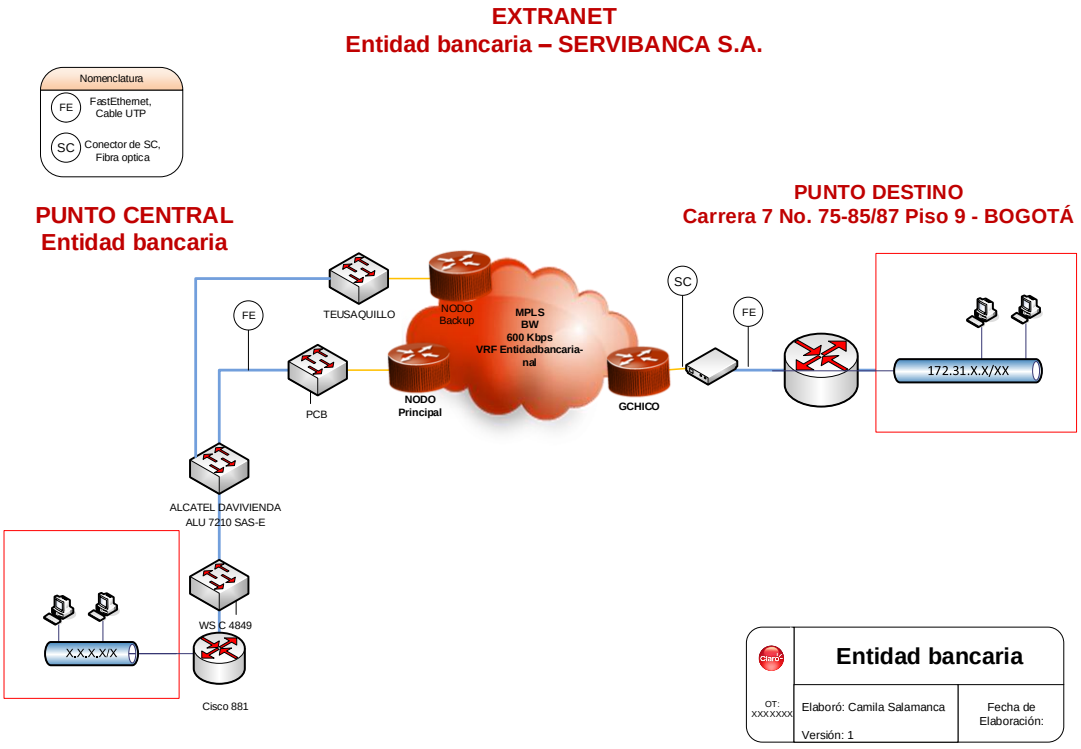


Ilustración 102. *Diagrama de ingeniería actual extranet entidad financiera – Servibanca S.A.*

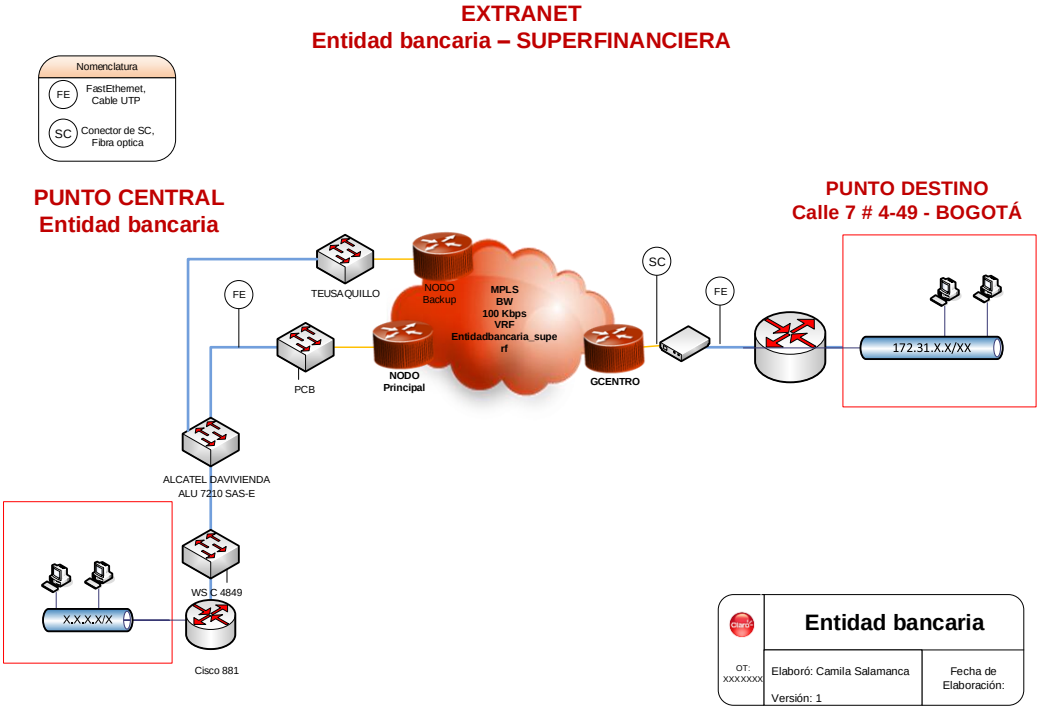


Ilustración 103. *Diagrama de ingeniería actual extranet entidad bancaria – Superfinanciera.*

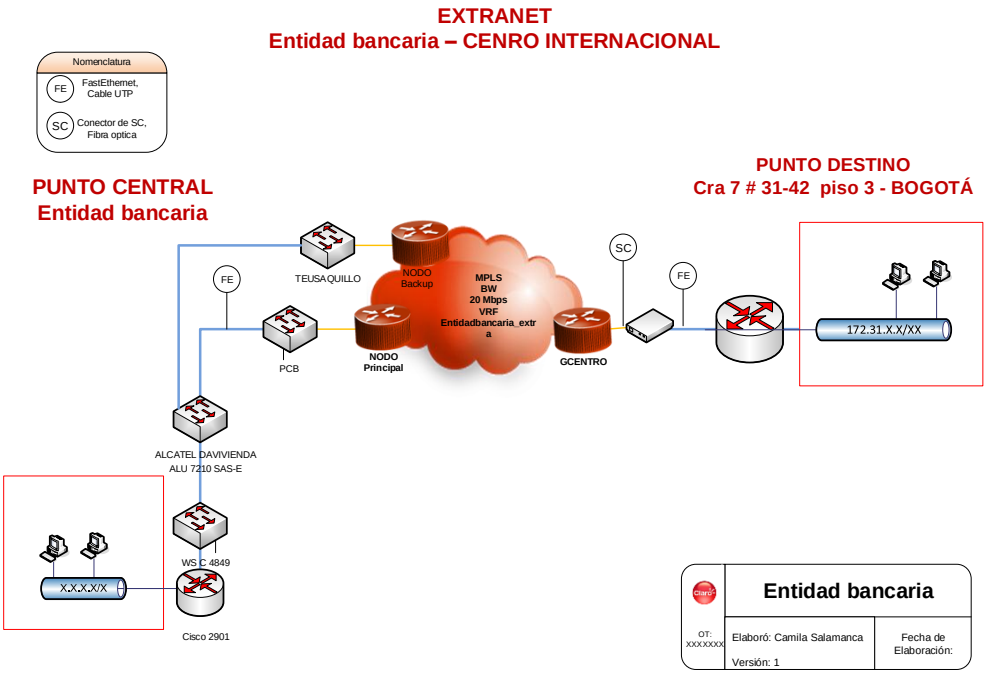


Ilustración 104. *Diagrama de ingeniería actual extranet entidad financiera – Centro Internacional.*

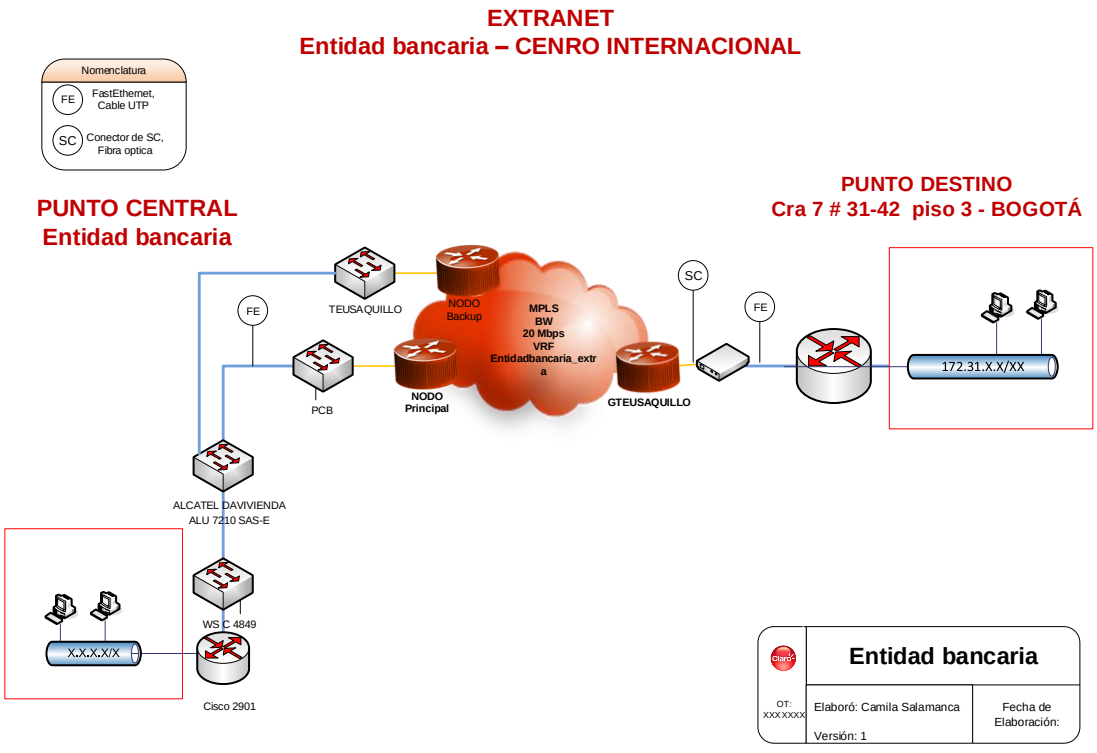


Ilustración 105. *Diagrama de ingeniería actual entidad financiera – Centro Internaciona.*