# DISEÑO DE UN PLAN DE CONTINGENCIA PARA UN ENLACE CRÍTICO DEL BANCO FINANCORP

**DANIEL OLAYA TOLEDO**
**EDWIN ANDRÉS BENAVIDES GUAYACAN**

**UNIVERSIDAD PILOTO DE COLOMBIA.**
**FACULTAD DE INGENIERÍA**
**ESPECIALIZACIÓN EN TELECOMUNICACIONES**
**BOGOTÁ D.C**
**2018**

# DISEÑO DE UN PLAN DE CONTINGENCIA PARA UN ENLACE CRÍTICO DEL BANCO FINANCORP

**DANIEL OLAYA TOLEDO**
**EDWIN ANDRÉS BENAVIDES GUAYACAN**

**Trabajo de grado para optar por el título de Especialista en Telecomunicaciones**

**Tutor**
**ALVARO ESCOBAR ESCOBAR**
**Director Especialización**

**UNIVERSIDAD PILOTO DE COLOMBIA.**
**FACULTAD DE INGENIERÍA**
**ESPECIALIZACIÓN EN TELECOMUNICACIONES**
**BOGOTÁ D.C**
**2018**

**Nota de Aceptación**

_____
_____
_____
_____
_____
_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

Bogotá D.C., abril de 2018

## AGRADECIMIENTOS

Quiero agradecer en primer lugar al ser que hace posible que todo esto suceda mi Dios, quien me ha conducido y acompañado en este largo camino llamado vida, me ha bendecido y me ha brindado oportunidades en la vida para lograr conseguir todo lo que me he propuesto. Así mismo a mi familia, a mis padres por brindarme el apoyo incondicional en mi formación profesional y personal, a mi esposa e hijo quienes han sido el motor de mi vida y me han impulsado para cumplir este propósito profesional.

A los profesores de la Universidad Piloto de Colombia, quienes con sus conocimientos y experiencias aportaron de distintas formas a la consecución de cumplir con este objetivo. A mi compañero de trabajo por el esfuerzo realizado en el cumplimiento de nuestro proyecto y por las gratas y enriquecedoras experiencias compartidas.

Edwin Andrés Benavides Guayacán

En primera instancia agradecer a Dios por esta nueva oportunidad de crecer como profesional, a mi esposa y nuestra bebe, a mis padres, a mí hermano, y demás personas como amigos y compañeros que ayudaron durante este proceso.

A la Universidad Piloto de Colombia, por poner a disposición toda su área profesional y brindar las diferentes herramientas para el aprendizaje, a mi compañero de proyecto por la labor realizada, me enriquece tener una nueva experiencia muy grata en mi vida.

Daniel Olaya Toledo

**CONTENIDO**

## LISTA DE FIGURAS

**pág.**

## LISTA DE CUADROS

**pág.**

## LISTA DE GRÁFICAS

**pág.**

# INTRODUCCIÓN

El enlace de datos que comunica el servidor principal del Banco Financorp con otras entidades bancarias representa uno de los servicios más importantes y de mayor criticidad debido al tipo de información que transporta, es por este motivo que se debe garantizar una disponibilidad completa y continua, que lleva a generar una disponibilidad cercana al 100%.

Para garantizar esta disponibilidad, se diseñará un plan de contingencia sobre un enlace de datos, utilizando técnicas de conmutación que permitan tiempos de respuesta muy rápidos, lo cual conlleva saltos de transmisión entre diferentes medios de acceso de forma casi instantánea, ya que al estar cualquiera de los equipos por fuera de la red, conmutará automáticamente al que se encuentre activo y si este segundo presenta una falla, realizará la misma operación al servicio de contingencia, sin que esto represente pérdidas de paquetes o caídas en el servicio, garantizando que no sea percibido en la operación del cliente Banco Financorp

Como canal de comunicación se utiliza un servicio guiado a través de un medio físico (fibra óptica), así mismo se van a gestionar medios de trasmisión, equipos de conmutación y diferentes tecnologías de capa 2 y capa 3 del modelo 0SI[1] o capa 1 y capa 2 del modelo TCP/IP[2], que garanticen el objetivo final trazado.

De igual forma se realizará un comparativo de los resultados teóricos obtenidos y las simulaciones desarrolladas en el software GNS3, versus los prácticos que serán gestionados en ventanas de mantenimiento previamente coordinadas en los equipos de transmisión de la red.

[1] Open Sistem Interconection
[2] Internet Protocolo de Control y Trasmisión

# 1. JUSTIFICACIÓN

El proyecto surge debido a la necesidad de solucionar una caída, falla o amenaza en la red principal del Banco Financorp. Actualmente el servicio cuenta con un enlace principal que se encuentra respaldado por otro enlace de características técnicas iguales, denominado backup, sin embargo, dada la importancia del mismo; éste servicio está expuesto a una posible falla en sus dos enlaces que puede originarse por variables como: energía, rupturas de fibra, mantenimientos, obsolescencia de equipos o vencimientos de licencias, entre otros, que pueden afectar ambos enlaces y generar la interrupción del servicio.

Aunque la probabilidad de ocurrencia es pequeña, la falla de los dos enlaces no es un evento imposible, y el impacto en caso de ocurrencia es más que significativo. De aquí surge la necesidad de diseñar un plan de contingencia que respalde los dos enlaces (principal y backup), con lo cual se minimice el riesgo.

Para llevar a cabo este proyecto se realizaron estudios de ingeniería, diseños y ejecución en herramientas de simulación y las pruebas necesarias para tener un servicio de 99.999 % de efectividad en la red principal.

Otro de los aspectos que promueven la investigación en este proyecto, es el de mitigar y disminuir el impacto que genera una falla en el servicio, tanto en el aspecto económico (nota crédito) y en la percepción de servicio ISC, (Índice de satisfacción cliente), lo cual garantiza una mejor y duradera relación comercial.

# 2. PROBLEMA DE INVESTIGACIÓN

## 2.1 PLANTEAMIENTO DEL PROBLEMA

El Core de red del cliente Banco Financorp, demanda una disponibilidad total de sus enlaces de datos. Partiendo de esta premisa, se hace necesario generar un plan de acción que permita al ISP[3] garantizar una disponibilidad cercana al 100%, y cumplir de esta forma con los ANS [4] pactados, en la actualidad la infraestructura de la entidad bancaria cuenta con una red principal y otra backup, la cual ha presentado algunas fallas e indisponibilidades, por tal motivo es necesario crear un plan de contingencia que entre a respaldar el funcionamiento de la red y garantizar el mayor tiempo posible de prestación del servicio.

Así mismo mediante un estudio de ingeniería, ejecución de pruebas, y configuración de los equipos del cliente Banco Financorp en un entorno controlado y previas simulaciones que se asemejan a la realidad a través del programa GNS3, se realizarán pruebas desde la sede del cliente (extremo A) hacia los servicios de extranet y MPLS[5] (extremo B), donde se debe contemplar los posibles escenarios que se puedan presentar y que afecten la disponibilidad del enlace.

## 2.2 FORMULACIÓN DEL PROBLEMA

¿Cuáles son las ventajas de diseñar un plan de contingencia en una red cítrica para el cliente Banco Financorp y a su vez verificar el costo beneficio de su funcionalidad?

[3] Proveedor de Servicios de Internet
[4] ANS (acuerdo de Niveles de Servicio)
[5] Multiprotocol laberl switching

# 3. OBJETIVOS

## 3.1 OBJETIVO GENERAL

Implementar en un ambiente controlado un plan de contingencia para la red de datos del cliente Banco Financorp.

## 3.2 OBJETIVOS ESPECÍFICOS

- Analizar la infraestructura de la red de datos actual del cliente Banco Financorp y establecer las necesidades y los requerimientos del plan de contingencia.

- Diseñar el plan de contingencia, que incluya configuración, análisis, riesgos pruebas de ensayo y error, equipos y costos de la red de datos.

- Validar el plan de contingencia diseñado utilizando las diferentes herramientas de simulación para identificar su correcto funcionamiento.

- Realizar un estudio de ingeniería para validar el impacto durante la implementación, transición y pruebas del plan de contingencia.

## 4. MARCO TEÓRICO

Como objetivo principal y con el fin de mejorar la necesidad real y garantizar una disponibilidad del 99.999% para un cliente, debido a la criticidad de la operación, se debe generar un plan de acción de impacto real, que garantice los ANS[6] establecidos, utilizando diferentes técnicas de transmisión en caso de que falle el enlace principal.

Teniendo en cuenta esta premisa, cabe investigar los posibles escenarios que se pueden presentar y que involucren la afectación del servicio. Primero hay que conocer los siguientes conceptos, los cuales, serán utilizados a lo largo del desarrollo del proyecto:

En tal sentido, el plan de contingencias es un análisis de los posibles riesgos y eventuales siniestros a los cuales puede estar expuesto programas, equipos de cómputo o de red, archivos e infraestructura física, una solución alterna que permita restituir rápidamente los sistemas de información de la Entidad ante la eventual presencia de siniestros que los paralicen parcial o totalmente.

Como se observa en la figura 1, se relacionan los componentes que, a nivel de IT, se van a ocupar de generar el plan de contingencia y los aspectos más importantes a desarrollar:

**Figura 1. Plan de contingencia**


Fuente: Autores

[6] Acuerdo de Nivel de Servicio

**Elementos que contienen un plan de contingencia**

- Plan de comunicación de crisis: es una estructura que contiene los procedimientos internos y externos en los que las entidades deben preparar ante un desastre. Este plan debe estar ejecutado a la par con los demás planes para asegurar que solo decisiones aprobadas sean divulgadas y que solamente personal autorizado sea el encargado de ejecutar, asignar y responder las diferentes inquietudes y de generar los reportes del balance presentado durante la afectación al personal y al público.

- Plan de continuidad de operaciones por sede o filial (COOP por sus siglas en inglés, Continuity of Operations Plan): se establece en el preámbulo del CGC 1 que su función es asignar a las entidades no gubernamentales. La planificación de la continuidad facilita el desempeño de funciones esenciales durante emergencias de todos los peligros u otras situaciones que puedan interrumpir a través de una emergencia catastrófica. Se orienta a realizar sus funciones normales en otra sede alterna que sea filial a la entidad, y realizar las mismas funciones en un plazo de 30 días antes de retornar labores normales.

- Plan de respuesta a ciber-incidentes: está diseñado para detectar y dar respuesta a los ataques cibernéticos, hackers malignos, o amenazas en el ciberespacio contra un sistema de Tecnología Informática (TI) de una entidad.

Estas actividades son diseñadas para permitirle al personal de seguridad en informática identificar, analizar, mitigar y recuperarse de fallas, averías o incidentes de cómputo maliciosos tales como: Acceso no autorizado a los sistemas o bases de datos, Negación de servicio, o acceso a cualquiera de los dispositivos de la red “hardware o software”.

**Planes de contingencia orientados a TI**

- Plan de recuperación de desastres (DRP): está diseñado para responder a eventos de suma importancia, usualmente relacionados a catástrofes que niegan el acceso a la normal conectividad por un período extenso. Con frecuencia, el DRP se refiere a un plan enfocado en TI diseñado para restaurar y recuperar la operatividad del sistema, aplicación o acceso a la red o sistema de cómputo, objetivo en un sitio alterno después de una emergencia.

El alcance de un DRP se puede asimilar con el de un Plan de Contingencia de TI; sin embargo, el DRP es más amplio en su alcance y en el impacto y no cubre interrupciones menores que no requieren reubicación.

Fases que conforman un plan de continuidad de negocio. Estas fases han sido formuladas por el Instituto de Recuperación de Desastres (DRI – Disaster Recovery

Institute)[7]

- Inicio y gestión del proyecto.
- Análisis y Evaluación del riesgo.
- Análisis de impacto del negocio (BIA).
- Desarrollo de estrategias para la continuidad del negocio.
- Respuesta ante emergencias.
- Desarrollo e implementación del BCP
- Programa de concientización y capacitación.
- Mantenimiento y ejercicio del BCP
- Comunicación de crisis.
- Coordinación con las autoridades públicas.

## 4.1 TIPOS DE CONMUTACIÓN

Existen tres tipos de conmutación, sin embargo, para el presenta caso serán utilizadas solo dos:

**4.1.1 Conmutación de circuitos**. En la conmutación de circuitos, el camino (llamado "circuito") entre los extremos del proceso de comunicación se mantiene de forma permanente mientras dura la comunicación, de forma que es posible mantener un flujo continuo de información entre dichos extremos.

**4.1.2 Características**. Una vez establecida la ruta de comunicación, el circuito no cambia, por lo que es imposible reajustar la ruta de comunicación en cada momento para lograr el menor costo entre los nodos, es decir, una vez que se ha establecido el circuito, no se aprovechan los posibles caminos alternativos con menor coste que puedan surgir durante la sesión.

El circuito es fijo, una vez establecido el circuito no hay pérdidas de tiempo calculando y tomando decisiones de encaminamiento en los nodos intermedios. Cada nodo intermedio tiene una sola ruta para los paquetes entrantes y salientes que pertenecen a una sesión específica, este tipo de conmutación simplifica la gestión de los nodos intermedios una vez que se ha establecido el circuito físico, no hay que tomar más decisiones para encaminar los datos entre el origen y el destino.

Uno de los peores inconvenientes de la conmutación de circuito es la poca tolerancia a fallos. Si un nodo intermedio falla, todo el circuito se viene abajo. Hay que volver a establecer conexiones desde el principio [8].

[7] RODRÍGUEZ, Edith Yolima. Plan de continuidad BS 25999. [en línea]. Bogotá: Sisteseg [citado 27, agosto, 2017]. Disponible en Internet: < URL: http://www.sisteseg.com/files/Microsoft_Word_-_Articulo_BS_25999_DEF1.pdf>

[8] IDICT, Carlos. Conmutación (Redes de comunicación). [en línea]. Bogotá: Ecured [citado 12, mayo, 2017]. Disponible en Internet: < URL: https://www.ecured.cu/EcuRed:Enciclopedia_cubana>

## 4.2 CONMUTACIÓN DE PAQUETES

La conmutación de paquetes se trata del procedimiento mediante el cual, cuando un nodo quiere enviar información a otro lo divide en paquetes, todos del mismo tamaño, los cuales contienen la dirección del nodo destino, en este caso, no existe un circuito permanente entre los extremos y, la red, simplemente, se dedica a encaminar paquete a paquete la información entre los usuarios.

**4.2.1 Características**. Es la conmutación más usadas, en caso de error en un paquete solo se reenvía ese paquete, sin afectar a los demás que llegaron sin error, se limita el tamaño de los paquetes a enviar de manera que ningún usuario pueda monopolizar una línea de transmisión durante mucho tiempo, por lo que las redes de conmutación de paquetes pueden manejar tráfico interactivo, esto hace que aumente la flexibilidad y rentabilidad de la red.

En caso de algún fallo se puede alterar sobre la marcha el camino seguido por una comunicación así, un nodo puede seleccionar de su cola de paquetes en espera de ser transmitidos aquellos que tienen mayor prioridad.

Los equipos de conmutación utilizados son de mayor complejidad ya que necesitan mayor velocidad y capacidad de cálculo para determinar la ruta adecuada en cada paquete, también es capaz de retrasmitir paquetes en caso de que un paquete tarde demasiado en llegar a su destino, en este caso el receptor no envía el acuse de recibo al emisor, por lo cual el receptor volverá a retransmitir los últimos paquetes del cual no recibió el acuse, pudiendo haber redundancia de datos[9].

## 4.3 OPERACIONES Y ANTECEDENTES DE HSRP

Una forma de lograr que el tiempo de actividad de la red esté cerca del 100% es utilizar HSRP, que ofrece redundancia de red para las redes IP, asegurando que el tráfico de usuarios se recupere de forma inmediata y transparente de los errores de primer salto en los dispositivos de borde de red o circuitos de acceso.

Al compartir una dirección IP y una dirección MAC (Capa 2), dos o más routers pueden funcionar como un solo router “virtual”. Los miembros del grupo del router virtual intercambian continuamente mensajes de estado. De esta forma, un router puede asumir la responsabilidad de ruteo de otro, en el caso de que esté fuera de servicio por razones planificadas o no. Los hosts continúan reenviando paquetes IP a una dirección IP y MAC coherente y el cambio de dispositivos que realizan el ruteo es transparente [10].

[9] TOMASI, Wayne. Sistemas de comunicaciones electrónicas. México: Prentice Hall Inc, 2003.p. 626.
[10] CISCO. Documentos Cisco. [en línea]. Bogotá: Cisco [citado 25, mayo, 2017]. Disponible en Internet: < URL: http://www.cisco.com/c/es_mx/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html>

## 4.4 MECANISMOS DE DETECCIÓN DINÁMICA DE ROUTERS

A continuación, se incluyen descripciones de los mecanismos de descubrimiento dinámico del router que están disponibles para los hosts. Muchos de estos mecanismos no proporcionan la flexibilidad de la red necesaria para los administradores de red. Esto puede deberse a que el objetivo inicial del protocolo no era proporcionar flexibilidad de la red o porque no es posible que cada host en una red ejecute el protocolo. Además de lo mencionado a continuación, es importante destacar que muchos hosts sólo permiten configurar una Gateway predeterminada[11].

## 4.5 PROTOCOLO DE RUTEO DINÁMICO

Algunos hosts IP ejecutan (o indagan) un protocolo de ruteo dinámico como el Routing Information Protocol (RIP) o abrir trayecto más corto primero (OSPF) para descubrir routers. La desventaja del uso de RIP es que la adaptación a los cambios en la topología es lenta. Es posible que no se pueda ejecutar un protocolo de ruteo dinámico en cada host por numerosos motivos, incluidos los gastos administrativos, los gastos de procesamiento, los problemas de seguridad o la falta de implementación del protocolo de algunas plataformas[12].

## 4.6 OPERACIÓN DE HSRP

Una amplia clase de implementaciones de host heredadas que no soportan la detección dinámica pueden configurar un router predeterminado. Es posible que no pueda ejecutar un mecanismo de detección dinámica de routers en cada host por numerosos motivos, incluidos los gastos administrativos, los gastos de procesamiento, los problemas de seguridad o la falta de implementación del protocolo de algunas plataformas. HSRP proporciona servicios de conmutación por error a estos hosts.

Un conjunto de routers que ejecutan HSRP trabaja en equipo para darle la impresión a los hosts de la LAN de que son un único router virtual. Este conjunto es conocido como un grupo de HSRP o grupo en espera.

En una LAN determinada, pueden coexistir y superponerse varios grupos en espera en caliente. Cada grupo en espera emula un único router virtual. Los routers individuales pueden participar en varios grupos. En este caso, el router mantiene estados y temporizadores separados para cada grupo.

Cada grupo en espera tiene una dirección MAC única y conocida, así como una

[11] CISCO. Soporte Cisco. [en línea]. Bogotá: Cisco [citado 8, agosto, 2017]. Disponible en Internet: < URL: https://www.cisco.com/support/LA/es/TS/7/73391/hsrpguidetoc.shtml>
[12] Ibíd., p.2.

Dirección IP.

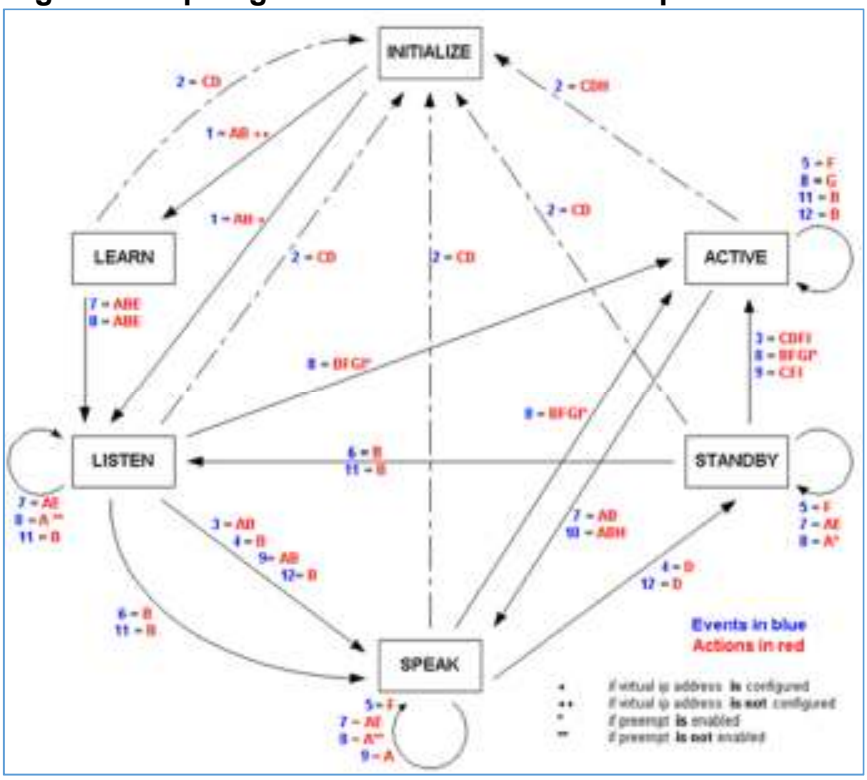
**4.6.1 Direccionamiento HSRP**. En la mayoría de los casos, cuando se configuran routers para que formen parte de un grupo HSRP, estos escuchan la dirección MAC de HSRP de ese grupo como también su propia dirección MAC establecida en fábrica. La excepción son los routers cuyos controladores Ethernet sólo reconocen una única dirección MAC (por ejemplo, el controlador Lance en los routers Cisco 2500 y Cisco 4500). Estos routers usan la dirección MAC de HSRP cuando actúan como router activo y su dirección establecida en fábrica cuando no actúan como tal.

Nota: Cuando HSRP se ejecuta en un entorno de conexión en bridge con ruteo (SRB) de origen por anillos múltiples y los routers de HSRP residen en diferentes anillos, el uso de direcciones funcionales puede ocasionar confusión de Campo de información de ruteo (RIF). Por ejemplo, en un entorno SRB, es posible que un router en espera de HSRP resida en un anillo diferente del router activo. Cuando este router en espera pase al estado activo, las estaciones del mismo anillo que el router activo anterior necesitan un nuevo RIF para enviar paquetes al nuevo router activo. No obstante, dado que el router en espera (activo ahora) utiliza la misma dirección funcional que el router activo anterior, las estaciones no advierten que deben enviar exploradores para un nuevo RIF. Por este motivo, se ha introducido el comando use-bia.

**4.6.2 Tabla de estados de HSRP**. La figura 2 evidencia los cambios de estado de la máquina de estados de HSRP. Cada vez que ocurre un evento, la acción asociada se lleva a cabo y el router pasa al siguiente estado de HSRP. En el diagrama, los números designan eventos y las letras la acción asociada. La tabla de la sección Eventos HSRP define los números y la tabla de la sección Acciones HSRP define las letras. Utilice este diagrama sólo como referencia. El diagrama es detallado y no es necesario para resolver problemas generales, en la figura 3 se puede observar el flujo de paquetes dentro de cualquier red de datos[13].

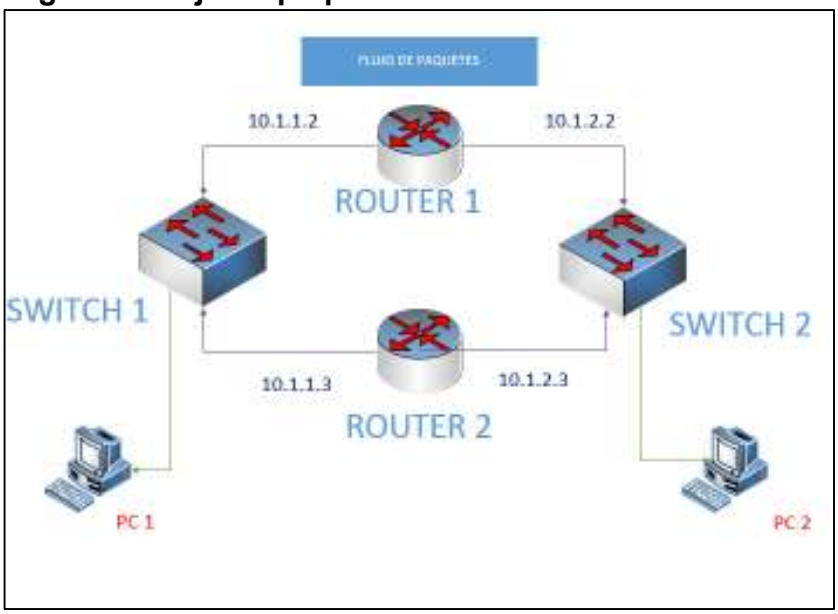
[13] SANZ, Juan Manuel. Security Ar work. [en línea]. Bogotá: Security Ar work [citado 3, marzo, 2017]. Disponible en Internet: < URL: https://www.securityartwork.es/2013/09/26/ataque-al-protocolo-hsrp/>

**Figura 2. Topología de red conmutación Hsrp**




Fuente: SANZ, Juan Manuel. Security Ar work. [en línea]. Bogotá: Security Ar work [citado 3, marzo, 2017]. Disponible en Internet: < URL: https://www.securityartwork.es/2013/09/26/ataque-al-protocolo-hsrp/>

**Figura 3. Flujo de paquetes**




Fuente: Autores

## 4.7 EXTRANET

Extranet es una red privada la cual usa protocolos de Internet y servicios de telecomunicaciones que se transportan en redes públicas. En la misma hay ordenadores para aplicaciones y servicios basados en Intranet, que son accesibles de manera segura a usuarios y organizaciones externas, gracias a contraseñas específicas y dispositivos de seguridad adecuados. Lo que quiere decir que una extranet es la extensión de una o más Intranets[14].

**4.7.1 El uso de una extranet**. Intercambiar grandes cantidades de datos, enviar catálogos de productos a un público selecto Cooperar con otras empresas para conseguir un objetivo común. Unificar e intercambiar tecnologías entre varias empresas y realizar programas de formación comunes. Acceder a servicios que ofrecen otras empresas (por ejemplo, una aplicación de gestión de banca en línea, que ofrece una empresa para una transacción de pago a un banco afiliado). Difundir noticias de interés común exclusivamente a un grupo de empresas afiliadas.

Extranet es una oportunidad comercial interesante, sobre todo para empresas de software[15].

## 4.8 PROTOCOLO DE ENRUTAMIENTO BGP

En el campo de las telecomunicaciones más conocido como protocolo de puerta de enlace de frontera “Border Gateway Protocol”, el cual está basado en el intercambio de información encaminada entre sistemas autónomos, utilizando como principal característica un modelo del vector distancia como se observa en la figura 4 en la que se puede observar el envío de información a través del protocolo vector distancia, a continuación, se resalta los aspectos más relevantes del protocolo BGP.

- Protocolo de enrutamiento usado para intercambiar información de enrutamiento entre diferentes redes.

- Exterior gateway protocol (protocolo externo)

- Descrito en RFC 4271

- RFC4276 describe la implementación de BGP, RFC4277 describe experiencias operacionales

[14] MATHEUS, Norma. Computación – Informática. [en línea]. Bogotá: El Autor [citado 6, agosto, 2017]. Disponible en Internet: < URL: https://nmatheus.wordpress.com/2012/01/20/redes-internet-intranet-extranet/>

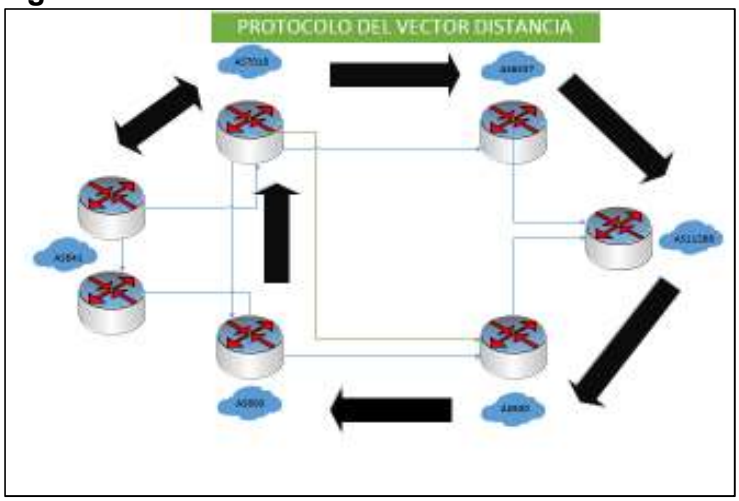
[15] ANTEPORTAMLATINAM, José María. Comercio electrónico. [en línea]. Bogotá: El Autor [citado 18, junio, 2017]. Disponible en Internet: < URL: http://docplayer.es/3916381-Comercio-electronico-una-introduccion-general.html>

- El Sistema Autónomo (AS) es la clave esencial de BGP:

- Propósito: identifica de forma única un grupo de redes bajo una administración de enrutamiento común

- Protocolo de Vector de Trayectoria
- Actualizaciones Incrementales
- Muchas opciones para forzar medidas administrativas (de rutas)
- Soporta Enrutamiento Inter-Dominio Sin Clases
- Muy utilizado en la “espina dorsal” de Internet
- Sistemas Autónomos

**Figura 4. Protocolo del vector distancia**



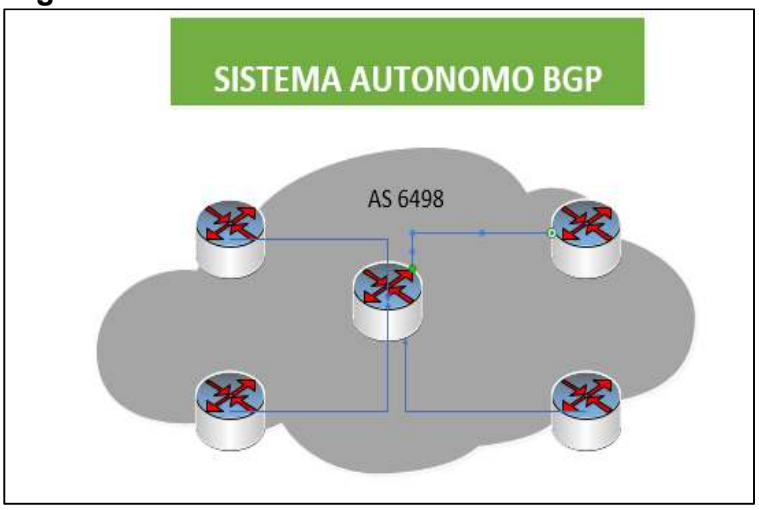

Fuente: Autores

**4.8.1 Sistema autónomo (AS).** Un sistema autónomo “Autonomous System” (Ver figura 5), hace referencia a un conjunto de redes IP que posee una regla de rutas propias e independientes, con el objetivo primordial de realizar su propia gestión de tráfico desde el hacia los restantes sistemas autónomos que forman la internet, cada AS tiene o se le asigna un único número diferente con el cual se puede diferenciar dentro de internet, sus principales características son:

- Colección de redes bajo la misma política de enrutamiento
- Con un mismo protocolo de enrutamiento
- Usualmente bajo un mismo propietario y control administrativo
- Identificado por un único número entero de 32 bits, conocido como Numero de Sistema Autónomo (ASN)[16].

[16] BARBANCHO, Julio; CONCEJERO, Jaime; BENJUMEA, Octavio; RIVERA, Mª Del Carmen; ROMERO, Jorge; ROPERO, Gemma y SANCHEZ Anton. Sistemas Microninformaticos y Redes. España: Ediciones paraninfo, 2014.p. 209.

**Figura 5. Sistema autónomo BGP**




Fuente: Autores

Dos rangos:

- 0-65535 (rango original de 16 bits)
- 65536-4294967295 (rango de 32 bits - RFC4893)

Uso:

- 0 and 65535 (reservado)
- 1-64495 (para Internet publica)
- 64496-64511 (para documentación - RFC5398)
- 64512-65534 (sólo para uso privado)
- 23456 (representar 32 bits en 16 bits)
- 65536-65551 (documentación - RFC5398)
- 65552-4294967295 (para Internet pública)

Operación de BGP

1. Acumula múltiples trayectorias de BGP anunciadas por routers internos y externos

2. Escoge la mejor trayectoria para cada prefijo de red anunciada, y la instala en la tabla de reenvío

3. La mejor trayectoria su vez se envía a los routers BGP vecinos

4. Las políticas se aplican modificando la selección de la mejor trayectoria

Construyendo la Tabla de Reenvío

Proceso de “entrada” de BGP

- Recibe información de trayectoria de sus enrutadores pares (peers)

- El resultado de la selección de trayectoria de BGP se coloca en la tabla de rutas de BGP

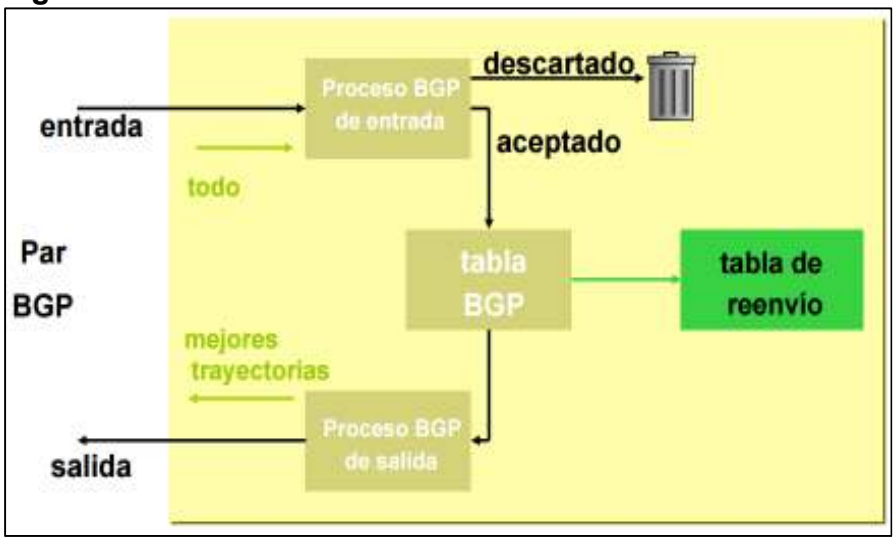
- Se marca la “mejor trayectoria”

En la figura 6 se muestra él envió de información del protocolo BGP en lo relacionado con la entrada y salida de datos y la tabla de reenvió de la información de este protocolo.

- Anuncia “mejor trayectoria” a sus pares

- Las mejores trayectorias se instalan en la tabla de reenvío si: El prefijo y su longitud son únicos y tienen la menor “distancia al destino” desde el punto de vista del protocolo[17].

**Figura 6. Reenvió de información Protocolo BGP**




Fuente: CISCO. Soporte Cisco. [en línea]. Bogotá: Cisco [citado 8, agosto, 2017]. Disponible en Internet: < URL: https://www.cisco.com/support/LA/es/TS/7/73391/hsrpguidetoc.shtml>

[17] NSRC. Introducción a BGP. [en línea]. Bogotá: El Autor [citado 4, febrero, 2017]. Disponible en Internet: < URL: https://nsrc.org/workshops/2011/walc/routing/raw-attachment/wiki/Agenda/Intro_BGP.pdf>

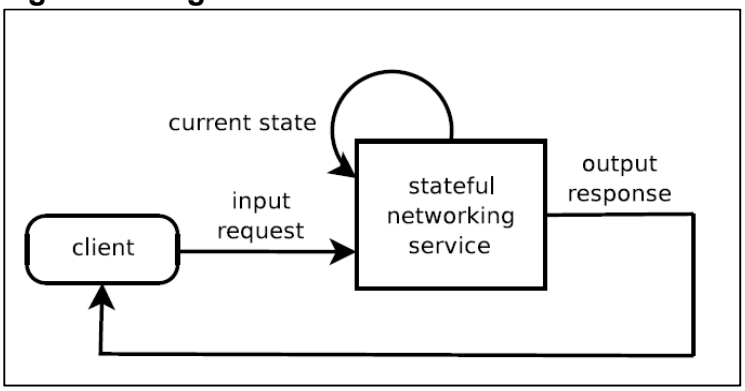
## 4.9 REDUNDANCIA Y ALTA DISPONIBILIDAD DE LOS SISTEMAS

La redundancia física no es suficiente para garantizar la disponibilidad de un servicio implementado por un software con estados puesto que la réplica desconoce los estados de las peticiones que estaba manejando la réplica que ha sufrido un fallo. Es por ello por lo que las réplicas de respaldo no pueden recuperar el servicio apropiadamente puesto que desconocen el estado de las peticiones circulantes.

El objetivo general es el de proponer mejoras para aumentar la disponibilidad del software con estados en entornos en los que el alto rendimiento es un requisito que satisfacer[18].

Dependiendo del estado de la petición asociada a dicha entrada, es decir, el estado actual de la petición es un parámetro que determina de qué forma se despliega el servicio. La ausencia de dicho estado tiene un impacto impredecible en el servicio desplegado.

**Figura 7. Diagrama de Servicio de red con estados**




Fuente: CANDEA, G and FOX. Crash-only software. In 9th Workshop on Hot Topics in Operating Systems, 2003. p.23.

De la figura 7, se concluye que toda entrada puede potencialmente producir un cambio de estado. Esta afirmación se expresa mediante la siguiente formula:

- Siguiente_estado : Estado × Entrada = Estado

Dicha fórmula viene definida en la implementación del software con estados, y puede representarse de la siguiente manera:

- Siguiente_estado = Rj(Entrada, Sk) = Sm
-

[18] AYUSO, Pablo Neira. Tolerancia a fallos para la alta disponibilidad. En: Revista del Departamento de Lenguajes y Sistemas Informáticos. Marzo-abril, 2012.vol.6, no. 11, p.9.

En caso de que Sk = Sm, se considera que la entrada no produjo ningún cambio de estado, obsérvese que los estados previos a Sk no son necesarios para calcular la transición a un estado, por tanto, únicamente se requiere el estado actual para garantizar que un cierto servicio se despliega correctamente, de esta forma, se concluye que los estados pasados no son necesarios.

Por otra parte, los clientes emplean una primitiva unicast confiable mediante la que envían las entradas al software con estados que despliega el servicio. De esta forma, se asume que las peticiones no se pierden nunca, concretamente la primitiva garantiza que, si una petición no es atendida en un lapso de tiempo, esta es vuelta a ser enviada.

La base de toda solución destinada a garantizar una alta disponibilidad de un software se fundamenta en dos conceptos:

Redundancia: se establecen una o múltiples replicas que están capacitadas para desplegar un mismo servicio, algunas de ellas actúan como replicas activas, otras actúan como replicas respaldo. En caso de fallo, un algoritmo de selección de réplica segura, agreement protocol en inglés, selecciona un reemplazo que garantice que el servicio continuara siendo desplegado de manera apropiada[19].

Monitorización: Se define una serie de mecanismos de monitorización del estado de las réplicas y del servicio para garantizar el correcto funcionamiento de la solución.

Las soluciones ofrecidas por la industria ignoran si un software carece o no de estados, por tanto, no son suficientes para garantizar la alta disponibilidad de un software con estados. Es por ello que deben ser complementadas por otras soluciones que abarquen los aspectos propios de dicho software.

## 4.10 TÉCNICAS DE REPLICACIÓN

El software con estados hace necesaria la introducción de algoritmos de replicación. Dichos algoritmos mantienen la consistencia entre las réplicas mediante el intercambio de mensajes de sincronización, de forma que, en caso de fallo, la réplica seleccionada para retomar el servicio dispone del estado de las peticiones. Garantizando así que las peticiones pendientes durante el fallo no quedan interrumpidas.

**4.10.1 Primario-Respaldo.** En la réplica acción Primario-Respaldo[20], cada cliente envía sus peticiones a la réplica primaria, que es la que acepta y procesa todas las peticiones recibidas, y propaga los cambios de estado a las réplicas de respaldo,

[19] AVIZIENIS. A. IEEE Computer. EEUU. Mc Graw Hill,1997, p.321.
[20] BUDHIJARA, N; MARZULLO, K y SCHNEIDER, F. The primary-backup approach. In Distributed Systems. USA: Mc Graw Hill, 2003, p.199.

que son aquellas que son candidatas a reemplazar a las réplicas primarias en caso de fallo. La replicación se divide en cuatro etapas: En primer lugar, el cliente realiza una petición a la réplica primaria (Etapa 1), la réplica primaria propaga el cambio de estado a las réplicas mediante una primitiva multicast (Etapa 2), las réplicas de respaldo confirman a la primaria la correcta recepción de dichos cambios de estados (Etapa 3), es entonces cuando la primaria envía la respuesta a la petición realizada por el cliente (Etapa 4). Esta solución es sencilla y elegante.

# 5. DESARROLLO METODOLÓGICO

## 5.1 FINANCORP COLOMBIA

Es una corporación bancaria con más de 570 mil clientes, cuenta con una red de 164 puntos de atención que hacen presencia en las siguientes ciudades y municipios del país: Armenia, Barrancabermeja, Barranquilla, Bogotá, Bucaramanga, Cali, Cartagena, Caucasia, Cúcuta, Ibagué, Manizales, Medellín, Montería, Pasto, Pereira, Popayán, Rionegro, Santa Marta, Tunja, Villavicencio, durante el año 2016, FINANCORP Colombia consolidó sus resultados como el sexto banco más grande del país, con activos por $30,8 billones, pasivos por $27,2 billones y patrimonio de $3,6 billones, a cierre de 2017, presenta 31 Billones en Activos, 21 Billones en Cartera, 570 Mil Clientes, 3650 Empleados y 177 Cajeros Automáticos propios.

A partir del 1 de abril de 2016 la casa matriz del Banco Financorp Colombia, Financorp en Chile, se fusionó con el banco Basí de Chile dando como resultado el banco Basí Financorp. A partir de este momento el accionista controlador de la casa matriz es Basí Unibanco, compañía basada en Brasil. Basí Unibanco es actualmente el banco privado más grande de ese país con activos cercanos a los USD $ 415.704 millones, con ganancias en el año 2016 cerca de USD $ 7.250 millones con más de 60 millones de clientes, presencia en 19 países del mundo (Américas, Europa y Asia), cerca de 90 mil colaboradores, 5 mil sucursales y 26 mil cajeros automáticos. Es la única institución financiera de América Latina que forma parte del Dow Jones Sustainability Index desde hace 17 años, cuando se creó dicho índice.

Entre los temas más relevantes llevados a cabo en el frente de Infraestructura, Telecomunicaciones, Seguridad Tecnológica, Mesa de Ayuda y DRP (Disaster Recovery Plan), se destacan las siguientes:

• Fortalecimiento de la Plataforma Tecnológica del Core Phoenix (Hardware, base de datos y sistema de almacenamiento), logrando mejoras sustanciales en el desempeño de la operación batch y línea.

• Unificación arquitectura Directorio Activo para las dos redes y Sincronización de usuarios del DA.

• Implementación de la nueva plataforma de FW, en el Centro de Procesamiento de Datos de la Calle 100.

• Aprovisionamiento recursos tecnológicos para proyectos: Originación, Clic, Inteligencia Comercial (S.A.S), Banca Móvil APP, Nueva versión Kondor+.

• Renovación tecnológica de PC en áreas centrales (800 pc´s). • Implementación

Finesse Virtual en áreas Centrales (XenApp).
• Unificación de herramienta control de salida a Internet WebSense.

• Implementación FireEye (herramienta prevención de fuga de información, detección y control de malware de día cero).

• Integración Telecomunicaciones de FINANCORP e Basí BBA Colombia.

• Aprovisionamiento de infraestructura y telcos para pruebas DRP Red Azul y Red Naranja. En el segundo Frente, construir el futuro con la implementación de las iniciativas del Proyecto Core y Conexos, la estrategia definida para la integración Operativa y Tecnológica tiene como objetivo la migración de datos de la Red FINANCORP al Core Phoenix. La implementación de los gaps identificados, la unificación de canales y la integración con el ecosistema que se interrelaciona con el Core Phoenix dio inicio al Proyecto Core y Conexos.

## 5.2 DISPONIBILIDAD DE LOS SISTEMAS

De acuerdo con Gray[21], los sistemas teniendo en cuenta su disponibilidad se clasifican de la siguiente forma, se puede observar en el cuadro 1, que contiene los ítems de caracterización para los sistemas de alta disponibilidad.

**Cuadro 1. Clasificación de los sistemas de acuerdo con su disponibilidad**

| Tipo de sistema | Indisponibilidad (minutos por año) | Disponibilidad ( porcentaje) | Clase de indisponibilidad. |
|---|---|---|---|
| No manejada | 50000 | 90 | 1 |
| Manejada | 5000 | 99 | 2 |
| Bien manejada | 500 | 99,9 | 3 |
| Responsablemente manejada | 50 | 99,99 | 4 |
| Alta disponibilidad. | 5 | 99,999 | 5 |
| Muy alta disponibilidad. | 0,5 | 99,9999 | 6 |
| Ultra Disponible | 0,05 | 99,99999 | 7 |

Nota: elaborada por Autores con base en datos de GRAY,Jim. ACM DL Liberia Digital. The ACM Guide to Computing Literature. [en línea] Texas: El Autor [citado 4, septiembre, 2017]. Disponible en Internet: < URL: https://dl.acm.org/>

En un sistema de alta disponibilidad, el tiempo máximo de indisponibilidad del sistema es de 5 minutos por año. En el sector bancario de Colombia, para el año 2016, Bancolombia, por ejemplo, tuvo una falla de 2:40 horas, lo que conlleva aun tiempo de indisponibilidad del sistema de más de 200 minutos con lo que podría

[21] GRAY,Jim. ACM DL Liberia Digital. The ACM Guide to Computing Literature. [en línea]. Texas: El Autor [citado 4, septiembre, 2017]. Disponible en Internet: < URL: https://dl.acm.org/>

ubicarse en la clase de los sistemas Bien manejados. Es de notar que Bancolombia es el banco que maneja el 20% del mercado, convirtiéndose en el más grande y maneja el mayor número de transacciones on-line del mercado[22].

Dado lo anterior se podría afirmar que en Colombia no todos los bancos del sector tienen sistemas de alta disponibilidad, es decir los tiempos de indisponibilidad del sistema anual superan los 5 minutos. Parece natural preguntarse cómo se puede entonces disminuir el tiempo de indisponibilidad de los sistemas, de tal manera que se llegue a un sistema que se encuentre entre la clase de sistemas de Alta disponibilidad. En el cuadro 2, se muestran fallas críticas de gran impacto en el sector bancario, las fallas presentaron afectación en el usuario final y para estas indisponibilidades no se tuvo un plan de contingencia.

**Cuadro 2. Fallas críticas en el sector bancario**

| Banco | Fecha | Fuente | Tiempo Indisponibilidad | Medida | Falla | Motivo de la falla |
|---|---|---|---|---|---|---|
| Bancolombia | 9/08/2014 | Revista semana | 24 | horas | plataforma electrónica | Se dañó el principal y se saturo el backup. |
| Bancolombia | 27/02/2017 | Blu radio | 2:34 | horas | Oficinas | Falla en el sistema operativo |
| Bancolombia | 16/06/2016 | W radio | 2:40 | horas | plataforma electrónica | Situación técnica de la entidad |
| Banco Davivienda | 15/01/2015 | www.elespectador.com | 2:30 | horas | Red de cajeros electrónicos | Falla técnica de la entidad |
| Banco de Bogotá | 14/01/2017 | http://www.dinero.com | 1:30 | horas | plataforma electrónica | Falla técnica de la entidad |
| Banco BBVA | 16/12/2017 | lopezdoriga.com | 24 | horas | Banca en línea | Actualización de sistemas |

Fuente: Autores

Para el caso de la entidad Bancolombia ya fue sancionada por la superintendencia financiera por la suma de 800 millones de pesos a mediados de febrero del 2017, por las fallas e inconvenientes sobre su red presentados a mediados del 2016 y actualmente se encuentra bajo la supervisión de la entidad reguladora[23].

**5.2.1 Generalización del Sistema.** Considere un sistema $S$, cuyo tiempo de indisponibilidad es superior a 5 minutos, es decir no es un sistema de alta disponibilidad. $S = \{p, b\}$, Puede estar compuesto por dos redes: $p$ la red principal, $b$ la red del Backup o un sistema de la forma $S = \{p, b, c^*\}$, compuesto por tres redes: $p$ la red principal, $b$ la red del Backup y $c^*$ un enlace de contingencia.

[22] RANKIA. Mejores Bancos en Colombia. [en línea]. Bogotá: El Autor [citado 28, agosto, 2017]. Disponible en Internet: < URL: https://www.rankia.co/blog/mejores-cdts/3449454-mejores-bancos-colombia-2017>

[23] DIARIO PORTAFOLIO. Multan a Bancolombia con $840 millones por mal servicio en plataforma electrónica. [en línea]. Bogotá: El Autor [citado 24, febrero, 2017]. Disponible en Internet: < URL http://www.portafolio.co/negocios/empresas/superfinanciera-multa-a-bancolombia-por-mal-servicio-de-plataforma-digital-503646>

El sistema $S$, puede convertirse en un sistema de alta disponibilidad si:

- Se identifican los factores determinantes del riesgo.

- Se incluye un enlace de contingencia de tal forma que se pueda obtener un sistema clasificado como de alta disponibilidad.

- En caso de que exista el enlace, este se optimiza.

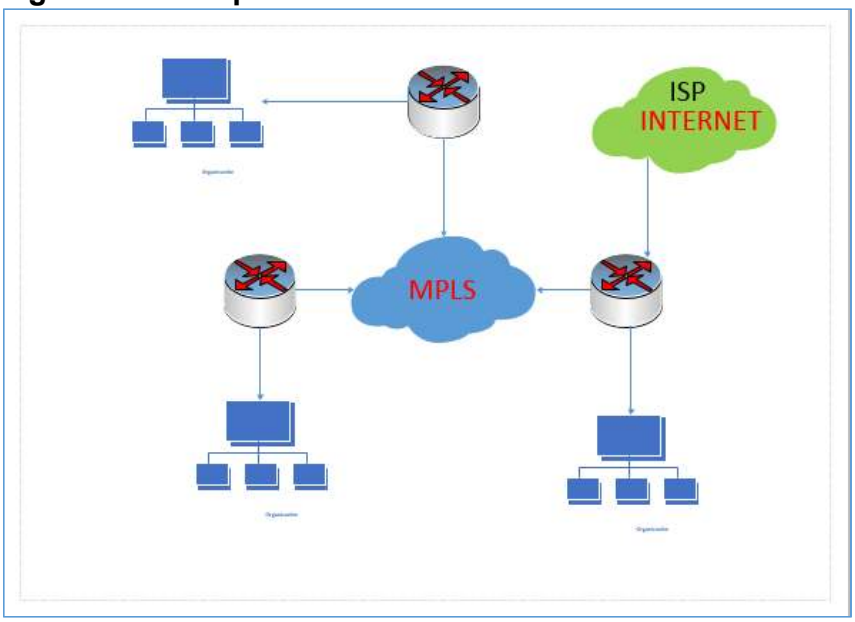
Este trabajo se orienta en introducir de manera general los pasos para llevar a cabo la transición de un sistema que no es de alta disponibilidad a un sistema de alta disponibilidad. Dado que no existe una configuración general para todos los bancos de Colombia, no solo teniendo en cuenta las diferencias entre las topologías de red, los servicios prestados, la distribución geográfica, el poder adquisitivo, etc, se introduce una entidad de referencia, con la que se desarrolla la metodología. Esta entidad tiene un sistema, $S = \{p, b\}$ , inicialmente compuesto por dos redes: principal $(p)$ y backup $(b)$. La red de datos cuenta con un canal principal, un canal Backup, y servicios extranet hacia otras entidades financieras como, por ejemplo: Banco de la República, Datacredito, visa entre otros y que demande una disponibilidad del 99.999%. Es importante aclarar que el alcance del mismo únicamente se enmarca a nivel WAN y se garantiza la operatividad hasta el equipo de última milla que se entrega en el CPE[24] del cliente.

A continuación, se hace referencia a la red MPLS que puede presentarse en un escenario real como se evidencia en la figura 8.

Red Mpls: La red [25]Mpls hace referencia a un sistema diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y en conmutación de paquetes, MPLS reemplazó a Frame Relay y ATM como la tecnología preferida para llevar datos de alta velocidad y voz digital en una sola conexión, MPLS puede transportar diferentes tipos de tráfico como voz y datos, siendo él envió de tráfico Voip como su mayor ventaja.

[24] CPE - Customer Premise Equipment
[25] MPLS - Multiprotocol Label Switching

**Figura 8. Red Mpls**




Fuente: Autores

**5.2.2 Red principal.** Una red de datos está conformada básicamente por dos divisiones WAN y LAN, a nivel WAN una red de datos como se muestra en la figura 10, debe contar con ciertos elementos y características, sus principales componentes son: Un PE, una red de acceso que hace referencia a un Switch que opera en la capa dos del modelo OSI, un conversor de medio (transceiver, u ONT), un router (CPE), a nivel LAN, la topología depende del requerimiento del usuario o cliente final, sin embargo, en la mayoría de casos se tienen los siguientes equipos: switch de distribución, un servidor, un firewall, un modem, acces point, entre otros. Estos dispositivos de red no son estándar para el plan de contingencia ya que hacen parte de la red LAN y pueden variar dependiendo de la necesidad del usuario final. Para el proyecto, en la red principal cuenta con las siguientes características descritas en el cuadro 3.

**Cuadro 3. Elementos y características de la red principal**

| Ítem | Descripción |
|---|---|
| Ciudad | Bogotá D.C |
| Ubicación | Sede principal |
| Tipo de cliente | Banco Financorp |
| Nivel de criticidad | 1 |
| Dirección_IP WAN[26] | 10.20.4.2/30 |
| P.E “Provider Edge” | BOG-31001 – A |
| Puerto P. E | Fastethernet 0/0 |

[26] A nivel WAN, los ISP entregan direccionamiento privado por política de seguridad

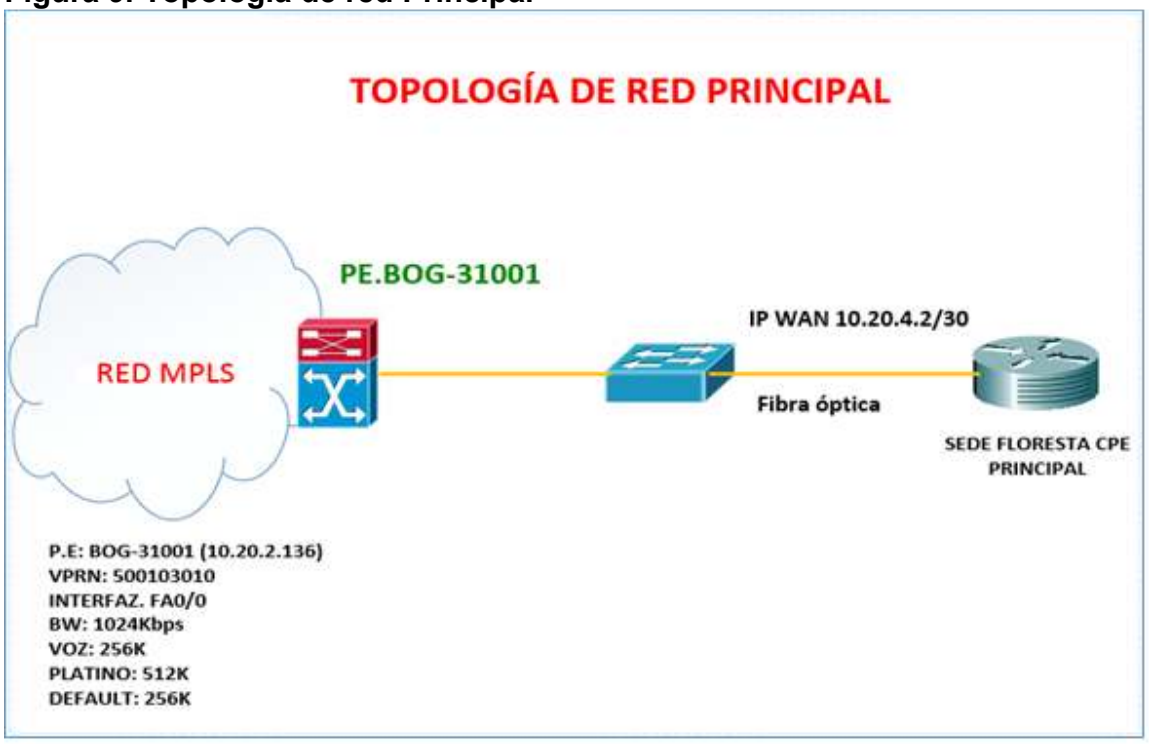
| | |
|---|---|
| CPE “Customer Provider Edge” | Router cisco 3945 E |

Cuadro 3 (continua)

| Ítem | Descripción |
|---|---|
| Transceiver | Raisecom Rc 512 |
| Vprn | 500103010 |
| Voz | 256 k |
| Platino | 512 k |
| Default | 256 k |

Fuente: Autores

**Figura 9. Topología de red Principal**



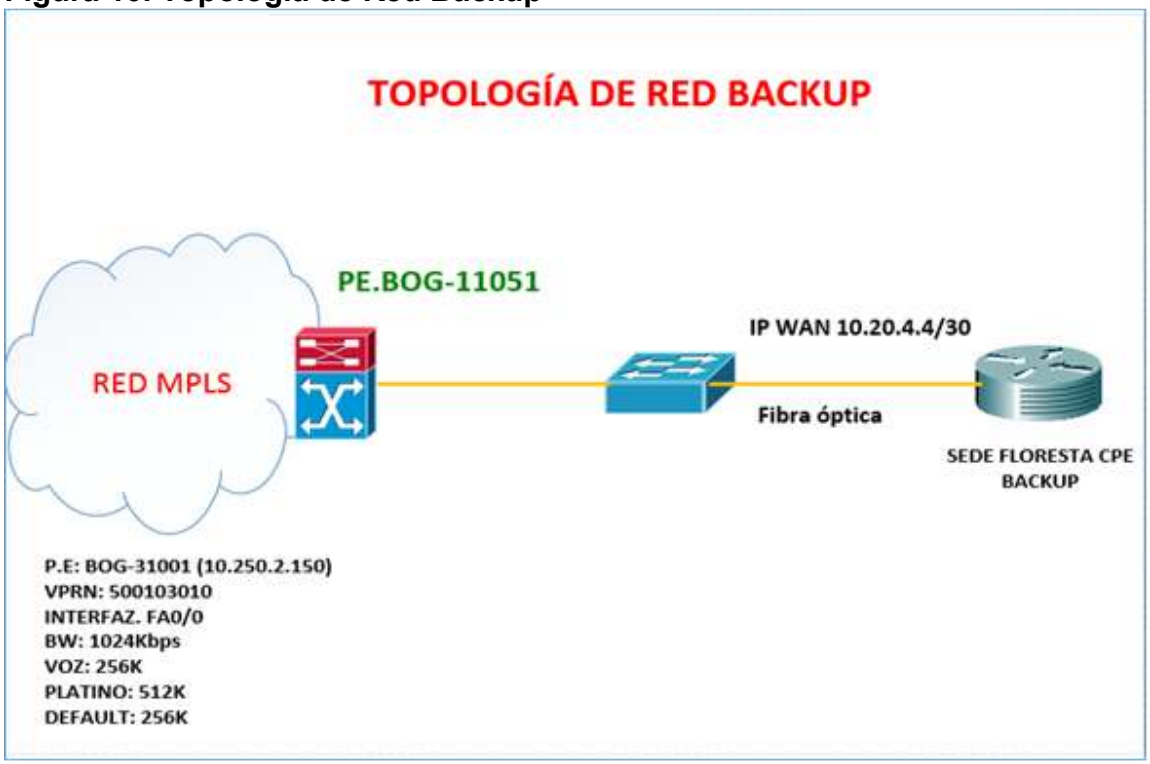

Fuente: Autores

**5.2.3 Red Backup.** La red backup del banco Financorp como se observa en la figura 11, cuenta con los dispositivos de red a nivel WAN ,conformando actualmente la red de respaldo, a nivel WAN que es el objeto del estudio, debe tener asociados los siguientes elementos, Un PE, una red de acceso que está formada por un Switch capa dos que trabaja en la capa de red del modelo OSI, un conversor de medio (transceiver, u [27]ONT) un router (CPE), a nivel LAN, la topología depende del requerimiento del usuario o cliente final, sin embargo, en la mayoría de casos se tienen los siguientes equipos, switch de distribución, un servidor, un firewall, un modem, acces point, entre otros con las mismas características que el enlace

[27] Optical Network Terminal

principal.
Para el proyecto, en la red backup cuenta con las siguientes características que se pueden observar en el cuadro 4

**Figura 10. Topología de Red Backup**




Fuente: Autores

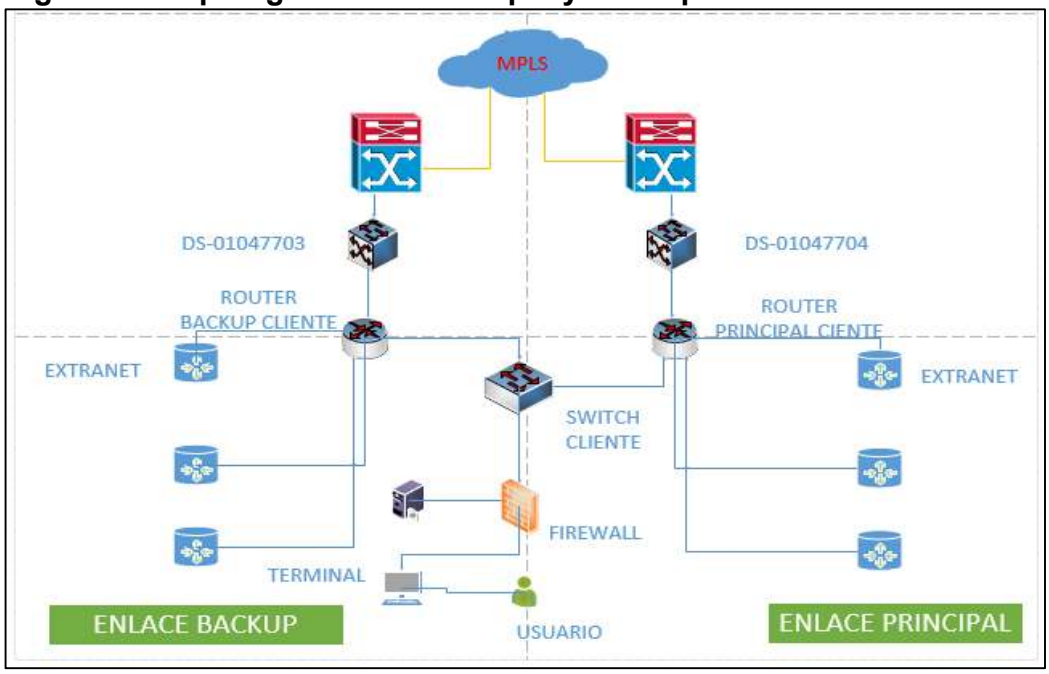
**Cuadro 4. Elementos y características de la red Backup**

| Ítem | Descripción |
|---|---|
| Ciudad | Bogotá D.C |
| Ubicación | Sede principal |
| Tipo de cliente | Banco Financorp |
| Nivel de criticidad | 1 |
| Dirección_IP WAN[28] | 10.20.4.4/30 |
| P.E “Provider Edge” | BOG-11051 |
| Puerto P. E | Fastethernet 0/0 |
| CPE “Customer Provider Edge” | Router cisco 3945 E |
| Transceiver | Raisecom Rc 512 |
| Vprn | 500103010 |
| Voz | 256K |
| Platino | 512k |
| Default | 256k |

[28] A nivel WAN, los ISP entregan direccionamiento privado por política de seguridad

A continuación como se observa en la figura 11, se relaciona el diseño de ingeniería de la red actual, topología principal y back up, se presenta un solo diseño para los dos ya que se encuentran en la misma sede física, pero cuenta con diferente Router, PE y red de acceso, con lo que se garantiza la llegada del servicio por una ruta alternativa y en caso de ruptura en algún medio, no se verá afectado la operatividad de la otra red ya que son completamente independientes, pero por motivos de ubicación física no está excepto a catástrofes naturales o fallas eléctricas graves, que pueda llevar a la afectación de los dos servicios, por tal motivo se crea un plan de contingencia para mitigar los riesgos, el cual entra en operación cuando la dos redes estén fallando.

**Figura 11. Topología de red Principal y Backup**




Fuente: Autores

A esta entidad de referencia se le realizó:

1) Se introduce el enlace de contingencia.
2) Se minimiza el riesgo de falla de las tres redes.

## 5.3 FASE DE ANÁLISIS Y EVALUACIÓN DE RIESGOS

El objetivo de la evaluación de riesgos es identificar, analizar, medir y prevenir las amenazas internas y externas, incluyendo concentraciones de riesgos, que pueden causar la interrupción o pérdida de las actividades críticas de una organización, así como la probabilidad (o frecuencia) de que ocurra una amenaza, permitiendo

priorizar y manejar un plan de acción de gestión del riesgo.
Proceso de administración de riesgos Norma AS/NZS 4360 de 2004 - NTC 5254 de 2006

La Norma Técnica Colombiana 5254 de ICONTEC es una traducción idéntica de la norma australiana AS/NZS 4360

El estándar basado en la norma 5254 de ICONTEC provee una guía genérica para la administración de riesgos, además de entregar los componentes para su administración. Es genérico e independiente de cualquier tipo de industria o sector económico, en este caso enfocado al sector económico y su diseño e implementación depende de las necesidades de la organización.

Objetivos norma colombiana 5254 de ICONTEC

- Una mejor base para la planeación y la toma de decisiones.
- Mejor identificación de oportunidades y riesgos.
- Ganar valor de la incertidumbre y la variabilidad.
- Administración proactiva en vez de reactiva.
- Mayor efectividad en la distribución y uso de recursos.
- Mejora en la administración de incidencias con una reducción de pérdidas y costos,
- incluyendo primas de seguros.
- Mejorar la confianza y credibilidad de las partes interesadas.
- Mejora en el cumplimiento con la legislación relevante.

Definiciones tomadas de la norma 5254 NTC

- **Análisis del riesgo**. Proceso sistemático para entender la naturaleza del riesgo y deducir el nivel del riesgo.

- **Consecuencia**. Resultado o impacto de un evento.

- **Control**. Proceso, política, dispositivo, práctica u otra acción existente que actúa para minimizar el riesgo negativo o potenciar oportunidades positivas.

- **Evaluación del control**. Revisión sistemática de los riesgos para garantizar que los controles aún son eficaces y adecuados.

- **Evento.** Ocurrencia de un conjunto particular de circunstancias

- **Frecuencia**. Medición del número de ocurrencias por unidad de tiempo.

- **Posibilidad**. Se usa como descripción general de la probabilidad o la frecuencia.

- **Monitorear**. Verificar, supervisar o medir regularmente el progreso de una actividad, acción o sistema para identificar los cambios en el nivel de desempeño requerido.

- **Probabilidad**. Medida de la oportunidad de ocurrencia expresada como un número entre 0 y 1.

- **Riesgo**. La oportunidad que suceda algo que tendrá impacto en los objetivos.

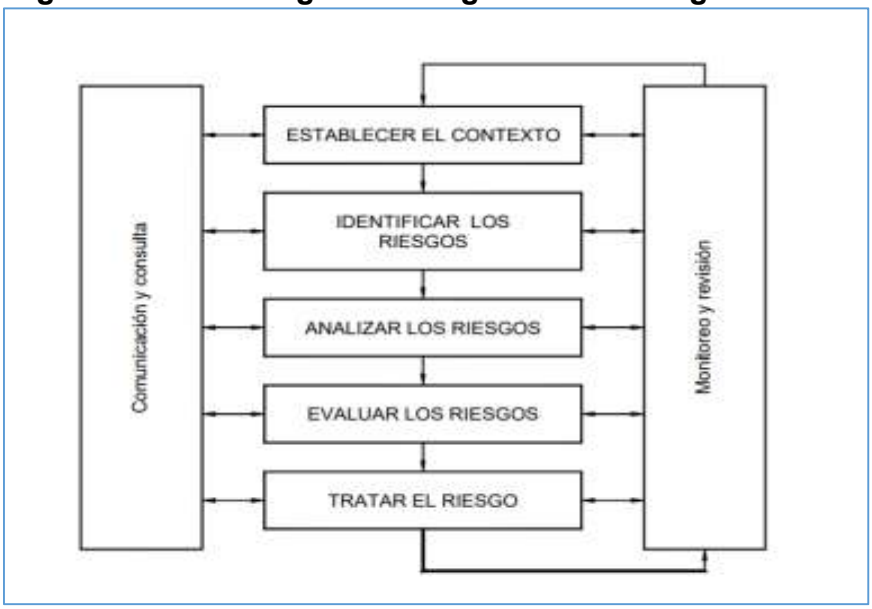
- **Riesgo residual**. Riesgo remanente después de la implementación del tratamiento del riesgo.

- **Valoración del riesgo**. Proceso total de identificación, análisis y evaluación del riesgo.

- **Criterios del riesgo**. Términos de referencia mediante los cuales se evalúa la importancia del riesgo.

- **Reducción del riesgo**. Acciones que se toman para reducir la posibilidad y consecuencias asociadas a un riesgo[29].

**Figura 12. Proceso general de gestión del riesgo**




Fuente. ICONTEC. Instituto Colombiano de Normas Técnicas y Certificación. Norma Técnica Colombiana NTC 5254. Gestión de Riesgo.

[29] ICONTEC. Instituto Colombiano de Normas Técnicas y Certificación. Norma Técnica Colombiana NTC 5254. Gestión de Riesgo. Bogotá: ICONTEC. 2006, p. 6.

Bogotá: ICONTEC. 2006, p. 6.

**5.3.1 Análisis de riesgo.** El riesgo es la probabilidad de ocurrencia de eventos o sucesos negativos que impidan o perjudiquen los equipos y su correcto funcionamiento en la red en la entidad, el análisis conlleva a obtener una evaluación del impacto de afectación que puedan causar estos acontecimientos negativos, existen diferentes tipos de impacto de acuerdo con los daños sufridos, pero con el plan de contingencia se debe mitigar las diferentes afectaciones que sufra la red[30].

Se debe tener un total entendimiento y análisis de los riesgos, para poder evaluar cómo deben de ser tratados a nivel de costo-efecto, esto Involucra:

- La probabilidad de ocurrencia
- La determinación de su impacto a nivel potencia (consecuencias)
- Análisis de riesgos, mediante la fusión de impacto y su probabilidad de ocurrencia

Evaluación de Controles

- Se deben identificar los controles existentes en los procesos y actividades que ayudan a minimizar los riesgos negativos o mejoran los riesgos positivos.

- Se debe evaluar sus fuerzas y debilidades de los controles.

Los diferentes tipos de impacto de acuerdo con su afectación son:

- Bajo: es el que no presenta afectación en la disponibilidad de la red y se puede recuperar en menos de una hora

- Medio: es el que causa daño a la infraestructura de la red en tanto lo relacionado con la parte física y lógica, y no puede ser recuperado en menos de 4 horas

- Alto: este afecta toda la operación en la red, los daños no son recuperables en corto tiempo y por el contrario pueden tomar días en su solución, para este tipo de daños se diseña el plan de contingencia.

Para el diseño de esta red se debe garantizar una alta disponibilidad del servicio del 99.999 % a continuación se describe los porcentajes y la definición para realizar los cálculos de las diferentes disponibilidades en el área de redes de comunicaciones. Alta disponibilidad es un diseño del sistema y su implementación debe asegurar un alto de grado de operatividad en un determinado tiempo, la disponibilidad se refiere al acceso de usuarios para acceder al sistema, realizar modificaciones, efectuar operaciones, realizar consultas, o simplemente acceder al servicio. Si un usuario no

[30] KOHLER, Alois; BLOEMERTZ, Lena y JÜLICH, Sebastian. Una base para la gestión de riesgo, México: Trillas editores, 2004. p.35.

puede acceder al sistema se dice que está no disponible. El término tiempo de inactividad (Down time) es usado para definir cuándo el sistema no está disponible y acarrea costos para los operadores de comunicaciones que prestan el servicio o para el administrador de la red de comunicaciones.

La Magnitud del Riesgo. La Magnitud de un riesgo se determina por su probabilidad de ocurrencia y sus consecuencias o impactos asociados.

Matriz de Priorización. El riesgo se debe medir de acuerdo con el impacto y la probabilidad y se debe ubicar en la Matriz de priorización que se encuentra descrita en la figura 14 y se observa su desarrollo[31]. [20]

Probabilidad: frecuencia que podría presentar el riesgo.

Alta: es muy factible que el riesgo se presente
Media: es factible que el riesgo se presente
Baja: es muy poco factible que el riesgo se presente

Impacto: forma en la cual el riesgo podría afectar los resultados del proceso.

Alto: afecta en alto grado la disponibilidad del servicio
Medio: afecta en grado medio la disponibilidad del servicio
Bajo: afecta en grado bajo la disponibilidad del servicio

A continuación, se presenta la Matriz de Priorización, con la cual se clasificarán los riesgos de acuerdo a su Magnitud, donde:

Magnitud A: Nivel Alto de riesgo “Critico”
Magnitud B: Nivel Medio de riesgo “Grave”
Magnitud C: Nivel Bajo de riesgo “Leve”

**Cuadro 5. Matriz de priorización**

| | | | | |
|---|---|---|---|---|
| Probabilidad | Alta | B | A | A |
| | Media | B | B | A |
| | Baja | C | B | A |
| | | *Bajo* | *Medio* | *Alto* |
| | | IMPACTO | | |

Fuente: Autores

[31] MONTERO, Fernando. Gestión del Riesgo en Infraestructura y Comunicaciones TI, para Empresa del Sector Financiero. Chile: Universidad Técnica Federico Santa María,2011. p. 45.

El tiempo de inactividad planificado es el resultado del mantenimiento que resulta perjudicial para la operación del sistema, eventos que generan tiempos de inactividad planificados quizás incluyen actualizaciones del sistema que requieran un reinicio d equipos o cambios en la configuración que tardan cierto tiempo en retomar el correcto funcionamiento. En general el tiempo de inactividad planificado es usualmente el resultado de un evento lógico o físico planificado por el administrador de la red o el usuario final, las actividades más comunes de inactividad planificada son las que se observan en el cuadro 6, en el cual se entrega primordialmente la información sobre la magnitud de los riesgos analizados en tiempo de inactividad planificados, la cual será de suma importancia para evaluar en donde serán priorizados o clasificados según los criterios de análisis definidos[32].

**Cuadro 6. Análisis de riesgos "tiempos de inactividad planificados"**

| Evento | Efecto sobre la Red | Respaldo sugerido | Probabilidad | Impacto | Magnitud de riesgo |
|---|---|---|---|---|---|
| Pruebas de conmutación de enlaces | Caída del servicio afectado | Enlaces de respaldo | Media | Bajo | B |
| Reinicio controlado de equipos | Caída del servicio afectado | Enlaces de respaldo | Media | Medio | B |
| Mantenimiento de Ups | Caída del servicio afectado | | Alto | Bajo | B |
| Traslado de equipos dentro de la sede | Caída total de los servicios | Enlaces de respaldo | Baja | medio | B |
| Apagado de equipos controlado por parte de los usuarios | Caída del servicio afectado | Enlaces de respaldo | Baja | Medio | B |
| Obras civiles donde se encuentran alojados los servicios | Caída total de los servicios | Sede de respaldo | Baja | Alto | A |
| Desconexión física hacia proveedor principal | Caída del servicio afectado | Red backup de respaldo | Baja | Alto | A |
| Desconexión física hacia proveedor backup | Caída del servicio afectado | Red principal de respaldo | Baja | Medio | B |

Fuente: Autores

Los tiempos de inactividad no planificada son los eventos que surgen al azar y puede afectar de forma menor, grave o critica a la red. Estos eventos suelen ser ajenos al usuario final y más relacionado con el proveedor de servicios bajo ciertas excepciones. Los eventos más comunes de inactividad no panificada son las que se observan enel cuadro 7, también se observa la magnitud del riesgo siendo mayor que los tiempos de fallos planificados, por tal motivo se debe clasificar dentro de los criterios definidos.

[32] MICROSOFT. Microsoft TechNet. [en línea]. Bogotá: El Autor [citado 20, julio, 2017]. Disponible en Internet: < URL: https://technet.microsoft.com/es-co/library/aa998704(v=exchg.65).aspx

**Cuadro 7. Análisis de riesgos "tiempos de inactividad no planificados"**

| Riesgo | Efecto sobre la Red | Respaldo sugerido | Probabilidad | Impacto | Magnitud de riesgo |
|---|---|---|---|---|---|
| RFC o mantenimientos de emergencia no aprobados por el usuario final. | Caída total de todos los servicios | Red de respaldo | Media | Alto | A |
| Ruptura, atenuación o cambio de fibra óptica. | Caída del servicio afectado | Red de respaldo | Media | Alto | A |
| Fallas en los equipos de red Core, o eventos masivos sobre la red del operador. | Caída del servicio afectado | Red de respaldo | Media | Alto | A |
| Corte de energía | Caída total de los servicios | Respaldo de Ups | Media | Medio | B |
| Desactualización de equipos y licencias | Caída parcial de los servicios | Red de respaldo | Baja | Bajo | C |
| Falla en equipos de ventilación | Caída parcial de los servicios | Mantenimiento mensual | Baja | Bajo | C |
| Inundaciones | Caída total de todos los servicios | Data center en 5° piso de altura | Baja | Alto | A |
| Terremotos | Caída total de todos los servicios | | Baja | Alto | A |
| Tsunami | Caída total de todos los servicios | Data center en 5° piso de altura | Baja | Alto | A |
| Incendios | Caída total de todos los servicios | Sistema contra incendios | Baja | Alto | A |
| Saturación sobre la red | Caída parcial de los servicios | Red de respaldo | Media | Medio | B |

Fuente: Autores

Del análisis anterior se plantea los siguientes escenarios de contingencia que aplican a cualquier red del sector financiero, estos son los de mayor impacto y que no tiene una solución inmediata y requiere de un plan de contingencia:

- Interrupción de funcionamiento normal de sistemas
- Catástrofes naturales (terremoto, inundaciones, incendios)
- Falla eléctrica mayor

## 5.4 MINIMIZACIÓN DEL RIESGO

Considere un sistema $S = \{p, b, c\}$, compuesto por tres redes. Donde $p$ la red principal, $b$ la red del Backup y $c$ la red de contingencia. A continuación, se definen las siguientes probabilidades.

- $P(p)$, es la probabilidad de falla de la red principal.
- $P(b)$, es la probabilidad de falla de la red del Backup.
- $P(c)$, es la probabilidad de falla de la red de contingencia.
- $P(p \wedge b \wedge c)$, es la probabilidad de falla de las redes principal, Backup y la red de contingencia.

Cabe notar que el enlace de contingencia entraría como respaldo en caso de que falle el principal y el backup, es por esto, que la probabilidad de falla del sistema $S$, estará dada por la probabilidad de falla de la red de contingencia $c$, dado que fallaron las redes principal $p$ y backup $b$. En términos de probabilidades, puede escribirse como:

$$P(S) = P\big(c \mid (b \wedge p)\big) = \frac{P(p \wedge b \wedge c)}{P(p \wedge b)}.$$

La minimización del riesgo se puede realizar a través de la identificación, análisis y mitigación de los determinantes del riesgo. En la sección anterior se concluyó que los riesgos en el escenario de contingencia son:

I. Catástrofes naturales (terremoto, inundaciones, incendios).
II. Falla eléctrica mayor
III. Interrupción de funcionamiento normal de sistemas.

Una de las características principales de una red de datos es encontrar el enlace principal Y backup en una misma ubicación física. Esto se debe en parte a la facilidad de operar la red por parte del administrador de recursos y a la capacidad de respuesta al momento de presentarse alguna falla o algún requerimiento que se necesite para su mayor funcionamiento.

Por lo anterior en los factores de riesgo como, fallas eléctricas y catástrofes naturales el principal y el backup se tratan como un solo ente. Es claro que la ubicación geográfica es un determinante para el tratamiento de estos factores de riesgo. La pregunta fundamental entonces es se tiene el enlace principal y el backup en Bogotá en que ciudad o departamento se debe ubicar la red de contingencia. Para esto se diseñó un scoring de riesgo por departamento que permite elegir el departamento y la ciudad en la que se puede diseñar el nuevo enlace.

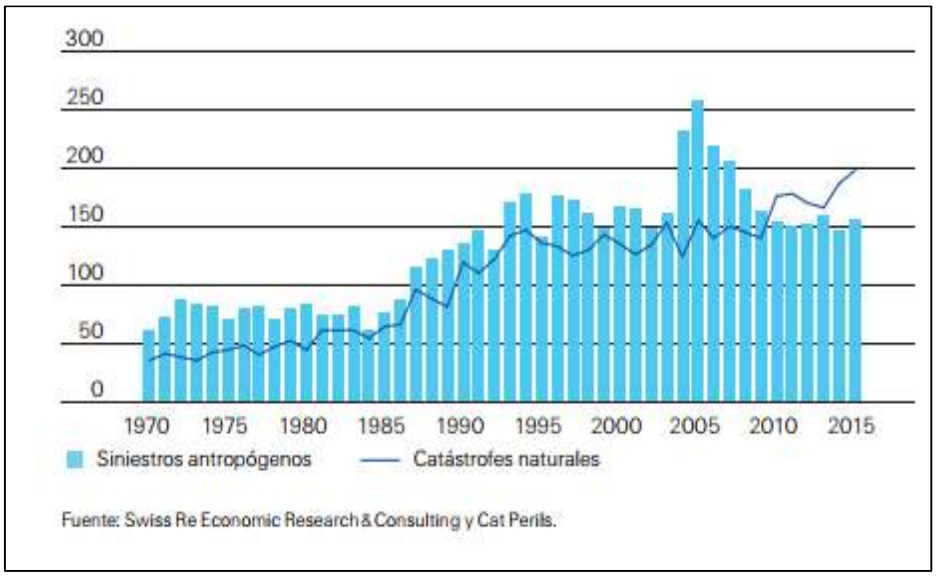
I) Catástrofes naturales (terremoto, inundaciones, incendios).

Para construir el scoring de riesgo se tuvo en cuenta:

- El número de catástrofes reportadas por la Swiss Re.

Mediante la publicación Sigma la reaseguradora Swiss Re[33], publica de manera anual las más grandes catástrofes Naturales y Humanas para el mundo. La Swiss Re clasifica los siniestros como antropogénicos, si fueron originados por el hombre, como atentados terroristas, etc, y las catástrofes naturales. Como se observa en la gráfica 1 a medida que ha pasado el tiempo el número de siniestro Naturales ha ido aumentando, mientas que el número de siniestros antropogénicos ha disminuido en los últimos años.

**Gráfica 1. Catástrofes naturales**

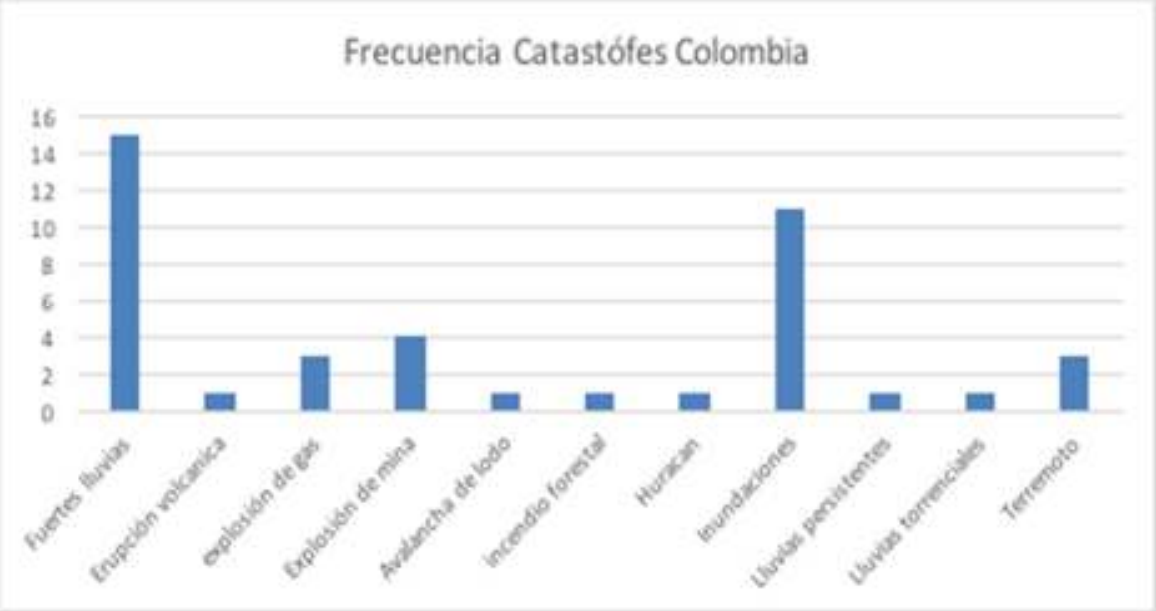



Fuente: SWISS RE. Catástrofes naturales y siniestros antropógenos en 2015. [en línea]. Bogotá: El Autor [citado 20, julio, 2017]. Disponible en Internet: < URL: http://media.swissre.com/documents/sigma1_2016.es.pdf>

La Swiss Re no publica todas las catástrofes, solo los que superan cierto umbral en pérdidas aseguradas o más de 97,7 millones de dólares en pérdidas totales o generó más de 20 muertos, 50 heridos, y más de 2000 personas sin Hogar. Cada año la revista publica el consolidado de los siniestros del año anterior (ver gráfica 2) que cumplieron con los criterios establecidos. Así las cosas, se procedió a levantar de la revista Sigma los siniestros reportados para Colombia desde el año 2002 hasta el año 2015:

[33] SWISS RE. Catástrofes naturales y siniestros antropógenos en 2015. [en línea]. Bogotá: El Autor [citado 20, julio, 2017]. Disponible en Internet: < URL: http://media.swissre.com/documents/sigma1_2016.es.pdf>

**Gráfica 2. Catástrofes en Colombia 2002-2015**



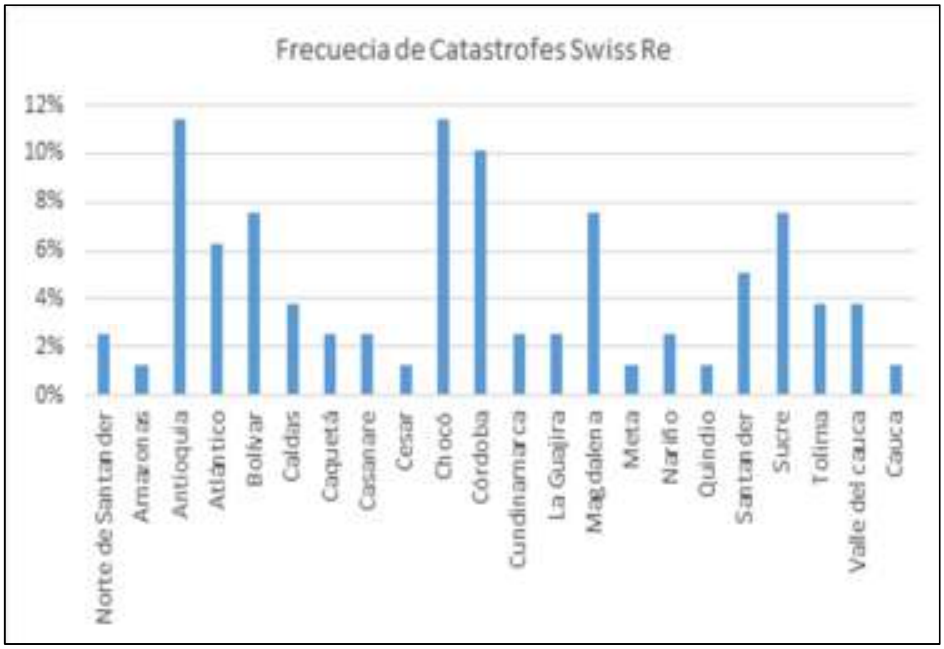

Fuente: Cálculos de Autores a partir de datos de SWISS RE. Catástrofes naturales y siniestros antropógenos en 2015. [en línea]. Bogotá: El Autor [citado 20, julio, 2017]. Disponible en Internet: < URL: http://media.swissre.com/documents/sigma1_2016.es.pdf>

Los eventos más comunes son Inundaciones y fuertes lluvias. Dado que no se registran todos los siniestros sucedidos en Colombia, los datos de la Swiss Re, nos permite generar una primera calificación de eventos de alto impacto por departamento. Para determinar la calificación con respecto a las catástrofes de la Swiss Re se define la frecuencia de sismicidad por departamento como:

$$Frec_{Swiss\ Re} = \frac{Número\ de\ catastrófes\ \ en\ el\ departamento}{Número\ total}$$

En un mismo siniestro, la Swiss Re, relaciona múltiples departamentos, dado lo anterior, para construir la frecuencia se contó un departamento tantas veces como aparecía reportado el o alguno de sus municipios en las publicaciones de Swiss Re. Y como número total, se sumó el número de veces que aparecía cada departamento. Dado que dentro de la base inicial se encontraban siniestros como atentados con carros bombas, explosiones, etc, se seleccionaron los eventos cuyo origen era natural. A continuación, se presenta gráficamente el resultado de la frecuencia:

**Gráfica 3. Frecuencia de las catástrofes en Colombia**




Fuente: Cálculos de Autores a partir de datos de SWISS RE. Catástrofes naturales y siniestros antropógenos en 2015. [en línea]. Bogotá: El Autor [citado 20, julio, 2017]. Disponible en Internet: < URL: http://media.swissre.com/documents/sigma1_2016.es.pdf>

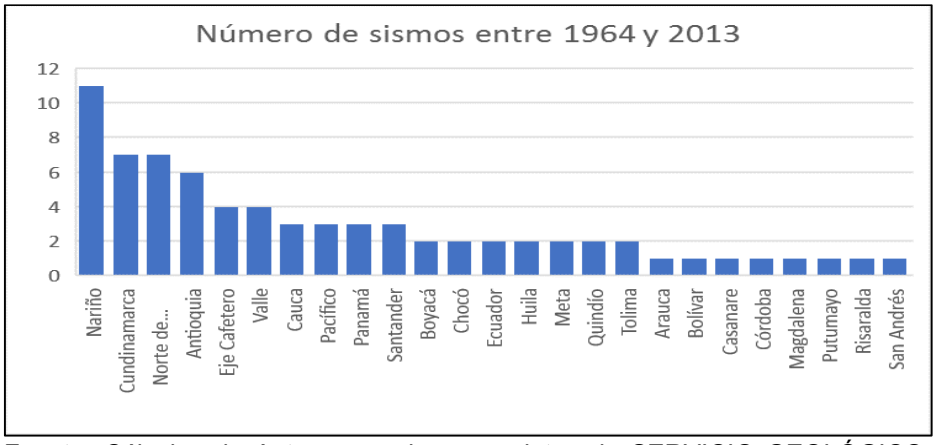
Antioquía aparece como el departamento, con mayor probabilidad de ocurrencia de un evento catastrófico de gran magnitud de acuerdo con los datos publicados por la Swiss Re.

- El número de sismos ocurridos en Colombia.

Dado que los datos de la Swiss Re, contenían un subconjunto de las catástrofes, pues solo se tienen en cuenta las que superan ciertos niveles. Esta información puede no representar la realidad de todo el territorio nacional. Por esto se consideraron otras fuentes de información adicional que se observan en la gráfica 4 donde esta discriminada por departamentos. Estas estadísticas se tomaron del servicio Geológico Colombiano de su página de internet[34]. De acuerdo con las cuales el departamento con más sismos es Nariño, con 11 sismos, seguido por los departamentos de Cundinamarca y Norte de Santander.

[34] SERVICIO GEOLÓGICO COLOMBIANO. Sismicidad histórica de Colombia. [en línea]. Bogotá: El Autor [citado 20, octubre, 2017]. Disponible en Internet: < URL: http://sish.sgc.gov.co/visor/#>

**Gráfica 4. Número de sismos en Colombia 1964 – 2013**



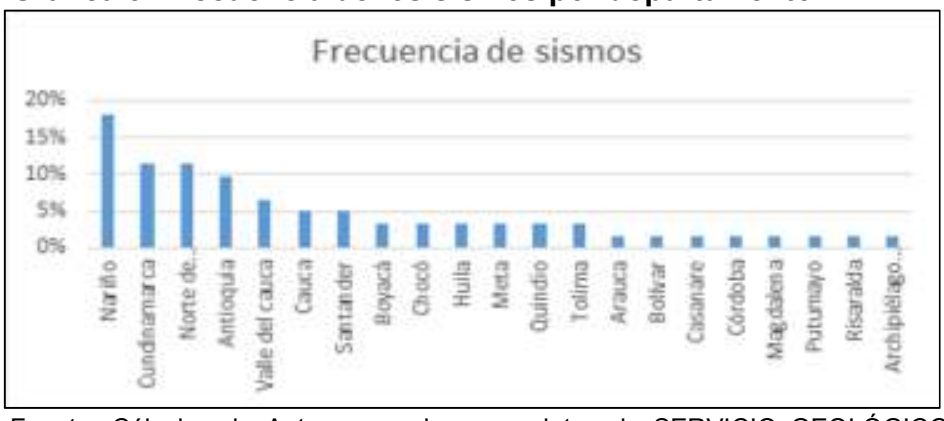

Fuente. Cálculos de Autores con base en datos de SERVICIO GEOLÓGICO COLOMBIANO. Sismicidad histórica de Colombia. [en línea]. Bogotá: El Autor [citado 20, octubre, 2017]. Disponible en Internet: < URL: http://sish.sgc.gov.co/visor/#> [35].

Para determinar la calificación con respecto a los sismos se define la frecuencia de sismicidad por departamento como:

$$Frec_{sis} = \frac{Número\ de\ sismos\ en\ el\ departamento}{Número\ de\ sismos\ totales}$$

A continuación, en la gráfica 5, se presenta la calificación por departamento de los sismos:

**Gráfica 5. Frecuencia de los sismos por departamento**




Fuente. Cálculos de Autores con base en datos de SERVICIO GEOLÓGICO COLOMBIANO. Sismicidad histórica de Colombia. [en línea]. Bogotá: El Autor

[35] Para los cálculos se eliminó de la base de datos un sismo ocurrido en 1885, que no tenía ubicación geográfica.

[citado 20, octubre, 2017]. Disponible en Internet: < URL: http://sish.sgc.gov.co/visor/#>

A partir de las fuentes ya definidas el scoring se construyó como:

$$Cal\ depto_{cat} = Frec_{sis} + Frec_{Swiss\ Re}$$

Así se obtiene la calificación por departamento:

**Cuadro 8. Scoring riesgo de catástrofe por departamento**

| Departamento | FSWISS RE (Frec_sis) | F SISMOS (Frec_(Swiss Re)) | Score |
|---|---|---|---|
| Antioquia | 11% | 10% | 21% |
| Nariño | 3% | 18% | 21% |
| Chocó | 11% | 3% | 15% |
| Cundinamarca | 3% | 11% | 14% |
| Norte de Santander | 3% | 11% | 14% |
| Córdoba | 10% | 2% | 12% |
| Valle del cauca | 4% | 7% | 10% |
| Santander | 5% | 5% | 10% |
| Bolívar | 8% | 2% | 9% |
| Magdalena | 8% | 2% | 9% |
| Sucre | 8% | 0% | 8% |
| Tolima | 4% | 3% | 7% |
| Atlántico | 6% | 0% | 6% |
| Cauca | 1% | 5% | 6% |
| Meta | 1% | 3% | 5% |
| Quindio | 1% | 3% | 5% |
| Casanare | 3% | 2% | 4% |
| Caldas | 4% | 0% | 4% |
| Boyacá | 0% | 3% | 3% |
| Huila | 0% | 3% | 3% |
| Caquetá | 3% | 0% | 3% |
| La Guajira | 3% | 0% | 3% |
| Arauca | 0% | 2% | 2% |
| Archipiélago de San Andrés, Providencia y Santa Catalina | 0% | 2% | 2% |
| Putumayo | 0% | 2% | 2% |
| Risaralda | 0% | 2% | 2% |
| Amazonas | 1% | 0% | 1% |
| Cesar | 1% | 0% | 1% |

Fuente: Autores

En el ejemplo en cuestión, se consideró que el principal y el backup estaban ubicados en Bogotá. En el siguiente cuadro se presentan algunos ejemplos de cuál sería la probabilidad de falla del sistema en los próximos 13 años:

**Cuadro 9. Calculo probabilidad falla del sistema**

| Departamento | P(falla del contingente) | P(p, b) | P(p,b,c) | P(S) |
|---|---|---|---|---|
| Santander | 10% | 14% | 1,4% | 10,0% |
| Tolima | 7% | 14% | 1,0% | 7,1% |
| Boyacá | 3% | 14% | 0,5% | 3,3% |
| Risaralda | 2% | 14% | 0,2% | 1,6% |

Fuente: Autores

Así las cosas, la probabilidad de falla del sistema, disminuyen a medida que disminuye la probabilidad de falla del departamento o municipio en que se va a ubicar el enlace contingente. Pero hay que tener en cuenta, que los municipios en los que se ubique la red del contingente deben tener vías de acceso, entre otras características, por ejemplo, si bien es cierto amazonas tiene una calificación de 0, puede no ser muy conveniente ubicar el enlace contingente en medio de la selva. Mo obstante, en la simulación se puede obtener un tiempo de indisponibilidad de 5 minutos al año, se deben configurar las variables exógenas de tal forma que se minimice la probabilidad de falla del sistema[36].

**RPO (Recovery Point Objective).** RPO se refiere al volumen de datos en riesgo de pérdida que la organización considera tolerable. ¿Las transacciones de cuánto tiempo se está dispuestos a perder, o a tener que reintroducir al sistema?

La respuesta va a depender del volumen de transacciones por unidad de tiempo, y de los mecanismos de backup, pero siempre aumenta el volumen de datos 'huérfanos' a medida que pasa el tiempo desde la última copia de seguridad.

El RPO determina el objetivo de posible pérdida máxima de datos introducidos desde el último backup, hasta la caída del sistema, y no depende del tiempo de recuperación. La casuística es amplísima.

La empresa debe averiguar cuánto tiempo pueden permitirse de no tener disponible estos datos antes de que falle el negocio. La respuesta es crucial para el desarrollo de un programa de copias de seguridad de los servicios y componentes del sistema[37].

[36] Los scoring por municipio se pueden construir con las bases de datos de desinventar.org, con la metodología aquí presentada.
[37] MARÍN, Diego. Sistemas de almacenamiento. IFCT0310. España: Ic Editorial, 2014. p.23.

**Cuadro 10. Estimación del RPO**

| Valor | Descripción |
|---|---|
| 1 | La actividad o el proceso requieren disponer del 100% de los datos. |
| 2 | La actividad o el proceso toleran la pérdida de los datos generados o modificados en las últimas 4 horas. |
| 3 | La actividad o el proceso toleran la pérdida de los datos generados o modificados en las últimas 8 horas. |
| 4 | La actividad o el proceso toleran la pérdida de los datos generados o modificados en las últimas 24 horas. |
| 5 | Otros requisitos menos restrictivos que los indicados previamente. |

Fuente. Autores

Para este caso el valor del RPO debe ser de 1.

**RTO (Recovery Time Objective).** Expresa el tiempo durante el cual una organización pueda tolerar la falta de funcionamiento de sus aplicaciones y la caída de nivel de servicio asociada, sin afectar a la continuidad del negocio.

La respuesta dependerá de la criticidad de cada aplicación.

Es un tiempo objetivo para la reanudación de sus servicios después de un desastre. Un negocio que ha establecido reanudar sus operaciones totalmente en una semana antes de ser plenamente operativo de nuevo no tiene por qué invertir demasiado dinero en la preparación de la recuperación de desastres a diferencia de otra empresa que necesita estar operando a las dos horas.

Si una empresa ha definido que tiene un tiempo muy corto de RTO, entonces debe invertir fuertemente en sistemas de recuperación de desastres, inclusive considerar tener un site de contingencia. Este site de contingencia podría mantener una copia de seguridad completa del sistema con estaciones de trabajo, que permitan mantener la operación del negocio a niveles aceptables mientras se ejecuta el plan de continuidad del negocio.

**Cuadro 11. Estimación del RTO**

| Valor | Descripción |
|---|---|
| 1 | La actividad o el proceso requieren alta disponibilidad (100%). |
| 2 | La actividad o el proceso no pueden estar interrumpida más de 8 horas. |
| 3 | La actividad o el proceso no pueden estar interrumpida más de 24 horas. |
| 4 | La actividad o el proceso no pueden estar interrumpida más de 72 horas. |
| 5 | Otros requisitos menos restrictivos que los indicados previamente. |

Fuente. Autores

Para el proyecto el RTO es de 1, ya que el proceso requiere de alta disponibilidad

**Un análisis de RPO vs RTO.** Ambos son elementos de recuperación de desastres y de la gestión de la continuidad del negocio. Uno de ellos es acerca de cuánto es el tiempo máximo de los datos que van a ser restaurados mientras que el otro se trata del tiempo máximo que lleva reanudar las operaciones. Por ejemplo, un

La empresa podría tener un RPO de 1 semana, pero un RTO de 1 solo día.

**Cuadro 12. Estimación de la capacidad de sistemas en términos de RTO**

| Valor | Descripción |
|---|---|
| 1 | Los servicios y herramientas TIC de los que dependen la actividad o el proceso disponen de una configuración de alta disponibilidad (100%). |

Fuente. Autores

**5.4.1 Análisis de riesgo durante la implementación.** El riesgo es la probabilidad de ocurrencia de eventos o sucesos negativos que impidan o perjudiquen los equipos y su correcto funcionamiento en la red en la entidad, el análisis conlleva a obtener una evaluación del impacto de afectación que puedan causar estos acontecimientos negativos, existen diferentes tipos de impacto de acuerdo con los daños sufridos, pero con el plan de contingencia se debe mitigar las diferentes afectaciones que sufra la red[38].

Los diferentes tipos de impacto de acuerdo con su afectación son:

- Menor: es el que no presenta afectación en la disponibilidad de la red y se puede recuperar en menos de una hora.

- Grave: es el que causa daño a la infraestructura de la red en tanto lo relacionado con la parte física y lógica, y no puede ser recuperado en menos de 4 horas.

- Crítico: este afecta toda la operación en la red, los daños no son recuperables en corto tiempo y por el contrario pueden tomar días en su solución, para este tipo de daños se diseña el plan de contingencia.

Para el diseño de esta red se debe garantizar una alta disponibilidad del servicio del 99.999 % a continuación se describe los porcentajes y la definición para realizar los cálculos de las diferentes disponibilidades en el área de redes de comunicaciones. Alta disponibilidad es un diseño del sistema y su implementación debe asegurar un alto de grado de operatividad en un determinado tiempo, la disponibilidad se refiere al acceso de usuarios para acceder al sistema, realizar modificaciones, efectuar

[38] KOHLER, Op, cit., p. 33.

operaciones, realizar consultas, o simplemente acceder al servicio. Si un usuario no puede acceder al sistema se dice que está no disponible. El término tiempo de inactividad (Down time) es usado para definir cuándo el sistema no está disponible y acarrea costos para los operadores de comunicaciones que prestan el servicio o para el administrador de la red de comunicaciones.

El tiempo de inactividad planificado es el resultado del mantenimiento que resulta perjudicial para la operación del sistema, eventos que generan tiempos de inactividad planificados quizás incluyen actualizaciones del sistema que requieran un reinicio d equipos o cambios en la configuración que tardan cierto tiempo en retomar el correcto funcionamiento. En general el tiempo de inactividad planificado es usualmente el resultado de un evento lógico o físico planificado por el administrador de la red o el usuario final, las actividades más comunes de inactividad planificada son las que se observan en el cuadro 13[39].

**Cuadro 13. Tiempo de inactividad planificado**

| Fallas planificadas | Responsable |
|---|---|
| Pruebas de conmutación de enlaces | Banco Financorp |
| Reinicio controlado de equipos | Banco Financorp |
| Mantenimiento preventivo o correctivo de Ups | Banco Financorp / proveedor |
| Traslado de equipos dentro de la sede | Banco Financorp |
| RFC[40] autorizados por parte del cliente y el operador prestador de servicios | Banco Financorp / Operador de servicios |
| Apagado de equipos controlado por parte de los usuarios | Banco Financorp |
| Obras civiles donde se encuentran alojados los servicios | Banco Financorp / Agentes externos |

Fuente: Autores

Los tiempos de inactividad no planificada son los eventos que surgen al azar y puede afectar de forma menor, grave o critica a la red. Estos eventos suelen ser ajenos al usuario final y más relacionado con el proveedor de servicios bajo ciertas excepciones. Los eventos más comunes de inactividad no panificada son las que se observan en el cuadro 14.

[39] MICROSOFT.,op,cit,p.2.
[40] Request for coments (peticiones de comentarios)

**Cuadro 14. Fallas no planificadas**

| Fallas no planificadas | Responsable |
|---|---|
| RFC o mantenimientos de emergencia no aprobados por el usuario final. | Operador de servicios |
| Ruptura, atenuación o cambio de fibra óptica. | Operador de servicios / Banco Financorp |
| Fallos en la red eléctrica externa o interna, en caso de una falla interna en la sede, el usuario final debe contar con un respaldo eléctrico, ya que esta afectación es ajena al proveedor de servicios. | Banco Financorp / Proveedores |
| Fallos en los equipos, recalentamiento, alto procesamiento, falla del sistema operativo IOS. | Operador de servicios / Proveedores |
| Fallas en los equipos de red Core, o eventos masivos sobre la red del operador. | Operador de servicios / Factores externos |
| Eventos catastróficos incendios, inundaciones, derrumbes, terremotos, entre otros. | Factores externos |

Fuente: Autores

El termino disponibilidad es usualmente expresado como un porcentaje del tiempo de funcionamiento en un año dado, el número de minutos de tiempo de inactividad no planeado es registrado para un sistema, el tiempo de inactividad no planificado agregado es dividido por el número total de minutos en un año (aproximadamente 525.600) produciendo un porcentaje de tiempo de inactividad; el complemento es el porcentaje de tiempo de funcionamiento el cual es lo que se denomina como disponibilidad del sistema. Valores comunes de disponibilidad, típicamente enunciado como número de "nueves" para sistemas altamente disponibles son:

- 99,9% = 43.8 minutos/mes u 8,76 horas/año ("tres nueves")
- 99,99% = 4.38 minutos/mes o 52.6 minutos/año ("cuatro nueves")
- 99,999% = 0.44 minutos/mes o 5.26 minutos/año ("cinco nueves")

Es de hacer notar que tiempo de funcionamiento y disponibilidad no son sinónimos.

Es decir, un sistema puede estar en funcionamiento y no disponible como en el caso de un fallo de red. Se puede visualizar que estos valores de disponibilidad son visibles mayormente en documentos de ventas o marketing ya l momento de realizar ajustes en la facturación de las tarifas del servicio, en lugar de ser una especificación técnica completamente medible y cuantificable.

Para este proyecto la alta disponibilidad es de 99.999 % debido a que se encuentran

tres enlaces con redundancia y que cumplen con los estándares de implementación. La gran mayoría de los sistemas altamente disponibles extraen a un patrón de diseño simple: un sistema físico multipropósito simple de alta calidad con redundancia interna comprensible ejecutando todas las funciones interdependientes emparejadas con un segundo sistema en una localización física separada.

En este caso el diseño de este plan cuenta con dos enlaces ubicados en una misma localización física, pero un tercer enlace en distinta localización.

**5.4.2 Análisis del impacto durante la implementación y fallas que presente la red de datos.** Teniendo en cuenta las fallas que se han presentado en la implementación o adecuación de nuevos servicios, los incidentes reportados en el manejo de la operación diaria de la red del Banco Financorp, se elabora el cuadro 15, donde se citan varios de los riegos que están sujetos a presentarse en el proceso de acoplamiento del enlace de contingencia

**Cuadro 15. Factores de riesgo durante la implementación del pan de contingencia**

| Riesgo | Causa | Consecuencia | Acciones | Nivel de riesgo | Responsable |
|---|---|---|---|---|---|
| • Fallas eléctricas<br>• Electromagnetismo<br>• Picos eléctricos<br>• Perdida de fluido eléctrico (apagones) | • Cableado eléctrico defectuoso o sobrecargado.<br>• Instalaciones eléctricas no adecuadas por el proveedor eléctrico<br>• Eventos ajenos tanto al proveedor de comunicaciones como al usuario final | • Daño en equipos<br>• Perdida de información<br>• Posibles afectaciones en la infraestructura física | • Tener plantas eléctricas o baterías de respaldo<br>• Tener Ups o supresores de picos eléctricos<br>• Revisar el cableado eléctrico de la sede | Bajo | Usuario final o factores externos |
| • Sistema operativo “IOS” de router desactualizado | • El fabricante cisco actualmente saca nuevas actualizaciones sobre sus equipos | • Incompatibilidad con los demás dispositivos periféricos de la red | • Realizar validaciones constantes sobre los nuevos sistemas operativos y tener actualizados los equipos de la red. | Bajo | Proveedor de servicios o fabricantes de equipos |

Fuente: Autores

Durante la implementación del plan de contingencia, se debe tener en cuenta la realización de ventanas de mantenimiento de dos horas, a fin de generar pruebas de conmutación entre los diferentes servicios; las fallas que se presenten se tendrán en cuenta para ser solucionadas por el área de implementación del proveedor de servicios, de igual forma, se cuenta con la simulación virtual de Gns3 antes de implementar el plan de contingencia, pero cabe resaltar que cuando se realizan las implementaciones se pueden presentar factores que influyan en la actividad tales como: perdida de fluido eléctrico, caída de los enlaces, actividades o cambios de emergencia, estas ventanas de mantenimiento deben de ser diseñadas y aprobadas para el usuario final al momento de realizar la implementación.

## 5.5 DISEÑO DEL PLAN DE CONTINGENCIA

Un plan de contingencia se define, como un conjunto de actividades que tiene el fin de cumplir metas y resultados que permitan a la entidad controlar el riesgo asociado a fallas, la disponibilidad de un servicio es de mucha importancia en la operación de la entidad ya que se ven involucrados terceros y clientes muy importantes para la compañía, los cuales requieren una conectividad 7*24.

En el plan se define el alcance, los responsables, los factores críticos, los equipos, el diseño del enlace, la infraestructura física y todos los aspectos generales que permitirán mantener la operatividad de la red cuando se presenten eventos que puedan afectar el desempeño del enlace principal y su backup, por lo cual debe ser parte de un sistema integral de la compañía que sirva para evitar posibles fallas leves, moderadas o críticas, y que se pueda utilizar como guía para dar una solución eficaz y oportuna al momento de restablecer los servicios.

Es importante garantizar a los usuarios finales en todo momento la operatividad del servicio, con los diferentes portales que ofrece la entidad a través de la red, como, por ejemplo: visa, data crédito, Banco de la república, CIFIN entre otros, y acceso a todos los servicios de la entidad por parte del usuario final, que permita brindar una inmediata, oportuna y eficaz respuesta a una falla que pueda presentarse por fenómenos naturales, técnicos o humanos.

Como se muestra en el cuadro 16, se describe detalladamente los elementos con los que cuenta el diseño del enlace de contingencia.

**Cuadro 16. Elementos y características de la red de contingencia**

| Ítem | Descripción |
|---|---|
| Ciudad | Cali |
| Ubicación | Sede principal |
| Tipo de cliente | Banco Financorp |
| Nivel de criticidad | 1 |

**Cuadro 16 (continua)**

| Ítem | Descripción |
|---|---|
| Dirección_IP WAN[41] | 10.20.4.6/30 |
| P.E “Provider Edge” | CAL-CEN |
| Puerto P. E | Fastethernet 0/0 |
| CPE “Customer Provider Edge” | Router cisco 3945 E |
| Transceiver | Raisecom Rc 512 |
| Vprn | 500103010 |
| Voz | 256K |
| Platino | 512k |
| Default | 256k |

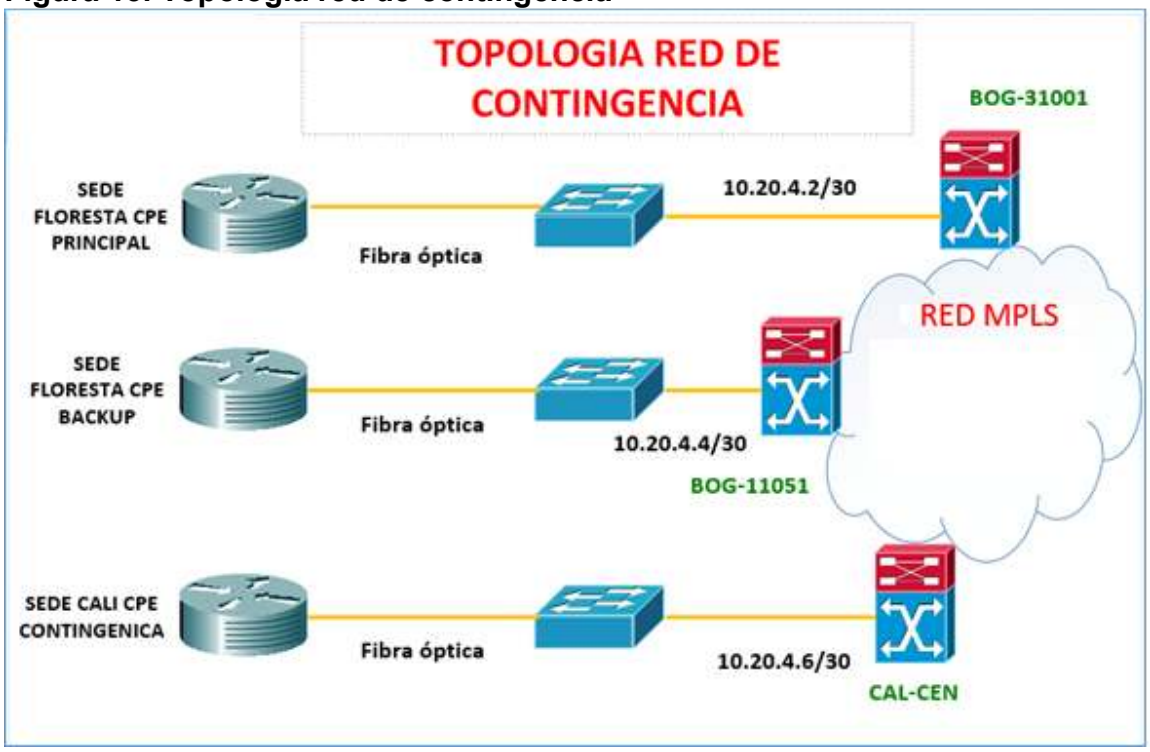
Fuente: Autores

**5.5.1 Red de contingencia.** Al igual que la red principal, la de contingencia cuenta con los mismos equipos internos, sin embargo, se tiene un cambio importante y es la ubicación física y geográfica ya que se encuentra ubicado en otra ciudad a la que se le conoce como sede remota, según la recomendación dada por la ITU[42], sin embargo, esto también depende de una variable que es presupuesto del cliente final respecto a los costos que brinda el proveedor de servicios.

Dentro del diseño de ingeniería relacionado en la figura 13, contiene el diseño de las redes tanto principal como backup de la entidad que operan en la ciudad de Bogotá en la misma sede a la que se le conoce como sede administrativa, y en la ciudad de Cali en este caso en particular se tiene la red de contingencia que opera en la sede remota, con esta topología se da cumplimiento a la norma de la UIT , lo que garantiza la exclusión de fenómenos naturales en el sector geográfico, problemas por fibra óptica, incidentes que se presenten en el Datacenter principal o demás factores externos al proveedor de servicios y usuario final.

[41] A nivel WAN, los ISP entregan direccionamiento privado por política de seguridad
[42] Unión Internacional de Telecomunicaciones

**Figura 13. Topología red de contingencia**




Fuente: Autores

Para realizar la simulación de los diferentes servicios de extranet e intranet, se configura a modo de prueba las siguientes vlans con su respectivo direccionamiento ip, en el cuadro 17 se puede analizar y validar la información detallada de cada vlan configurada en las tres redes.

**Cuadro 17. Configuración y direccionamiento de Vlans**

| Vlan | Servicio | Ip física principal | Ip física backup | Ip física contingencia |
|---|---|---|---|---|
| Vlan 22 | Credibanco | 172.17.253.42/29 | 172.17.253.46/29 | 172.17.253.43/29 |
| Vlan 24 | Banrepública | 10.213.26.23/28 | 10.213.26.24/28 | 10.213.26.25/28 |
| Vlan 28 | Firewall | 172.27.254.14/25 | 172.27.254.15/25 | 172.27.254.12/25 |
| Vlan 32 | Firewall | 172.16.254.213/29 | 172.16.254.214/29 | 172.16.254.212/29 |
| Vlan 75 | Visa | 172.31.4.200/24 | 172.31.4.201/24 | 172.31.4.202/24 |
| Vlan 76 | Cifin | 172.30.4.200/24 | 172.30.4.201/24 | 172.30.4.202/24 |

Fuente: Autores

La configuración y nombre de las vlans, los segmentos de red son asignadas directamente por el prestador de servicios, para este ejemplo puntual son tomadas a modo de prueba con el fin de realizar las diferentes simulaciones.

El proveedor de servicios alquila dentro de los contrato establecidos para las tres redes equipos cisco modelo 3945/K9 y transceiver raisecom Rc512, para este ejemplo puntual se tienen en cuenta estos equipos ya que son con los que cuenta actualmente las redes de datos, pero es indiferente la marca, modelo, seriales y especificaciones técnicas, sin embargo si se desea iniciar un nuevo proyecto se debe realizar un estudio con los requerimientos que el usuario o cliente final necesiten para suplir sus necesidades, en los cuadros 18 y 19 respectivamente, se puede observar las especificaciones técnicas de cada uno que son las más relevantes que tanto prestador de servicios como cliente deben conocer para su instalación (alimentación, dimensiones, consumo), requerimientos (capacidad, velocidad, memoria), uso y posibles fallas que puedan presentarse.

**Cuadro 18. Especificaciones técnicas Router cisco 3945/K9**

| | |
|---|---|
| Código del producto | CISCO3945/K9 |
| Servicios de perfomance y máquina de modulo | w/SPE 150 |
| Interfaces | 3 integrated 10/100/1000 Ethernet ports with 2 ports capable of RJ-45 or SFP connectivity |
| Expansión de slots | 4 service module slots<br>1 Internal Services Module slot<br>4 onboard digital signal processor (DSP) slots<br>4 Enhanced High-Speed WAN Interface Card (EHWIC) slots |
| Memoria RAM | 1 GB (installed) / 2 GB (max) |
| Memoria Flash | 256 MB (installed) / 8 GB (max) |
| Dimensiones | 47.6 cm x 43.8 cm x 13.3 cm |
| Peso | 21.84 kg |
| Unidades de Rack | 3 unidades de rack |

Fuente: Autores

**Cuadro 19. Especificaciones técnicas transceiver Raisecom RC512**

| | |
|---|---|
| Interfaz fija | 1*fiber interface 1*copper interface |
| Indicadores | Fuente de alimentación RMD para la unidad remota RLK para puerto óptico TLK para puerto óptico ACT para puerto óptico LNK / ACT para el puerto de cobre 100M para el puerto de cobre FDX para el puerto de cobre |
| Velocidad | 100M interfaz de fibra fija 10 / 100M auto-negociación Interfaz de cobre |

**Cuadro 19 (continua)**

| | |
|---|---|
| Dimensiones | Módulo:<br>91 (W) * 155 (D) * 25 (H) mm<br>Autónomo:<br>120 (W) * 157 (D) * 32 (H) mm |
| Fuente de alimentación | AC: 90~264V, 47~63Hz DC: -75~-36V |
| Poder de consumo | ≤ 5W (at max load) |
| Ambiente de trabajo | Temp: 0 ~ 45 centígrados RH: 20 ~ 90% sin condensación |
| Ambiente de almacenamiento | Temp: -25 ~ 85 centígrados RH: 20 ~ 90% sin condensación |
| Seguridad de conformidad | CE, UL and NEBS |

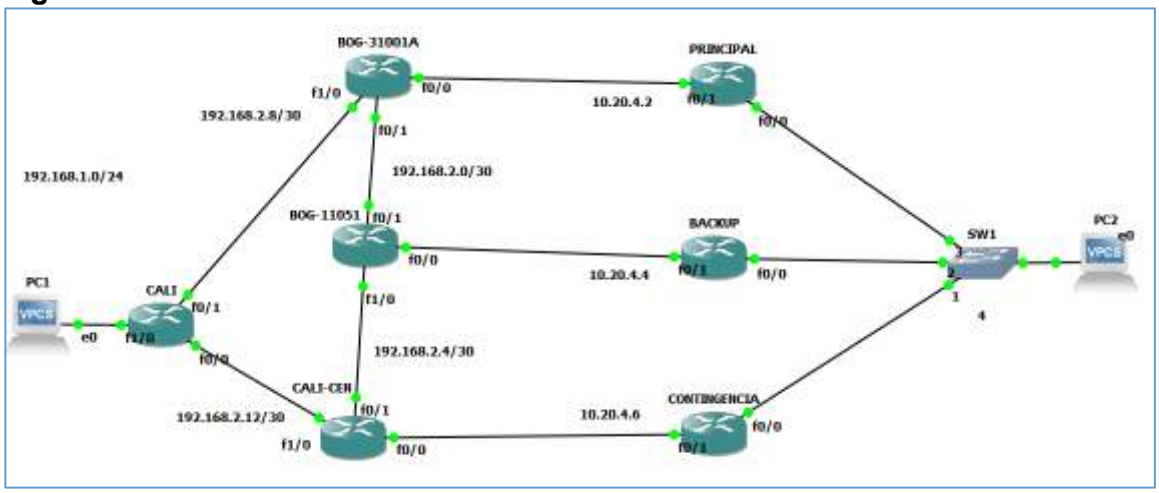
Fuente: Autores

En el diseño del plan de contingencia a modo de pruebas, se realizará una simulación en el software Gns3, el cual permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos en los que se evidencia la implementación del plan de contingencia.

## 5.6 SIMULACIÓN DEL PLAN DE CONTINGENCIA EN UNA MÁQUINA VIRTUAL GNS3

Se utiliza este software ya que contiene la mayoría de los equipos instalados en la red física con sus respectivos sistemas operativos y frente a los demás simuladores el Gns3 permite operar comandos reales, así mismo es un programa open source, el cual permite ser utilizado en múltiples sistemas operativos y puede trabajar con los IOS de router reales. En la figura 14 se puede observar el diseño de la red en el simulador.

**Figura 14. Simulación en software GNS3**




Fuente: Autores

Los routers nombrados como BOG-31001A, BOG-11051 y CAL-CEN, representan los 3 P.E en la topología final y cada uno va conectado a su respectiva red.

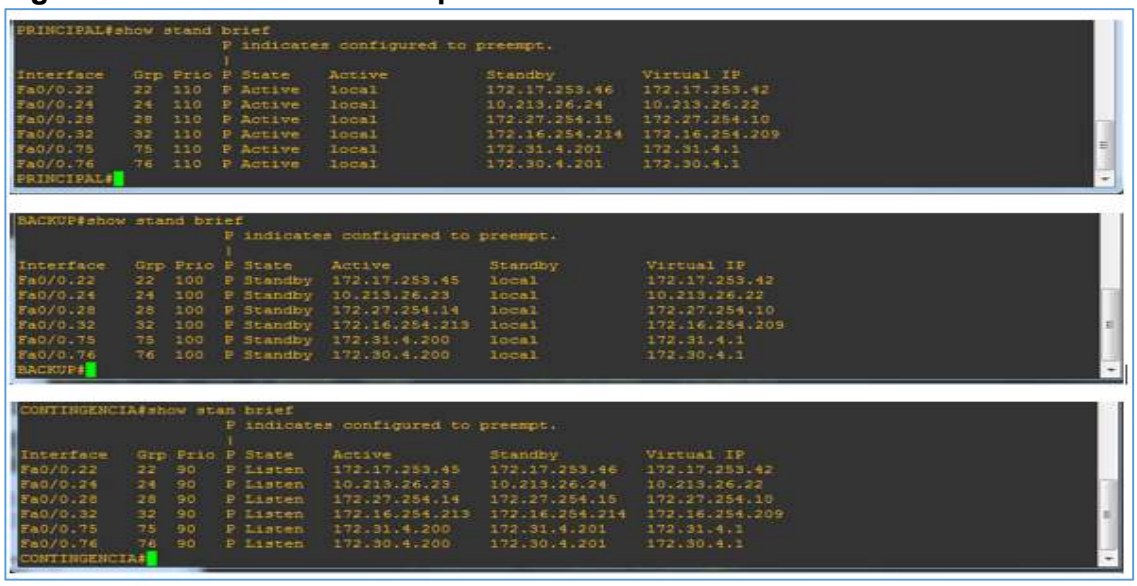
Para la conectividad entre los PE, de BOG-31001A, BOG-11051 ,CAL-CEN y la sede remota “CALI”, se utiliza direccionamiento privado clase C, el cual se escoge para realizar la simulación y está alojado en el segmento 192.168.2.0/30, esto con el fin de simular conectividad entre los PE, a nivel de capa 3.

El direccionamiento desde los PE, hacia los router que se encuentran en la sede del cliente del sector financiero es de tipo privado y es clase A, el cual es asignado por el operador de servicio al cliente según la disponibilidad de IP y para este proyecto los segmentos de red tienen mascara 29.

Al momento de realizar las pruebas de simulación en Gns3, se presentan tres escenarios diferentes enumerados a continuación:

- Escenario 1. El primer escenario la red de la entidad se encuentra funcionando en completa normalidad, validando la configuración del protocolo HSRP para este caso en particular, se tiene configurado para el router principal una prioridad de 110, para el router de backup un prioridad de 100 y para el router de contingencia una prioridad de 90, todos con un decremento de 30 que se encuentra asociado a un trac que está configurado para que entre a operar cuando se presente caída de la interface WAN asignada sobre cada router , en la figura 15 se observa la red en correcto funcionamiento que corresponde al escenario 1 donde se ve afectado el canal principal, siendo los estados del protocolo HSRP para el router principal activo, router backup standby y router de contingencia en listen.

**Figura 15. Estados HSRP sin presentarse fallas en la red**



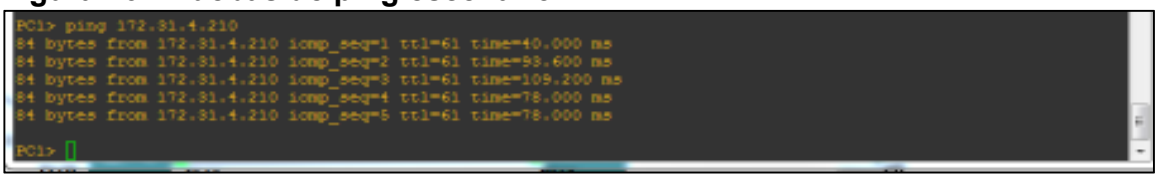

Fuente: Autores

La figura se interpreta de la siguiente manera:

a) Router principal, estado activo, prioridad 110
b) Router backup, estado standby, prioridad 100
c) Router contingencia, estado listen, prioridad 90

En la figura 16 se encuentra cómo se realizan las pruebas a ping desde la sede remota hacia la sede principal en lo correspondiente para el escenario 1.

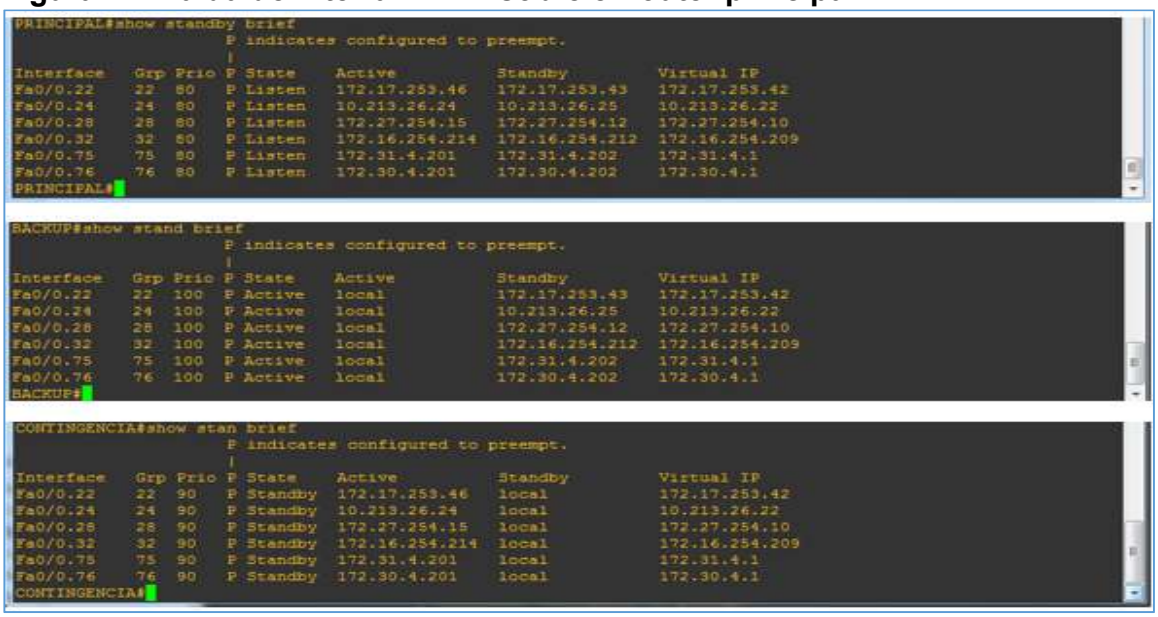
**Figura 16. Pruebas de ping escenario 1**




Fuente: Autores

- Escenario 2. En el segundo escenario a modo de pruebas, se baja administrativamente la interfaz WAN del router principal, este procedimiento se realiza ingresando al router y ejecutando en el comando shutdown, esto equivale en un ambiente real a un ruptura de fibra, falla del router, desconexión de equipos, fallas sobre el P.E o sobre la red de acceso, o cualquier otro evento que pueda afectar la red principal, como se observa en la figura 17 entra a funcionar el trac creado que decrementa en 30 el HSRP configurado, pasando de 110 a 80, y el estado pasa de activo a listen, siendo el router de backup ahora el activo y la contingencia el standby.

**Figura 17. Caída de interfaz WAN sobre el router principal**



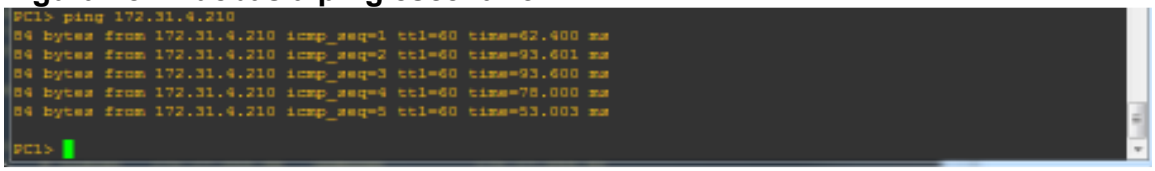

Fuente: Autores

La figura se interpreta de la siguiente manera:

a) Router principal, estado Listen, prioridad 80
b) Router backup, estado activo, prioridad 100
c) Router contingencia, estado standby, prioridad 90

En la figura 18 se detalla las pruebas a ping desde la sede remota hacia la sede principal para el escenario 2, estas se realizan cuando ya se ha visto afectación sobre el canal principal, las pruebas se realizan con el fin de probar conectividad entre la sede remota y la sede principal.

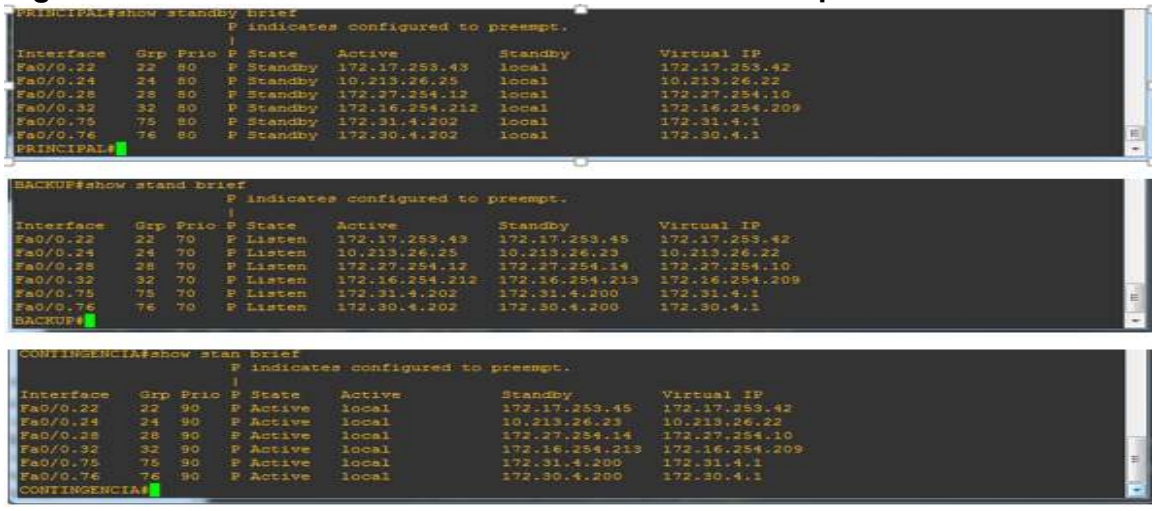
**Figura 18. Pruebas a ping escenario 2**




Fuente: Autores

- Escenario 3. En el tercer escenario a modo de pruebas, se baja administrativamente la interfaz WAN del router backup, igual que en el anterior escenario se realiza esta operación ejecutando el comando shutdown sobre la interfaz que conecta el P.E hacia el router backup, esto equivale en un ambiente real a un ruptura de fibra, falla del router, desconexión de equipos, fallas sobre el P.E o sobre la red de acceso, o cualquier otro evento que pueda afectar la red backup, cabe resaltar que la red principal también se encuentra caída; como se observa en la figura 19 entra a funcionar el trac creado que decrementa en 30 el HSRP configurado en el backup pasando de 100 a 70, y el estado pasa de activo a listen, siendo el router de contingencia ahora el activo y el principal el standby.

**Figura 19. Caída de interfaz WAN sobre el router backup**



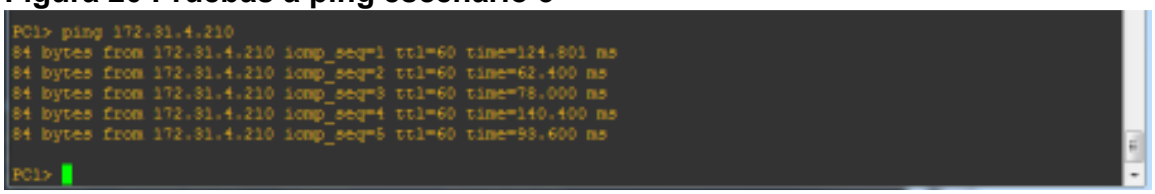

Fuente: Autores

La figura se interpreta de la siguiente manera:

a) Router principal, estado standby, prioridad 80
b) Router backup, estado listen, prioridad 70
c) Router contingencia, estado activo, prioridad 90

En la figura 20 se analiza las pruebas a ping desde la sede remota hacia la sede principal para el escenario 3, esta es la prueba más importante ya que se entra a evidenciar la operatividad del canal de contingencia, se observa que los tiempos de respuesta son muy similares a los presentados en los escenarios anteriores, cabe resaltar que los tiempos en una simulación virtual no corresponden a los que se puedan presentar en equipos reales, ya que el software gns3, está diseñado para simular equipos y depende del procesamiento de la maquina en la que está instalado.

**Figura 20 Pruebas a ping escenario 3**




Fuente: Autores

# 6. CONCLUSIONES

- En importante en primera instancia realizar un estudio exhaustivo de la topología de red del cliente banco Financorp y evaluar las necesidades y requerimientos antes de diseñar el plan de contingencia, se debe tener en cuenta el nivel de disponibilidad de la red que requiere el cliente, para entrar a evaluar el diseño del plan de contingencia, el alcance que se quiere con la implementación del plan de contingencia, se evidencia que el impacto es alto debido a que es una entidad financiera, es importante realizar pruebas en la etapa inicial para evaluar la disponibilidad que se tiene de la red sin haber implementado el plan de contingencia, esto con el fin de justificar su implementación.

- Los aspectos más relevantes durante el diseño del plan de contingencia, es en primera instancia buscar otro sector geográfico apartado de donde se encuentra la red principal y backup, esto con el fin de prevenir si se presentan siniestros, catástrofes o eventos provocados por terceros que puedan afectar las instalaciones físicas donde se encuentran las redes, se tiene en cuenta los equipos requeridos para la solución final del cliente, direccionamiento ip, creación de vlans, la correcta configuración y pruebas del protocolo hsrp, esto debido a que cuando se realicen las pruebas de conmutación entre en funcionamiento tanto el canal de backup, como el plan de contingencia.

- Aunque el escenario real y la simulación no son iguales, realizar la simulación antes de implementar el plan de contingencia, permiten prevenir errores de configuración, pruebas de conectividad, simular los diferentes escenarios cuando se presentan las fallas en la red y validar las conmutaciones hacia la red de contingencia. Sin embargo, al momento de realizar las pruebas de simulación el software Gns3, se debe tener en cuenta que los tiempos de ping entre los equipos son más altos que en la práctica debido a que son máquinas virtuales. Simular los diferentes escenarios cuando se presentan las fallas en la red y validar las conmutaciones hacia la red de contingencia, permite determinar en el escenario real el impacto y la criticidad de las fallas que puedan presentarse.

- En el periodo en el cual se implementa la red de contingencia, se presentan fallas de conectividad, enrutamiento, falla de aplicativos, de este modo es aconsejable realizar la implementación y sus pruebas durante mínimo tres ventanas de mantenimiento, donde este involucrados tanto personal técnico del cliente como del proveedor de servicios, y tener en cuenta las posibles eventualidades que puedan presentarse, estas actividades deben ser controladas tanto por el cliente como el prestador de servicios con un minutograma previamente diseñado y un rollback, en caso de la que las pruebas y la implementación no arrojen los resultados esperados.

## BIBLIOGRAFÍA


ANTEPORTAMLATINAM, José María. Comercio electrónico. [en línea]. Bogotá: El Autor [citado 18, junio, 2017]. Disponible en Internet: < URL: http://docplayer.es/3916381-Comercio-electronico-una-introduccion-general.html>

AVIZIENIS. A. IEEE Computer. EEUU. Mc Graw Hill,1997,391p.

AYUSO, Pablo Neira. Tolerancia a fallos para la alta disponibilidad. En: Revista del Departamento de Lenguajes y Sistemas Informáticos. Marzo-abril, 2012.vol.6, no. 11, 69 p.

BARBANCHO, Julio; CONCEJERO, Jaime; BENJUMEA, Octavio; RIVERA, Mª Del Carmen; ROMERO, Jorge; ROPERO, Gemma y SANCHEZ Anton. Sistemas Microninformaticos y Redes. España: Ediciones paraninfo, 2014.407 p.

BUDHIJARA, N; MARZULLO, K y SCHNEIDER, F. The primary-backup approach. In Distributed Systems. USA: Mc Graw Hill, 2003, 296 p.

CANDEA, G and FOX. Crash-only software. In 9th Workshop on Hot Topics in Operating Systems, 2003. p.23.

CISCO. Documentos Cisco. [en línea]. Bogotá: Cisco [citado 25, mayo, 2017]. Disponible en Internet: < URL: http://www.cisco.com/c/es_mx/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html>

CISCO. Soporte Cisco. [en línea]. Bogotá: Cisco [citado 8, agosto, 2017]. Disponible en Internet: < URL: https://www.cisco.com/support/LA/es/TS/7/73391/hsrpguidetoc.shtml>

DIARIO PORTAFOLIO. Multan a Bancolombia con $840 millones por mal servicio en plataforma electrónica. [en línea]. Bogotá: El Autor [citado 24, febrero, 2017]. Disponible en Internet: < URL http://www.portafolio.co/negocios/empresas/superfinanciera-multa-a-bancolombia-por-mal-servicio-de-plataforma-digital-503646>

GRAY,Jim. ACM DL Liberia Digital. The ACM Guide to Computing Literature. [en línea].Téxas: El Autor [citado 4, septiembre, 2017]. Disponible en Internet: < URL: https://dl.acm.org/>

ICONTEC. Instituto Colombiano de Normas Técnicas y Certificación. Norma Técnica Colombiana NTC 5254. Gestión de Riesgo. Bogotá: ICONTEC. 2006, 42 p.

IDICT, Carlos. Conmutación (Redes de comunicación). [en línea]. Bogotá: Ecured [citado 12, mayo, 2017]. Disponible en Internet: < URL: https://www.ecured.cu/EcuRed:Enciclopedia_cubana>

KOHLER, Alois; BLOEMERTZ, Lena y JÜLICH, Sebastian. Una base para la gestión de riesgo, México: Trillas editores, 2004. 192 p.

MARÍN, Diego. Sistemas de almacenamiento. IFCT0310. España: Ic Editorial, 2014. 128 p.

MATHEUS, Norma. Computación – Informática. [en línea]. Bogotá: El Autor [citado 6, agosto, 2017]. Disponible en Internet: < URL: https://nmatheus.wordpress.com/2012/01/20/redes-internet-intranet-extranet/>

MICROSOFT. Microsoft TechNet. [en línea]. Bogotá: El Autor [citado 20, julio, 2017]. Disponible en Internet: < URL: https://technet.microsoft.com/es-co/library/aa998704(v=exchg.65).aspx>

MONTERO, Fernando. Gestión del Riesgo en Infraestructura y Comunicaciones TI, para Empresa del Sector Financiero. Chile: Universidad Técnica Federico Santa María,2011, 231 p.

NSRC. Introducción a BGP. [en línea]. Bogotá: El Autor [citado 4, febrero, 2017]. Disponible en Internet: < URL: https://nsrc.org/workshops/2011/walc/routing/raw-attachment/wiki/Agenda/Intro_BGP.pdf>

RANKIA. Mejores Bancos en Colombia. [en línea]. Bogotá: El Autor [citado 28, agosto, 2017]. Disponible en Internet: < URL: https://www.rankia.co/blog/mejores-cdts/3449454-mejores-bancos-colombia-2017>

RODRÍGUEZ, Edith Yolima. Plan de continuidad BS 25999 [en línea]. Bogotá: Sisteseg [citado 27, agosto, 2017]. Disponible en Internet: < URL: http://www.sisteseg.com/files/Microsoft_Word_Articulo_BS_25999_DEF1.pdf>

SANZ, Juan Manuel. Security Ar work. [en línea]. Bogotá: Security Ar work [citado 3, marzo, 2017]. Disponible en Internet: < URL: https://www.securityartwork.es/2013/09/26/ataque-al-protocolo-hsrp/>

SERVICIO GEOLÓGICO COLOMBIANO. Sismicidad histórica de Colombia. [en línea]. Bogotá: El Autor [citado 20, octubre, 2017]. Disponible en Internet: < URL: http://sish.sgc.gov.co/visor/#>

SWISS RE. Catástrofes naturales y siniestros antropógenos en 2015. [en línea]. Bogotá: El Autor [citado 20, julio, 2017]. Disponible en Internet: < URL: http://media.swissre.com/documents/sigma1_2016.es.pdf>

TOMASI, Wayne. Sistemas de comunicaciones electrónicas. México: Prentice Hall Inc, 2003, 721 p.