PROPUESTA DE ALTA DISPONIBILIDAD PARA UNA ORGANIZACIÓN DE SERVICIOS DE TURISMO, RECREACIÓN Y SERVICIOS SOCIALES

PRESENTADO POR:
JOHN ESTEBAN NOVOA MORENO
JORGE ASDRUBAL TAMAYO REINEL

ASESOR TÉCNICO DE PROYECTO:
INGENIERO JOHN FREDY CHACON SANCHEZ

UNIVERSIDAD EL BOSQUE
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD DE REDES TELEMÁTICAS
BOGOTÁ, COLOMBIA
Septiembre 2022

RESUMEN

El objetivo principal de este trabajo es realizar una propuesta de alta disponibilidad a los dispositivos de infraestructura principales de red, que son de alto impacto operacional en la organización objeto del presente estudio y que presta servicios de turismo, recreación, crédito social entre otros. La metodología propuesta consiste en realizar un levantamiento de información donde se determinará cuáles son los dispositivos de infraestructura de red de mayor importancia, con esta información se genera un análisis de puntos de único fallo que generan riesgos de la información en cuanto a su componente de disponibilidad. Con el anterior levantamiento de información se generará un informe con los hallazgos y se entregarán una serie de recomendaciones y buenas prácticas para mitigar los riesgos que cumplan con los estándares de la compañía, en especial a la mejora de la disponibilidad de la información que transita por la red local de la sede principal.

PALABRAS CLAVE

Disponibilidad, seguridad, infraestructura, análisis, sistemas, servicios, información, evaluación.

ABSTRACT

The main objective of this work is to make a high availability proposal for the main network infrastructure devices, which have a high operational impact on the organization that is the object of this study and that provides tourism, recreation, and social credit services, among others. The proposed methodology consists of carrying out an information survey where it will be determined which are the most important network infrastructure devices, with this information an analysis of single failure points that generate information risks in terms of its availability component is generated. . With the previous collection of information, a report will be generated with the findings and a series of recommendations and good practices will be delivered to mitigate the risks that comply with the company's standards, especially to improve the availability of the information that passes through the local network of the headquarters.

KEYWORDS

Availability, security, infrastructure, analysis, systems, services, information, evaluation.

Tabla de contenido

RESUMEN 2
PALABRAS CLAVE 2
ABSTRACT 2
KEYWORDS 2
1. Título 5
2. Introducción 5
3. Descripción general del proyecto 5
3.1 Definición del problema 5
3.2 Aspectos a solucionar 6
3.3 Solución propuesta 7
4. Estado del arte 7
4.1.1 Conceptos 9
5. Glosario de términos 15
6. Justificación 18
7. Objetivos 19
7.1. General 19
7.2. Específicos 19
8. Requerimientos 19
8.1 Requerimientos funcionales 19
8.2 Requerimientos no funcionales 19
8.3 Requerimientos de restricción 20
9. Metodología 20
10. Diagnóstico de la Infraestructura Existente 21
11. Diseño de Red en Alta Disponibilidad 33
11.1 Diagramas de Red Propuesta en Alta Disponibilidad 33
11.2 Selección de Equipos de Red 36

11.2.1 Descripción de Especificaciones Técnicas de Switches 39
11.2.1.1 Performance and Scaling 39
11.2.1.2 External Ports/Slots 39
11.2.1.3 Stacking Ports 40
11.2.1.4 PoE Power Budget 41
11.3 Simulación de Red Propuesta 41
12. Resultados 42
13. Discusión 46
14. Conclusiones 48
15. Documentación de Referencia 49
16. Anexos 50

Tabla de Ilustraciones

Ilustración 1 Amenaza vs Vulnerabilidad 12
Ilustración 2 Diagrama de Red de la Sede Principal 25
Ilustración 3 Monitoreo 1 Switch Core Icinga 27
Ilustración 4 Monitoreo 2 Switch Core Icinga 28
Ilustración 5 Diagrama de Red de Infraestructura de Servidores en modalidad de Cloud Privado 29
Ilustración 6 Diagrama de Red de Puntos de Único Fallo 30
Ilustración 7 Diagrama de Red de Puntos de Único Fallo Servidores Cloud Privado 31
Ilustración 8 Diagrama de Red Sede Principal Propuesta 32
Ilustración 9 Diagrama de Red Infraestructura de Servidores Cloud Privado Propuesta 34
Ilustración 10 Cuadrante mágico de actores del mercado. Tomado de Gartner© 2022 35
Ilustración 11 Consumos típicos de recurso de procesamiento de Firewall 37
Ilustración 12 Diagrama de Red Sede Principal Propuesta Simulación 40
Ilustración 13 Apagado Switch CORE2 42
Ilustración 14 Pruebas de Conectividad Apagado Switch CORE2 43
Ilustración 15 Apagado Switch CORE1 44
Ilustración 16 Pruebas de Conectividad Apagado Switch CORE1 45

1. Título

PROPUESTA DE ALTA DISPONIBILIDAD PARA UNA ORGANIZACIÓN DE SERVICIOS DE TURISMO, RECREACIÓN Y SERVICIOS SOCIALES

2. Introducción

El presente proyecto busca la evaluación de una red de datos existente en una organización en la cual se realizará la recomendación de implementación de una arquitectura segura primordialmente desde el componente de la disponibilidad a partir de controles y recomendaciones normalmente aceptados en este tipo de proyectos.

3. Descripción general del proyecto

3.1 Definición del problema

La organización objeto del presente estudio se dedica a prestar distintos tipos de servicios que abarcan desde turismo, recreación, deportes, créditos financieros hasta prestación de servicios de salud de primer nivel. Para prestar los anteriores servicios se cuenta con una infraestructura de servicios de TI que se encuentra alojada en una nube privada, y otra de pruebas en modalidad "on premise". La red LAN de la sede principal de la organización, ubicada en la ciudad de Bogotá, hace parte de la infraestructura física de cableado del edificio y cuenta con dispositivos conmutadores que se encuentran en el final de su vida útil y evidencian obsolescencia tecnológica y que sirve a un aproximado de 250 usuarios conectados a través de sus equipos de escritorio o portátiles.

En la sede principal de la organización se evidencian deficiencias a nivel de seguridad en la red local, entendida en su componente de disponibilidad de la información transmitida y compartida a través de la red local LAN.

Lo anterior a causa de:

- Inadecuados dispositivos conmutadores de red por falta de una debida y correcta configuración, como también la obsolescencia de algunos de ellos.

- No se cuenta con plantillas de aseguramiento de los mismos dispositivos.

- No se tiene una simulación ni dispositivos de respaldo de red que permita a los administradores realizar pruebas de configuración e implementación de nuevas configuraciones que facilite realizar pruebas previas a su despliegue.

- No se cuenta con diagrama de red actualizados que permita el entendimiento general de la arquitectura de la red existente, como también la identificación de puntos de único fallo.

La operación diaria de los distintos procesos que son llevados a cabo dentro de la sede principal manifiesta constantes intermitencias, lentitud y carencia de controles de seguridad para dispositivos externos que se conectan a la red. Lo anterior ocasiona eventualmente falta de disponibilidad de la información en momentos de alta demanda de la red LAN, que ocasiona retrasos en las actividades propias de los procesos y al mismo tiempo, la falta de controles de seguridad genera brechas que podrían ser aprovechadas por criminales para tener acceso a la información transmitida en la misma red.

3.2 Aspectos a solucionar

- No se cuenta con los diagramas de red actualizados que identifique dispositivos, marca, direccionamiento, nombre de host y sus conexiones.

- No se cuenta con mecanismos de alta disponibilidad, ni la posibilidad de identificar puntos de único fallo en la red.

- No se cuenta con una simulación de la red existente donde se pueda evidenciar configuraciones de los dispositivos de red en producción.

- No se cuenta con plantillas de aseguramiento o "hardening" para los equipos de red LAN.

3.3 Solución propuesta

Realizar un diseño de la nueva arquitectura de red donde se evidencie la eliminación de puntos de único fallo, el reemplazo de los equipos conmutadores existentes (Switches) obsoletos para la nueva infraestructura de red, para posteriormente proporcionar la configuración adecuada de los dispositivos de red LAN y sus plantillas de aseguramiento, previamente validado por una simulación en computador que permite asegurar un nivel de alta disponibilidad de la solución antes de realizar el despliegue en producción.

4. Estado del arte

Actualmente se tiene establecido que la seguridad de la información se basa en tres pilares básicos, a saber, la disponibilidad, la confiabilidad y la integridad de la información (Castro, 2018). Los anteriores pilares son constitutivos de todo tipo de proyectos encaminados a asegurar cualquier sistema informático incluyendo redes informáticas, donde no cabe duda de la importancia que tiene la seguridad de la información, así es, como "la salvaguarda de la información en los sistemas informáticos ha sido una preocupación permanente tanto para usuarios, profesionales de la información como para los entes reguladores, de tal forma se han desarrollado diferentes metodologías y procedimientos encaminados al análisis y evaluación de riesgos" (Tamayo, 2020).

4.1 Marco de referencia teórico

En la actualidad es casi imposible imaginar una organización que para el cumplimiento de sus objetivos misionales no realice procesamiento de información en alguno de sus procesos a través de herramientas, equipos u otro tipo de elementos, y buscar maximizar la consecución de valor en estas actividades, así tenemos que "la información es vital para el funcionamiento de cualquier empresa y, por el otro lado, que la informática es la ciencia que estudia todos los procesos que se pueden hacer sobre la información, pero con la ayuda de dispositivos automáticos" (Urbina, 2016).

Dada la dependencia que tienen las empresas y organizaciones de la información, esta se convierte en un activo muy importante, en que la falta, alteración o pérdida de su confidencialidad puede impactar seriamente a sus actividades productivas, y "si queremos que una empresa siempre funcione de forma adecuada, al menos desde el punto en el cual se procesa la información, es necesario e imperativo tener la certeza de que esa información está segura en cualquiera de los procesos ... en la recepción, el envío, el almacenamiento y el análisis de datos, que al ser procesados se convierten en información" (Urbina, 2016).

Lo anterior se explica en razón a la búsqueda permanente de las empresas por volver más eficientes sus procesos y de alguna forma mantener competitiva a la organización frente a sus rivales comerciales y maximizar elementos diferenciadores en la prestación del servicio o entrega de productos a sus clientes, es como "las empresas, de forma consciente o inconsciente, han volcado sus procesos de negocio netamente a los sistemas de información. Siempre con el fin de volverse más productivas, ahorrar costos y poder realizar negocios en todas partes del mundo" (Portantier, 2012).

Al tratar la seguridad informática es necesario hablar de cada uno de los componentes de un sistema informático, en el que cada uno varía a nivel funcional, amenazas, riesgos o controles aplicables, dado que realizan un tratamiento diferenciado de la información y la misma incluso puede encontrarse en tránsito entre uno u otro a través de medios de comunicación, es así que "cuando una información es transmitida por un canal de comunicaciones la información está sometida a riesgos porque existe amenaza (alguien está interesado en la información) y el canal de comunicaciones tiene vulnerabilidades (un canal de comunicaciones es, en la mayoría de los casos, esencialmente inseguro)" (Gutiérrez & Ayuso, 2003). Por esto es necesario dotar a las comunicaciones de distintos controles que deben involucrar la correcta configuración de dispositivos, adecuadas políticas de seguridad y actualizaciones tecnológicas entre otros.

En algunos casos pueden encontrarse vulnerabilidades asociadas a la falta de configuración de los dispositivos de red, es decir instalaciones con parámetros de fábrica, “Muchos dispositivos de red tienen una configuración por defecto que facilita la instalación o intenta conseguir las máximas prestaciones en detrimento de aspectos de seguridad. Una instalación sin la debida atención a la corrección de estas opciones puede acarrear serios

problemas potenciales" (Soriano, 2014). Lo anterior puede facilitar la materialización de riesgos a través de puertos o servicios activos de forma innecesaria, falta de protocolos de cifrado en las comunicaciones o simplemente accesos remotos permitidos con usuarios y contraseñas por defecto bien conocidos de acuerdo con el modelo y marca del dispositivo.

Lo anterior se basa en el entendimiento de los siguientes conceptos primordiales que son objeto de análisis y estudio.

4.1.1 Conceptos

Disponibilidad: Se trata de la posibilidad que la información o un servicio informático se encuentre presente cuando se necesite. En la práctica no es imposible asegurar una disponibilidad absoluta, es decir del 100% del tiempo, debido a la misma naturaleza física con que se debe hacer el tratamiento de la información. Por lo anterior en el caso de servicios, sistemas o dispositivos informáticos se utilizan tablas en escala porcentual que miden el nivel de disponibilidad.

Disponibilidad	Máximo Tiempo de Tolerancia al Año
99%	87 h y 36 mins
99.5%	43 h y 48 mins
99.95%	4 h y 23 mins
99.99%	53 mins
99.999%	5 mins

Para lo anterior es importante entender la mayor dificultad que representa técnicamente el acercarse más y más a una disponibilidad del 100%, este hecho se enmarca dentro del concepto de Alta Disponibilidad (HA), en donde se debe apelar a estrategias donde la probabilidad de materialización de un riesgo que afecta la disponibilidad se vea mitigado por la existencia de servicios o dispositivos informáticos alternos que proporcionen de forma automatizada la capacidad de migración tras un error al dispositivo alterno, con el objetivo de brindar a los usuarios y demás sistemas un funcionamiento continuo. De esta forma el

porcentaje o nivel de disponibilidad será mayor al de una alternativa no HA, a efectos prácticos niveles iguales o superiores al 99.95% entran a considerarse como soluciones HA.

Hardware: Es un término que hace referencia a aquellas partes electrónicas que conforman un sistema de computación de forma física que se puede tocar; por lo tanto, podemos decir que una computadora es un dispositivo de hardware capaz de interpretar y ejecutar órdenes programadas con base en una lógica y realizar operaciones de entrada, salida y procesamiento.

Información: La información no consiste en un conjunto de datos simples, sino procesados de alguna forma; por ejemplo, ordenados y resumidos, para proporcionar un resultado, interpretado como información por el usuario o personal encargado de la toma de decisiones, que supone que la importancia que se concede a la información se debe a su función clave como minimizador de incertidumbre en el proceso de toma de decisiones (Vega-Pérez et al., 2017).

Informática: Es un término que abarca todas aquellas técnicas y conocimientos científicos que posibilitan hacer un tratamiento de forma automatizada de la información por medio de un hardware y software.

Protocolo: Un protocolo se define como el formato y el orden de los mensajes intercambiados entre dos o más entidades que se comunican, así como las acciones tomadas en la transmisión y/o la recepción de un mensaje u otro suceso (Kurose & Ross, 2010).

Software: Es el componente intangible de cualquier sistema de cómputo que abarca las instrucciones u órdenes que indican al hardware que es lo que debe hacer con los datos para producir un resultado. Dado que el funcionamiento esperado de un sistema de cómputo involucra la captura, procesamiento y entrega de datos, convierte al software en un elemento clave en cualquier computadora y al mismo tiempo otorga la más amplia versatilidad de uso del hardware para distintas aplicaciones en entornos de trabajo igualmente diferentes.

Redes de Datos: Es un conjunto de dispositivos de cómputo (hardware y software) que se denominan hosts o sistemas terminales, los cuales se encuentran interconectados mediante enlaces de comunicación y dispositivos de conmutación de paquetes (Kurose & Ross, 2010).

Algunos de los medios que podemos encontrar son:

- **Punto a punto.-** El puerto de comunicación del equipo se conecta a un solo puerto del otro equipo.
- **Nube.-** Cada equipo está conectado en Red.
- **Multipunto.-** Diversos equipos pueden ser conectados al mismo medio.
- **WAN (Wide Area Network).-** Es aquella que se expande a través de una zona geográfica de un país o continente. Los medios de transmisión que se usan para cubrir estas distancias pueden ser microondas, cables de cobre, fibra óptica, satélite, etc.
- **MAN (Metropolitan Area Network).-** Es una versión más grande que la LAN en cuanto a topología, protocolos y medios de transmisión.
- **LAN (Local Area Network).-** Es un sistema de comunicación de datos que permite conectar un conjunto de recursos y compartirlos. Su extensión va de unos cuantos metros a unos 5 kilómetros.

Seguridad física comprende el sitio geográfico donde se encuentra localizado el activo de información y los controles de seguridad asociados al acceso físico al activo.

Seguridad lógica es la que hace referencia al aseguramiento y control del componente lógico de un sistema de cómputo, es decir el software, como por ejemplo programas y aplicaciones, aunado al transporte de los datos a través de la red de datos y los servicios de seguridad pertenecientes a uno o más mecánismos de seguridad.

Seguridad de control es aquella que tiene un alcance más general y de supervisión de la seguridad física y lógica, además de buscar una periódica capacitación del recurso humano, y liderar acciones correctivas que busquen mitigar riesgos a la seguridad informática, el cierre de brechas de seguridad o implementen controles relativos a la salvaguarda de un activo de información.

Una **VULNERABILIDAD** son ciertas condiciones inherentes a los activos, o presentes en su entorno, que facilitan que las amenazas se materialicen y los llevan a la condición de vulnerabilidad. Las vulnerabilidades son de diversos tipos como por ejemplo: la falta de conocimiento de un usuario, la transmisión a través de redes públicas, entre otros (Cordero, 2015)

Las **AMENAZAS** se aprovechan de las vulnerabilidades, siempre existen y son aquellas acciones que pueden ocasionar consecuencias negativas en las operaciones de la organización, comúnmente se referencia como amenazas a las fallas, a los ingresos no autorizados, a los virus, a los desastres ocasionados por fenómenos naturales o ambientales, entre otros. Las amenazas pueden ser de carácter físico como una inundación, o lógico como un acceso no autorizado a la base de datos (Cordero, 2015).

Un **RIESGO** es la probabilidad de materialización de un evento o amenaza aprovechando una vulnerabilidad que pueda imposibilitar el cumplimiento de un objetivo, de manera cuantitativa, el riesgo es una medida de las posibilidades de incumplimiento o exceso del objetivo planteado (Cordero, 2015). Así definido un riesgo puede producir 2 tipos de consecuencias: Ganancias o pérdidas.

Ilustración 1 Amenaza vs Vulnerabilidad

Las amenazas más comunes que pueden comprometer la seguridad en una empresa son:

- **Factores humanos:** errores asociados a las personas o usuarios que pueden ser de origen accidental o premeditado.
- **Falla en sistemas de información:** errores a nivel de instalación, programación o configuración.
- **Desastres naturales:** incendio, inundaciones o fallas estructurales de la infraestructura.
- **Malware:** código malicioso que permite a un atacante ejecutar acciones sobre los activos de información (botnets, spyware, malware, virus, troyanos, phishing, trashing).

Seguridad en Redes. Son los esfuerzos en seguridad informática dirigidos a la correcta configuración y buenas prácticas centradas en mejorar la disponibilidad, confidencialidad e integridad de dispositivos y hosts de redes de datos, con el fin de lograr mayor resistencia frente a ataques, realizar un descarte selectivo de paquetes y la protección de infraestructuras.

4.2 Marco de referencia tecnológico

Los dispositivos conmutadores (Switches) de capa 2 y enrutadores (Routers) de capa 3, son equipos electrónicos capaces de interconectar una red de computadoras, conectados mediante medios de comunicación como cables, ondas o cualquier otro medio de transporte de datos, basado en el protocolo Ethernet.

Los anteriores dispositivos obedecen reglas de funcionamiento y estructuración que se enmarcan en una pila de capas de protocolos que en su conjunto se organizan dentro de un modelo denominado Modelo de Referencia OSI, que consta de cinco capas, a saber, capa 1 o capa física, capa 2 o capa de enlace, capa 3 o capa de red, capa 4 o capa de transporte y capa 5 o capa de aplicación.

En la capa 3 agrupamos un grupo de protocolos que son gestionados por dispositivos

que se mencionaron anteriormente, como es el caso de routers, que cuentan con ciertas capacidades y que son responsables "de trasladar los paquetes de la capa de red, conocidos como datagramas, de un host a otro. El protocolo de la capa de transporte (TCP o UDP) de Internet de un host de origen pasa un segmento de la capa de transporte y una dirección de destino a la capa de red, al igual que damos al servicio de correo postal una carta con una dirección de destino. Luego, la capa de red proporciona el servicio de suministrar el segmento a la capa de transporte del host de destino" (Kurose & Ross, 2010).

Ahora al hablar de capa 2 nos referimos a una capa de enlace que "encamina un datagrama a través de una serie de routers entre el origen y el destino. Para trasladar un paquete de un nodo (host o router) al siguiente nodo de la ruta, la capa de red confía en los servicios de la capa de enlace. En concreto, en cada nodo, la capa de red pasa el datagrama a la capa de enlace, que entrega el datagrama al siguiente nodo existente a lo largo de la ruta. En el siguiente nodo, la capa de enlace pasa el datagrama a la capa de red. Entre los ejemplos de protocolos de la capa de enlace se incluye Ethernet" (Kurose & Ross, 2010).

Tanto protocolos como dispositivos de capa 2 y capa 3 son susceptibles de ser abordados desde una perspectiva de seguridad informática y seguridad de redes, dado su carácter constitutivo dentro de la configuración de una red de datos.

Para el análisis y estudio de diseño de topologías de red, en donde encontremos como partes constitutivas dispositivos de capa 2 y capa 3, es posible el uso de software de simulación que permita configurar, probar y evaluar el comportamiento de redes reales simples o complejas, de una forma previa a un proceso de despliegue y que no involucra la consecución o utilización de los dispositivos de red físicos, haciendo también posible realizar análisis y resolución de problemas de redes ya existentes.

En el mercado de software de simulación de red existen 2 grandes referentes, el primero y más conocido es el desarrollado por la empresa Cisco, llamado Packet Tracer de carácter privativo y el segundo es el software de código abierto GNS3 (Graphical Network Simulator). Ambos programas se encuentran actualmente soportados y con equipos de desarrollo que realizan mejoras y corrigen "bugs" o fallos en las versiones estables disponibles para descargas.

Como ventajas del programa Packet Tracer encontramos su facilidad de uso, versatilidad, capacidad de simulación de distintos protocolos de capa de aplicación y enrutamiento la no necesidad de contar con un hardware robusto para soportar las operaciones de simulación, soporte de casi por completo del sistema operativo de dispositivos de red Cisco denominado "ios", ser extremadamente útil y didáctico para estudiantes o personas que inician sus estudios en redes mostrando cómo funcionan.

Dentro de las desventajas se encuentran su limitada capacidad de simular características que se encuentran en el hardware real, solo permite simular redes con dispositivos de la marca Cisco, no permite interactuar con los sistemas operativos reales de los dispositivos.

Para el caso del programa GNS3 se encuentran como ventajas, su gran versatilidad para emular o simular todo tipo de dispositivos de red de distintos y de muy variados fabricantes de hardware, permite el uso del sistema operativo (ios) real de los fabricantes, emular casi por completo las características, funcionalidades y capacidades reales de los dispositivos, es posible encontrar software gratuito de distintos fabricantes para ser usado en GNS3 para emulación de los dispositivos.

5. Glosario de términos

Administración centralizada: Es donde se realiza la gestión y administración de los equipos de red desde un punto central.

Amenaza: Todo elemento o acción que atenta contra la seguridad de la información, las amenazas surgen a partir de la existencia de vulnerabilidades.

Análisis de vulnerabilidades: Proceso de identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de estas.

Ataque cibernético: Los ataques a las redes pueden ser definidos como diferentes tipos de actividades sistemáticas dirigidas a disminuir o corromper su seguridad. Desde este

punto de vista, un ataque puede ser definido como una amenaza sistemática generada por una entidad de una manera artificial, deliberada e inteligente (Soriano, M. 2014).

Ataque de Vulnerabilidad: Este ataque implica el envío de unos pocos mensajes bien construidos a una aplicación o sistema operativo vulnerable que esté ejecutándose en un host objetivo. Si se envía la secuencia de paquetes correcta a una aplicación o un sistema operativo vulnerable, el servicio puede detenerse o, lo que es peor, el host puede sufrir un fallo catastrófico (Kurose & Ross, 2010).

Confidencialidad: La confidencialidad hace referencia a la protección de la información frente a su divulgación a entidades o individuos no autorizados (organizaciones, personas, máquinas, procesos). Nadie debe poder leer los datos a excepción de las entidades específicas previstas (Soriano, M. 2014).

Clave: Es una palabra, número o cadena de caracteres que necesita el algoritmo criptográfico para cifrar el texto en claro o para descifrar el criptograma (Soriano, M. 2014).

Firewall: Un firewall o cortafuegos es un dispositivo que se utiliza para proteger la red interna de una organización. Esta protección se lleva a cabo mediante la separación de la red interna del mundo exterior, o Internet (Soriano, M. 2014).

Firma Digital: Una firma digital es una firma electrónica que se puede utilizar para autenticar la identidad del remitente de un mensaje o el firmante de un documento. Asimismo, también garantiza la integridad del mensaje (Soriano, M. 2014).

Firmware: El firmware o soporte lógico inalterable es un programa informático que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo.

Hardening: Es el proceso de asegurar un sistema para reducir sus vulnerabilidades en búsqueda de generar la reducción de las formas de ataque disponibles generalmente incluye el

cambio de contraseñas predeterminadas, la eliminación de software innecesario nombres de usuario o inicios de sesión innecesarios, y la desactivación o eliminación de servicios innecesarios combinado con la actualización de los sistemas.

Link Agreggation Control Protocol (LACP): El Protocolo de Agregación de Enlaces de Control – LACP, es un protocolo definido en el estándar 802.1ad y que puede ser implementado en los switches (Molina Ruiz, J. E. 2012).

Lista de control de Acceso (ACL): Las listas de control de acceso (ACL / Access Control List) incluyen una de descripción de los usuarios y grupos de usuarios con diferentes permisos sobre los archivos y carpetas de un volumen NTFS (New Technology File System) (Molina Ruiz, J. E. 2012).

Información: Es un conjunto de datos y cuyo objetivo es ampliar conocimientos, informar o aportar ideas sobre un tema determinado.

Infraestructura de Red: Son todos los componentes básicos y necesarios para que los servicios de red sean funcionales

Monitoreo: Consiste en monitorear los equipos de red y sistemas en busca de posibles fallas mediante reportes y alertas predeterminadas por el administrador.

Norma ISO/IEC 27001: Norma que determina los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información.

Norma ISO 9001: Norma que determina los requisitos para un Sistema de Gestión de la Calidad.

Política de seguridad: Una deficiencia de la política de seguridad es una frase comodín para indicar que una política de seguridad de la empresa, (o tal vez, la falta de política), genera amenazas de seguridad en la red de forma inconsciente (Soriano, M. 2014).

Puerto: Es una interfaz de tipo físico o virtual a través de la cual se pueden enviar y recibir los diferentes tipos de datos.

Protocolo de Comunicaciones: Es un sistema de reglas que permiten que dos o más sistemas de comunicaciones se comuniquen entre ellas para transmitir información a través de diversos medios físicos.

Redes LAN: Son aquéllas que vinculan computadoras que se halla en un espacio físico pequeño como edificio, oficina, la cual se realiza a través de un cable u ondas (Oroya Acosta, 2019).

Redes WAN: Esta red a diferencia de LAN cubre una gran zona geográfica y su función principal es interconectar diversas LAN, aunque no todas estén en una misma ubicación física, WAN funciona a través de routers (Oroya Acosta, 2019).

Redes WLAN: Las redes inalámbricas (Wireless networks, WLAN) gozan actualmente de gran popularidad ya que permiten la movilidad de los usuarios y de los equipos dentro del área de cobertura de la red. Estas redes permiten la conexión a Internet en casi todas partes y ofrecen servicios de comunicación de voz y datos (Soriano, M. 2014).

Riesgo informático: Problema que potencialmente puede ocurrir que afecte la continuidad del sistema informático.

Switch: Menciona que es un dispositivo de capa 2 y puede ser referido como un bridge multipuerto. Los switches toman las decisiones de envío basadas en las direcciones MAC contenidas dentro de las tramas de datos transmitidas (Molina Ruiz, J. E. 2012).

Sistema operativo: Es el software principal o un conjunto de programas de un sistema informático que gestiona los recursos de hardware y provee servicios a los programas de aplicación de software.

Servicios de Seguridad: Un servicio de seguridad es un servicio que garantiza que los sistemas de información o las transferencias de datos puedan tener la seguridad adecuada. Los servicios de seguridad se implementan mediante mecanismos de seguridad y de acuerdo a las políticas de seguridad (Soriano, M. 2014).

Telnet: Protocolo de red para acceder de forma remota a un equipo de red.

6. Justificación

El correcto y fiable funcionamiento de una red LAN permite asegurar una parte importante de las actividades propias de la organización a nivel de sus diferentes procesos, permitiendo que sean capaces de comunicarse, compartir datos, aplicaciones y en general todo tipo de información, lo cual aumenta la eficiencia y la calidad del desempeño de los procesos, que se traduce a nivel económico como también en óptimos tiempos de respuesta. Además de evitar fugas o pérdidas de confidencialidad de la información que es transmitida a través de la red local.

Con la operación de equipos obsoletos dentro de la red LAN sumado al hecho de falta de configuraciones seguras se crean brechas de seguridad que pueden comprometer la integridad de la información transmitida o compartida a nivel local y en determinados momentos en los que aumenta la demanda del recurso falla la disponibilidad en la forma de intermitencias o lentitudes percibidas en la operación de aplicaciones, servicios o sistemas de información. Así mismo se corren riesgos de pérdida de confidencialidad producto de las amenazas a las que son susceptibles este tipo de redes que requieren para su implementación una debida planeación, diseño y ejecución de actividades y configuraciones de los dispositivos conmutadores que hacen parte de la infraestructura de red.

Los efectos a mediano o largo plazo por la falta de una red segura a nivel económico son muy cuantiosos en la medida que los procesos no disponen de recursos óptimos para el desempeño de sus actividades propias dentro de la organización, así mismo, las demandas, procesos judiciales o sanciones producto de la pérdida de la disponibilidad y confidencialidad de información sensible, como por ejemplo datos personales de afiliados, clientes, proveedores o

incluso colaboradores, pone en riesgo la misma continuidad de la organización.

7. Objetivos

7.1. General

Diseñar la seguridad con un enfoque de alta disponibilidad de la red LAN de una empresa cuya red de datos soporta los diferentes procesos, de tal forma que se pueda establecer una comunicación local estable, confiable y que incluya controles de seguridad adecuados para una óptima operación de la organización.

7.2. Específicos

- Realizar el inventario de información, software, hardware y servicios de la organización.
- Identificar los puntos de único fallo de la red existente.
- Diseñar y simular la infraestructura establecida para lograr una mejor disponibilidad aceptada por la organización.
- Elaborar y entregar a la organización un documento guía de recomendaciones con un diseño óptimo orientado a brindar una alta disponibilidad.

8. Requerimientos

8.1 Requerimientos funcionales

- Se debe diseñar una arquitectura de red segmentada de acuerdo con las áreas funcionales de la organización objeto de estudio.

8.2 Requerimientos no funcionales

- Se debe realizar un inventario de los equipos de conmutación de capa 2 existentes en la organización y su configuración, que permitan la elaboración de la arquitectura de red existente.
- El software de simulación de red que sea utilizado para documentar el diseño producto del desarrollo del proyecto, debe ser de carácter libre o gratuito para evitar generar costos no contemplados inicialmente por pagos de licenciamiento.

8.3 Requerimientos de restricción

Las plantillas de aseguramiento de los dispositivos de conmutación de capa 2 deben ser específicas a la marca de hardware que la organización pretende adquirir.

La organización objeto de estudio solicita, al máximo, la contención de los costos de implementación de la solución propuesta.

9. Metodología

Dado que se pretende trabajar de forma secuencial y cada una de las fases es requisito para la siguiente, se decide utilizar una metodología de desarrollo del proyecto en cascada (Waterfall), en donde se establecen unos tiempos para cada actividad y se controla su cumplimiento.

Esta metodología corresponde a un enfoque tradicional en la gestión y ejecución de proyectos y corresponde a una de las primeras metodologías usadas, sobre todo en proyectos de diseño de sistemas y manufactura.

Su estructuración es de tipo lineal, donde cada fase u objetivo del proyecto se desglosa en actividades en cada una es el requisito de la siguiente. De esta forma se logra estimar el tiempo total de cada fase a partir de los tiempos estimados para completar cada una de las actividades.

Las etapas a considerar en este proyecto corresponden a una inicial de levantamiento de activos de información de la organización objeto de estudio para su sede principal, las actividades de esta etapa deben considerar el inventario de activos tales como sistemas de información, servidores, enrutadores, Firewalls, Switches o cualquier otro dispositivo que haga parte de la red de datos y es considerado un paso necesario para iniciar el levantamiento de la topología existente y tiene una duración estimada de 4 semanas.

La siguiente etapa es la elaboración del diagrama de red actualizado en la que se identifican los activos de información previamente listados en el inventario, dicho diagrama debe

mostrar las conexiones y la ubicación de los dispositivos de red que puedan mostrar mediante un análisis posterior posibles problemáticas a nivel de conectividad y falencias que puedan ir en detrimento de la disponibilidad actual de la red de datos. Se estima una duración de 1 semana y es necesaria para continuar con la fase de análisis.

Para la fase de análisis se realizará una evaluación de las vulnerabilidades a nivel de disponibilidad y el posible impacto que tendría para la organización la falla de algún elemento identificado como crítico, es decir que su fallo ocasione una indisponibilidad del servicio de red que soporta los sistemas de información de la organización. El anterior análisis de impacto será cuantificado en pérdida de dinero asociado a la falta de operación de las áreas funcionales de la organización que son responsables de la venta y prestación de servicios. Dentro de esta misma fase de análisis se encuentra la identificación de aquellos puntos de único fallo o críticos que afectan de forma muy relevante la disponibilidad de la red al producirse una incidencia. Se estima la duración de esta fase en 2 semanas y es necesaria su finalización para continuar con la fase de diseño de la solución.

A continuación, tenemos la fase de diseño de la solución, en la que se pretende realizar los diagramas de una topología de red y configuración de equipos que aseguren una disponibilidad a un nivel que pueda considerarse como alta disponibilidad, aunado a lo anterior la selección de los equipos recomendados para realizar la implementación de la solución. Para lo anterior se estima un tiempo de 2 semanas y la conclusión de esta fase es necesaria para iniciar la etapa siguiente de simulación.

Para la última fase tenemos la simulación de la solución, que se debe realizar con un software capaz de emular las condiciones más parecidas a las que serían encontradas en la etapa productiva, que permita realizar pruebas que validen la falla de equipos y constatar la tolerancia a fallos y así asegurar el nivel de disponibilidad proyectado. Esta fase se estima con una duración de 1 semana.

10. Diagnóstico de la Infraestructura Existente

10.1 Inventario de Activos de Información

Como parte del levantamiento de información de la organización objeto de estudio, se hace necesario contar con un inventario de activos de información que incluya tanto equipos de red y servidores, que actualmente son responsabilidad, como propietarios de los activos, del área de Tecnología (TI).

Nombre	Servicio	Conf	Int	Disp	Valor	Descripción	Software	Ubicación	Cores	RAM GB	Disco GB
BD Intermedias	Sistema información ISOlucion y BD Intermedias	IR	A	1	ALTO	Servidor de las bases de datos intermedias de las interfaces, la aplicación y bases de datos iSolución.	SQL Server 2008 - IIS Windows 2008 Server	Cloud Privado	8	8	500
Febe	App Interfaces	IR	A	2	ALTO	Servidor que contiene la aplicación de interfaz contable Generic Transfer, para las interfaces de los sistemas con el ERP	Microsoft IIS - SQL Management - UnoEE Windows 2012 R2 Server	Cloud Privado	4	6	200
C-Erp	App Siesa	IR	A	1	ALTO	Servidor que contiene el sistema de información SIESA (ERP), este es el entorno aplicación de Siesa se encuentran todos los formatos, reportes y plantillas personalizadas por el proveedor.	UnoEE - HiTechPoolMgr - Windows 2012 R2 Server	Cloud Privado	4	6	200
Apolo	BD Sisu	IR	A	1	ALTO	Servidor productivo de la base de datos de la aplicación Web SISU.	MySQL (Maria DB 5.5) CentOS 6.5	Cloud Privado	4	6	360
Pegaso-BD	BD Oracle	IR	A	2	ALTO	Servidor que tiene la base de datos de pruebas del ERP en Oracle sobre ambiente Solaris en Cloud Privado	Oracle RedHat Enterprise	Cloud Privado	10	126	1500
C-docuware	BD Docuware	IR	A	2	ALTO	Servidor donde estará instalada la aplicación Web Docuware, para la gestión documental del archivo de solo consulta de la organización, esta debe quedar instalada	Microsoft SQL Server 2012 - IIS Windows 2012 R2 Server	Cloud Privado	2	6	600

						la versión web Docuware 6.10 más la base de datos.					
DomainDC	Dominio Principal	IR	A	1	ALTO	Servidor de dominio, en este se encuentran instalados los servicios de Active Directory y DNS primario.	Microsoft AD - DNS Windows 2012 R2 Server	Cloud Privado	2	3	100
C-Web	Portal WEB	IC	A	1	ALTO	Servidor productivo que contiene, la página web corporativa, el portal transaccional de créditos y la aplicación GLPI.	MariaDB -Apache 2 Ubuntu Server 18.04	Cloud Privado	4	4	400
C-novasoft	Novasoft - ESET	IR	A	2	ALTO	Servidor que tiene alojado el sistema de información de nómina (Novasoft), contiene la aplicación y base de datos de la aplicación mencionada, adicionalmente tiene una tarea programada con un script que realiza la copia de seguridad de la base de datos, aplicación y la base de datos del sistema biométrico de forma diaria. Se encuentra la consola del antivirus ESET.	Novasoft ESET Endpoint console Windows 2012 R2 Server	Cloud Privado	2	8	120
C-biome	Biométrico	IR	A	3	ALTO	Servidor que entrega el servicio de Biométrico. Se utilizó como base servidor de Newhotel que fue clonado	Software Biométrico Windows 2008 Server	Cloud Privado	2	4	160
Selene	Jurídica	IR	A	2	ALTO	Servidor que contiene la aplicación del CRM Odoo, fue utilizada por comunicaciones para el envío masivo de correos a usuarios y afiliados, GLPI comunicaciones y una demo de intranet con GRAV y mesa ayuda Zammad	Postgres, 10.0.38-MariaDB - Ubuntu Server 16.04.1	Cloud Privado	2	2	120
Copernico	Comfa-informix	IR	A	2	ALTO	Copia no funcional de la base de datos histórica de contabilidad. El motor de la base de datos no	Informix BD SUSE Linux	Cloud Privado	2	2	190

						inicia, pero se mantiene una copia de la base de datos.					
Gemini	App Sisu	IR	A	1	ALTO	Servidor productivo de la aplicación web SISU, específicamente sus fuentes, corre servidor apache.	Aplicación WEB SISU CentOS 6.5	Cloud Privado	6	16	600
Tauro	Tauro Impresión	IC	A	1	ALTO	Servidor de Impresión que tiene instalado el software controlador de impresoras multifuncionales PaperCut	PaperCut Windows 2012 R2 Server	Cloud Privado	4	8	500
CISCO SG100 - 16	Switch	IC	A	1	ALTO	Switch no administrable	N/A	Sede Principal	N/A	N/A	N/A
ARUBA 2930F - 48	Switch	IC	A	1	ALTO	Switch administrable	N/A	Sede Principal	N/A	N/A	N/A
HP 2920 – 24	Switch	IC	A	1	ALTO	Switch administrable	N/A	Sede Principal	N/A	N/A	N/A
HP E3800 – 48	Switch	IC	A	1	ALTO	Switch administrable	N/A	Sede Principal	N/A	N/A	N/A
H3C S5800 – 48	Switch	IC	A	1	ALTO	Switch administrable	N/A	Sede Principal	N/A	N/A	N/A
HP 1920 - 48	Switch	IC	A	1	ALTO	Switch administrable	N/A	Sede Principal	N/A	N/A	N/A
3COM 45106 – 24	Switch	IC	A	1	ALTO	Switch administrable	N/A	Sede Principal	N/A	N/A	N/A
Cisco SF-500 – 48	Switch	IC	A	1	ALTO	Switch administrable	N/A	Sede Principal	N/A	N/A	N/A
HP V1910 – 48	Switch	IC	A	1	ALTO	Switch administrable	N/A	Sede Principal	N/A	N/A	N/A
CISCO SF-500 – 48	Switch	IC	A	1	ALTO	Switch administrable	N/A	Sede Principal	N/A	N/A	N/A
HP E3800 – 24	Switch	IC	A	1	ALTO	Switch administrable	N/A	Sede Principal	N/A	N/A	N/A
HP 1920 – 16	Switch	IC	A	1	ALTO	Switch administrable	N/A	Sede Principal	N/A	N/A	N/A

Del anterior inventario se identifican los siguientes dispositivos de red de capa 2/capa 3 y sus capacidades.

Marca	**Marca**	**Capacidad**	**Cantidad**
CISCO	SG100 - 16	16 puertos 100/1000 Mbps	1
ARUBA	2930F - 48	48 puertos 100/1000 Mbps + 4	1

		puertos 1000 Mbps/10 Gbps, Administrable	
Hewlett Packard	HP 2920 – 24	24 puertos 10/100/1000 Mbps + 4 puertos SFP+ 1/10 Gbps, Administrable	1
Hewlett Packard	HP E3800 – 48	48 puertos 100/1000 Mbps + 4 puertos 1000 Mbps/10 Gbps, Administrable	1
H3C	H3C S5800 – 48	48 puertos 100/1000 Mbps + 4 puertos 1000 Mbps/10 Gbps, Administrable	1
Hewlett Packard	HP 1920 - 48	48 puertos 10/100/1000 Mbps + 4 puertos SFP 100/1000 Mbps, Administrable	1
3COM	3COM 45106 – 24	24 puertos 10/100/1000 Mbps, Administrable	1
CISCO	Cisco SF-500 – 48	48 puertos 10/100/1000 Mbps, Administrable	3
Hewlett Packard	HP V1910 – 48	48 puertos 10/100/1000 Mbps, Administrable	1
Hewlett Packard	HP E3800 – 24	24 puertos 10/100/1000 Mbps, Administrable + 2 puertos SFP+ 1/10 Gbps	1
Hewlett Packard	HP 1920 – 16	16 puertos 10/100/1000 Mbps + 4 puertos SFP 100/1000 Mbps, Administrable	1

10.2 Diagramas de Red Actual

De acuerdo con el anterior inventario de activos y el resto de información suministrada por la organización objeto de estudio, que involucra las conexiones existentes entre dispositivos se realizó el siguiente diagrama que ilustra la red existente en el edificio de la sede principal.

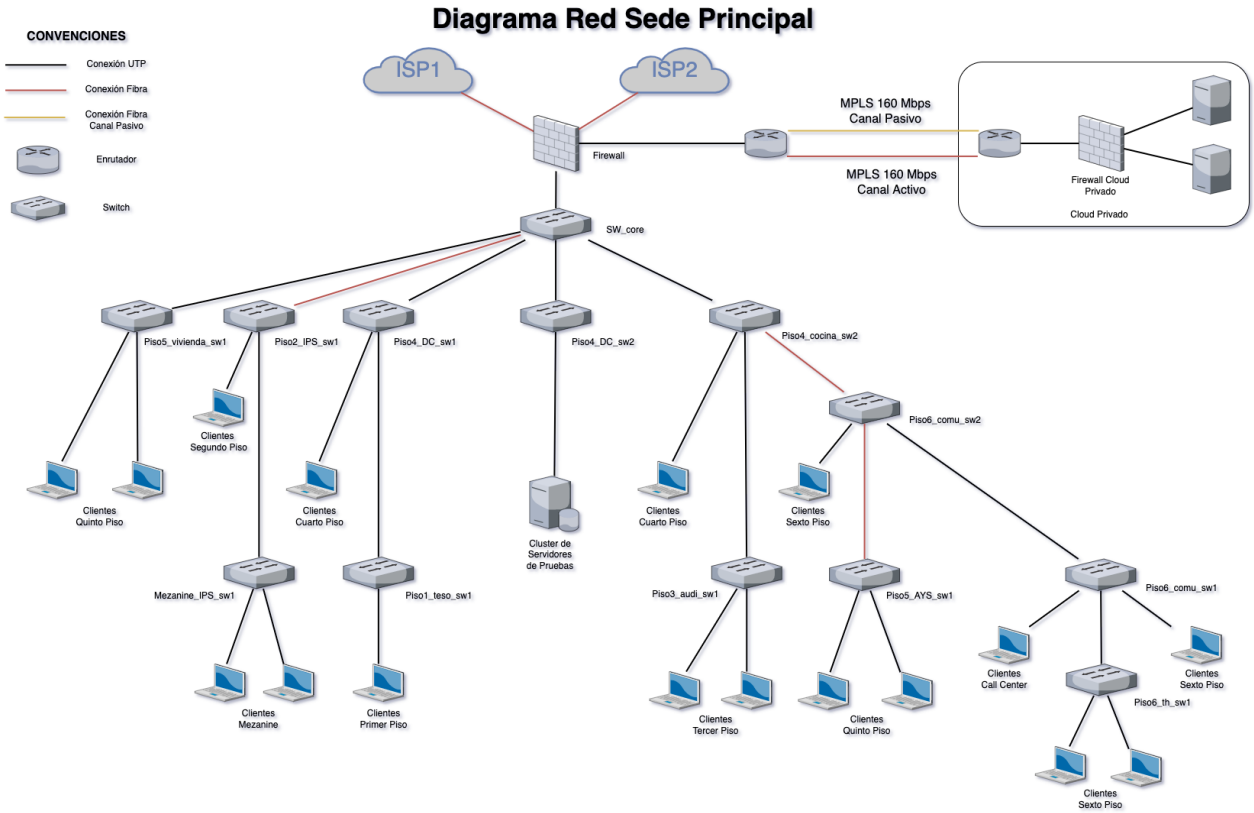

Ilustración 2 Diagrama de Red de la Sede Principal

La anterior arquitectura evidencia varios problemas entre otros la existencia un único Switch Core, que en caso de un fallo tiene el riesgo de ocasionar una falla masiva en la red de datos de la organización, lo que es llamado como punto de único fallo y es un riesgo asociado a la disponibilidad del servicio.

Asegurar niveles de disponibilidad adecuados representan en muchos casos la mitigación de riesgos de pérdidas de clientes por fallas de la red que impidan la atención oportuna, como también la imposibilidad de venta de servicios, a continuación, se presenta una evaluación cuantitativa de pérdidas operacionales ocasionadas por la falla de un Switch Core cuyo tiempo de reemplazo puede alcanzar las 96 horas (4 días). Para lo anterior se parte de los ingresos generados por la organización de forma general por venta de servicios, así:

INGRESOS POR VENTA DE SERVICIOS

Área/Proceso	Participación %	Ingresos $ Anual	Ingresos $ mensual	Ingreso Diario $	Ingreso Hora $
Ventas Agencia de Viajes	15,00%	$1.575.000.000,00	$131.250.000,00	$4.375.000,00	$182.291,67
Crédito Social	10,00%	$1.050.000.000,00	$87.500.000,00	$2.916.666,67	$121.527,78
Hoteles	40,00%	$4.200.000.000,00	$350.000.000,00	$11.666.666,67	$486.111,11
Ventas en línea	10,00%	$1.050.000.000,00	$87.500.000,00	$2.916.666,67	$121.527,78
Alquiler Salones de Eventos	5,00%	$525.000.000,00	$43.750.000,00	$1.458.333,33	$60.763,89
Educación	15,00%	$1.575.000.000,00	$131.250.000,00	$4.375.000,00	$182.291,67
Gimnasio	5,00%	$525.000.000,00	$43.750.000,00	$1.458.333,33	$60.763,89

La afectación de la red de datos impactaría directamente a las áreas de Agencia de Viajes, Ventas en línea y Crédito Social, así tendríamos las siguientes pérdidas operativas:

PÉRDIDAS POR INDISPONIBILIDAD DE RED DE DATOS

Área/Proceso	Participación %	Ingresos $ Anual	Ingresos $ mensual	Ingreso Diario $	Ingreso Hora $
Ventas Agencia de Viajes	15,00%	$ 6.075.000.000,00	$ 506.250.000,00	$ 16.875.000,00	$ 703.125,00
Crédito Social	10,00%	$ 4.050.000.000,00	$ 337.500.000,00	$ 11.250.000,00	$ 468.750,00
Ventas en línea	10,00%	$ 4.050.000.000,00	$ 337.500.000,00	$ 11.250.000,00	$ 468.750,00
				TOTAL	**$ 1.640.625,00**

Pérdidas por horas	96	**$**	**157.500.000**

Las pérdidas se estiman en $157’500.000 por ventas sin contar con pérdidas de imagen, reputación de la marca y lealtad de clientes.

Así mismo la organización ha venido presentando caídas y presentando intermitencias que generan indisponibilidad de sistemas de información de forma eventual y esporádica, a continuación, se muestran capturas de monitoreo del Switch Core de la sede, donde se evidencia los problemas manifestados por la organización.

Ilustración 3 Monitoreo 1 Switch Core Icinga

Ilustración 4 Monitoreo 2 Switch Core Icinga

De acuerdo con las estimaciones realizadas a través del servicio de monitoreo tenemos la siguiente tabla con las indisponibilidades redondeadas a minutos para el último mes en las fechas indicadas.

Fecha	Minutos
22/11/22	15
19/11/22	7
17/11/22	1

13/11/22	1
08/11/22	1
02/11/22	1
28/10/22	1
25/10/22	1
TOTAL	28

A partir de lo anterior se puede extrapolar que, de un total de 28 minutos por 12 meses en 336 minutos, es decir 5 horas y 36 minutos, que nos entrega un nivel de disponibilidad del 99.9%.

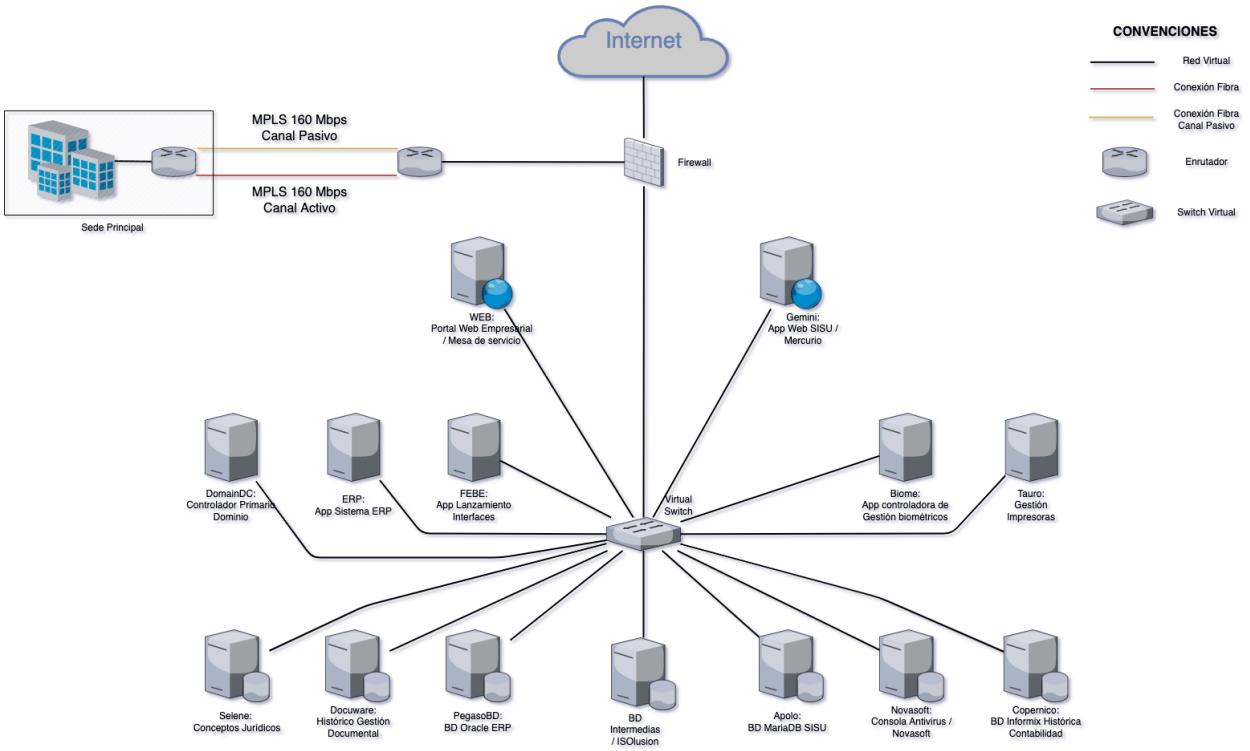

Ilustración 5 Diagrama de Red de Infraestructura de Servidores en modalidad de Cloud Privado

La infraestructura de servidores se encuentra contratada por la compañía con un tercero que entrega un servicio en modalidad de Cloud privado, que utiliza una tecnología de virtualización y de la cual no se tienen detalles técnicos debido a la reserva que mantiene el

tercero, así que, se muestra la arquitectura lógica de red para dicho Cloud.

10.3 Identificación de Puntos de Único Fallo

Haciendo uso de los anteriores diagramas como herramienta de análisis se busca aquellos dispositivos que, ante el riesgo de una eventual falla, puedan llegar a ocasionar una masiva indisponibilidad del servicio de red de datos, con un alto impacto para la organización al no permitir la prestación normal de servicios a usuarios, clientes y afiliados. Dado que la organización objeto del presente estudio no considera los dispositivos de Capa 2 y 3 "Switches" en nivel de Acceso como críticos por no considerarse como puntos de único fallo, no se sugiere su implementación en modalidad de alta disponibilidad (HA).

De acuerdo con lo anterior se muestran a continuación en la siguiente figura, indicados en círculos de color rojo, aquellos dispositivos que se consideran puntos de único fallo.

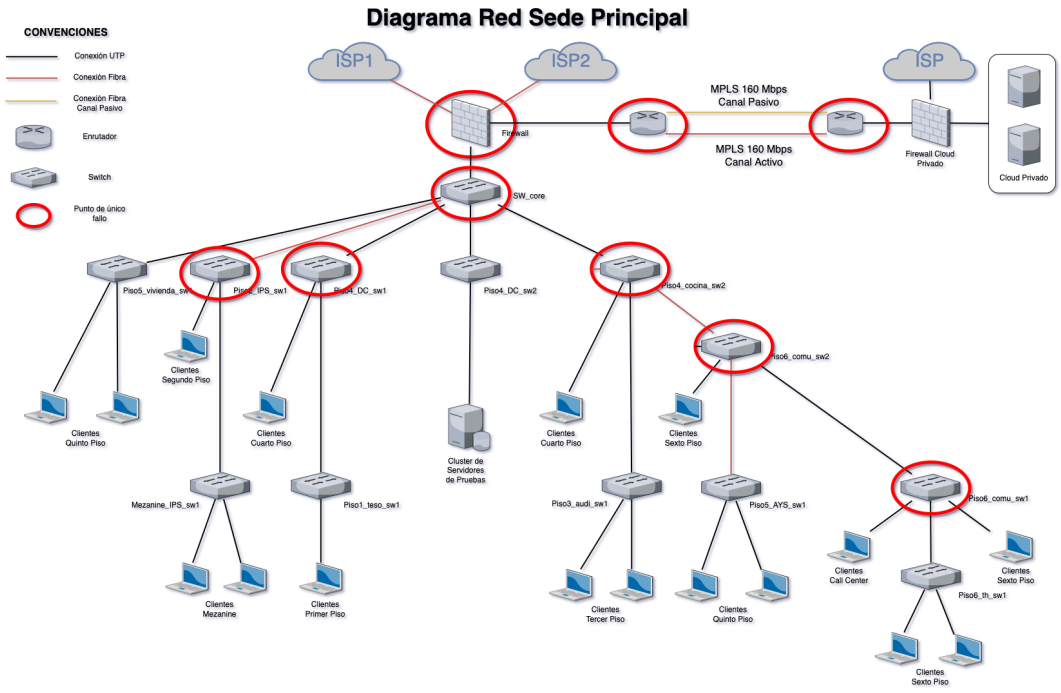

Ilustración 6 Diagrama de Red de Puntos de Único Fallo

En total se encuentran 9 puntos de único fallo, entre dispositivos Cortafuegos, Switches de nivel de distribución y enrutadores hacia Cloud privado. Ahora se procede a identificar los mismos en la infraestructura del Cloud privado contratado por la organización.

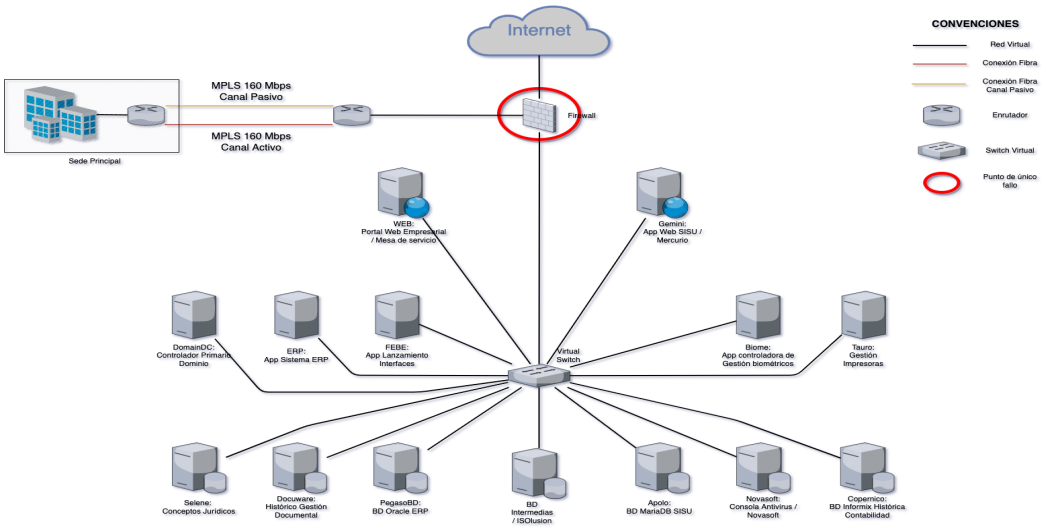

Ilustración 7 Diagrama de Red de Puntos de Único Fallo Servidores Cloud Privado

Del anterior se identifica un solo punto de único fallo localizado en el Firewall. Aquí es importante mencionar que no se consideran los puntos en dispositivos enrutadores debido a que fueron identificados en el diagrama de la red en la sede principal, tampoco se considera el Switch Core, en la medida que se trata de un Switch Virtual que de acuerdo a cláusulas contractuales que se tienen con el proveedor de servicios, estos están montados en una infraestructura en modalidad de alta disponibilidad (HA), sujeta a unos acuerdos de nivel de servicios (SLA) de cumplimiento del 99.9%.

11. Diseño de Red en Alta Disponibilidad

11.1 Diagramas de Red Propuesta en Alta Disponibilidad

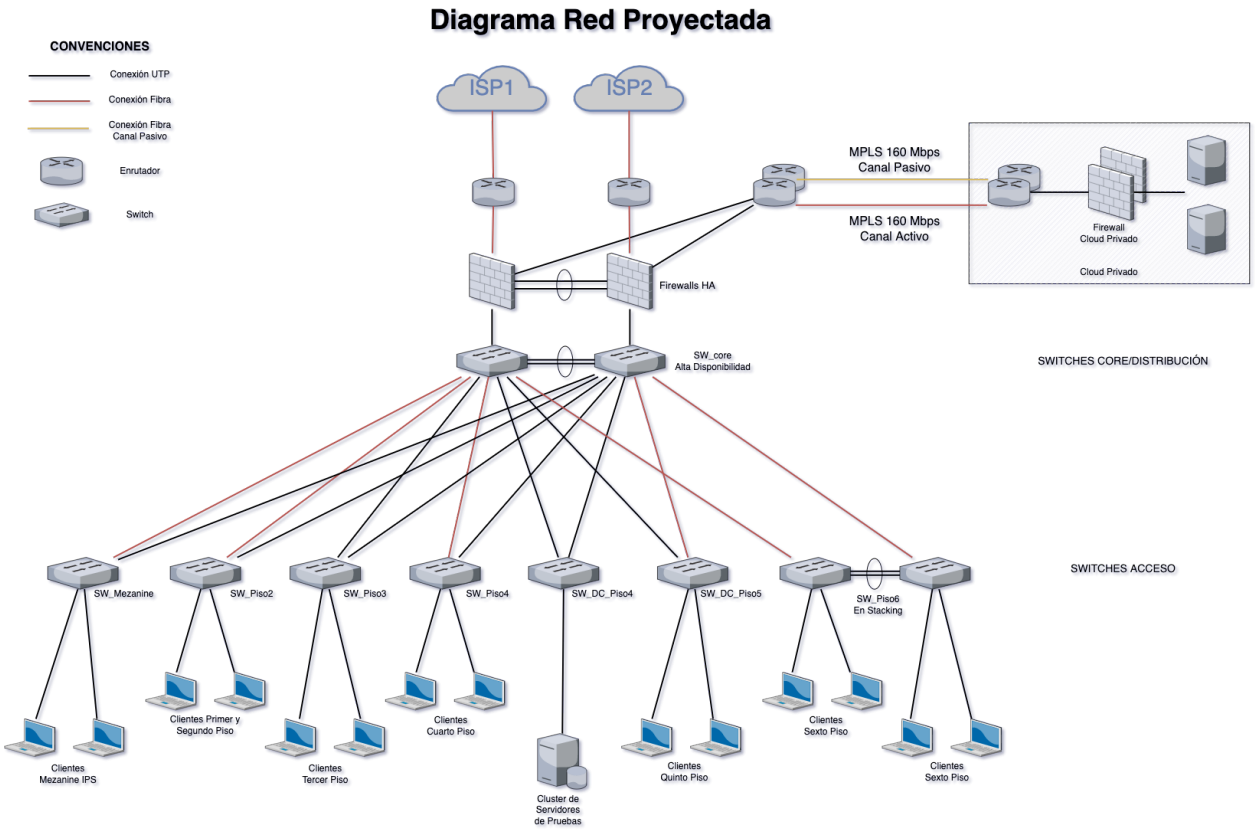

Ilustración 8 Diagrama de Red Sede Principal Propuesta

Basados en la infraestructura encontrada se propone un diseño que contempla 2 equipos Firewall configurados en modalidad de alta disponibilidad (HA) cada uno con recomendación de fuente redundante, lo anterior tiene como objetivo es que ante la eventual falla de la fuente de poder el equipo entrega la respectiva alerta, pero en ningún momento significa su salida de operación. En casos más extremos en donde falle totalmente uno de los dos equipos Firewall y al estar configurados en alta disponibilidad tampoco sería causal de falla masiva de la red de datos, esto permite dar el suficiente tiempo para que la organización active su plan de reemplazo y sustitución de equipos y de esta forma realizar una sustitución de forma transparente para el servicio prestado.

De igual forma se diseñó el establecimiento de un Switch Core en la misma modalidad de alta disponibilidad (HA), a través de una configuración en forma de apilamiento "Stacking" de los dos dispositivos, se busca evitar la falla masiva de la red al presentarse un daño en alguno de los dispositivos. Este tipo de configuración, a diferencia de una en cascada, es efectiva dado que cada uno de los Switches Core cuenta con una conexión física independiente con los Switches de acceso, aun cuando por limitaciones presupuestales, una en fibra óptica y otra en cableado UTP la conectividad no se pierde en ningún momento por falla de dispositivo.

Aun cuando no es un objetivo central de este trabajo, se recomienda encarecidamente la realización de una segmentación de la red, que permita aislar equipos de áreas críticas de la organización y en dado caso servir como contención ante distintos tipos de ataques como Ransomware o intrusiones, que mitigue riesgos a la confidencialidad e integridad de la información. Lo anterior utilizando un diseño de "subnetting" que contemple las áreas funcionales de la organización, para lo cual se adjunta al presente documento el Anexo 2, con las siguientes subredes consideradas:

ID	ÁREA FUNCIONAL	VLAN_ID	Host Totales
1	IMPRESORAS	22	100
2	APORTES_SUBSIDIOS	23	20
3	MEZANINE	24	20
4	CONTABILIDAD	25	15
5	COMPRAS_ADMINISTRATIVO	26	15
6	FIDELIZACION	27	10
7	TECNOLOGIA	28	10
8	IPS	29	10
9	RRHH	30	10
10	DIRECCIÓN	31	5
11	TESORERÍA	32	5
12	ARCHIVO	33	5
13	COMUNICACIONES	34	5
14	JURÍDICA	35	5
15	CONTROL_INTERNO	36	5
16	AGENCIA_TURISMO	37	5
17	CALL_CENTER	38	5
18	TARJETAS	39	5

19	ZONA_RECREATIVA	40	5

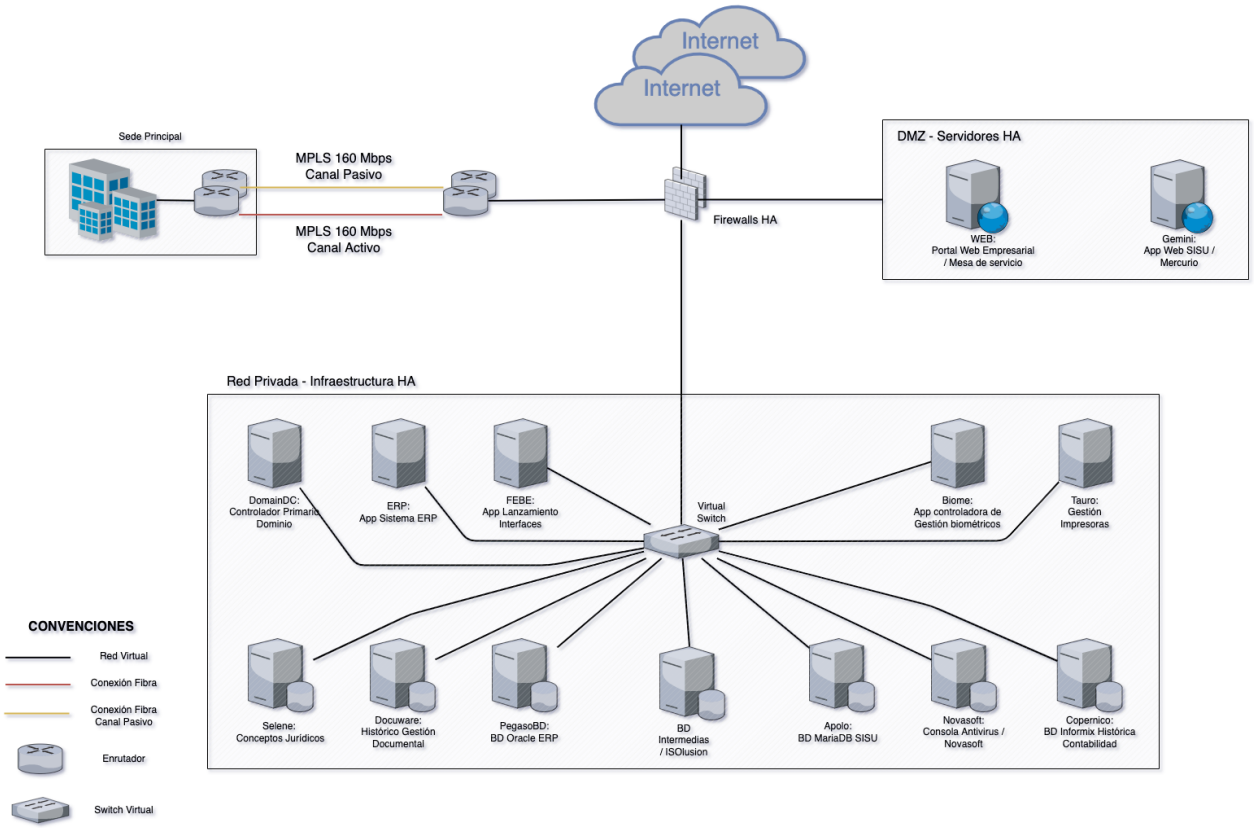

Ilustración 9 Diagrama de Red Infraestructura de Servidores Cloud Privado Propuesta

Para el "cloud" privado se recomienda, a través del diseño anterior, la contratación de un sistema de Firewall con un ANS igual o superior al del resto de la infraestructura Cloud contratada.

También se contempla la creación de una zona DMZ para aquellos servidores que se encuentran expuestos en Internet, en este caso los servidores WEB y GEMINI, de esta forma se aíslan de los servidores de aplicaciones cliente servidor, bases de datos y aplicaciones Web expuestos en modo local.

La conectividad a través de la conexión MPLS se diseña también con equipos enrutadores trabajando igualmente configurados en alta disponibilidad, permitiendo de esta manera la tolerancia a fallos de hardware en algún dispositivo.

11.2 Selección de Equipos de Red

De acuerdo con una restricción realizada por la organización objeto del presente trabajo referente a la disminución de costos de implementación, se desarrolla un análisis de costo beneficio, en la que los dispositivos de la marca (vendor) de Switching seleccionada para el despliegue de la solución es Extreme Networks, basados en lo siguiente:

Se contemplan únicamente marcas líderes en el mercado, por lo que se consultó la información que hay al respecto y publicada por la firma independiente Gartner para el análisis de empresas fabricantes de la industria de redes, en resumen se muestra el resultado obtenido a través de una gráfica denominada "Cuadrante Mágico de Gartner", en las que se clasifican empresas como de nicho de mercado, visionarias, retadoras y líderes, siendo la última la mejor clasificación, es decir la encontrada en la parte superior derecha.

Ilustración 10 Cuadrante mágico de actores del mercado. Tomado de Gartner© 2022

Una importante premisa para la organización objeto de estudio, es el ahorro económico

que se pueda hacer sin hacer mayores sacrificios a nivel de disponibilidad de la infraestructura, es así que es necesario tener en cuenta que los dispositivos seleccionados cuenten con la capacidad de agruparse en "Stacking", también con interfaces troncales para comunicación entre Switches de distribución y de acceso a velocidades de transmisión de 1/10 Gbps, con gamas de opción de 24 y 48 puertos de acuerdo a la cantidad de usuarios por piso en la sede principal, fuente redundante, soporte PoE para energizar aparatos de telefonía IP con que cuentan actualmente los colaboradores de la empresa y capacidad de "link aggregation" para la suma de anchos de banda de interfaces.

Dentro de cualquier proyecto de este tipo es absolutamente necesario contar con soporte técnico y garantía por parte de los canales de distribución con que cuentan los fabricantes, para este efecto la empresa objeto de análisis cuenta con 3 proveedores, aprobados jurídica y técnicamente, que ofertaron dispositivos que cumplen las capacidades anteriores, en marcas Cisco y Extreme Networks.

Switch Model	**Marca**	**Aggregated Switch Bandwidth***	**Frame Forwarding Rate***	**Power Redundant**	**Stacking**	**PoE**	**Precio USD$**
C9200L-24P-4X	Cisco	128 Gbps	155 Mpps	X	80 Gbps	30W por Puerto	3,040
C9200L-48T-4X	Cisco	176 Gbps	190 Mpps	X	80 Gbps	30W por Puerto	3,741
X440-G2-24p-10GE4	Extreme Networks	128 Gbps	95.2 Mpps	✓	40 Gbps por Unidad	30W por Puerto	1,456
X440-G2-48p-10GE4	Extreme Networks	176 Gbps	130.9 Mpps	✓	40 Gbps por Unidad	30W por Puerto	2,304

Se realizó validación de cumplimiento de requisitos para ambas marcas y se encontró a nivel económico una diferencia de costos que, por el volumen de equipos a comprar, representa

una propuesta mucho más atractiva para la empresa los dispositivos marca Extreme Networks.

A nivel de equipo Firewall, este dispositivo de referencia Fortigate 200F es entregado por el proveedor de servicios de Internet (ISP) en modalidad de servicio junto con su administración y de acuerdo con la organización el proveedor presenta excelente calidad de servicio, para constatar lo anterior se toman muestras de consumo de recursos en horarios pico y se observó la siguiente estadística típica.

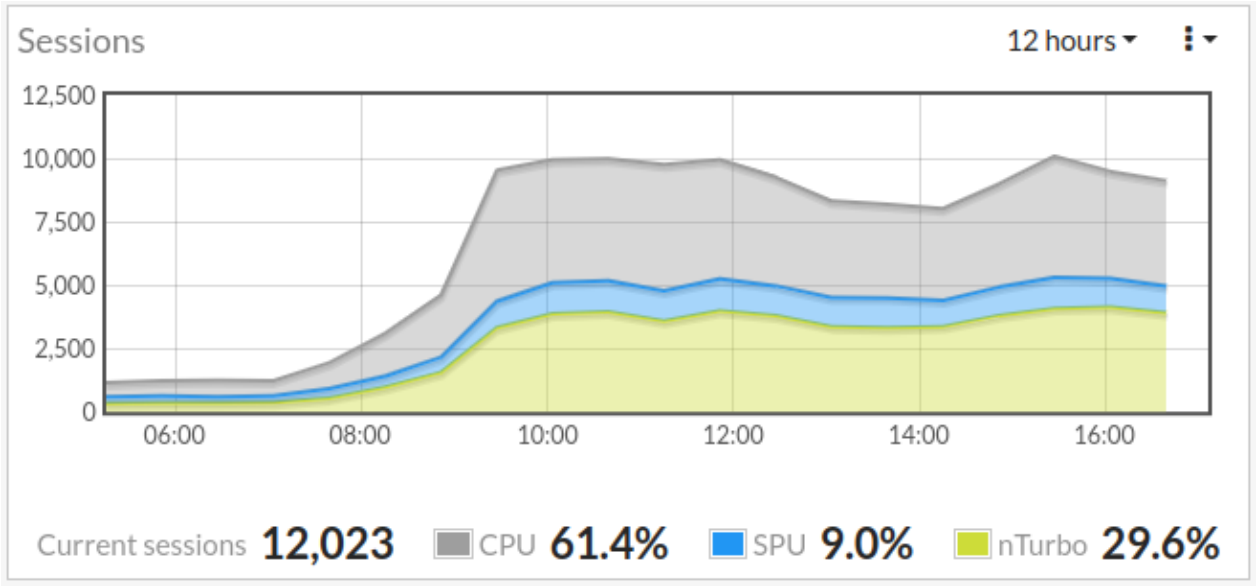

Ilustración 11 Consumos típicos de recurso de procesamiento de Firewall

Los anteriores consumos muestran un nivel aceptable de consumo, por lo que es posible sugerir el tipo de implementación que se muestra en la ilustración 6, un diseño en alta disponibilidad pasivo activo utilizando el protocolo FGCP para configuración del modo HA. El protocolo FGCP es de tipo propietario y es utilizado por la empresa Fortinet para generar este tipo de configuraciones de 2 o más equipos en modalidad clúster. La selección de la marca Fortinet corresponde a una decisión de la organización basados en el desempeño adecuado que ha presentado el proveedor de servicios, quien es a su vez es un canal de distribución de dicha marca y de acuerdo con lo expresado por la organización no se tiene intención de realizar cambio de proveedor.

Con las anteriores consideraciones en cuanto a redundancia de dispositivos, redundancia de fuentes de poder, diseño de red y conectividad, consideradas como estrategias de Alta Disponibilidad HA, se está alcanzando una disponibilidad para la organización de 99.95%.

11.2.1 Descripción de Especificaciones Técnicas de Switches

11.2.1.1 Performance and Scaling

Switch Model	Maximum 10/100/1000 Base-T Ports	Maximum Active 1Gb SFP Ports	Maximum 10Gb SFP+ Ports	Aggregated Switch Bandwidth	Frame Forwarding Rate
X440-G2-24p-10GE4	24	8 (4 + 4 Combo)	4 via license	128 GBPS	95.2 MPPS
X440-G2-48p-10GE4	48	8 (2 + 6 Combo)	4 via license	176 GBPS	130.9 MPPS

11.2.1.2 External Ports/Slots

Switch Hardware	Ports
X440-G2-24p-10GE4	• 24 x 10/100/1000BASE-T PoE-Plus • 4 x 1GBASE-X SFP (unpopulated) combo ports • 4 x 1GBASE-X SFP (unpopulated rear-panel ports) upgradeable to 10Gb Ethernet via licensing • 1 x Serial (console port RJ-45) with RTS/CTS modem control • 1 x 10/100/1000BASE-T out-of-band management port • 2x7 RPS port

X440-G2-48p-10GE4	• 48 x 10/100/1000BASE-T PoE-Plus • 4 x 1GBASE-X SFP (unpopulated) combo ports • 2 x 1GbE copper combo ports upgradable to 10GbE on rear-panel • 4 x 1GBASE-X SFP (unpopulated rear-panel ports) upgradeable to 10Gb Ethernet via licensing • 1 x Serial (console port RJ-45) with RTS/CTS modem control • 1 x 10/100/1000BASE-T out-of-band management port • 2x9 RPS port

11.2.1.3 Stacking Ports

X440-G2 Switches	Stack Ports #	Physical Uplink Port # On Chassis
48 Port Models	1	49 (Rear Panel, Dedicated SFP+ Port)
	2	50 (Rear Panel, Dedicated SFP+ Port)
24 Port Models	1	27 (Rear Panel)
	2	28 (Rear Panel)

11.2.1.4 PoE Power Budget

Switch Model	Power Supply Input Socket	Redundant Power Supply Input Socket
X440-G2-24p-10GE4	380W	380 W – Redundant Power Only
X440-G2-48p-10GE4	740W	1440 W – Additive Power 740 W – Redundant Power

11.3 Simulación de Red Propuesta

De acuerdo con los diagramas de red propuestos y equipos seleccionados se desarrolla la respectiva simulación, utilizando el programa GNS3 en favor de otros programas como por ejemplo Packet Tracer, por razones explicadas más adelante. Es importante anotar que no se realiza simulación de la red de servidores, en razón a que el Cloud privado no se encuentra dentro del alcance de este proyecto, por ser responsabilidad de un tercero que debe cumplir cláusulas contractuales que contemplan la entrega de un servicio con base en los requerimientos que solicite el cliente.

Se realizó la selección del programa GNS3 en vez de otras alternativas, en razón a que con este aplicativo es posible usar las versiones de iOS (firmware) originales del fabricante y de esta forma poder llegar a simular condiciones más reales de la infraestructura que se pretende desplegar en ambiente productivo.

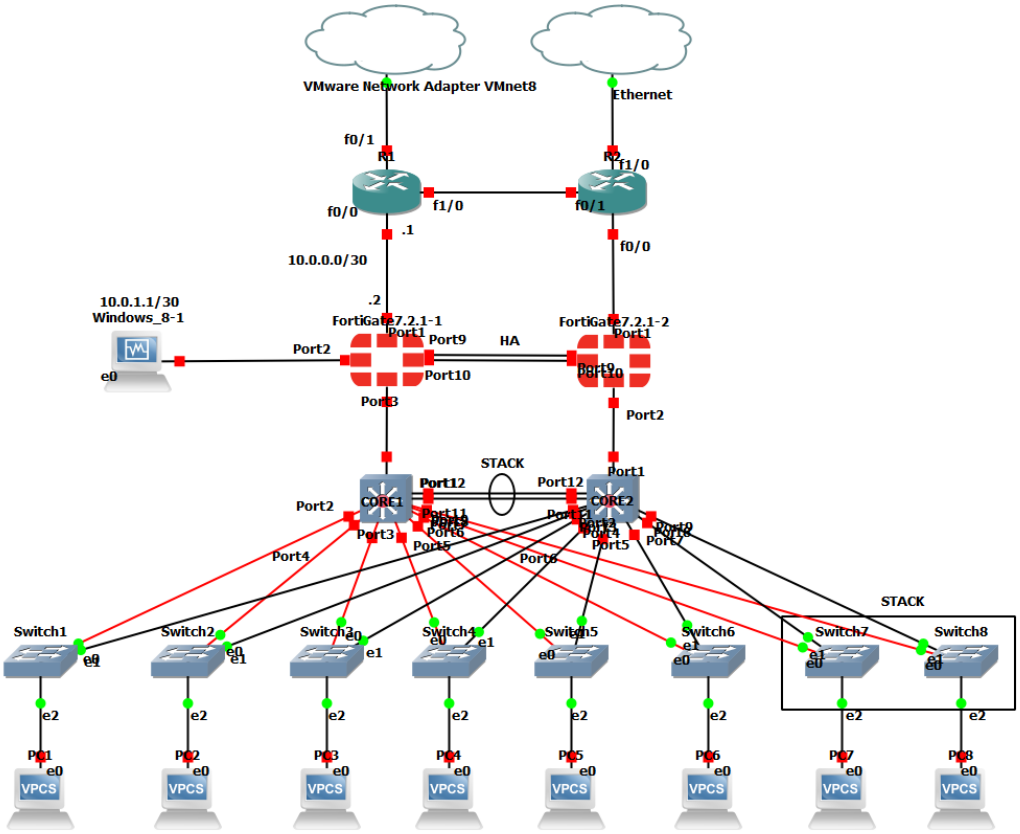

Ilustración 12 Diagrama de Red Sede Principal Propuesta Simulación

12. Resultados

Se encontró, de acuerdo con la simulación, una capacidad de la nueva red de una tolerancia a fallos de dispositivos principales como Switch Core, Firewalls y cableado que aseguran el cumplimiento de niveles de disponibilidad apropiados para la organización.

Se obtuvieron diseños y diagramas actualizados tanto de la red local existente como de la proyectada, así como una simulación muy cercana a una implementación real capaz de servidor como herramienta de análisis para realizar modificaciones de configuración que además facilita el nivel de entendimiento de la infraestructura para los administradores y material de entrenamiento para nuevos colaboradores del área de TI de la organización.

Se establecieron de acuerdo con la marca de dispositivos Switches seleccionada por la organización, plantillas de aseguramiento que facilitan su configuración inicial y despliegue en producción, que además robustece la seguridad de la red.

Se realizan pruebas de conectividad y de HA de la red simulada, en donde se apaga uno de los Switches CORE o Distribución quedando el otro activo y sin generar pérdida en la disponibilidad del servicio:

Primera prueba se realiza el apagado del Switch CORE2 y se evidencia continuidad de conectividad entre los PC 1, 5, 8 y el Switch CORE1 como lo evidenciamos en las siguientes ilustraciones:

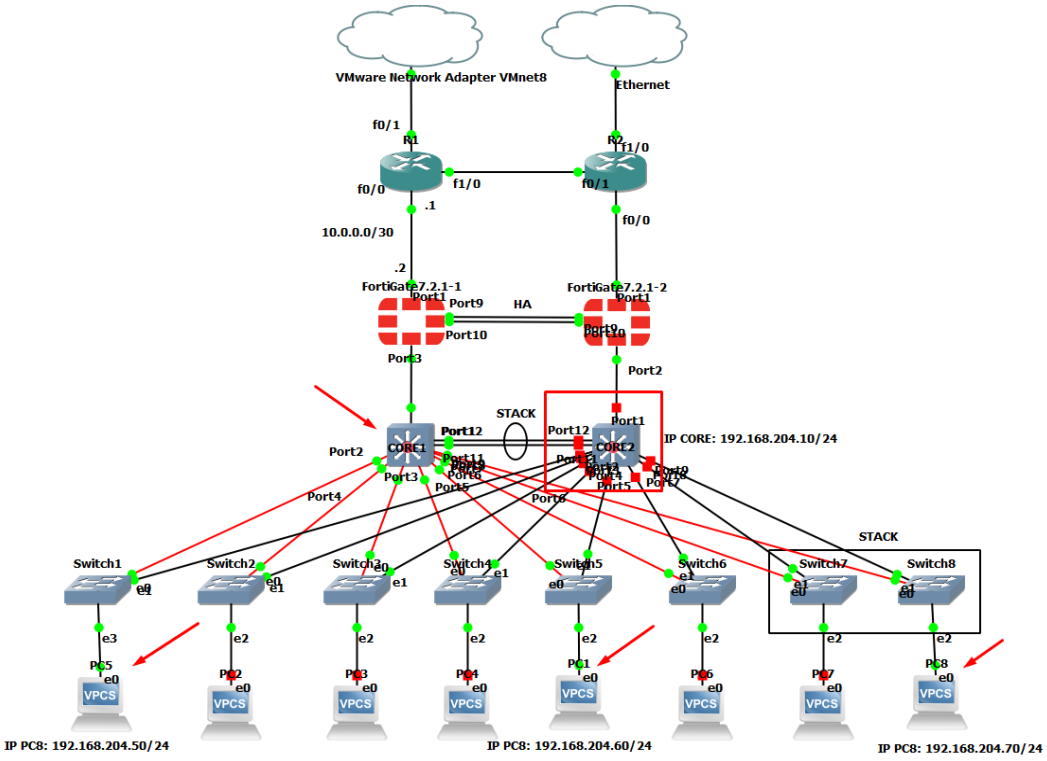

Ilustración 13 Apagado Switch CORE2

```
PC1> ping 192.168.204.10

84 bytes from 192.168.204.10 icmp_seq=1 ttl=64 time=1.023 ms
84 bytes from 192.168.204.10 icmp_seq=2 ttl=64 time=2.067 ms
84 bytes from 192.168.204.10 icmp_seq=3 ttl=64 time=1.010 ms
84 bytes from 192.168.204.10 icmp_seq=4 ttl=64 time=1.056 ms
84 bytes from 192.168.204.10 icmp_seq=5 ttl=64 time=1.030 ms

PC1> ping 192.168.204.60

84 bytes from 192.168.204.60 icmp_seq=1 ttl=64 time=2.020 ms
84 bytes from 192.168.204.60 icmp_seq=2 ttl=64 time=2.185 ms
84 bytes from 192.168.204.60 icmp_seq=3 ttl=64 time=1.682 ms
84 bytes from 192.168.204.60 icmp_seq=4 ttl=64 time=1.974 ms
84 bytes from 192.168.204.60 icmp_seq=5 ttl=64 time=1.843 ms

PC1> ping 192.168.204.70

84 bytes from 192.168.204.70 icmp_seq=1 ttl=64 time=1.769 ms
84 bytes from 192.168.204.70 icmp_seq=2 ttl=64 time=1.870 ms
84 bytes from 192.168.204.70 icmp_seq=3 ttl=64 time=2.704 ms
84 bytes from 192.168.204.70 icmp_seq=4 ttl=64 time=1.494 ms
84 bytes from 192.168.204.70 icmp_seq=5 ttl=64 time=1.737 ms

PC1> show ip

NAME        : PC1[1]
IP/MASK     : 192.168.204.50/24
GATEWAY     : 192.168.204.10
DNS         :
MAC         : 00:50:79:66:68:00
LPORT       : 20123
RHOST:PORT  : 127.0.0.1:20124
MTU         : 1500

PC1>
```

```
PC5> show ip

NAME        : PC5[1]
IP/MASK     : 192.168.204.60/24
GATEWAY     : 192.168.204.10
DNS         :
MAC         : 00:50:79:66:68:01
LPORT       : 20129
RHOST:PORT  : 127.0.0.1:20130
MTU         : 1500

PC5>
PC5> ping 192.168.204.10

84 bytes from 192.168.204.10 icmp_seq=1 ttl=64 time=0.835 ms
84 bytes from 192.168.204.10 icmp_seq=2 ttl=64 time=1.130 ms
84 bytes from 192.168.204.10 icmp_seq=3 ttl=64 time=0.914 ms
84 bytes from 192.168.204.10 icmp_seq=4 ttl=64 time=1.264 ms
84 bytes from 192.168.204.10 icmp_seq=5 ttl=64 time=1.483 ms

PC5> ping 192.168.204.50

84 bytes from 192.168.204.50 icmp_seq=1 ttl=64 time=4.689 ms
84 bytes from 192.168.204.50 icmp_seq=2 ttl=64 time=2.024 ms
84 bytes from 192.168.204.50 icmp_seq=3 ttl=64 time=2.757 ms
84 bytes from 192.168.204.50 icmp_seq=4 ttl=64 time=2.262 ms
84 bytes from 192.168.204.50 icmp_seq=5 ttl=64 time=2.134 ms

PC5> ping 192.168.204.70

84 bytes from 192.168.204.70 icmp_seq=1 ttl=64 time=1.437 ms
84 bytes from 192.168.204.70 icmp_seq=2 ttl=64 time=1.980 ms
84 bytes from 192.168.204.70 icmp_seq=3 ttl=64 time=1.681 ms
84 bytes from 192.168.204.70 icmp_seq=4 ttl=64 time=2.077 ms
84 bytes from 192.168.204.70 icmp_seq=5 ttl=64 time=2.632 ms

PC5>
```

```
PC8> show ip

NAME        : PC8[1]
IP/MASK     : 192.168.204.70/24
GATEWAY     : 192.168.204.10
DNS         :
MAC         : 00:50:79:66:68:02
LPORT       : 20127
RHOST:PORT  : 127.0.0.1:20128
MTU         : 1500

PC8>
PC8> ping 192.168.204.10

84 bytes from 192.168.204.10 icmp_seq=1 ttl=64 time=0.915 ms
84 bytes from 192.168.204.10 icmp_seq=2 ttl=64 time=1.185 ms
84 bytes from 192.168.204.10 icmp_seq=3 ttl=64 time=1.118 ms
84 bytes from 192.168.204.10 icmp_seq=4 ttl=64 time=1.243 ms
84 bytes from 192.168.204.10 icmp_seq=5 ttl=64 time=1.061 ms

PC8> ping 192.168.204.50

84 bytes from 192.168.204.50 icmp_seq=1 ttl=64 time=1.569 ms
84 bytes from 192.168.204.50 icmp_seq=2 ttl=64 time=3.049 ms
84 bytes from 192.168.204.50 icmp_seq=3 ttl=64 time=1.728 ms
84 bytes from 192.168.204.50 icmp_seq=4 ttl=64 time=1.675 ms
84 bytes from 192.168.204.50 icmp_seq=5 ttl=64 time=1.628 ms

PC8> ping 192.168.204.60

84 bytes from 192.168.204.60 icmp_seq=1 ttl=64 time=2.115 ms
84 bytes from 192.168.204.60 icmp_seq=2 ttl=64 time=1.889 ms
84 bytes from 192.168.204.60 icmp_seq=3 ttl=64 time=2.983 ms
84 bytes from 192.168.204.60 icmp_seq=4 ttl=64 time=1.686 ms
84 bytes from 192.168.204.60 icmp_seq=5 ttl=64 time=1.656 ms
```

Ilustración 14 Pruebas de Conectividad Apagado Switch CORE2

Segunda prueba se realiza el apagado del Switch CORE1 y se evidencia continuidad de conectividad entre los PC 1, 5, 8 y el Switch CORE2 como lo evidenciamos en las siguientes ilustraciones:

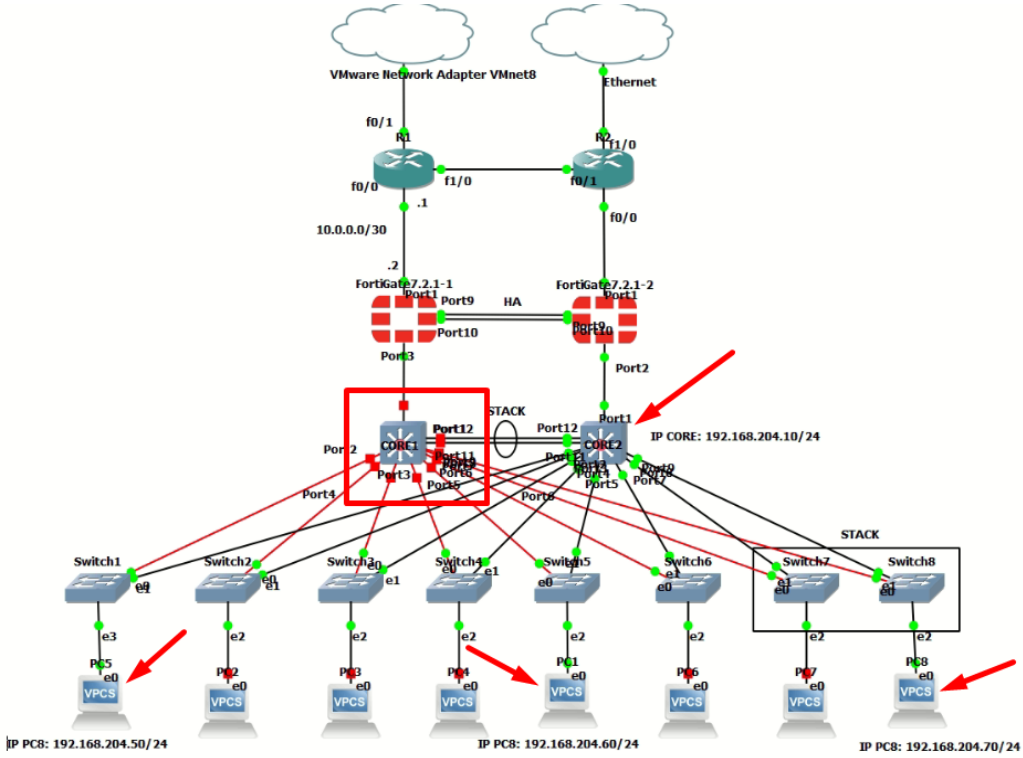

Ilustración 15 Apagado Switch CORE1

```
PC1> ping 192.168.204.10

84 bytes from 192.168.204.10 icmp_seq=1 ttl=64 time=1.023 ms
84 bytes from 192.168.204.10 icmp_seq=2 ttl=64 time=2.067 ms
84 bytes from 192.168.204.10 icmp_seq=3 ttl=64 time=1.010 ms
84 bytes from 192.168.204.10 icmp_seq=4 ttl=64 time=1.056 ms
84 bytes from 192.168.204.10 icmp_seq=5 ttl=64 time=1.030 ms

PC1> ping 192.168.204.60

84 bytes from 192.168.204.60 icmp_seq=1 ttl=64 time=2.020 ms
84 bytes from 192.168.204.60 icmp_seq=2 ttl=64 time=2.185 ms
84 bytes from 192.168.204.60 icmp_seq=3 ttl=64 time=1.682 ms
84 bytes from 192.168.204.60 icmp_seq=4 ttl=64 time=1.974 ms
84 bytes from 192.168.204.60 icmp_seq=5 ttl=64 time=1.843 ms

PC1> ping 192.168.204.70

84 bytes from 192.168.204.70 icmp_seq=1 ttl=64 time=1.769 ms
84 bytes from 192.168.204.70 icmp_seq=2 ttl=64 time=1.870 ms
84 bytes from 192.168.204.70 icmp_seq=3 ttl=64 time=2.704 ms
84 bytes from 192.168.204.70 icmp_seq=4 ttl=64 time=1.494 ms
84 bytes from 192.168.204.70 icmp_seq=5 ttl=64 time=1.737 ms
```

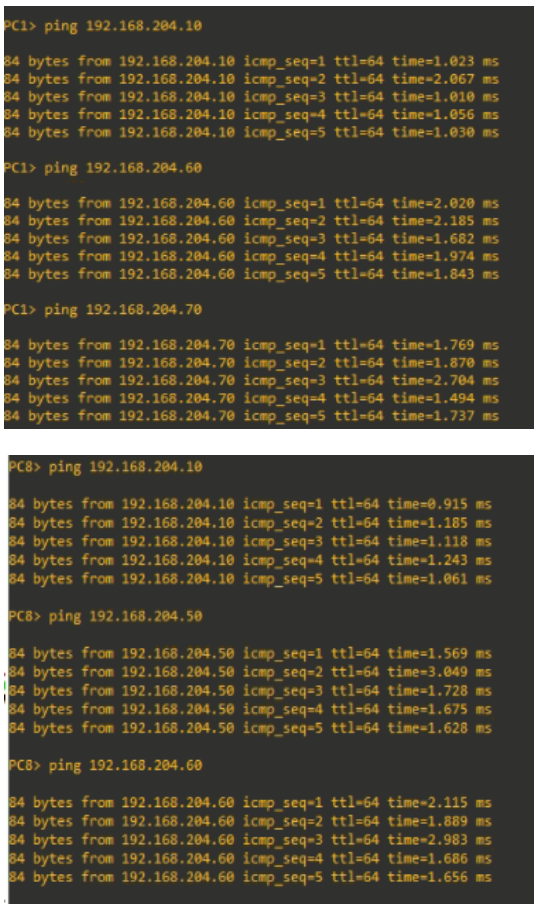

Ilustración 16 Pruebas de Conectividad Apagado Switch CORE1

13. Discusión

Dado que la infraestructura de servidores es muy importante para asegurar la continuidad del negocio de la organización en razón a que todos los sistemas informáticos que hace parte de la operación son soportados por estos servidores, y estos se encuentran contratados con un proveedor de servicios que adicionalmente entrega un canal MPLS de comunicación con la sede principal, por lo anterior se recomienda ajustar los acuerdos de nivel de servicio ANS en un porcentaje superior al actualmente contratado, es decir, superior al 99.9% que se sugiere en el 99.95%.

Otro hecho notable es encontrar que el canal pasivo de contingencia de la conexión MPLS es contratado con el mismo proveedor de servicios, lo que en primera instancia lo hace vulnerable a fallos por daños físicos del medio de transmisión, que en este caso es la fibra óptica tendida por el mismo proveedor, por lo anterior sería recomendable contratar este canal de contingencia con otro proveedor que demuestre independencia de infraestructura de red física.

Durante el desarrollo del presente trabajo fue evidente que la organización hace uso de 2 dispositivos Access Point para entrega de servicio de red inalámbrica (WiFi) para sus colaboradores e invitados, pero estos escapan al alcance de este documento, mas sin embargo se debería realizar un estudio posterior que involucre la seguridad de este servicio, tanto en disponibilidad como integridad y confidencialidad.

Como futuros trabajos sería recomendable la realización de un análisis de vulnerabilidades en etapa productiva de la solución propuesta, que permita dar un mayor alcance a nivel de confidencialidad e integridad de la red de datos en la sede principal de la organización.

14. Conclusiones

Como parte del análisis a la infraestructura y red de datos realizado a una organización que presta distintos servicios, se realizó un inventario de activos de información que permitió evaluar las capacidades de la infraestructura presente y que se encuentra sujeta a mejoramiento desde el punto de vista de la disponibilidad.

Se logró, de acuerdo a un análisis de la red objeto de estudio, la identificación de puntos críticos utilizando como herramienta diagramas actualizados que permitieron evidenciar la existencia de 10 puntos de único fallo, es decir, elementos componentes críticos que ante un eventual problema físico o lógico, se convierten en incidencias de alto impacto para la organización.

De acuerdo con las actividades de implementación recomendadas se estima un tiempo de implementación total del proyecto de 3 semanas incluyendo pruebas de funcionamiento, con un costo para la renovación total de la infraestructura de USD $43.016 IVA incluido.

Se logró documentar una propuesta de solución con niveles de alta disponibilidad del 99.95% para la red de datos que soporta la operación diaria de la organización objeto de estudio, que se convierte en un elemento muy importante para la toma de decisiones, teniendo en cuenta que los servicios informáticos son directamente impactados por cualquier incidencia en la disponibilidad de la red de datos y los costos por indisponibilidad pueden llegar a ser muy altos y necesariamente deben ser cuantificados para ser tenidos en cuenta en ejercicios de análisis de riesgos.

15. Documentación de Referencia

Bibliografía

Castro, M. I. R., Morán, G. L. F., Navarrete, D. S. V., Cruzatty, J. E. Á., Anzúles, G. R. P., Mero, C. J. Á., ... & Merino, M. A. C. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades (Vol. 46). 3Ciencias.

Cordero José & García Yadimyr. (2015). Análisis de riesgos y recomendaciones de seguridad de la información del Hospital E.S.E. San Bartolomé de Capitanejo, Santander. http://repository.unad.edu.co/handle/10596/6366

Gutiérrez, J., & Ayuso, J. G. T. (2003). *Protocolos criptográficos y seguridad de redes*. Ed. Universidad de Cantabria.

Kurose, J. F., & Ross, K. W. (2010). *Redes de computadoras: Un enfoque descendente, quinta edición*. Pearson Educación.

Portantier, F. (2012). *Seguridad informática*. Usershop.

Soriano, M. (2014). Seguridad en redes y seguridad de la información. *Obtenido de http://improvet. cvut. cz/project/download/C2ES/Seguridad_de_Red_e_Informacion. pdf*.

Tamayo, J. (2020). *Adaptación de una metodología para el análisis y gestión de riesgos informáticos para organizaciones del sector salud en Colombia* [Proyecto Aplicado o Tesis, Repositorio Institucional UNAD]. https://repository.unad.edu.co/handle/10596/35868

Vega-Pérez, C. A., Grajales-Lombana, H. A., & Restrepo, L. A. M. (2017). *Sistemas de información: Definiciones, usos y limitantes al caso de la producción ovina colombiana*. *Orinoquia*, *21*(1), 64-72.

Urbina, G. B. (2016). *Introducción a la seguridad informática*. Grupo Editorial Patria.

Molina Ruiz, J. E. (2012). Propuesta de segmentación con redes virtuales y priorización del ancho de banda con QoS para la mejora del rendimiento y seguridad de la red LAN en la Empresa Editora El Comercio Planta Norte.

Oroya Acosta, M. F. Rediseño de la Red Lan en la empresa Vlacar SAC-Chimbote; 2019.

16. Anexos

ANEXO 1

Plantilla de Configuración de Switches y Aseguramiento

EQUIPO: _____

	APLICADO		
COMANDO	**SI**	**NO**	**JUSTIFICACIÓN DE NO APLICACIÓN**
###Configurar hora			
configure timezone -300			
configure ntp server add (IP_ADDRESS) vr VR-D			
enable ntp vr VR-D			
###Configurar nombre			
conf snmp sysName HOSTNAME			
###Creacion Usuarios			
create account admin (USER)			
PASSWORD			
PASSWORD			
###Politica Usuarios			
configure account all password-policy min-length 8			
configure account all password-policy lockout-on-login-failures on			
configure account all password-policy lockout-time-period 5			
# COMANDOS DE PROTECCION DE CONTRASEÑAS			
enable cli-config-logging			
configure cli password prompting-only on			
configure idletimeout 10			
configure cli max-sessions 8			
configure cli max-failed-logins 3			

# COMANDO DE PROTECCION DE MEMORIA			
configure log target memory-buffer alert percent-full 90			
# COMANDO DE COLECCION DE DIAGNOSTICO			
enable tech-support collector			
### Habilitar eventos de auditoria completos			
enable cli config-logging			
### SSH			
enable ssh			
y			
disable telnet			
###Proteccion DDOS (OPCIONAL)			
enable dos-protect sim			
###DESHABILITAR LLDP			
enable lldp port all			
disable igmp			
#QOS			
configure vlan default delete ports all			
create qosprofile "QP6"			
configure dot1p type 5 qosprofile QP6			
configure diffserv examination code-point 46 qosprofile QP6			
configure diffserv replacement priority 5 code-point 46			
enable dot1p examination ports (PUERTOS_USER)			
enable dot1p replacement ports (PUERTOS_USER)			
enable diffserv examination ports (PUERTOS_USER)			
enable diffserv replacement ports (PUERTOS_USER)			
configure port (PUERTOS_USER) rate-limit flood multicast 30000			
configure port (PUERTOS_USER) rate-limit flood broadcast 30000			

enable diffserv replacement ports (PUERTOS_USER) qosprofile QP1			
enable diffserv replacement ports (PUERTOS_USER) qosprofile QP6			
enable diffserv replacement ports (PUERTOS_USER) qosprofile QP8			
enable dot1p replacement ports (PUERTOS_USER) qosprofile QP1			
enable dot1p replacement ports (PUERTOS_USER) qosprofile QP6			
enable dot1p replacement ports (PUERTOS_USER) qosprofile QP8			
#VLAN			
create vlan IMPRESORAS tag 22			
create vlan APORTES_SUBSIDIOS tag 23			
create vlan MEZANINE tag 24			
create vlan CONTABILIDAD tag 25			
create vlan COMPRAS_ADMINISTRATIVO tag 26			
create vlan FIDELIZACION tag 27			
create vlan TECNOLOGIA tag 28			
create vlan IPS tag 29			
create vlan RRHH tag 30			
create vlan DIRECCION tag 31			
create vlan TESORERIA tag 32			
create vlan ARCHIVO tag 33			
create vlan COMUNICACIONES tag 34			
create vlan JURIDICA tag 35			
create vlan CONTROL_INTERNO tag 36			
create vlan AGENCIA_TURISMO tag 37			
create vlan CALL_CENTER tag 38			
create vlan TARJETAS tag 39			
create vlan ZONA_RECREATIVA tag 40			
create vlan ADMIN_SWITCHES tag 1000			

create vlan INTERNET_ETB_CC tag 200			
create vlan INTERNET_IFX_PUBLIC tag 100			
create vlan INTERNET_C&W tag 300			
create vlan INTERNET_IFX_PRIV tag 400			
create vlan SERVIDORES_CHAPI tag 500			
create vlan VOIP tag 21			
#DESCRIPCION			
configure port 1 description (DESCRIPCION)			
#SHARING			
enable sharing (PUERTO_MASTER) grouping (PUERTO_MASTER+PUERTOS) algorithm address-based L2 lacp			
#DIRECCIONAMIENTO			
configure vlan IMPRESORAS ipaddress 192.168.12.2/25			
configure vlan APORTES_SUBSIDIOS ipaddress 192.168.12.130/27			
configure vlan MEZANINE ipaddress 192.168.12.162/27			
configure vlan CONTABILIDAD ipaddress 192.168.12.194/27			
configure vlan COMPRAS_ADMINISTRATIVO ipaddress 192.168.12.226/27			
configure vlan FIDELIZACION ipaddress 192.168.13.2/28			
configure vlan TECNOLOGIA ipaddress 192.168.13.18/28			
configure vlan IPS ipaddress 192.168.13.34/28			
configure vlan RRHH ipaddress 192.168.13.50/28			
configure vlan DIRECCION ipaddress 192.168.13.66/28			
configure vlan TESORERIA ipaddress 192.168.13.82/28			
configure vlan ARCHIVO ipaddress 192.168.13.98/28			
configure vlan COMUNICACIONES ipaddress 192.168.13.114/28			
configure vlan JURIDICA ipaddress 192.168.13.130/28			
configure vlan CONTROL_INTERNO ipaddress 192.168.13.146/28			

configure vlan AGENCIA_TURISMO ipaddress 192.168.13.162/28			
configure vlan CALL_CENTER ipaddress 192.168.13.178/28			
configure vlan TARJETAS ipaddress 192.168.13.194/28			
configure vlan ZONA_RECREATIVA ipaddress 192.168.13.210/28			
configure vlan ADMIN_SWITCHES ipaddress 192.168.10.2/24			
configure vlan INTERNET_ETB_CC ipaddress 192.168.14.2/24			
configure vlan SERVIDORES_CHAPINERO ipaddress 192.168.20.2/24			
configure vlan VOIP ipaddress 192.168.21.2/24			
configure iproute add default 192.168.10.1			
enable ntp vlan GESTION_SWITCHES			
configure dns-client add name-server 172.16.3.18 vr VR-Default			
#PORT-VLAN UNTAG			
configure vlan (NAME_VLAN) add port 1 untag			
#PORT-VLAN TAG			
configure vlan (NAME_VLAN) add port 1 tag			
#STP			
create stpd RSTP_COMFA			
configure stpd RSTP_COMFA mode dot1w			
configure stdp RSTP_COMFA rapid-root-failover			
configure stpd RSTP_COMFA default-encapsulation dot1d			
enable stpd RSTP_COMFA auto-bind vlan 1-4094			
configure stpd RSTP_COMFA ports link-type edge (PUERTOS_USER) edge-safeguard enable bpdu-restrict recovery-timeout 60			
configure stpd RSTP_COMFA ports link-type point-to-point (PUERTOS_TRUNK)			
disable stpd "s0"			
enable stpd RSTP_COMFA			
#SLPP			

enable slpp guard ports (PUERTOS_USER)			
#ELRP			
enable elrp-client			
configure elrp-client periodic (NAME_VLAN) ports all interval 1 log-and-trap disable-port ingress permanent (Aplicar para cada una de las VLAN)			
#JUMBO FRAMES			
enable jumbo-frame ports all			
#SNMP_V3			
configure snmpv3 add user (USER) authentication md5 (PASSWORD_MD5) privacy des (PASSWORD_DES)			
configure snmpv3 add group (NAME_GROUP) user (USER) sec-model usm			
configure snmpv3 add access (NAME_GROUP) sec-model usm sec-level priv read-view defaultAdminView write-view defaultAdminView notify-view defaultAdminView			
enable snmp access snmpv3			
disable snmpv3 default-group			