UNIVERSIDAD RICARDO PALMA

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

Diseño de servicios gestionados que impactan positivamente en el rendimiento de la gestión empresarial

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el título profesional de Ingeniera Electrónica

AUTOR

Llerena Reyes, Karen Christian Elsa

ORCID: 0009-0006-7448-7212

Lima, Perú

2024

METADATOS COMPLEMENTARIOS

Datos del autor

Llerena Reyes, Karen Christian Elsa
DNI: 45972928

Datos del jurado

JURADO 1
Burneo Gonzalez, Katia Janet
DNI: 09391942
ORCID: 0000-0002-7046-8106

JURADO 2
Rivas Leon, Javier Hipolito
DNI: 10250991
ORCID: 0000-0002-8365-4346

JURADO 3
Terukina Oshiro, Nelly Luz
DNI: 07808963
ORCID: 0000-0002-9654-7961

JURADO 4
Rodriguez Alcazar, Jose Luis Antonio
DNI: 08242196
ORCID: 0000-0003-2238-3017

Datos de la investigación

Campo del conocimiento OCDE: 02.02.01
Código del Programa: 712026

DECLARACIÓN JURADA DE ORIGINALIDAD

Yo, Karen Christian Elsa Llerena Reyes, con código de estudiante N°200612695, con DNI N°45972928, con domicilio en Pasaje El Huerto 281 departamento 103 Ciudad Satélite Santa Rosa, distrito Callao, provincia y departamento de Callao, en mi condición de bachiller en Ingeniería Electrónica de la Facultad de Ingeniería, declaro bajo juramento que:

El presente trabajo de suficiencia profesional titulado: "Diseño de servicios gestionados que impactan positivamente en el rendimiento de la gestión empresarial." es de mi única autoría, y no existe plagio y/o copia de ninguna naturaleza, en especial de otro documento de investigación presentado por cualquier persona natural o jurídica ante cualquier institución académica o de investigación, universidad, etc.; el cual ha sido sometido al antiplagio Turnitin y tiene el 23% de similitud final.

Dejo constancia que las citas de otros autores han sido debidamente identificadas en el trabajo de suficiencia profesional, el contenido de estas corresponde a las opiniones de ellos, y por las cuales no asumo responsabilidad, ya sean de fuentes encontradas en medios escritos, digitales o de internet.

Asimismo, ratifico plenamente que el contenido íntegro del trabajo de suficiencia profesional es de mi conocimiento y autoría. Por tal motivo, asumo toda la responsabilidad de cualquier error u omisión en el trabajo de suficiencia profesional y soy consciente de las connotaciones éticas y legales involucradas.

En caso de falsa declaración, me someto a lo dispuesto en las normas de la Universidad Ricardo Palma y a los dispositivos legales nacionales vigentes.

Surco, 14 de marzo de 2024

Karen Christian Elsa Llerena Reyes
DNI N°45972928

INFORME DE ORIGINALIDAD–TURNITIN

Diseño de servicios gestionados que impactan positivamente en el rendimiento de la gestión empresarial

INFORME DE ORIGINALIDAD

23%	22%	1%	10%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	2%
2	repositorio.urp.edu.pe Fuente de Internet	2%
3	repositorioacademico.upc.edu.pe Fuente de Internet	2%
4	dspace.espoch.edu.ec Fuente de Internet	2%
5	latam.kaspersky.com Fuente de Internet	2%
6	legadmi.com Fuente de Internet	1%
7	1library.co Fuente de Internet	1%
8	Submitted to Universidad Ricardo Palma Trabajo del estudiante	1%
9	repositorio.puce.edu.ec Fuente de Internet	

DEDICATORIA

Dedico este trabajo a mis padres por su apoyo incondicional

A mi madre Elsa Reyes que ha guiado cada uno de mis pasos, que me ha enseñado a ser perseverante y luchar por cada uno de mis objetivos, siempre tomando mi mano.

A mi padre Dante Llerena por sus consejos, esfuerzo, cariño y comprensión.

AGRADECIMIENTO

Quiero agradecer a mis abuelos a mi mamá Lolo y a mi papá Pepe por la dedicación y amor.

A Charo, Rosa, Nancy y Juan Carlos por todos sus consejos y amor.

A mis abuelos Dante y Emma por su amor y ejemplo.

A Dante, Gabriela, y Mikayla por ser mis cómplices en la vida.

A mis profesores por la ayuda y conocimientos impartidos en mi etapa de alumna.

A mis amigos por compartir conmigo sus conocimientos en mi desarrollo de mi etapa profesional, motivándome y apoyándome en la culminación de este informe.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

El siguiente informe técnico tiene la finalidad de demostrar la experiencia profesional adquirida en el área de diseño de servicios gestionados e implantación de proyectos dentro del campo de telecomunicaciones.

Las soluciones integrales garantizan que las transacciones de los clientes puedan realizarse manera segura, confiable y en tiempo real, sin importar su ubicación geográfica.

El presente informe se presenta el diseño de la solución integral de servicios gestionados que impactan en el rendimiento de la gestión empresarial, en una de las empresas de retail (de ahora en adelante empresa-target) a la que se le brindó soluciones técnicas en base a las necesidades principales: alta disponibilidad y un mejor performance de los enlaces.

A la empresa-target se le planteo la siguiente propuesta según sus requerimientos técnicos y económicos, con el objetivo de garantizar la continuidad del servicio.

Para fines de este informe se enfocará en la sede la sede principal conocida también como cabecera, una sede remota, y el internet nube, como se muestra en la figura N°5.

CAPITULO I: ASPECTO GENERALES

1.1 Planteamiento del problema

1.1.1 Marco situacional

El gran impacto social, cultural y económico que ejerce la tecnología, debido a que es una herramienta de desarrollo y eficiencia, hace que las empresas busquen la renovación tecnológica, que les permitiría un mejor performance y una mejora de sus procesos.

En la actualidad los clientes no solo necesitan una conexión de internet, si no soluciones integrales, permitiendo que sus transacciones se realicen de forma segura, confiable y en tiempo real, independiente de su ubicación geográfica.

El crecimiento que las empresas experimentan implica una expansión y la necesidad de optimiza procesos.

1.1.2 Problematización

La empresa-target enfrentaba diferentes problemas en su red:

- Deficiencia en los servicios gestionados que afecta el desempeño de la gestión empresarial.
- Ancho de banda limitado, presentando lentitud en los enlaces.
- La red carece de calidad de servicio (QoS) en sus enlaces para la priorización de envío de la información, presentando saturación.
- Centralización de los recursos de red en una sola sede.
- La red carece de políticas de ciberseguridad y se evidencia un uso ineficiente de los recursos disponibles.
- La empresa-target contaba con medios de transmisión que limitaban el crecimiento del ancho de banda.

Tras analizar la situación de los enlaces y considerando las problemáticas mencionadas anteriormente, se exploraron posibles soluciones integrales que ofrecer a la empresa Este informe está enfocado en la gestión de su sede principal y una de sus sedes remotas.

La empresa-target contaba con una red de servicios a nivel nacional como se muestra en la tabla 1, que está conformada con los siguientes servicios:

Tabla 1

Enlaces a nivel nacional

SERVICIO	ACCESO BW	CANTIDAD DE ENLACES
INTERNET SIMÉTRICO	4M	1
SPEEDY	1200/256K	1
	600/256K	1
IP-VPN	1M	1
	1M	2
	128K	2
	256K	1
	512K	1
TOTAL DE ENLACES		12

1.1.3 Importancia

Con la implementación de la solución integral, que permitió la modernización e renovación de los equipos de la empresa-target en base a sus necesidades, se logró que ésta fuera más competitiva en el mercado empresarial.

La solución implementada que se propuso para mejorar la red dio como resultado la mejora del performance de los enlaces para aprovechar los recursos asignados, la priorización del ancho de banda (BW) con QoS para mejorar el rendimiento y la seguridad de sus enlaces.

1.2 Objetivos

1.2.1 Objetivos generales

Diseñar una solución integral de servicios gestionados que influyen en el mejor desempeño de la gestión empresarial.

1.2.2 Objetivos específicos

- Mejorar el performance de los enlaces con el incremento de ancho de banda, según los requerimientos de cada sede.
- Analizar y proponer la configuración de calidad de servicio (QoS) para la priorización de la voz, video y datos críticos.
- Descentralizar (red distribuida) las sedes remotas para que no dependan de la sede principal para el acceso a internet.
- Analizar y proponer filtros de contenido y firewalls como elementos de seguridad requerida.
- Consolidar y uniformizar la conectividad de la red en fibra óptica.

CAPITULO II: MARCO TEÓRICO

2.1 Comunicaciones

2.1.1 Fibra óptica

"La fibra óptica es un medio de transmisión completamente diferente a los conductores y líneas coaxiales de cobre no solamente con respecto a la estructura y materiales que lo componen, sino también de la forma de transmisión de señales" (Japan International Cooperation Agency (JICA) - Instituto Nacional de Investigación y Capacitación de Telecomunicaciones (INICTEL)).

Ésta se clasifica en fibra óptica multimodo y fibra óptica monomodo (Ver Tabla 2). Sus características están reguladas por la UIT-T (Recomendaciones G.651 a G.657 y sus anexos) (Ver Tabla 3).

De acuerdo a la definición del Ing. Vidal Roncal (2012):

> La fibra óptica es una guía de onda que permite la transmisión de información, a través de portadores de luz (modos de luz) que se propagan en su interior cumpliendo el principio de la reflexión total. (Principio de reflexión de la luz que se presenta en el límite entre dos medios con índice de refracción diferente, de todo haz de luz incidente).

Tabla 2

Clasificación de la fibra óptica

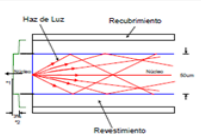
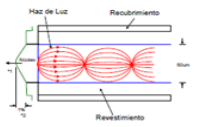
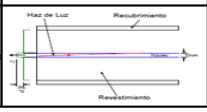
TIPO DE FIBRA	GRÁFICA	ESTRUCTURA	CARACTERISTICAS DE TRANSMISION		CARACTERÍSTICAS DE EMPALME Y ACOPLAMIENTO		CAMPO DE APLICACIÓN
		Diámetro de Núcleo/Diámetro o de Revestimiento(um)	Pérdida de Transmisión dB/Km (longitud de onda en um)	Ancho de Banda (MHz-Km)	Empalme	Rendimiento Acoplamiento con Fuente	
Multimodo Índice Escalón		50/125 62.5/125 100/140	<6(0.85)	<100	Fácil	Grande	Comunicación de capacidad pequeña y enlaces cortos(Red Lan)
Multimodo Índice Gradual		50/125 62.5/125	<3(0.85) <1(1.3)	100~2000	Un poco fácil	Mediano	Comunicación de capacidad y enlaces medianos (comunicación hasta 140Mbps)
Monomodo		9/125	<1(1.3) <0.5(1.55)	>varios millares	Un poco difícil	Pequeño	Comunicación de gran capacidad y larga distancia (comunicación de mas de 140Mbps)

Tabla 3

Normas Técnicas relacionadas a los conductores ópticos

NORMA TÉCNICA	TIPO DE FIBRA	DIÁMETROS DE LA ESTRUCTURA		LONGITUD DE ONDA DE APLICACIÓN	AMBITO DE APLICACIÓN
		NÚCLEO	REVESTIMIENTO		
G.651	Multimodo de índice gradual	50um	125um	850nm 1300nm	Txn analógica y digital. Usadas en la actualidad en redes de datos de corta longitud (hasta 2 km)
G.652	*Monomodo* Fibra estándar de dispersión no desplazada	8.6um~ 9.5um	125um	1310nm 1510nm	Puede utilizarse en segunda ventana (con peor atenuación) o en tercera ventana (con peor dispersión).
G.653	Fibra de dispersión desplazada (DSF)	7.8um~ 8.5um	125um	1550nm	Al tener dispersión cero a la longitud de onda de emisión, se incrementa un fenómeno llamado mezclado de cuatro ondas (FWM), que degrada la transmisión, y dificulta la multiplexación WDM.
G.654	Fibra óptica monomodo con corte desplazado	9.5um~ 10.5um	125um	1550nm	Se aplica para enlaces de muy larga distancia. Es de aplicación limitada debido a la reducida performance en cuanto a la dispersión cromática. Normalmente no es aplicable para sistemas STM-16a 2,5 Gb/s.
G.655	Non-zero dispersión shifted.	8um ~11um	125um	1550nm	Es una FO con la dispersión desplazada, pero evitando que el cero de dispersión caiga dentro de la banda de transmisión. Así con una penalización en de dispersión negativa) dispersión (que se puede corregir con FO se evita el FWM.
G.656	Las fibras y cables con dispersión no nula para el transporte óptico de banda ancha	7um ~ 11um	125um	1460 1625	Esta fibra se puede utilizar para los sistemas CWDM y DWDM
G.657	Monomodo insensibles a la pérdida por flexión para la red de acceso	8.6um~ 9.5um	125um	1310nm 1550nm	A causa de las limitaciones de espacio y las numerosas manipulaciones, la fibra debe ser fácil de manipular y poco sensible a la Flexión. Gran ancho de banda

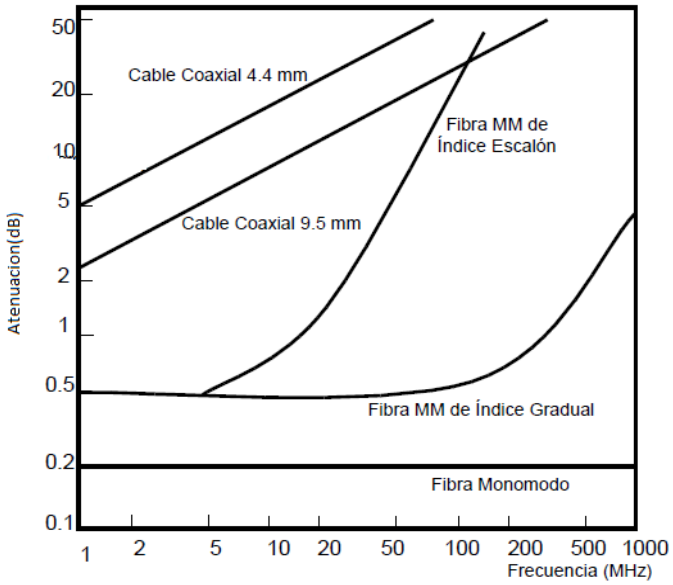
Nota. www.itu.int/rec/T-REC-G/es

A continuación, se detallarán alguna de las características y ventajas de la fibra óptica:

- Como se observa en la figura 1, la fibra óptica tiene menor valor de atenuación sobre los otros medios de transmisión.
- La fibra óptica permite un mayor ancho de banda y, por tanto, la transmisión de grandes cantidades de datos y un mejor rendimiento. (Japan International Cooperation Agency (JICA) - Instituto Nacional de Investigación y Capacitación de Telecomunicaciones (INICTEL)).

Figura 1

Modulación de frecuencia

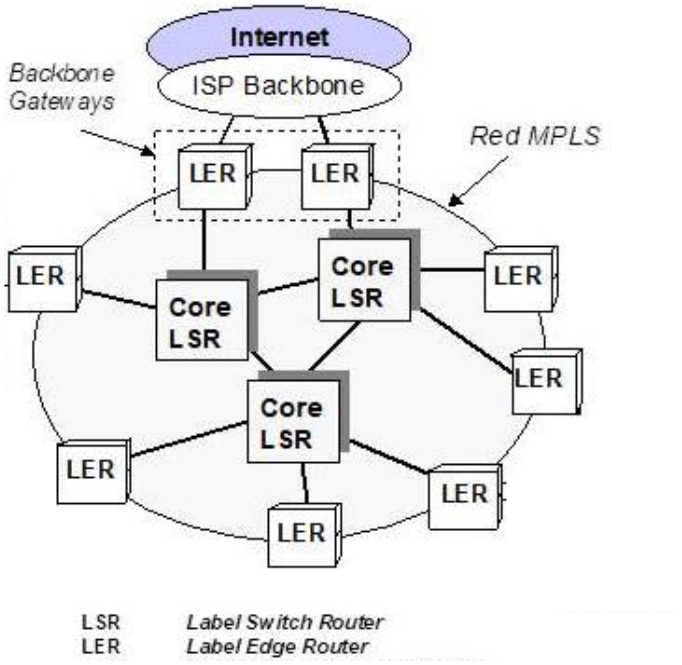


2.1.2 Multiprotocol Label Switching (MPLS)

MPLS es un estándar IP de conmutación de paquetes del Internet Engineering Task Force (IETF), que establece rutas predefinidas y efectivas. En la figura 2 se muestra la arquitectura de red MPLS, donde se muestra los dos tipos de nodos LER (label Edge routers) y los LSR (label switching routers) y estos intercambian información mediante protocolos de encaminamiento. (Huidobro Moya & Millan Tejedor, 2002)

Figura 2

Arquitectura MPLS

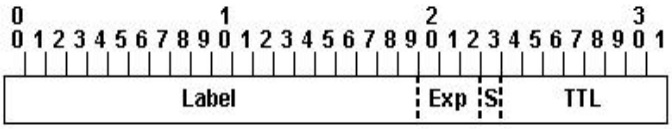


En la MPLS la etiqueta es un segmento de información añadido al comienzo del paquete. Los campos de la cabecera MPLS de 4 bytes (Véase figura 3), son los siguientes:

- *Label* (20 bits). Determinará el próximo salto del paquete.
- CoS (3 bits). Indica la calidad de servicio para diferenciar y priorizar el tráfico.
- Stack (1 bit). Mediante este bit indica si existen más etiquetas MPLS. (Huidobro Moya & Millan Tejedor, 2002).
- TTL (Time to live-8 bits). Estos bits se copian de la cabecera IP y proporciona la funcionalidad de tiempo de vida del paquete; reduce el valor inicial en una unidad por cada nodo que pase el paquete (García, 2009).

Figura 3

Cabecera MPLS



- **Escritura de la etiqueta -** Valor de etiqueta (no estructurado), 20 bits
- **Exp -** Uso experimental, 3 bits; utilizado actualmente como campo del Clase de Servicio (CoS)
- **S -** Parte inferior del stack, 1 bit
- **TTL -** Time to Live, 8 bits

2.1.3 Virtual Private Network (VPN)

Es una tecnología de red privada, escalable y fiable que permite la creación de accesos simétricos lo cual permite garantizar el envío y recepción de información entre los elementos de una organización, utilizando tecnología MPLS la cual permite tener calidad de servicio y priorizar distintos tipos de tráfico como son voz, datos y video. A cada organización se le coloca un identificador llamado VPN ID único en la red, con ello se garantiza que no exista el intercambio de información entre organizaciones.

2.1.4 Internet simétrico

El internet simétrico es un servicio dedicado que permite tener la misma velocidad de subida que la de descarga garantizando un acceso más estable y seguro, lo cual permite intercambio de grandes volúmenes de información. Además, es un servicio confiable y escalable.

2.1.5 Telefonía IP

"Voz sobre IP es una tecnología que permite realizar una conversación oral haciendo uso de la red de conmutación de paquetes mediante el empleo del protocolo IP" (Schulzrinne y otros, 2003).

Las redes de datos, como es el caso de la red IP sobre la que se soporta este tipo de telefonía, son redes digitales. Esto significa que el caso de transportar señales vocales, originalmente analógicas, requiere que en algún punto de la red se realice la digitalización de la señal de audio. De esta forma, una señal continúa en el tiempo y que toma infinidad de valores es convertida y cuantificada a una secuencia de números discretos. Esta tarea suele realizarse, generalmente, en los propios terminales y el elemento vital involucrado de forma directa es el códec. (Barrera Orta, 2012).

2.1.5.1 Códec

Los códecs pueden tener varios factores que los describen, como su tasa de bits, la calidad del audio codificado, su complejidad, o el retardo que introducen.

Los códecs fueron diseñados inicialmente para ser usados en el rango de frecuencias, entre los 300 Hz y los 3,4 KHz con una frecuencia de muestreo de 8kHz, estos códecs se conocen como de banda estrecha (NB, NarrowBand).

La International Telecommunication Union (ITU-T, por sus siglas en ingles), posteriormente incluyó códecs capaces de trabajar en rangos más amplios, entre 50 Hz y 7 KHz con una frecuencia de muestreo de 16kHz., considerados de banda ancha (WB, WideBand).

Actualmente, la ITU-T (Véase tabla 4) ha desarrollado códecs de banda "superancha" (SWB, SuperWideBand), para el rango comprendido entre 50 Hz y 14 KHz, y de banda completa (FB, FullBand), para el intervalo de frecuencias de 50 Hz a 20 KHz (Cox y otros, 2009).

La banda completa o FullBand permite una alta calidad como se puede obtener con los códecs G.711.1 y G.722.

Tabla 4

Normas Técnicas relacionadas con códecs

CÓDEC	NOMBRE	TASA DE BITS(Kbps)	RETARDO (ms)	COMENTARIOS
G.711	PCM : Pulse Code Modulation	64 / 56	0.125	Dos leyes de compresion μ-law y A-law
G.723.1	Hybrid MPC-MLQ and ACELP	6,3 / 5,3	37,5	Se utiliza en VoIP
G.722.1	Transform Coder	32 / 24	40	Se utiliza en videoconferencias
G.711.1	WideBand G.711	96 / 80 / 64	11,875	Optimizado para uso de VoIP

https://www.itu.int/rec/T-REC-G/es

2.2 Seguridad perimetral

La seguridad perimetral es la integración de elementos para la protección de una empresa. Los ataques cibernéticos generan un gran impacto disruptivo, afectando no solo la reputación de la compañía, sino también la continuidad del servicio. El control de accesos, los filtros de contenido y protección de la red garantiza la confidencialidad y un correcto aprovechamiento de la infraestructura de los servicios. (Multicomp, 1998).

2.2.1 Unified Threat Management (UTM)

Unified Threat Managemet o gestión unificada de amenazas, son dispositivos que se encargan de proteger las redes, que ofrece múltiples funcionalidades de protección, con distintas políticas de seguridad que define el establecimiento de las conexiones.

Un producto UTM generalmente incluye funciones como antivirus, antispyware, antispam, firewall de red, prevención y detección de intrusiones, filtrado de contenido y prevención de fugas. Algunas unidades también ofrecen servicios como enrutamiento remoto, traducción de direcciones de red (NAT, *network address translation*) y compatibilidad para redes privadas virtuales (VPN, *virtual private network*). El atractivo de la solución es su sencillez. Las

empresas que utilizan servicios de proveedores o productos diferentes para cada tarea de seguridad ahora pueden reunirlos todos en una única solución, con asistencia de un único equipo, y ejecutarlos desde una sola consola. (Kaspersky, s.f.)

2.2.2 Virtual Domains (VDOMs)

El VDOM es el método para dividir en forma lógica un firewall de tal manera que puedan tenerse varios firewalls que operen de forma diferente en el mismo firewall, proporcionan dominios de seguridad que permiten: estar en zonas separadas, la autenticación de usuarios, políticas de seguridad, enrutamiento y configuraciones de VPN; éste VDOM incluye todas las interfaces físicas firewall, módem, subinterfaces VLAN, políticas de seguridad, configuración de enrutamiento y configuración de VPN.

En un VDOM, puede crear políticas de seguridad para conexiones entre subinterfaces o zonas de la LAN virtual (VLAN) en el VDOM. Los paquetes no cruzan el borde del dominio virtual internamente, cuando un paquete ingresa en una VDOM, se queda restringido a ese VDOM. Para viajar entre VDOM, un paquete debe pasar a través de un firewall en una interfaz física. Luego, llega a otro VDOM en una interfaz diferente, pero debe pasar a través de otro firewall antes de ingresar al VDOM. Ambos VDOM están en la misma unidad firewall. Inter-VDOMs cambia este comportamiento en que son interfaces internas; sin embargo, sus paquetes pasan por las mismas medidas de seguridad que en las interfaces físicas (Fortinetguru, 2016).

2.2.3 Seguridad en la nube

El servicio de seguridad en la nube tiene como base el esquema de firewall compartidos implementados en la red del proveedor, los equipos de seguridad manejan virtualización de dominios (VDOM). Así mismo se trata de un servicio en alta disponibilidad.

El servicio ofrece entre sus funcionalidades:

•Firewall

•Sistema de Prevención de Intrusos

•URL filtering.

2.3 Cloud computing

Los servicios en la nube son: escalables, flexibles y auto gestionable. El cloud computing permiten crecer o decrecer las capacidades pagando únicamente por lo que se consume.

2.3.1 Infraestructura como servicio (IAAS)

En IAAS las empresas principalmente adquieren CPU, memoria, red y almacenamiento como servicio. El usuario gestiona el sistema operativo y despliega los servidores, y el proveedor de servicio se encarga de la infraestructura física y lógica. (HostingRed, 2015)

2.3.2 Plataforma como servicio (PAAS)

En PAAS las empresas usan la solución, y el proveedor es el responsable de la automatización y el despliegue de dichas aplicaciones. (HostingRed, 2015)

2.3.3 Software como servicio (SAAS)

En SAAS la empresa interactúa con el servicio medio de un navegador por medio de licencias con usuario y contraseña, pero el usuario no controla ni el hardware, ni la plataforma. (HostingRed, 2015)

CAPITULO III: DESARROLLO DEL PROYECTO

3.1 Diseño de la red

La empresa-target cuenta con 10 sedes remotas o sucursales y una sede principal o cabecera. Las sedes remotas se encuentran conectadas a la cabecera para el intercambio de información y el control del uso de internet.

Para la solución propuesta se requirió dimensionar los caudales (QoS) para las VPNs y conocer el consumo de internet que necesitaba la empresa-target para brindarle una solución a medida.

3.1.1 Dimensionamiento

Para poder dimensionar las *VPNs* y con ello mejorar los enlaces, se le solicitó a la empresa-target, información correspondiente a su red LAN, (véase tabla 5). Con los datos proporcionados se pudieron dimensionar los caudales, de acuerdo a la figura 4.

Tabla 5

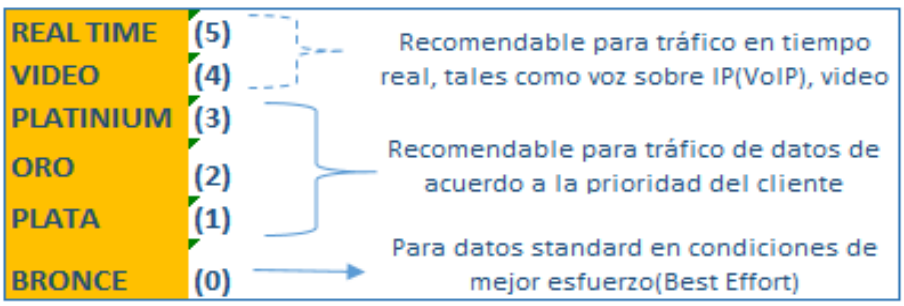
Red LAN del cliente

SEDES	DVR	ANEXOS IP	CANTIDAD DE PC	SERVIDORES
1 Sede Principal	1	15	20	1
1 Sede Lima	1	5	3	x
9 Sedes Remotas	1	5	3	x

Nota. Elaboración propia

Figura 4

Calidad de servicio



Nota. Elaboración propia

A las sedes remotas se les colocó el servicio de IPVPN de 4Mbps por fibra óptica en base a los datos presentados en la tabla 5, y figura 4:

- Para el caudal de voz (5) se priorizó la telefónica IP, se revisó el tipo de códec G711.1 y el número de llamadas en simultáneo que el cliente quería realizar. Para asegurar la calidad del servicio se colocó 100 kbps por cada canal; para los 5 canales se colocó 512k.
- Para el caudal de video (4), se priorizó la video vigilancia ya que cuenta con equipo DVR y el cliente nos indicó que la compresión y el formato de imagen, tenía un consumo máximo de 2M.
- En el caso de los caudales de datos, se dispone de 4 caudales diferentes *platinium* (3), oro (2), plata (1), y el caudal bronce (0); en el caso de este cliente se priorizo su servidor con prioridad *platinium* 1M, y el resto de tráfico en caudal bronce 512k.

Para dimensionar la IP VPN de la cabecera se realiza una suma de los anchos de banda de cada remota, en el caso del presente proyecto el cliente tiene 10 sedes de las mismas características:

- IP VPN 40M (caudal voz 5M, caudal video 20M, caudal *platinium* 10M, caudal bronce 5M) en el caso de este cliente todas las sedes se comunican hacia la cabecera.

Para dimensionar el INTERNET SIMETRICO, se evaluó la cantidad de PCs, y el uso que le darán los usuarios finales. El uso en la sede principal son las herramientas colaborativas, así como para el envío y recepción de correos, adicionalmente en esta sede se encuentra la gerencia de la empresa por eso se colocó un servicio de internet de 10Mbps.

En el caso del internet *cloud security* se dimensiona el internet por cada sede, cada remota tiene un aproximado de 3 PCs, siendo cada una de 3M. Se configurará el internet cloud security con un enlace de 30Mbps.

Todo el dimensionamiento mencionado anteriormente se encuentra resumido en la tabla 6.

Tabla 6

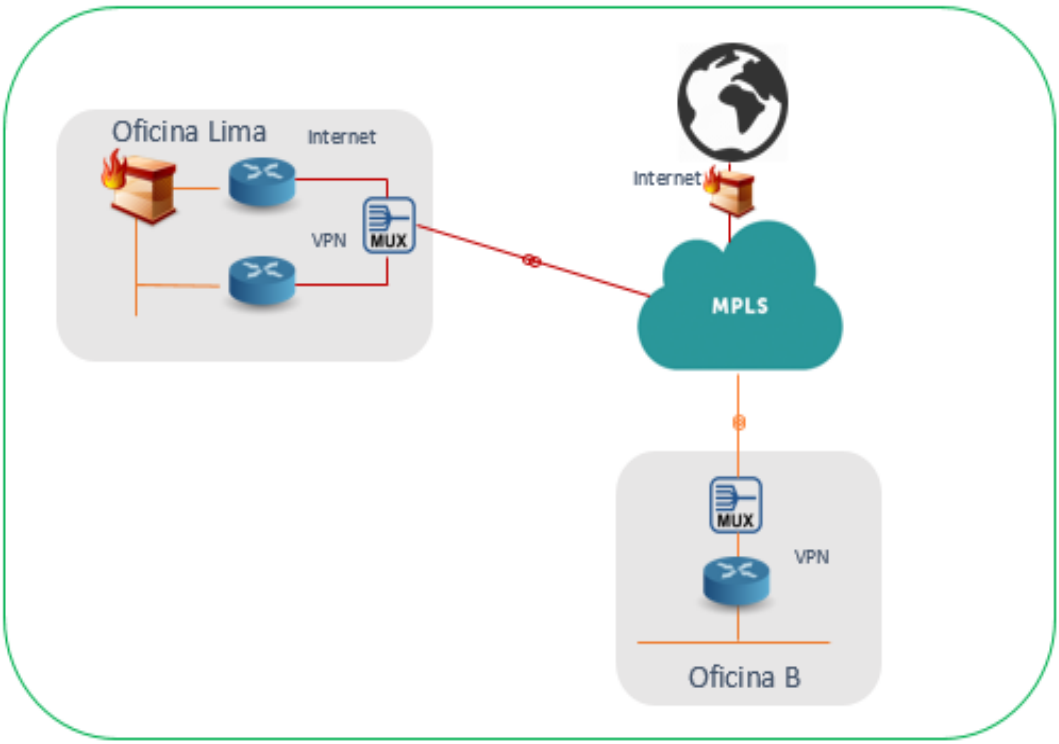
Dimensionamiento ofertado

SEDES	REAL TIME		CAUDAL DATOS			
	CAUDAL VOZ	CAUDAL VIDEO	CAUDAL PLATINIUM	CAUDAL ORO	CAUDAL PLATA	CAUDAL BRONCE
1 Sede Principal	5Mbps	20Mbps	10Mbps	x	x	5Mbps
1 Sedes Lima	512Kbps	2Mbps	1Mbps	x	x	512Kbps
9 Sedes Remotas	512Kbps	2Mbps	1Mbps	x	x	512Kbps

En la figura 5 se muestra la topología dimensionada que se le brindó al cliente; para fines de este informe se mostrará la sede principal y una sola sede remota ya que todas las sedes remotas cuentan con las mismas características técnicas.

Figura 5

Topología



Nota. Elaboración propia

Sede Principal (oficina Lima), cuenta con los siguientes servicios que tienen acceso por fibra óptica:

- IP VPN 40Mbps
- Internet simétrico 10Mbps
- Seguridad perimetral

Sede Remota (oficina B), medio de acceso fibra óptica

- IP VPN 4Mbps
- Internet *cloud security*

3.2 Solución Técnica

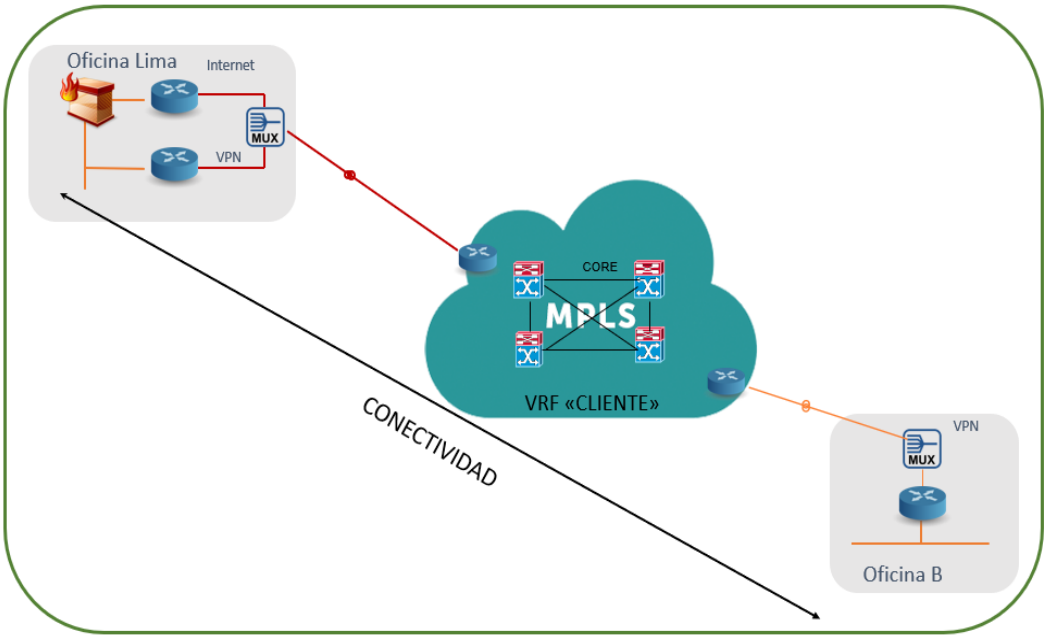
La tecnología implementada para los servicios empresariales tanto para los servicios IPVPN, así como para el INTERNET con un equipo de SEGURIDAD (UTM) y el INTERNET NUBE están dentro de la red IP/MPLS en la cual se puede asegurar la calidad de los servicios gestionados de extremo a extremo, así como también la disponibilidad.

La IP VPN permite la conexión de redes de área local (LAN) con características similares a las de estar físicamente en un mismo edificio, garantizando la privacidad y seguridad de la información.

En la figura 6 se muestra la conectividad entre la sede principal y la sede remota en el caso de la empresa-target, todas las sedes se comunican con la sede principal tanto para el envío como para la recepción de la información. En la figura 7 se explica como trabaja la QoS. Se tiene caudales exclusivos para la información más crítica, los caudales en la IP VPN son dinámicos a excepción del caudal de voz, esto indica que si no están siendo usados otro caudal puede usarlo hasta que este sea requerido.

Figura 6

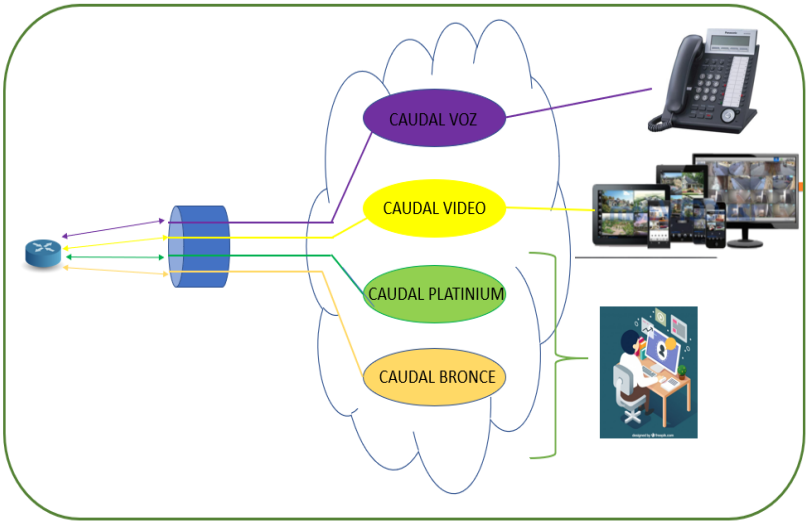
Conectividad IP VPN – Internet



Nota. Elaboración propia

Figura 7

Calidad de servicio del cliente en la IP VPN



Nota. Elaboración propia

La empresa- target tiene inconvenientes de energía comercial en su sede principal, como se muestra en la figura 6, debido a que las sedes remotas dependían de la cabecera para el uso del internet, ocasionando que todas las sedes pierdan conexión, por ellos la solución propuesta se colocó un INTERNET NUBE como se muestra en la figura 5.

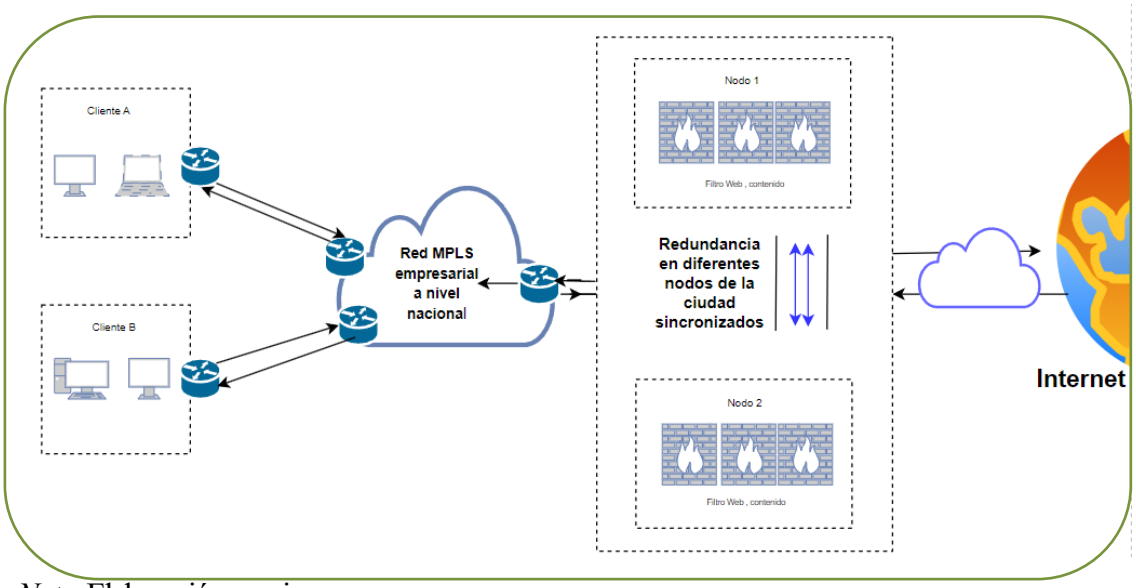
La virtualización es esencial para que mejore el rendimiento empresarial, con esta solución brindada a la empresa-target, no dependerá de la sede principal para hacer el uso de internet. El Internet nube es una plataforma hosteada en cloud que combina características empresariales con una escalabilidad superior.

Este servicio tiene como base el esquema de firewall como se muestra en la figura 8, garantizando el performance de los servicios, para este propósito se realizó la virtualización de dominios y se generó una VDOM por cada cliente. Y también ofrece funcionalidades como:

- Firewall
- Sistema de Prevención de Intrusos
- Antivirus y Antispyware.

Figura 8

Internet Nube



Nota. Elaboración propia

Para la seguridad física se instaló un equipo UTM para el uso de internet de la cabecera. A continuación, se indican algunas de sus funcionalidades:

- Protección de la infraestructura del servicio y red del cliente frente a Internet, mediante una plataforma redundante implementada en la red del proveedor de servicio.
- Protección contra virus y códigos maliciosos: Antivirus de Navegación HTTP y FTP.
- Filtrado de contenidos que permite limitar las capacidades de acceso a la Web de los usuarios, mediante la clasificación de contenidos y necesidades la empresa-target
- Posibilidad de entregar diferentes perfiles de usuario para acceso a los sistemas de gestión.
- Informes de uso y consumo del servicio.
- Posibilidad de conexión a la intranet.
- Capacidad de establecimiento de VPN sobre SSL, permitiendo la creación de túneles que permitirían el acceso a su red privada.
- Niveles de acceso personalizables, según las siguientes posibilidades:
    - Autenticación, directorio activo, certificado, etc.
    - Perfil personal de plantilla, personal ajeno, demo, etc.

3.2.1 Selección de equipos

En el mercado existen varias marcas con las que podemos implementar la solución, el aspecto económico varía dependiendo de la marca que elegimos. La empresa- target solicitó equipos de la marca CISCO, y para el caso del equipo de seguridad (UTM) equipos FORTINET.

3.2.1.1 Router

Para las sedes remotas que tienen un ancho de banda (BW) de 4Mbps seleccionamos equipos CISCO 1905 (Véase figura 9), debido a que el *datasheet* puede trabajar hasta 10Mbps (Véase Tabla 7).

Figura 9

Router cisco 1905

Nota. www.cisco.com/c/dam/en/us/products/routers/1905-serial-integrated-services-router-isr/data_sheet_c78-598372.pdf

Tabla 7

Descripción Cisco 1905

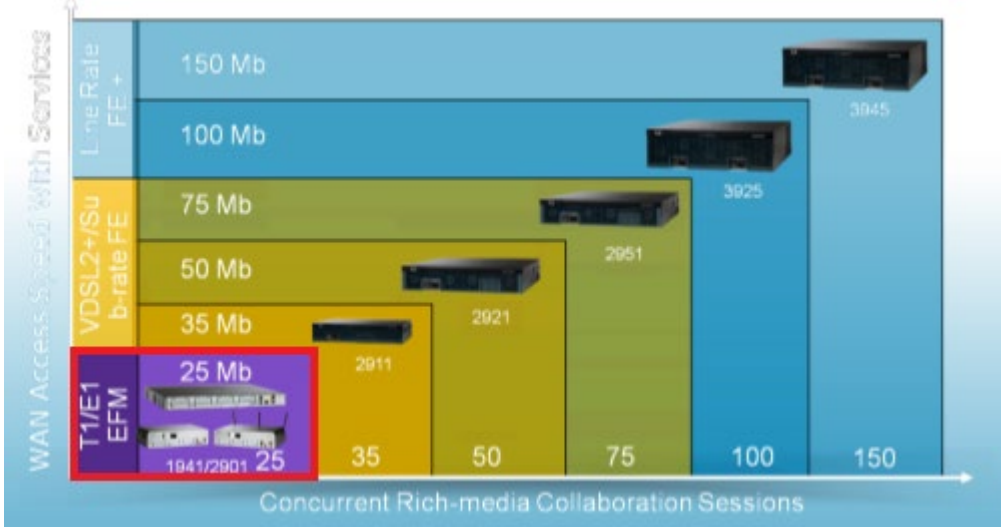
Benefits	Description
Service integration	• The Cisco 1905 offers increased levels of services integration with data, security, wireless, and mobility services enabling greater efficiencies and cost savings.
Services on demand	• A single Cisco IOS Software Universal image is installed on each Cisco ISR G2. The Universal image contains all of the Cisco IOS Software technology sets that can be activated with a software license, allowing your business to quickly deploy advanced features without downloading a new Cisco IOS Software image. Additionally, larger default memory is included to support the new capabilities.
High performance with integrated services	• The Cisco 1905 enables deployment in high-speed WAN environments with concurrent services enabled up to 10 Mbps.

Nota. www.cisco.com/c/dam/en/us/products/routers/1905-serial-integrated-services-router-isr/data_sheet_c78-598372.pdf

En el caso del enlace principal a pesar de tener un enlace de 10Mbps, el cliente solicitó un equipo para upgrades temporales. Se colocó un equipo de la serie CISCO 2900, específicamente el router 2901. Como se muestra en la figura 10 el equipo en mención puede trabajar hasta 25Mbps.

Figura 10

Router cisco 2901



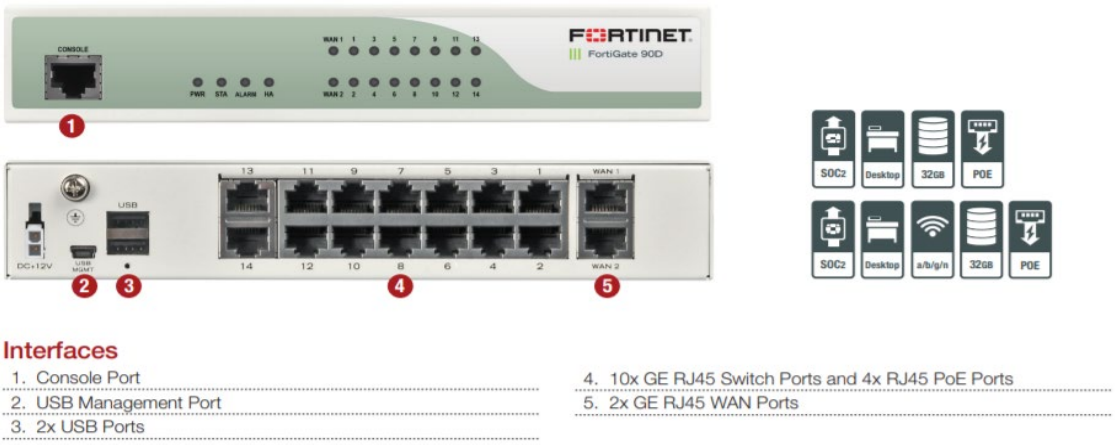
Nota. bbcusa.com/pdf/cisco-routers/cisco-routers-overview.pdf

3.2.1.2 UTM

Para la elección del equipo de seguridad para la sede principal se basó en la capacidad de hardware que este posee. La empresa-target seleccionó el equipo FG90D, que le daba las opciones de realizar todas las funcionalidades como filtro de contenido para hacer un uso óptimo de los recursos asignados. En la figura 11 se puede observar los puertos del equipo elegido.

Figura 11

FortiGate 90D



Nota. www.fortinet.com/content/dam/fortinet/assets/datasheets/FortiGate_FortiWiFi_90D_ Series.pdf

3.2.2 Topología de red y pruebas

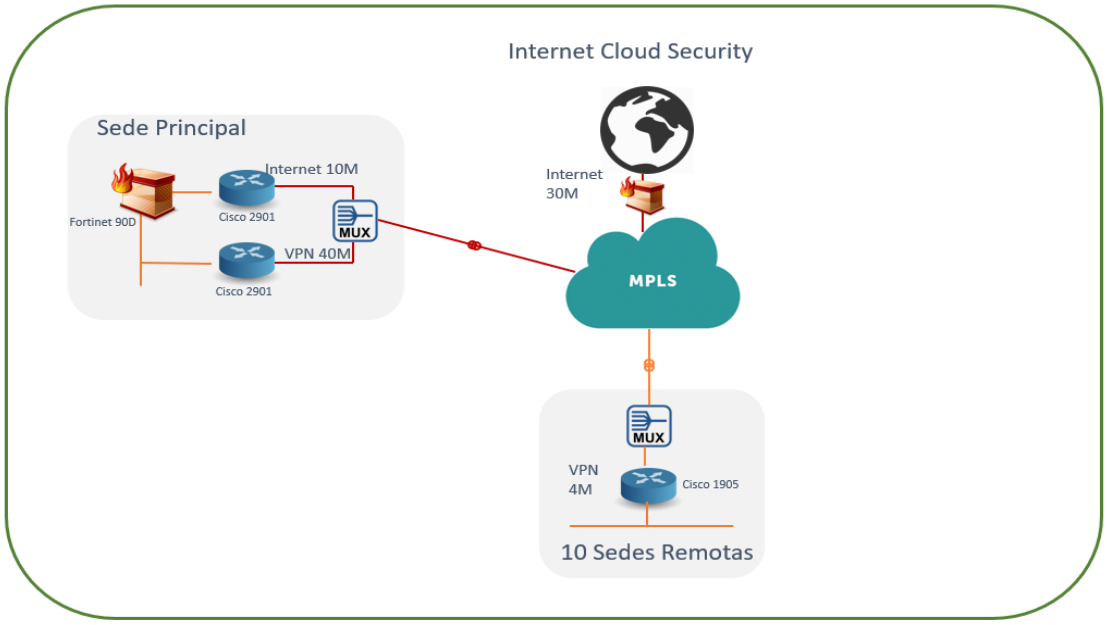
En esta sección se indicará la integración de los equipos, el direccionamiento propuesto, y las pruebas realizadas, evidenciando como la solución planteada mejoró el rendimiento operativo de la empresa.

3.2.2.1 Topología y direccionamiento

La solución propuesta a la empresa- target contaba con 10 sedes remotas y una principal o cabecera. En la figura 12 se muestra la integración de los equipos usados en la implantación.

Figura 12

Topología Implementada



Nota. Elaboración propia

El direccionamiento propuesto en la tabla 8 se realizó a partir del relevamiento de información pertinente (véase tabla 5).

Tabla 8

Direccionamiento IP de la sede principal y sedes remotas

SEDE	SERVICIO	SEGMENTO DE RED	MASCARA DE SUBRED	GATEWAY
PRINCIPAL	IP VPN 40M	192.168.20.0	/24	192.168.20.1
	INTERNET 10M	IP PUBLICA		
	SEGURIDAD			
	INTERNET NUBE			
REMOTA 1	IP VPN 4M	192.168.1.0	/24	192.168.1.1
REMOTA 2	IP VPN 4M	192.168.2.0	/24	192.168.2.1
REMOTA 3	IP VPN 4M	192.168.3.0	/24	192.168.3.1
REMOTA 4	IP VPN 4M	192.168.4.0	/24	192.168.4.1
REMOTA 5	IP VPN 4M	192.168.5.0	/24	192.168.5.1
REMOTA 6	IP VPN 4M	192.168.6.0	/24	192.168.6.1
REMOTA 7	IP VPN 4M	192.168.7.0	/24	192.168.7.1
REMOTA 8	IP VPN 4M	192.168.8.0	/24	192.168.8.1
REMOTA 9	IP VPN 4M	192.168.9.0	/24	192.168.9.1
REMOTA 10	IP VPN 4M	192.168.10.0	/24	192.168.10.1

Nota. Elaboración propia

Adicionalmente se recomendó el direccionamiento IP según la red LAN del cliente (véase tabla 9).

Tabla 9

Direccionamiento IP de la sede principal y sedes remotas

SEDE	DVR	IP TELEFONOS	RANGO DHCP	SERVIDOR	CENTRAL TELEFONICA
PRINCIPAL	192.168.20.20	192.168.20.200-192.168.20.235	192.168.20.100-192.168.20.150	192.168.20.10	192.168.20.109
REMOTA 1	192.168.1.20	192.168.1.200-192.168.1.205	192.168.1.100-192.168.1.120		
REMOTA 2	192.168.2.20	192.168.2.200-192.168.2.205	192.168.2.100-192.168.2.120		
REMOTA 3	192.168.3.20	192.168.3.200-192.168.3.205	192.168.3.100-192.168.3.120		
REMOTA 4	192.168.4.20	192.168.4.200-192.168.4.205	192.168.4.100-192.168.4.120		
REMOTA 5	192.168.5.20	192.168.5.200-192.168.5.205	192.168.5.100-192.168.5.120		
REMOTA 6	192.168.6.20	192.168.6.200-192.168.6.205	192.168.6.100-192.168.6.120		
REMOTA 7	192.168.7.20	192.168.7.200-192.168.7.205	192.168.7.100-192.168.7.120		
REMOTA 8	192.168.8.20	192.168.8.200-192.168.8.205	192.168.8.100-192.168.8.120		
REMOTA 9	192.168.9.20	192.168.9.200-192.168.9.205	192.168.9.100-192.168.9.120		
REMOTA 10	192.168.10.20	192.168.10.200-192.168.10.205	192.168.10.100-192.168.10.120		

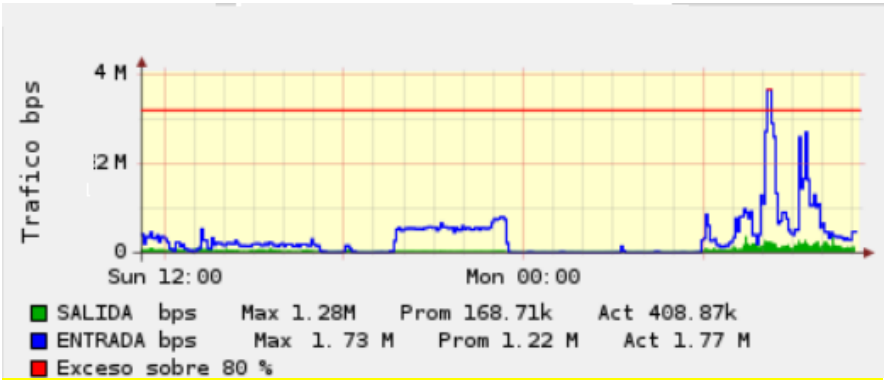
Nota. Elaboración propia

3.2.2.2 Pruebas

Luego de implementada la solución se realizaron pruebas de los enlaces para confirmar el buen funcionamiento de ésta. Como se valida con los resultados evidenciados en las figuras 13,14 y 15.

Figura 13

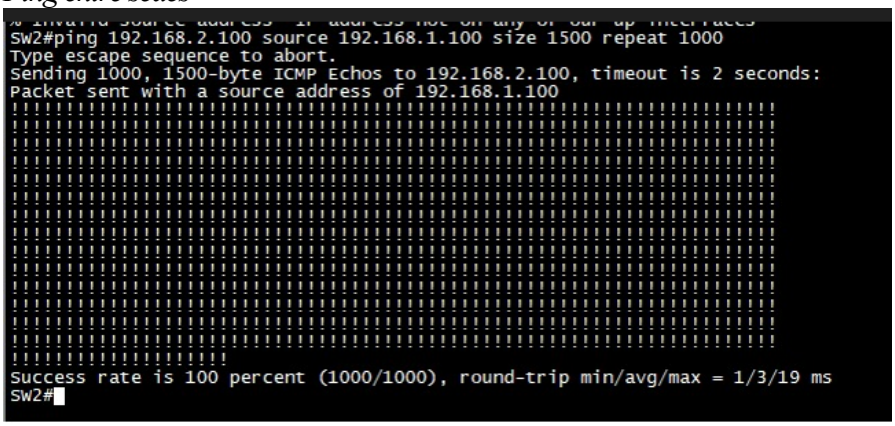
Consumo de ancho de banda sede remota



Nota. Elaboración propia

Figura 14

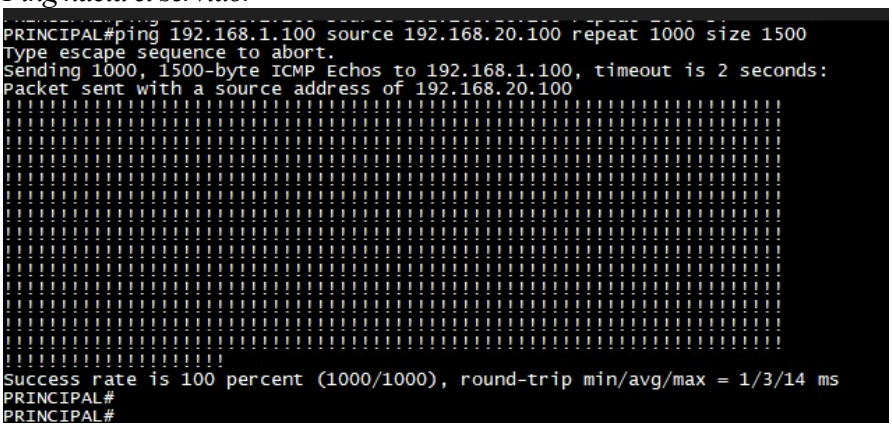
Ping entre sedes



Nota. Elaboración propia

Figura 15

Ping hacia el servidor



Nota. Elaboración propia

3.2.3 Diagrama de tiempo

Para indicar las actividades desarrolladas durante el proyecto y el tiempo empleado en ellas, se utilizó el método de PERT, el que proporciona una representación visual de la línea de tiempo de un proyecto y desglosa las tareas individuales (Véase tabla10:figura 16 y 17)

Tabla 10

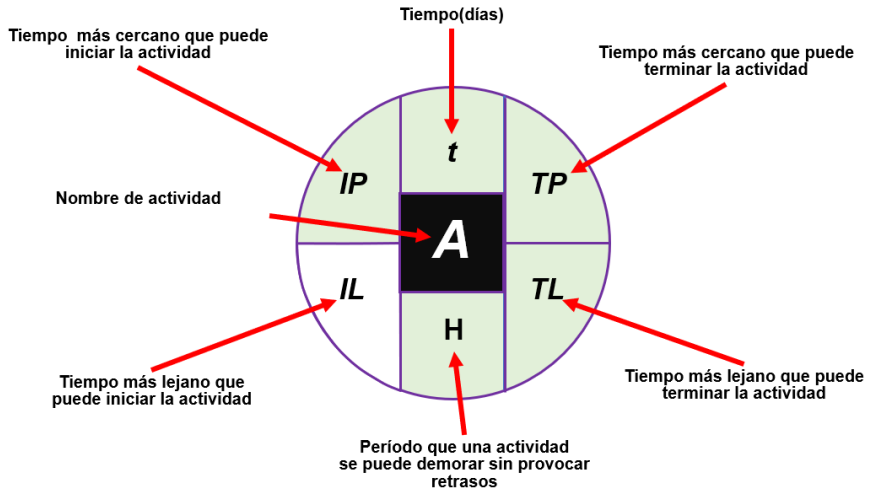
Actividades del proyecto

		PROYECTO	DISEÑO DE SERVICIOS GESTIONADOS QUE INFLUYEN EN EL MEJOR DESEMPEÑO DE LA GESTION EMPRESARIAL	
N° Actividades	Identificador	Actividades	Predecesora	Tiempo (días)
1	A	Relevamiento de informacion en cliente	-	1,00
2	B	Solicitud de costos y diseño de fibra	A	7,00
3	C	Diseño de la topologia de red y evaluacion de costos	A,B	3,00
4	D	Firma del proyecto	C	2,00
5	E	Emitir Orden de Compra y Confirmación	D	5,00
6	F	Presentacion del proyecto al area de instalaciones	D	1,00
7	G	Instalacion,migracion y pruebas	E,F	45,00
8	H	Conformidad	H	1,00
			Total	65,00

Nota. Elaboración propia

Figura 16

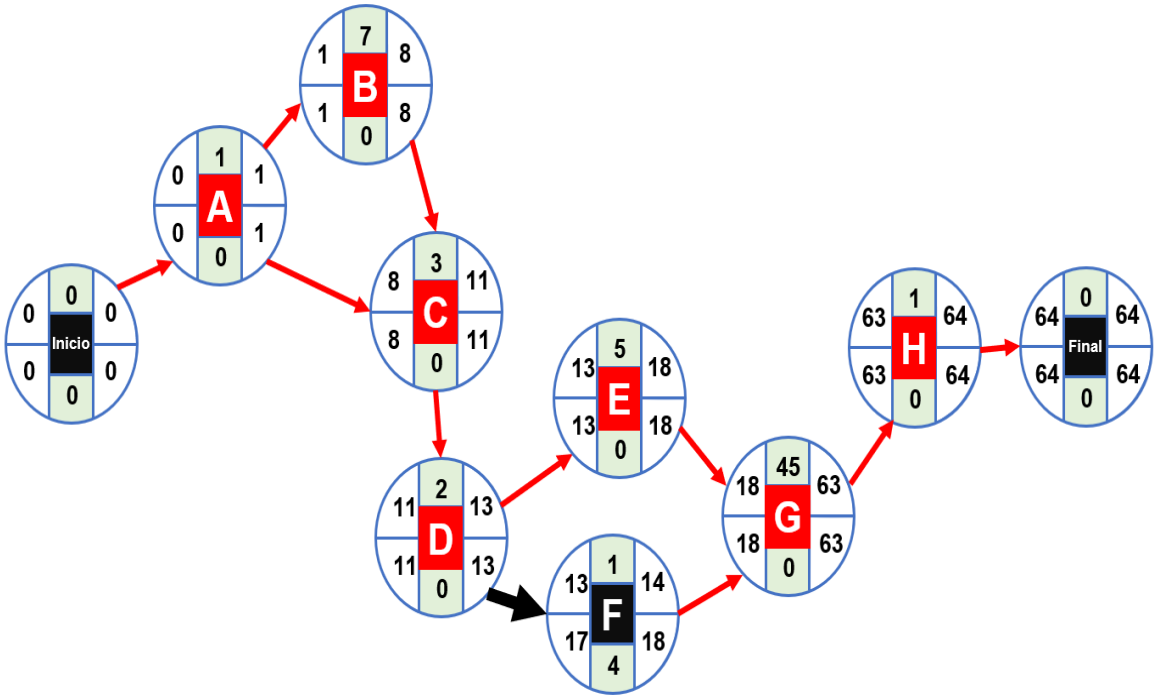
Representación para diagrama de PERT



Nota. Elaboración propia

Figura 17

Diagrama PERT del proyecto



Nota. Elaboración propia

3.3 Análisis económico

3.3.1 Inversión inicial

En la tabla 11 se detallan los costos asociados a la inversión inicial, dentro de cuales se incluyen los costos por equipamiento, instalación y configuración de los equipos

Tabla 11

Inversión inicial (CAPEX)

DESCRIPCIÓN	UNITARIO	CANTIDAD	TOTAL
Costo de fibra e instalación	1069.61	11	11,765.71
Demarcadores	325.00	11	3,575.00
Cisco 1905	300.00	10	3,000.00
Cisco 2901	1271.00	2	2,542.00
Fortinet 90D	1136.47	1	1,136.47
Costo de instalación de equipos y configuraciones	100.00	12	1,200.00
		TOTAL(USSD)	23,219.18

Nota. Elaboración propia

En la tabla 12 se detallan los costos asociados a los recursos acompañados de una breve descripción de las tareas dentro del proyecto; la duración de cada tarea está calculada en una jornada de 8 horas.

Tabla 12

Gastos asociados a personas asignadas al proyecto

PERSONAL	DESCRIPCIÓN	DURACIÓN	COSTO TOTAL
Jefe de Proyectos	Encargado de realizar el inicio del proyecto , y obtener la conformidad del cliente	4 dias	400.00
Ingeniero Preventa	Encargado de diseñar la solución	2 dias	200.00
Asistente Proyecto	Encargado de realizar el seguimiento y coordinación con el cliente para las instalaciones	30 horas	80.00
		TOTAL(USSD)	680.00

Nota. Elaboración propia

La inversión inicial del proyecto o capital expenditure (CAPEX, por sus siglas en ingles) se obtiene al sumar los totales de la tabla 11 y tabla 12, que dan como resultado un total de $23899.18 dólares americanos.

3.3.2 Costos recurrentes

En la tabla 13 se detalla los costos de red, mantenimiento por equipos y fibra, e impuestos varios, los cuales son gastos recurrentes del proyecto.

Tabla 13

Gastos mensuales

CONCEPTO	DESCRIPCIÓN	GASTO MENSUAL
Uso de la capacidad instalada		38.00
Mantenimiento por equipos y fo		140.00
Infraestructura de red		507.00
Tributo (fitel)	2%Renta	59.00
Gastos de gestion	0.5%Renta	14.80
Proporcion de cobertura de deuda	1%Renta	29.59
Participacion laboral		217.06
Impuesto a la renta		576.30
	TOTAL(USSD)	1,581.74

Nota. Elaboración propia

3.3.3 Evaluación de la rentabilidad

En esta sección se evalúa la rentabilidad del proyecto con un contrato con la empresa-target a 36 meses con un recurrente $2,958.58, con un ingreso total $106,509.00. Como se indica en la tabla 14 estos valores corresponden a un VAN positivo lo cual indica que se ha generado una ganancia. El playback indica el tiempo de recupero de la inversión a partir del mes 18.

Tabla 14

Indicadores financieros

INDICADORES	
Ingreso Total	106,509
Costos Directos	28,106
Utilidad Operativa	78,403
Margen Operativo	73,61
Capex	23,219
VAN	22,103
VAN / VAI	25%
Payback	18 meses

Nota. Elaboración propia

3.4 Limitaciones

Las propuestas a la empresa-target, fue entregada con una topología estrella, es decir, todas las sedes dependían de la cabecera para el acceso a internet. Sin embargo, debido a los problemas recurrentes de suministro eléctrico, se realizaron modificaciones a las propuestas iniciales.

Se encontraron que algunas sedes carecían de las condiciones adecuadas para la instalación de los equipos, lo que retrasó el inicio de las instalaciones.

CONCLUSIONES

- La solución entregada, que incluía una red MPLS con servicios integrados y gestionados de VPN, internet dedicado y ciberseguridad, mejoró el rendimiento de los enlaces y abordó satisfactoriamente las necesidades de la empresa- target.

- Se incrementaron los anchos de banda conforme al dimensionamiento detallado en el capítulo III, previniendo la saturación, como demostraron las pruebas realizadas, lo que optimizó la red de la empresa-target.

- Se configuró la QoS distribuyéndose los caudales según los requerimientos, priorizando la información crítica, mejorando la velocidad y evitando la saturación, como se mostró en las pruebas realizada en la figura 13, 14 y 15.

- Dentro de la solución se incorporó un servicio de acceso a internet a través de la nube, lo que permitió que las sedes no dependieran del acceso a internet de la cabecera. Cada sede opera de manera independiente, garantizando una mayor disponibilidad y manteniendo el mismo nivel de seguridad.

- Los dos tipos de seguridades el UTM, así como la seguridad en la nube, incluyeron diferentes características que permitieron que la red del cliente-target este protegido de ataques cibernéticos. Además, se establecieron filtros de acceso para garantizar un funcionamiento correcto y optimizar el uso del ancho de banda proporcionado.

- Se llevó a cabo la migración de todos los enlaces a fibra óptica. Como se muestra en la figura 1, la fibra presenta una menor atenuación en comparación con los enlaces de cobre, lo que posibilita aumentar los anchos de banda.

RECOMENDACIONES

1) Para un correcto funcionamiento de los equipos se recomendó a la empresa-target de tener un lugar habilitado exclusivamente para los equipos, que contara con una buena ventilación, energía, sistema a tierra, así como un sistema de alimentación ininterrumpida o Uninterruptable Power Supply (UPS, por sus siglas en ingles) para garantizar que el suministro eléctrico sea estable.

2) Para la segunda etapa del proyecto se le recomendó al cliente migrar sus servidores a la nube. Esto le permitiría prescindir del acceso a los servidores de la cabecera, reduciendo el CAPEX y se enfocara en el crecimiento de la empresa. Además, se evitaría el riesgo de la obsolescencia de los equipos.

REFERENCIAS

Barrera Orta, J. L. 2012). Ajuste analítico del rendimiento en la multiplexión de fuentes de VoIP con VAD. [Tesis de pregrado, Universidad de Sevilla, Sevilla-España]. http://bibing.us.es/proyectos/abreproy/12088

Cox, R. V., Neto, S. F., Lamblin, C. y Sherif, M. H. (2009). ITU-T Coders for Wideband, Superwideband and Fullband Speech. IEEE Communications Magazine, 106-109. https://www.researchgate.net/publication/224597598_ITU-T_coders_for_wideband_superwideband_and_fullband_speech_communication_Series_Editorial

Fortinetguru. (2016). Virtual domains. Fortinet GURU. https://www.fortinetguru.com/2016/12/virtual-domains/

García, A. (2009). Estudio de la inclusión del sistema PCE en redes GMPLS. [Tesis de pregrado, Universidad Politécnica de Catalunya, Barcelona-España]. https://upcommons.upc.edu/bitstream/handle/2099.1/8773/Proyecto%20PCE.pdf

HostingRed. (2015). Hosting Red. https://www.hostingred.com/cloud/informacion-cloud/

Huidobro Moya, J. M., & Millan Tejedor, R. J. (2006). Qué es...MPLS(MultiProtocol Label Switching). Consultoría estratégica en tecnologías de la información y comunicaciones. https://www.ramonmillan.com/tutoriales/mpls.php

Vidal, J. L. (2012). Guía de Laboratorio: "Estructura del conductor desnudo y revestido de fibra óptica". [Diapositiva PowerPoint].

Japan International Cooperation Agency (JICA) - Instituto Nacional de Investigación y Capacitación de Telecomunicaciones (INICTEL). (1988). Transmision por fibra óptica. INICTEL.

Kaspersky. (s.f.). ¿Qué es la gestión unificada de amenazas (UTM)? Kaspersky. https://latam.kaspersky.com/resource-center/definitions/utm

Multicomp. (1998). Seguridad perimetral. Multicomp. http://multicomp.com.mx/seguridad-informatica/seguridad-perimetral/

Schulzrinne, H., Casner, S., Frederick, R., & Jacobson, V. (2003). RFC 3550: “RTP: A Transport Protocol for Real-time Applications”.