

UNIVERSIDAD CATÓLICA  
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO  
MAESTRÍA EN TELECOMUNICACIONES

TEMA:

ANÁLISIS Y DISEÑO DE RED DE LA EMPRESA INFAMOTOR S.A.  
PARA INNOVACIÓN TECNOLÓGICA DE LOS SERVICIOS DE  
TELECOMUNICACIONES CON UNA ADMINISTRACIÓN  
CENTRALIZADA, OFRECIENDO ALTA DISPONIBILIDAD,  
FLEXIBILIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN CON SUS  
SUCURSALES.

AUTOR:

ING. MACIAS LOZA LEANDRO DANILO

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL GRADO  
ACADÉMICO DE MAGÍSTER EN TELECOMUNICACIONES

TUTOR:

ING. ROMERO PAZ MANUEL DE JESÚS, MSc.

Guayaquil, 19 de noviembre de 2020



UNIVERSIDAD CATÓLICA  
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO  
MAESTRÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación Análisis y diseño de red de la empresa Infamotor SA para innovación tecnológica de los servicios de telecomunicaciones con una administración centralizada, ofreciendo alta disponibilidad, flexibilidad y confidencialidad de la información con sus sucursales, fue realizado en su totalidad por Leandro Danilo Macías Loza, como requerimiento parcial para la obtención del Grado Académico de MAGÍSTER EN TELECOMUNICACIONES.

TUTOR

---

Ing. Romero Paz Manuel de Jesús, MSc.

DIRECTOR DEL PROGRAMA

---

Ing. Romero Paz Manuel de Jesús, MSc.

Guayaquil, 19 de noviembre de 2020



UNIVERSIDAD CATÓLICA  
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO  
MAESTRÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, Macías Loza, Leandro Danilo

DECLARO QUE:

El trabajo de titulación “Análisis y diseño de red de la empresa Infamotor SA para innovación tecnológica de los servicios de telecomunicaciones con una administración centralizada, ofreciendo alta disponibilidad, flexibilidad y confidencialidad de la información con sus sucursales”, previa a la obtención del grado Académico de Magíster en Telecomunicaciones, ha sido desarrollado, respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del Trabajo de Titulación del Grado Académico en mención.

Guayaquil, 19 de noviembre de 2020

EL AUTOR

---

Macías Loza, Leandro Danilo



UNIVERSIDAD CATÓLICA  
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO  
MAESTRÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, Macías Loza, Leandro Danilo

Autorizó a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del Trabajo de Titulación de Maestría titulado: **“Análisis y diseño de red de la empresa Infamotor SA para innovación tecnológica de los servicios de telecomunicaciones con una administración centralizada, ofreciendo alta disponibilidad, flexibilidad y confidencialidad de la información con sus sucursales”**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, 19 de noviembre de 2020

EL AUTOR

---

Macías Loza, Leandro Danilo

# REPORTE DE URKUND

**URKUND** Luis Córdoba Rivadeneria (luis\_cordova)

**Documento:** [TI Leandro Macías Loza.docx](#) (D02943159)

**Presentado:** 2020-10-27 17:13 (-05:00)

**Presentado por:** Luis Córdoba Rivadeneria (lcordova@yahoo.com)

**Recibido:** luis.cordova.ucsg@análisis.orkund.com

1% de estas 69 páginas, se componen de texto presente en 2 fuentes.

Lista de fuentes		Bloques
Categoría	Enlace/nombre de archivo	
	tesis final.docx	<input checked="" type="checkbox"/>
	<a href="https://docplayer.es/6049783-Universidad-nueva-esparta-facultad-de-ciencias-de-la-inf...">https://docplayer.es/6049783-Universidad-nueva-esparta-facultad-de-ciencias-de-la-inf...</a>	<input type="checkbox"/>
Fuentes alternativas		
Fuentes no usadas		

1 Advertencias   Reiniciar   Exportar   Compartir

Central Telefónica IP ( Servicio SIP Trunk)

Licenciamiento

SBC compatible

Certificado + FDQN Firewall

Habilitación del servicio de Troncal SIP en la matriz de convergencia. Instalación de equipo SBC certificado por Ms Teams en matriz principal. Configuración de direcciones IP y certificado digital en el SBC. Elaboración de un plan de marcación para Infamotor SA. Fase I: Instalación de Servicios. Configuración del servicio de troncal SIP en la central telefónica IP Yeastar y realización de pruebas de conectividad con el proveedor. Realización de llamadas entrantes y salientes a través de la central Yeastar. Configuración de políticas, perfiles de usuarios e IVR de la central Yeastar. Configuración del equipo SBC y pruebas de conectividad. Configuración del servicio de Ms Phone System Direct Routing. Habilitación de usuarios en la plataforma de Ms Office 365. Integración de Ms Teams con la central telefónica Yeastar.

Fase II: Configuración de equipos. Pruebas del servicio, puesta en producción y monitoreo. Capacitación de las funcionalidades base del servicio a usuarios finales. Fase III: Puesta en producción.

## **AGRADECIMIENTO**

Agradezco a Dios por ser mi fortaleza y darme la sabiduría para cumplir una nueva meta.

Agradezco a mis padres Danilo & Maritza por darme sus valiosos consejos, enseñarme valores fundamentales, siendo ejemplos a seguir de sencillez y humildad.

Agradezco a mi amiga-hermana Andrea Alvarado por todo el apoyo y aporte brindado en el desarrollo de la maestría.

Agradezco a la Abg. Yanina Infante por la apertura y permitirme desarrollar el proyecto de tesis en la empresa Infamotor SA.

Agradezco al Ing. Manuel Romero por ser guía y apoyo como tutor de mi trabajo de titulación.

**Leandro Danilo Macías**

## **DEDICATORIA**

A mi amada esposa Cecilia Ordoñez compañera de vida, te dedico este logro por ser mi motivación diaria, brindarme tu apoyo incondicional y empujar constantemente nuestro crecimiento como profesionales, personas y nuestra nueva etapa de padres.

A mi hijo Thiago Danilo el nuevo motor que impulsa mi vida, te dedico este logro por ser mi inspiración para seguir escalando y alcanzando todos los objetivos que nos proponemos para bienestar como familia.

Dedicado a mi abuela Sira Bertha Barahona, sin duda alguna estuvieras encantada de poder compartir juntos este logro, hoy no estas con nosotros, pero no significa que te haya dejado de extrañar y recordar todo aquello que me enseñaste.

**Leandro Danilo Macías**



UNIVERSIDAD CATÓLICA  
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO  
MAESTRÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f.   
ING. ROMERO PAZ MANUEL DE JESÚS, MSc

TUTOR

f.   
ING. CORDOVA RIVADENEIRA LUIS. MSc.  
REVISOR

f.   
ING. QUEZADA CALLE EDGAR. MSc.  
REVISOR

f.   
ING. ROMERO PAZ MANUEL DE JESÚS, MSc  
DIRECTOR DEL PROGRAMA

## ÍNDICE GENERAL

ÍNDICE DE FIGURAS .....	XII
ÍNDICE DE TABLAS .....	XIV
Resumen .....	XV
ABSTRACT .....	XVI
<b>Capítulo 1: Generalidades del proyecto .....</b>	<b>17</b>
<b>1.1 Introducción.....</b>	<b>17</b>
<b>1.2 Antecedentes .....</b>	<b>17</b>
<b>1.3 Planteamiento del problema.....</b>	<b>18</b>
1.3.2 Formulación del problema.....	19
<b>1.4 Objetivos.....</b>	<b>19</b>
1.4.1 Objetivo general. ....	19
1.4.2 Objetivos específicos.....	19
<b>1.5 Preguntas de la investigación .....</b>	<b>19</b>
<b>1.6 Hipótesis .....</b>	<b>20</b>
<b>1.7 Justificación .....</b>	<b>20</b>
<b>1.8 Metodología de investigación .....</b>	<b>20</b>
<b>Capítulo 2: Marco teórico.....</b>	<b>22</b>
<b>2.1 Modelos de estructura de red .....</b>	<b>22</b>
2.1.1 Modelo de red jerárquico. ....	22
2.1.2 Modelo de Arquitectura Empresarial. ....	24
<b>2.2 Red de área local (LAN) .....</b>	<b>28</b>
2.2.1 Tipos de interfaces LAN. ....	28
2.2.2 Hardware de redes LAN.....	30
<b>2.3 Redes inalámbricas de área local .....</b>	<b>31</b>
2.3.1 Estándares inalámbricos por área de cobertura. ....	31
2.3.2 Factores de afectación en señales Inalámbricas. ....	32
<b>2.4 Tecnologías de transporte en redes de área amplia .....</b>	<b>33</b>
<b>2.5 Protocolos de enrutamiento dinámico .....</b>	<b>37</b>
2.5.1 Protocolo EIGRP.....	39
2.5.2 Protocolo OSPF.....	40
2.5.3 Protocolo BGP.....	41
<b>2.6 Seguridad en redes y sistema de conexión.....</b>	<b>41</b>
2.6.1 Arquitectura de seguridad para empresas.....	43

2.6.2 Seguridad empresarial.....	44
<b>2.7 Tecnología VoIP .....</b>	<b>45</b>
2.7.1 Codificación de Voz.....	46
2.7.2 Protocolos de transporte y control de VoIP.....	47
2.7.3 Protocolo de Señalización SIP. ....	48
<b>Capítulo 3: Levantamiento de Información.....</b>	<b>49</b>
<b>3.1 Identificación de los requerimientos.....</b>	<b>49</b>
3.1.1 Identificar servicios y aplicaciones de red. ....	50
3.1.2 Definir la meta organizacional de la empresa. ....	54
3.1.3 Definir los objetivos técnicos. ....	54
3.1.4 Determinar las posibles limitaciones técnicas y organizacionales. ....	55
<b>3.2 Características de la red existente .....</b>	<b>56</b>
3.2.1 Información de la infraestructura existente. ....	56
3.2.2 Topología de red existente. ....	61
3.2.3 Herramientas de análisis de tráfico. ....	62
3.2.4 Análisis de la red empresarial existente. ....	63
<b>Capítulo 4: Desarrollo de la propuesta.....</b>	<b>71</b>
4.1 Modelo de arquitectura de red.....	71
<b>4.2 Selección de la infraestructura de red. ....</b>	<b>82</b>
4.2.1 Infraestructura de acceso LAN alámbrica e inalámbrica. ....	82
4.2.2 Plataformas de Seguridad de Red.....	87
4.2.3 Plataformas de Soluciones para Reuniones (Meeting).....	90
4.2.4 Infraestructura de nuevas aplicaciones y servicios.....	91
<b>4.3 Diseño de redes de comunicación.....</b>	<b>102</b>
4.3.1 Infraestructura de red LAN .....	103
4.3.2 Seguridad de la red empresarial .....	106
4.3.3 Solución de integración con proveedores.....	109
4.3.4 Solución SD-WAN con administración centralizada.....	111
4.3.5 Solución de Comunicaciones Unificadas (UC).....	117
<b>Conclusiones.....</b>	<b>122</b>
<b>Recomendaciones.....</b>	<b>123</b>
<b>Bibliografía.....</b>	<b>124</b>
<b>Anexos.....</b>	<b>129</b>
<b>Anexo No 1. Criterios técnicos para la elección de los equipos de acceso ....</b>	<b>129</b>

<b>Anexo No 2. Criterios técnicos para la elección de los equipos de núcleo-</b>	
<b>distribución colapsado .....</b>	<b>132</b>

## ÍNDICE DE FIGURAS

Figura 2.1: Diseño de red jerárquica de red de área local.....	23
Figura 2.2: Modelo de arquitectura empresarial. ....	24
Figura 2.3: Opciones de multihoming para conexión a Internet.....	26
Figura 2.4: Escenario de aplicación de VPN. ....	26
Figura 2.5: Fenómeno de refracción. ....	33
Figura 2.6: Esquema de conexión por cable modem. ....	35
Figura 2.7: Esquema de la red DWDM.....	36
Figura 2.8: Arquitectura de una red GPON. ....	37
Figura 2.9: Protocolos de enrutamiento IGP y EGP. ....	38
Figura 2.10: Distancia administrativa en los tipos de ruta. ....	39
Figura 2.11: Componentes de arquitectura de seguridad y áreas de protección. ..	44
Figura 2.12: Componentes fundamentales de un sistema VoIP.....	46
Figura 2.13: Codificación y decodificación de voz. ....	46
Figura 3.1: Organigrama de la empresa Infamotor S.A. ....	57
Figura 3.2: Dispositivos de red activos. ....	60
Figura 3.3: Topología física de dispositivos en edificio principal. ....	62
Figura 3.4: Tráfico de navegación por Internet.....	68
Figura 4.1: Secciones aplicadas del Módulo Campus empresarial.....	74
Figura 4.2: Secciones aplicadas del módulo borde empresarial. ....	76
Figura 4.3: Módulo proveedor de servicios de borde. ....	78
Figura 4.4: Módulo funcional remoto. ....	81
Figura 4.5: Esquema de integración de Yeastar con Ms Teams. ....	97
Figura 4.6: Tipo de conexión Multihoming tercera opción. ....	98
Figura 4.7: Esquema de conexión del diseño de solución tecnológica. ....	102
Figura 4.8: Topología lógica tipo estrella de Infamotor SA. ....	105
Figura 4.9: Categorías de las aplicaciones del NGFW FG-80E.....	106
Figura 4.10: Filtrado Web basado en categorías.....	107
Figura 4.11: Configuración Anti-virus opción CDR en modo proxy. ....	107
Figura 4.12: Solución SD-WAN seguras de Fortinet. ....	111
Figura 4.13: Categoría de las aplicaciones determinada por Fortinet.....	112
Figura 4.14: Ejemplo de configuración de interfaz SD-WAN.....	112

Figura 4.15: Ejemplo de configuración de criterios de load balanced. ....	112
Figura 4.16: Opciones para configuración de reglas de SD-WAN.....	113
Figura 4.17: Ejemplo de configuración de ruta por defecto SD-WAN.....	113
Figura 4.18: Configuración de seguridad a nivel de aplicaciones. ....	114
Figura 4.19: Diseño de solución SD-WAN con administración centralizada.....	114
Figura 4.20: Servicio de Soporte FortiCare. ....	115
Figura 4.21: Servicio de seguridad FortiGuard.....	115
Figura 4.22: Centralización de eventos y reportes con FortiAnalyzer.....	116
Figura 4.23: Ejemplo de integración de herramientas en FortiManager.....	117
Figura 4.24: Diseño de solución de comunicaciones unificadas.....	118
Figura 4.25: Requisitos de infraestructura de comunicaciones unificadas. ....	118
Figura 4.26: Fases de configuración e instalación de la solución de UC.....	121

## ÍNDICE DE TABLAS

Tabla 2.1: Diferentes tipos de medio para interfaces 10 GE.....	29
Tabla 2.2: Diferentes estándares para 40-100 Gbps.....	29
Tabla 2.3: Categorías de seguridad en matriz. ....	45
Tabla 2.4: Estándares de Códec. ....	47
Tabla 3.1: Resumen de servicios y aplicaciones actuales. ....	52
Tabla 3.2: Resumen de servicios y aplicaciones planificadas.....	53
Tabla 3.3: Distribución de número de empleados.....	58
Tabla 3.4: Detalle del total de puntos de red de datos y telefonía. ....	58
Tabla 3.5: Dispositivos de red activos. ....	59
Tabla 4.1: Criterio para determinar el total de interfaces en equipos de acceso... 83	83
Tabla 4.2: Capacidades mínimas de los equipos de acceso. ....	83
Tabla 4.3: Recomendación modelo de equipo para capa de acceso. ....	84
Tabla 4.4: Criterio para determinar interfaces en equipos núcleo-distribución. ... 84	84
Tabla 4.5: Capacidades mínimas de los equipos de núcleo-distribución.....	85
Tabla 4.6: Recomendación modelo de equipo para capa núcleo-distribución.....	85
Tabla 4.7: Recomendación modelo de equipo para sucursales.....	86
Tabla 4.8: Recomendación punto de acceso inalámbrico. ....	86
Tabla 4.9: Cuadro comparativo de capacidades con los diversos proveedores. ... 89	89
Tabla 4.10: Especificaciones técnicas equipos FortiGate 30E/80E. ....	89
Tabla 4.11: Cuadro comparativo de Cisco Webex y Ms Teams.....	91
Tabla 4.12: Módulos y funcionalidades de Asterik. ....	93
Tabla 4.13: Funcionalidades principales de la tecnología Denwa. ....	94
Tabla 4.14: Funcionalidades principales de la tecnología Yeastar. ....	95
Tabla 4.15: Niveles de Servicio Datacenter. ....	102
Tabla 4.16: Plan de direccionamiento IP. ....	104
Tabla 4.17: Parámetros de configuración por fase para VPN Site-to-Site.....	110

## **Resumen**

La evolución de las Tecnologías de la Información y la Comunicación (TIC) han revolucionado el mundo y su forma de hacer negocios. Actualmente, es difícil imaginar que las empresas desarrollen sus actividades y se mantengan en el mercado sin utilizar los recursos de las telecomunicaciones como telefonía, internet, entre otros. INFAMOTOR S.A es una empresa dedicada a satisfacer las necesidades del mercado automotriz mediante la importación, comercialización y distribución de repuestos y accesorios para vehículos de casi todas las marcas. Gracias a la dedicación de su fundador, Sr. Julio Infante Campoverde, la empresa ha crecido considerablemente, logrando establecer sucursales en varias ciudades del país, las mismas que mantienen comunicación permanente a través de internet. Gracias a la apertura del líder de la oficina matriz de la empresa en estudio, y con el afán de diseñar una solución tecnológica de red que permita gestionar los servicios de telecomunicaciones de INFAMOTOR S.A de forma centralizada, se procedió a analizar la infraestructura de red existente. Para tal efecto, fueron aplicados métodos y técnicas investigativas que, junto a la información de importantes autores y a la experiencia del autor, permitieron obtener un diseño que garantice alta disponibilidad, flexibilidad y confidencialidad de la información con sus sucursales. El diseño propuesto aborda las necesidades de la empresa en análisis con un enfoque modular, limitando el acceso externo y brindando seguridad en el manejo de información.

**Palabras claves:** LAN, EIGRP, OSPF, BGP, VoIP, SIP, SD-WAN.

## **ABSTRACT**

The evolution of Information and Communication Technologies (ICT) has revolutionized the world and its way of doing business. Currently, it is difficult to imagine that companies develop their activities and stay in the market without using the resources of telecommunications such as telephony, internet, among others. INFAMOTOR S.A is a company dedicated to meet the needs of the automotive market by importing, commercializing, and distributing parts and accessories for vehicles of almost all brands. Thanks to the dedication of its founder, Mr. Julio Infante Campoverde, the company has grown considerably, managing to establish branches in several cities of the country, which maintain permanent communication through the internet. Thanks to the opening of the head office leader of the company under study, and with the desire to design a technological network solution that allows to centralize management of INFAMOTOR SA telecommunications services, the existing network infrastructure was analyzed. For this purpose, investigative methods and techniques were applied with the information of important authors and the author's experience that allow to obtain a design that guarantees high availability, flexibility, and confidentiality of the information with its branches. The proposed design addresses the needs of the company in analysis with a modular approach, limiting external access and providing security in the handling of information.

**Keywords:** LAN, EIGRP, OSPF, BGP, VoIP, SIP, SD-WAN

## **Capítulo 1: Generalidades del proyecto**

Con la evolución competitiva del mercado y los avances tecnológicos, la empresa Infamotor SA necesita optimizar recursos, automatizar procesos y mejorar el desempeño de las operaciones que benefician la atención al cliente. Para esto, surgen los modelos de estructura de red aplicables para las pequeñas, medianas o grandes empresas, con el propósito de cumplir las expectativas, mejorando el rendimiento del sistema y adaptándolo a las necesidades del negocio.

### **1.1 Introducción**

Las telecomunicaciones actualmente se han constituido en una herramienta importante, para que las empresas de gestión centralizada puedan acceder a la información de forma confiable y comunicarse de manera efectiva para brindar un alto nivel de servicio hacia los clientes.

Infamotor S.A. es una empresa dedicada a satisfacer de manera directa las necesidades del mercado automotriz importando, comercializando, distribuyendo repuestos y accesorios de una gran variedad de marcas a los mejores precios. Gracias al esfuerzo del fundador de la empresa, el Sr. Julio Infante Campoverde, y la gran acogida que han tenido en el medio, el grupo INFANTE ha logrado la apertura de sucursales en algunas importantes ciudades del país.

Por el giro del negocio, Infamotor S.A. busca mejorar sus operaciones valiéndose de las Tecnologías de la Información y Comunicación (TICs) para alcanzar niveles altos de productividad que reflejen un crecimiento en el mercado, incorporando soluciones innovadoras adaptables a las necesidades empresariales que impulsen la competitividad.

### **1.2 Antecedentes**

La nueva era digital es responsable de los cambios continuos que ocurren en las redes de comunicaciones empresariales, sobre todo con la evolución de aplicaciones multimedia que demandan el incremento de velocidad de transmisión

y un alto rendimiento para compartir recursos. Por otra parte, las estrategias de mercado con la utilización de las TIC constituyen una de las herramientas más importantes para hacer a las empresas competitivas, desarrollando una revolución comercial que ofrece una mayor diversidad de servicios y productos en menor tiempo.

Infamotor SA como empresa importadora de repuestos y accesorios de las mejores marcas en el país, está enfocada en hacer más competitiva a la organización en su sector de actividad, requiriendo una solución de arquitectura de red completa que mejore la comunicación entre sucursales, distribuidores, proveedores, canales de comercialización y la experiencia del usuario. Para cumplir con estas necesidades, las marcas y proveedores han desarrollado soluciones que aportarán con beneficios para alcanzar las metas comerciales, como redes de área amplia definidas por software (Software Defined Wide Area Network, SD-WAN), herramientas de colaboración (meeting solutions), Switch Stacking (StackWise) y firewall de próxima generación (Next Generation firewall, NGFW).

### **1.3 Planteamiento del problema**

La matriz de la empresa Infamotor S.A. para los servicios de voz dispone de una central telefónica analógica con funcionalidades limitadas para la integración de servicios suplementarios, generación de indicadores de gestión y afectación en la calidad por la vulnerabilidad del medio físico.

La topología de red existente no realiza segmentación de usuarios, tampoco permite prioridades de acceso a internet por departamentos, los cuales están distribuidos por un concentrador (hub) que ocasiona tormentas de difusión (broadcast) y colisiones, reflejando lentitud en las transacciones o consultas realizadas a los catálogos de productos en las ventas.

Las sucursales tienen una disponibilidad del 98.0% con el servicio de internet que está implementado a través de un medio inalámbrico, mostrando desventajas como interferencias por el uso de bandas no licenciadas, tiempos altos de respuesta y errores de conexión en la comunicación, que afectan las negociaciones con los clientes.

La falta de un sistema de comunicación y gestión centralizada apropiado, condicionan a Infamotor S.A. disponer de herramientas claves para su desarrollo e incremento de productividad.

### **1.3.2 Formulación del problema.**

¿Cómo influye la innovación y el cambio tecnológico de las telecomunicaciones en la productividad, transformación económica y social de la empresa Infamotor S.A.?

## **1.4 Objetivos**

### **1.4.1 Objetivo general.**

Analizar y diseñar la solución de red que permita administrar los servicios de telecomunicaciones de forma centralizada, ofreciendo alta disponibilidad, flexibilidad y confidencialidad de la información desde matriz hacia las sucursales de la empresa Infamotor S.A.

### **1.4.2 Objetivos específicos.**

- Realizar el levantamiento de información sobre la infraestructura y topología de red existente, así como la interconexión de sucursales e intercambio de información hacia matriz.
- Analizar las condiciones actuales en infraestructura, seguridad y rendimiento de la red empresarial.
- Investigar el diseño de soluciones tecnológicas innovadoras como propuesta para mejorar la productividad de la empresa y estrategias comerciales.
- Determinar las funcionalidades de seguridad, protocolos de enrutamiento y alta disponibilidad que permitan fiabilidad en las conexiones.

## **1.5 Preguntas de la investigación**

- ¿Qué beneficios se tendría con una innovación tecnológica en las telecomunicaciones de la empresa Infamotor S.A.?

- ¿Podrá garantizar conectividad y flexibilidad la tecnología de acceso actualmente implementada?
- ¿Qué solución tecnológica ofrece escalabilidad sobre la marcha, en caso de fallas y congestión de red?
- ¿Qué modelo de estructura de red fiable permitirá obtener una gestión centralizada entre las sucursales y matriz?
- ¿Qué protocolos de cifrado de seguridad IP podría implementarse para garantizar la confidencialidad de información?

## **1.6 Hipótesis**

Si se implementa un modelo de estructura de red con tecnología innovadora y administración centralizada, se optimizarán las operaciones empresariales que lograrán elevar el nivel de satisfacción de los clientes de Infamotor S.A.

## **1.7 Justificación**

Los cambios e innovación tecnológica a través del desarrollo de un estudio técnico permitirán mejorar los accesos a las plataformas, prever las necesidades de los mercados, detectar nuevos productos, procesos y servicios de mayor calidad que incrementarán la competitividad a la empresa.

El resultado de esta investigación logrará reducir los costos operativos a la empresa, automatizando ciertas actividades que facultará a los profesionales en ventas que concentren su esfuerzo en nuevas técnicas y estrategias para alcanzar sus objetivos ofreciendo mejores servicios a sus clientes.

El desarrollo de una red de gestión centralizada con alta disponibilidad permitirá obtener información en tiempo real para tomar decisiones y un seguimiento al cumplimiento de metas.

## **1.8 Metodología de investigación**

De acuerdo al planteamiento del problema y los objetivos propuestos, la investigación a realizar está determinada por un conjunto de aspectos como normas, herramientas o técnicas indispensables para brindar solución, con un

enfoque analítico-sintético que separa los servicios de telecomunicaciones, topologías y plataformas para estudiar el rendimiento, procesamiento y comportamiento en la transferencia de información e integrarlas en un modelo de red robusto que mejore la producción fomentando la competitividad.

**Método analítico-sintético:** “Estudia los hechos, partiendo de la descomposición del objeto de estudio en cada una de sus partes para estudiarlas en forma individual (análisis), y luego se integran esas partes para estudiarlas de manera holística e integral (síntesis)” (Bernal, 2006).

## **Capítulo 2: Marco teórico**

Los diseños de red segmentan en capas independientes los elementos que son parte de una infraestructura tecnológica, asignando jerarquías que cumplen con funciones técnicas específicas. Sin embargo, la alta demanda de tráfico por la innovación de aplicaciones multimedia, junto con la evolución de soluciones orientadas a mejorar la producción, ha incrementado constantemente la complejidad e interconexión, creando la necesidad de modificar los diseños por un enfoque modular que facilita la escalabilidad de redes con un mayor rendimiento.

### **2.1 Modelos de estructura de red**

Con la complejidad de los diseños de red, los modelos de estructura logran simplificar los trabajos de operación, ampliación, administración y mantenimiento del departamento de TI (Tecnologías de la Información) de las empresas, incorporando ventajas técnicas que aportan al desarrollo del negocio. A continuación, los dos modelos conocidos extensamente (Ariganello, 2016):

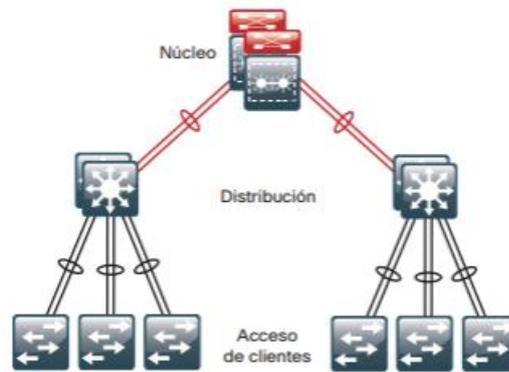
- Modelo de red jerárquico.
- Arquitectura de red empresarial.

#### **2.1.1 Modelo de red jerárquico.**

Facilita la implementación de redes, capaz de soportar los requerimientos actuales y futuros de una empresa. Consiste en dividir a la red en capas, cada una con funciones específicas y puede ser aplicado tanto para redes de área local (Local Area Network, LAN) como amplia (Wide Area Network, WAN).

La estructura modular permite utilizar un apropiado ancho de banda dentro de cada capa, brinda una fácil comprensión del diseño e identificación de puntos de falla lo cual ayuda a tener una reducción de costos en administración de red y capacitación de personal técnico.

La figura 2.1 muestra como el diseño jerárquico permite organizar la red en distintas capas, generando eficiencia, escalabilidad, inteligencia y simplicidad en la gestión.



**Figura 2.1:** Diseño de red jerárquica de red de área local.  
**Fuente:** (Vásquez & Triviño, 2019)

El modelo de red jerárquico para diseñar una red confiable incluye las siguientes capas (Ariganello, 2016):

- Capa de Acceso.
- Capa de Distribución.
- Capa de Núcleo.

#### **2.1.1.1 Capa de Acceso.**

Es aquella que brinda conectividad a los usuarios finales y presenta características como:

- Escalabilidad en velocidad de transmisión a capas superiores.
- Alta densidad de puertos y disponibilidad.
- Capacidad para ofrecer servicios de red convergente.
- Calidad de servicio.
- Seguridad de acceso.

#### **2.1.1.2 Capa de Distribución.**

Es capaz de procesar el volumen de tráfico total generado por los equipos conectados en la capa de acceso y soportar la convergencia de los dominios de broadcast, algunas de las funcionalidades son las siguientes (Reyes, 2017):

- Capacidad para integración de múltiples equipos de la capa de acceso.
- Alto procesamiento para enrutamiento de paquetes.
- Seguridad y políticas de conectividad.
- Calidad de servicio.
- Enlaces de alta velocidad redundantes entre las capas de núcleo y acceso.

### 2.1.1.3 Capa de Núcleo.

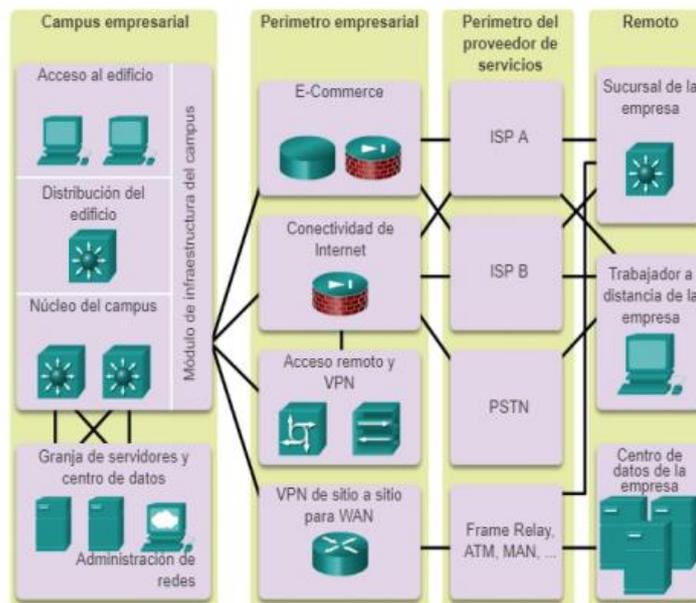
La capa de núcleo conocida como área de backbone, presenta equipos de alta capacidad para la conmutación de tráfico de forma eficiente, con funciones relevantes tales como (Reyes, 2017):

- Muy alto procesamiento para enrutamiento de paquetes.
- Alta disponibilidad en redundancia, resiliencia y baja latencia.
- Funciones avanzadas de calidad de servicio.

### 2.1.2 Modelo de Arquitectura Empresarial.

La arquitectura empresarial tiene como finalidad facilitar el diseño de redes extensas y sofisticadas por lo cual las divide en áreas y módulos (Campo, 2019):

- Módulo campus empresarial.
- Módulo área de borde o perímetro empresarial.
- Módulo proveedor de servicio.
- Módulo remoto.



**Figura 2.2:** Modelo de arquitectura empresarial.

**Fuente:** (Campo, 2019)

#### 2.1.2.1 Módulo campus empresarial.

El módulo campus empresarial está conformado por los submódulos centro de datos, campus núcleo, distribución y acceso de edificios, aplicables para los

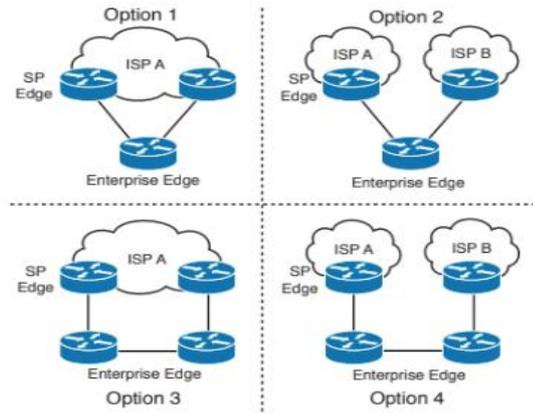
distintos tamaños de infraestructura de red de las empresas. Las principales ventajas que proporcionan son: alta velocidad de acceso y disponibilidad hacia los servidores de aplicaciones, servicios como configuración de huésped dinámico (Dynamic Host Configuration Protocol, DHCP), comunicación de voz mediante el protocolo de internet (Internet Protocol, IP), almacenamiento de archivos, entre otros (Prende & Castillo, 2019).

### **2.1.2.2 Módulo área de borde empresarial.**

El módulo área de borde empresarial permite la conectividad a los servicios de voz, video y datos hacia el exterior de la empresa, consiste en los siguientes submódulos (Bruno & Jordan, 2017):

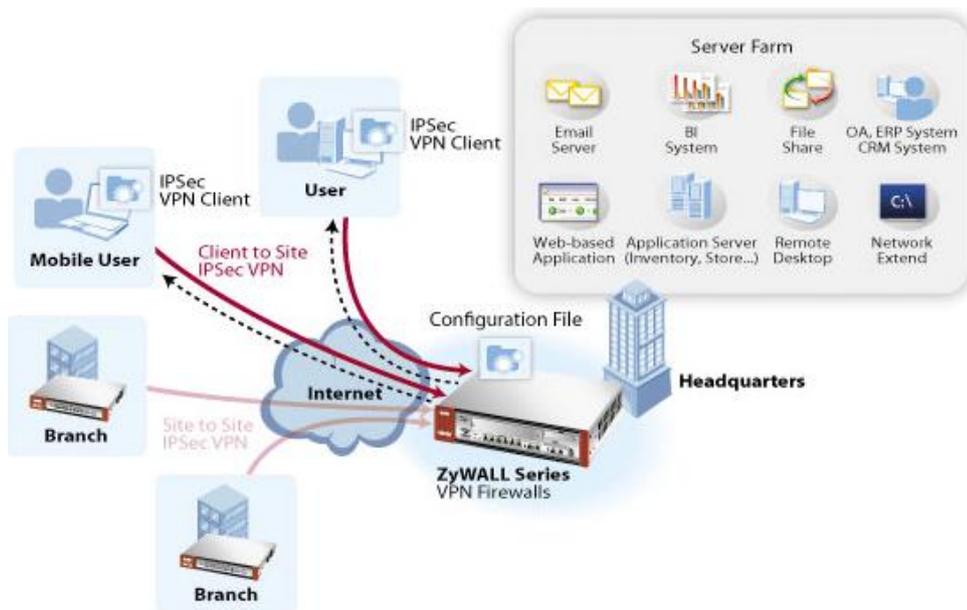
- 1. Redes y servidores de comercio electrónico:** utiliza una alta disponibilidad para la conectividad de los equipos ubicados en este submódulo, tales como (Bruno & Jordan, 2017):
  - Servidores web y de aplicaciones.
  - Servidores de base de datos.
  - Sistema de prevención de intrusos (Intrusion Prevention System, IPS).
- 2. Conectividad a Internet:** entre los componentes más relevantes de este submódulo están los siguientes (Bruno & Jordan, 2017):
  - Equipos de seguridad (Firewall).
  - Equipos de enrutamiento de borde.
  - Servidores de transferencia de archivos (File Transfer Protocol, FTP).
  - Servidores web o de transferencia de hipertexto (Hypertext Transfer Protocol, HTTP).
  - Servidores de retransmisión para la transferencia simple de correo (Simple Mail Transfer Protocol, SMTP).
  - Servidores de nombre de dominio (Domain Name System, DNS).

La figura 2.3 presenta varias opciones de solución multihoming para las conexiones con los proveedores de servicio de internet (Internet Service Provider, ISP), proporcionando redundancia y alta disponibilidad



**Figura 2.3:** Opciones de multihoming para conexión a Internet.  
**Fuente:** (Bruno & Jordan, 2017)

- Acceso remoto con red privada virtual (Virtual Private Network, VPN):** Una VPN es una combinación de factores como control de acceso, autenticación, túneles, encriptación y auditoría, utilizada para transportar tráfico TCP/IP a través de internet. Con la utilización de seguridad del protocolo de internet (Internet Protocol Security, IPSec) pueden implementarse conexiones seguras extremo a extremo, VPN site-to-site, entre sucursales y oficina central (Pomar, 2019). La figura 2.4 presenta un escenario de conexión a los servicios empresariales con la utilización de equipos de seguridad de gestión de amenazas unificadas (Unified Threat Management, UTM).



**Figura 2.4:** Escenario de aplicación de VPN.  
**Fuente:** (Zykel, 2020).

4. **Red de área amplia (WAN) empresarial:** Entre las tecnologías más utilizadas en redes de área amplia sobresalen las siguientes (**Bruno & Jordan, 2017**):

- Multiprotocolo de conmutación de etiquetas (Multiprotocol Label Switching, MPLS).
- Jerarquía digital síncrona (Synchronous Digital Hierarchy, SDH).
- Modo de transferencia asíncrona (Asynchronous Transfer Mode, ATM).
- Línea de Abonado Digital (Digital Subscriber Line, xDSL).
- Inalámbrica (wireless).
- Red óptica pasiva gigabit (Gigabit Passive Optical Network, GPON).

#### 2.1.2.3 Módulo de borde de los proveedores de servicio.

Con la evolución de las telecomunicaciones los proveedores de servicio ofrecen una gran variedad de opciones de solución empresarial (Bruno & Jordan, 2017), contenidos en la siguiente subdivisión:

- Servicio de Internet.
- Servicio de red WAN (Datos).
- Servicio de comunicación de Voz

#### 2.1.2.4 Módulo Remoto

El módulo remoto según el modelo de arquitectura empresarial integra los siguientes submódulos (Bruno & Jordan, 2017):

- 1) **Módulo sucursal:** hace referencia a oficinas o puntos de venta remotos que utilizan las conexiones de red WAN para acceder a los servicios y aplicaciones que ofrece el campus principal.
- 2) **Módulo centro de datos empresarial (*Data Center*):** se alojan los servidores de aplicación y almacenamiento garantizando una alta disponibilidad y continuidad del negocio, estos pueden ser locales o remotos e incluyen:
  - Infraestructura de red.
  - Servicios Interactivos.

- Administración del Data Center.
- 3) **Módulo Teletrabajador:** consiste en usuarios móviles o pequeñas oficinas que acceden de forma remota a los servicios de la empresa, conexiones que de forma segura se establecen a través de VPN.

## 2.2 Red de área local (LAN)

Una red de área local es una red informática de alta velocidad de transmisión de datos utilizada para interconectar dispositivos de red dentro de un espacio determinado. A continuación, los componentes que permiten la comunicación de los usuarios (Martinez, Amortegui, & Murillo, 2018):

- Tipos de interfaces LAN.
- Hardware de redes LAN.

### 2.2.1 Tipos de interfaces LAN.

La base fundamental para las tecnologías ampliamente usadas en redes LAN es Ethernet, que contiene tipos de medio a ser considerados en los diseños de solución, tales como:

- **Ethernet:** estándar 802.3 del Instituto de Ingeniería Eléctrica y Electrónica (Institute of Electrical and Electronics Engineers, IEEE) con una velocidad de transmisión de 10 Mbps Ethernet (Bruno & Jordan, 2017).
- **Fast-Ethernet:** estándar 802.3u de la IEEE, proporciona velocidades de 100 Mbps a través de cables de fibra o par trenzado no blindado (Unshielded twisted pair, UTP), utiliza detección de acceso múltiple (Carrier Sense Multiple Access Collision Detect, CSMA/CD). Los estándares más utilizados de la IEEE 802.3 son 100BASE-TX, 100BASE-T4 y 100BASE-FX (Cubillos & Manrique, 2019).
- **Giga-Ethernet:** estándar 802.3ab de la IEEE, la diferencia entre las velocidades anteriores aparece en la codificación, lo que permite tener un rendimiento de 1000 Mbps. Entre los estándares más utilizados están 1000BASE-T/LX/SX/CX cuyas especificaciones permiten utilizar cable UTP y fibra óptica (Bruno & Jordan, 2017).

- **Ten Giga-Ethernet:** estándar 802.3ae de la IEEE, define su operación para full dúplex sobre medios ópticos y eléctricos como UTP (Cubillos & Manrique, 2019). La tabla 2.1 especifica algunos de los diferentes estándares y limitaciones de distancia según el medio.

**Tabla 2.1: Diferentes tipos de medio para interfaces 10 GE.**

Tipo	Medio	Distancia
10GBASE-SR	MMF - Longitud de onda corta (850 nm)	Hasta 300 m
10GBASE-LR	SMF - Longitud de onda larga (1310 nm)	Hasta 10 Km
10GBASE-ER	SMF - Longitud de onda extralarga (1550 nm)	Hasta 40 Km
10GBASE-EW	SMF - Longitud de onda extralarga (1550 nm)	Hasta 40 Km
10GBASE-T	Cable UTP Cat. 6A	100 m

**Nota.** MMF (Multi-Mode Fiber); SMF (Single Mode Fiber).

Fuente: Autor

- **Nuevas tecnologías Ethernet:** Ha surgido un nuevo estándar 802.3ba nombrado por la IEEE para velocidades superiores a los 10 Gbps, como 40 Gbps y 100 Gbps (Bruno & Jordan, 2017). La tabla 2.2 especifica algunos de los diferentes estándares y limitaciones de distancia según el medio.

**Tabla 2.2: Diferentes estándares para 40-100 Gbps.**

Medio	Estándar 40 Gbps	Estándar 100 Gbps
30 m UTP Cat.8	40GBASE-T	-
100 m OM3 MMF	40GBASE-SR4	100GBASE-SR10
125 m OM4 MMF	-	100GBASE-SR4
10 km SMF	40GBASE-LR4	100GBASE-LR4

**Nota.** MMF (Multi-Mode Fiber); SMF (Single Mode Fiber).

Fuente: Autor

- **EtherChannel:** es una de las tecnologías desarrolladas por Cisco para agrupación de varias interfaces físicas en un solo canal lógico, conocido como port channel, utilizada para conexiones de área local switch-to-switch permitiendo el incremento de velocidad de transmisión, balanceo de carga, y redundancia. Para su funcionamiento utiliza protocolos propietarios o estándar como agregación de puertos (Port Aggregation Protocol, PAgP) de Cisco Systems y control de agregación de enlace (Link Aggregation Control Protocol, LACP) que es estándar (De Anda, 2018).

### 2.2.2 Hardware de redes LAN.

Los equipos LAN están categorizados en base al modo de operación del modelo de interconexión de sistemas abiertos (Open Systems Interconnection, OSI), los cuales son implementados según los roles y capacidades que vayan a ocupar en una solución de red. A continuación, la descripción de los más utilizados (Bruno & Jordan, 2017):

- **Concentradores (hubs):** equipos utilizados para la concentración de usuarios de las redes LAN, operan en la capa física del modelo OSI, no controlan el broadcast o dominio de colisiones; es decir, toman las tramas, amplifican la señal y los reenvían a otras interfaces (Zevallos, 2018).
- **Puentes (bridges):** dispositivos de almacenamiento y retransmisión que conectan segmentos separados de una red, operan en la capa de enlace del modelo OSI controlando los dominios de colisión. Para el reenvío de un frame realizan verificación de redundancia cíclica (Cyclic Redundancy Check, CRC) e implementan el protocolo de árbol de expansión (Spanning Tree Protocol, STP) para construir una topología de red libre de bucles (Zevallos, 2018).
- **Conmutadores (switch):** a diferencia de los bridges, utilizan circuitos integrados especializados para reducir la latencia, cada interfaz actúa como un dominio de broadcast guardando una tabla de control de acceso al medio (Media Access Control, MAC), implementan STP y trabajan en la capa de enlace del modelo OSI. Los switches no pueden controlar el broadcast en la red, pero pueden utilizar VLAN (Virtual Local Area Network,) para proporcionar una mayor segmentación de tráfico (Zevallos, 2018).
- **Enrutador (router):** equipo que toma decisiones de enrutamiento basado en las direcciones de la capa de red del modelo OSI, controlan los dominios de colisiones y broadcast que es separado por cada interfaz del router. Para el intercambio de información utilizan uno de los distintos protocolos que construyen una lista de destino de red identificando la mejor opción para alcanzar el destino (Zevallos, 2018).

## **2.3 Redes inalámbricas de área local**

Las redes inalámbricas de área local (Wireless Local Area Network, WLAN) eliminan el uso de cables, permitiendo la movilidad de los usuarios dentro de establecimientos e incluso sobre áreas metropolitanas. Las soluciones de red han adquirido un gran desarrollo, extendiéndose en los diversos sectores empresariales, proporcionando transmisión de contenido multimedia y recolección de datos, mediante el uso de tecnologías como WiFi (Wireless Fidelity, fidelidad inalámbrica) y la evolución de sus diferentes estándares (Baque, 2019).

La gran acogida de las redes inalámbricas ha generado la necesidad de proporcionar un tratamiento diferente al tráfico de datos, analizando los factores que afectan la transmisión de la señal con el fin de crear mecanismos para compensar los efectos producidos, asegurando una determinada calidad de servicio.

### **2.3.1 Estándares inalámbricos por área de cobertura.**

Las redes inalámbricas agrupan diferentes estándares por su área de cobertura o extensión geográfica, resumidos a continuación (Rao, Bojkovic, & Milovanovic, 2018):

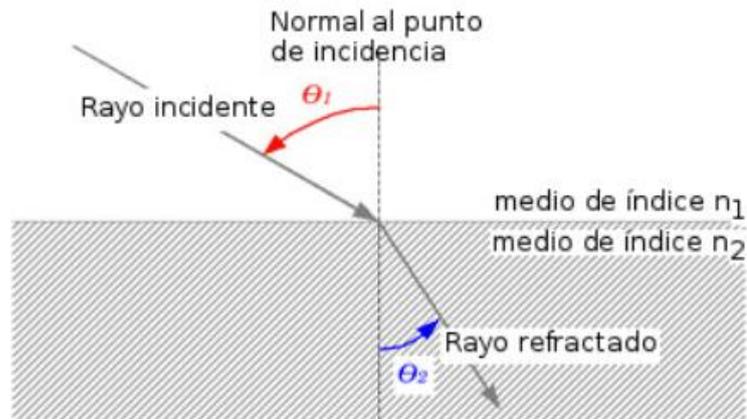
- Redes inalámbricas de área personal (Wireless Personal Area Network, WPAN):
  - Rango de distancia de 6 m.
  - Trabaja en la frecuencia de 2.4 GHz, Bluetooth.
- Redes inalámbricas de área local (Wireless Local Area Network, WLAN):
  - Rango de distancia de 100 m.
  - Trabaja en las frecuencias de 2.4 y 5 GHz.
- Redes inalámbricas de área metropolitana (Wireless Metropolitan Area Network, WMAN):
  - Cubren una mayor distancia, pero se limitan a la velocidad de transmisión que pueden brindar.
  - Tecnología de interoperabilidad mundial para acceso por microondas (Worldwide Interoperability for Microwave Access, WIMAX).

- Redes inalámbricas de área amplia (Wireless Wide Area Network, WWAN):
  - Baja velocidad de transferencia.
  - Tecnología celular.

### 2.3.2 Factores de afectación en señales Inalámbricas.

Las señales inalámbricas viajan a través de un medio fácilmente accesible por lo que pueden ser afectadas por los siguientes factores:

- **Absorción:** En las comunicaciones inalámbricas si las ondas electromagnéticas chocan con algún obstáculo, generalmente estas se debilitarán o atenuarán. La potencia que se pierde dependerá de la frecuencia de transmisión e inevitablemente por el material que esta atraviese. Los materiales más absorbentes para las microondas son el metal y el agua, debido a que las ondas electromagnéticas no podrán atravesar dicho material (García, 2019).
- **Reflexión:** Ocurre cuando las ondas entran en contacto con materiales reflectores, las propiedades de la señal reflejada son el ángulo incidente de llegada al obstáculo, la orientación y la longitud de la onda ( $\lambda$ ) (García, 2019).
- **Pérdida de señal (Free Path Loss):** Entre los factores que afectan la calidad de la señal, una de ellas es la distancia que existe entre el transmisor y el receptor. Sin obstáculos la potencia de la señal disminuye por la dispersión geométrica del frente de onda, fenómeno conocido como pérdida en espacio libre (Mejía, 2016).
- **Refracción:** Es el cambio de dirección de una onda electromagnética conforme pasa de un medio a otro de diferente densidad, variando la longitud de onda y velocidad de propagación. La refracción solo se produce si la onda incide oblicuamente sobre la superficie de separación de los dos medios, como se muestra en la figura 2.5 (García, 2019).



**Figura 2.5:** Fenómeno de refracción.  
Fuente: (García, 2019)

- **Línea de vista:** Es la capacidad de ver un dispositivo desde una ubicación sin que ningún o muy pocos elementos obstruyan la visión, siendo una de las condiciones más relevantes para implementar enlaces inalámbricos confiables (Mejía, 2016).
- **Dispersión:** Ocurre cuando hay muchos objetos en el recorrido de la onda con dimensiones pequeñas comparadas a la longitud de onda de la señal, entonces el frente de onda propagado se fragmentará en diversas direcciones, añadiéndose a las interferencias constructivas y destructivas de la misma (Mejía, 2016).
- **Múltiples trayectorias (Multipath):** La presencia de obstáculos ocasiona que se reflejen las ondas causando que múltiples copias con diferentes retardos sean recibidas, dependiendo de las diferencias en las longitudes de las ondas directas y reflejadas, la señal compuesta puede ser más larga o más pequeña que la señal origen, creando problemas como (Mejía, 2016):
  - Decaimiento de la amplitud de la señal.
  - Corrupción de la información.
  - Anulación de la señal.
  - Aumento de la amplitud de la señal.

## 2.4 Tecnologías de transporte en redes de área amplia

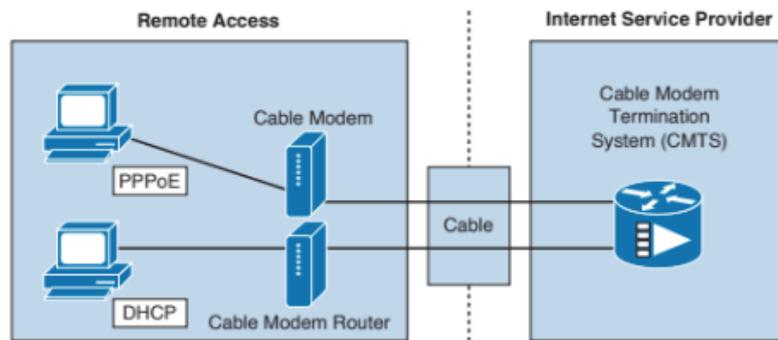
Para seleccionar una tecnología de transporte es importante analizar factores como administración de red, costo de operaciones, características del hardware,

velocidad de transmisión, disponibilidad y confiabilidad que brindarán a los servicios. Una empresa puede tener múltiples proveedores, sin embargo, para el diseño de redes WAN deben considerarse los siguientes puntos (Bruno & Jordan, 2017):

- **Acuerdo de nivel de servicio (Services Level Agreement, SLA):** define parámetros de la red como latencia, velocidad de transmisión, niveles de escalamiento, así como también tiempos de reparación en caso de alguna eventualidad, que han sido previamente acordados entre una empresa y el proveedor de servicio para garantizar la disponibilidad de la red.
- **Presupuesto y uso del servicio:** La red debe soportar los requerimientos de aplicaciones actuales y brindar flexibilidad ante un crecimiento.

La ubicación geográfica desempeña un rol clave para que las empresas dispongan de varias opciones de soluciones tecnológicas WAN, entre las de mayor relevancia están las siguientes:

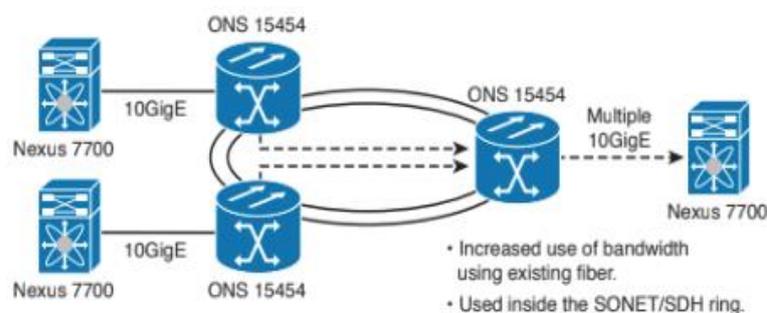
- **Línea de abonado digital (Digital Subscriber Line, DSL):** utiliza como transporte el par de cobre de una línea telefónica, pero en frecuencias distintas, ofreciendo servicios de internet y datos a través del mismo medio. Una de las tecnologías más utilizadas es la línea de abonado digital asimétrico (Asymmetric Digital Subscriber Line, ADSL) caracterizada por ofrecer alta velocidad de bajada; sin embargo, presenta limitaciones como la distancia y la vulnerabilidad de la red (Cabeza, 2018).
- **Cable:** tecnología de banda ancha para el transporte de datos por cable coaxial con la utilización de un sistema de distribución, el equipo utilizado para receptor los servicios en las instalaciones del cliente es un modem conectado a un sistema de terminación (Cable Modem Termination System, CMTS) ubicado en el ISP. Permiten la implementación de redes convergentes soportando video, voz y datos. A continuación, la figura 2.6 muestra un esquema de conexión por cable utilizando protocolos punto a punto sobre ethernet (Point-to-Point Protocol over Ethernet, PPPoE) y DHCP (Patricio, 2018).



**Figura 2.6:** Esquema de conexión por cable modem.  
**Fuente:** (Bruno & Jordan, 2017)

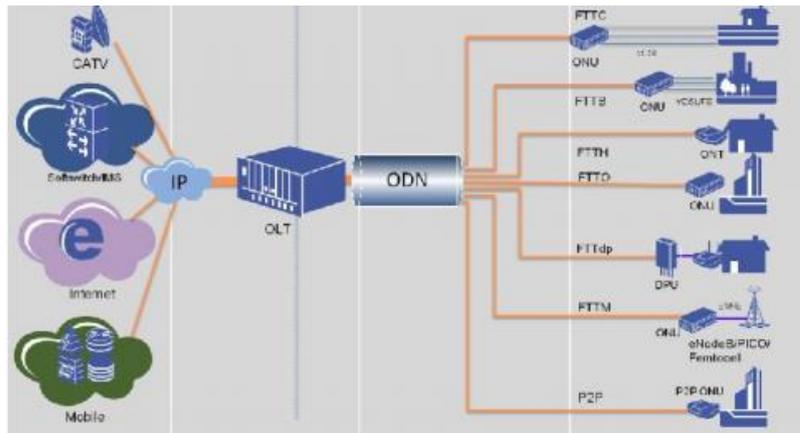
- **Inalámbrico:** Las tecnologías de red inalámbrica utilizan las ondas electromagnéticas para transportar datos y permitir la comunicación entre dos puntos, ejemplos como las redes móviles, sistema de posicionamiento global (Global Positioning System, GPS) o WiFi (Vera, 2018).
- **MPLS:** funciona marcando la cabecera de los paquetes con una etiqueta que puede ser configurada como dirección origen o con un valor de calidad de servicio (Quality of Service, QoS) diseñando rutas específicas a través de la red, los paquetes que están destinados al mismo punto final son enviados en base a la etiqueta sin una decisión de enrutamiento en cada salto. MPLS es utilizado en la implementación de ingeniería de tráfico maximizando la conmutación por el uso de etiquetas, anulando las tablas de enrutamiento (León, 2017). Los equipos que forman parte de la estructura reciben designaciones tales como:
  - Equipo de borde del cliente (Customer Edge, CE): punto donde se realiza el intercambio de información con el cliente.
  - Equipo de borde del proveedor (Provider Edge, PE): representa el ingreso a la red del proveedor de servicio
  - Equipo proveedor (Provider, P): utilizado como equipo de tránsito en el core de la red.
- **Multiplexación compacta por división en longitudes de onda (Dense Wavelength-Division Multiplexing, DWDM):** incrementa las capacidades de ancho de banda de la fibra óptica con el uso de diferentes longitudes de onda sobre la misma fibra, denominadas canales. Cada canal de fibra es equivalente a varios enlaces giga ethernet logrando aumentar

las capacidades de los servicios ofrecidos a los clientes, además integra dispositivos como enrutadores y conmutadores (Gómez, 2019).



**Figura 2.7:** Esquema de la red DWDM.  
**Fuente:** (Bruno & Jordan, 2017)

- **Red óptica pasiva giga (Gigabit Passive Optical Network, GPON):** es una red flexible de acceso con fibra óptica, diseñada para soportar una alta demanda de requerimientos de servicios residenciales y corporativos a un menor costo de implementación. La figura 2.8 muestra la arquitectura GPON, de dónde se resumen a continuación los componentes principales (Vega, 2017):
  - Terminal de línea óptico (Optical Line Terminal, OLT): ubicada en la oficina central (Central Office, CO) del proveedor de servicio, permite la integración con el backbone a través de puerto uplink de alta capacidad.
  - Red de distribución óptica (Optical Distribution Network, ODN): consiste en la distribución de las redes de fibra óptica que brindan cobertura y atención a las necesidades de los usuarios.
  - Terminal de red óptico (Optical Network Terminal, ONT): corresponde al equipo terminal colocado en las instalaciones del cliente.



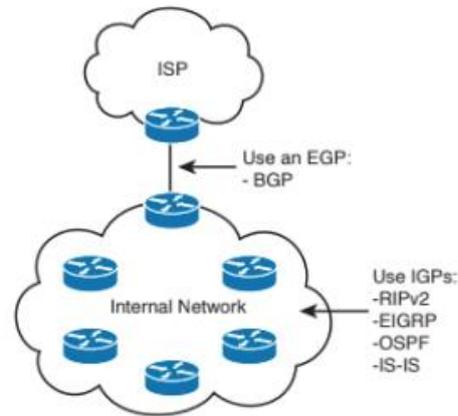
**Figura 2.8:** Arquitectura de una red GPON.  
**Fuente:** (Vega, 2017)

## 2.5 Protocolos de enrutamiento dinámico

Los protocolos de enrutamiento dinámico actualizan sus tablas según los cambios que experimente la red a través de los recursos que utilizan para identificar el estado de la misma, presentan diferentes tipos de características que son utilizadas para la selección adecuada a los requerimientos empresariales. Entre las propiedades principales están las siguientes:

- **Vector distancia, estado de enlace o ambas:** los protocolos de vector distancia utilizan un algoritmo para crear las tablas de enrutamiento, las rutas son publicadas como vectores de dirección que representan la IP del próximo destino y distancia como el número de saltos. Una desventaja es la limitación del número de saltos en redes extensas y el tiempo que tardan en actualizar las tablas de enrutamiento teniendo una convergencia lenta. En los protocolos de estado de enlace, los routers originan información sobre su direccionamiento, interfaces conectadas y el estado de las mismas. Esta información es compartida con los equipos que forman parte de la red, cada router hace una copia y reenvía la información sin cambios. Los equipos ejecutan un algoritmo de ruta más corta realizando un cálculo independiente de las mejores rutas hacia cada destino. Las actualizaciones se realizarán si existe un cambio en la topología, de lo contrario se realizarán en el tiempo establecido por defecto (Velez, 2018).
- **Interior o exterior:** los protocolos de enrutamiento también se categorizan como puerta de enlace interior (Interior Gateway Protocol, IGP) y puerta de enlace exterior (Exterior Gateway Protocol, EGP). Los

IGP están diseñados para establecer comunicación dentro de la red de una organización, sistemas intrautónomos, mientras que EGP permite la comunicación entre dominios exteriores, sistemas interautónomos (Velez, 2018).



**Figura 2.9:** Protocolos de enrutamiento IGP y EGP.  
**Fuente:** (Bruno & Jordan, 2017)

- **Enrutamiento interdomino sin clase:** por sus siglas CIDR (Classless Interdomain Routing) permite la publicación de grandes redes (supernetting) entre equipos (López, 2018).
- **Máscara de subred de longitud fija o variable:** por sus siglas VLSM (Variable Length Subnet Mask) conserva las direcciones dentro de una red, dando una visión de las redes pequeñas (subnetting) (López, 2018)
- **IPv4 o IPv6:** IPv6 soportado por las últimas versiones de los protocolos de enrutamiento.
- **Distancia administrativa:** para los equipos que ejecutan varios protocolos de enrutamiento es posible que tengan más de una ruta para alcanzar el mismo destino, cada router asigna una distancia administrativa al protocolo que tenga configurado. Por lo tanto, para seleccionar la mejor ruta, es considerada la longitud de coincidencia del prefijo (prefix length), si estas coinciden el siguiente parámetro a considerar es la distancia administrativa cuya selección de ruta será la de menor valor (López, 2018), de acuerdo al detalle mostrado en la figura 2.10.

Tipo de ruta	Valor distancia administrativa
Directamente conectado	0
Rutas estáticas	1
Rutas sumarizadas	5
Rutas EBGp	20
Rutas EIGRP	90
Rutas IGRP	100
Rutas OSPF	110
Rutas IS-IS	115
Rutas Rip	120
Rutas EIGRP (externo)	170
Rutas BGP	200

**Figura 2.10:** Distancia administrativa en los tipos de ruta.  
**Fuente: (López, 2018)**

### 2.5.1 Protocolo EIGRP.

El protocolo de enrutamiento de puerta de enlace interior mejorado (Enhanced Interior Gateway Routing Protocol, EIGRP) “es un protocolo vector distancia desarrollado por Cisco, que usa el mismo sistema de métricas sofisticadas que su antecesor IGRP (Interior Gateway Routing Protocol) y que utiliza DUAL (Diffusing Update Algorithm) para generar las tablas de topología” (Ariganello, 2016). Las principales características y beneficios que ofrece el protocolo IGP son descritas a continuación:

- Soporta VLSM y CIDR para la asignación escalable de direcciones IP.
- No envía actualizaciones periódicas, pero sí parciales cuando hay un cambio en la topología y puede utilizar autenticación de algoritmo de resumen del mensaje 5 (Message Digest Algorithm 5, MD5).
- Resume automáticamente (autosummarize) las redes y puede compartir carga en rutas de costo desigual.
- Es un protocolo avanzado que utiliza las características de vector distancia y estado de enlace.
- Para determinar rutas libres de bucles usa el algoritmo DUAL.

- La distancia administrativa es de 90, para rutas sumarizadas de 5 y para las externas de 170.
- Utiliza cinco tipos de paquetes: hello para el descubrimiento de adyacencias, ack o reconocimiento para confirmar la recepción de un paquete de actualización, update contiene la información de enrutamiento para alcanzar los destinos, query encuentra sucesores factibles a un destino y reply encargado de responder los paquetes de consulta (Ariganello, 2016).

### **2.5.2 Protocolo OSPF.**

“El protocolo OSPF (Open Shortest Path First) está especificado en la RFC2328. Se trata de un protocolo abierto, de estado de enlace, que funciona como protocolo interno, dentro de un entorno delimitado (AS o Autonomous System)” (Dordoigne, 2018). Las principales características y beneficios que ofrece el protocolo IGP son descritas a continuación:

- Es un protocolo avanzado que utiliza las características de estado de enlace con el algoritmo Dijkstra que calcula la ruta más corta para alcanzar los destinos (Dordoigne, 2018).
- Soporta VSLM, puede compartir carga en rutas de igual costo y tiene una distancia administrativa de 110.
- A través de multicast se comunica con los dispositivos, envía anuncios de estado de enlace para informar a los demás equipos sobre sus interfaces, la tabla de enrutamiento es construida individualmente por cada router.
- Utiliza paquetes hello para el descubrimiento de adyacencias en los cuales emite información como: autenticación con MD5, prioridades, identificadores del área y de router (Dordoigne, 2018).
- Usa áreas como medida preventiva para reducir el tamaño de la base datos, inundación de publicaciones e incremento de procesamiento de los equipos.
- Los equipos que participan en la configuración del protocolo están clasificados en : internos que están dentro de una misma área (Area Border Router, ARB), conectados a más de un área (Autonomous System Boundary Router, ASBR) publicando rutas externas aprendidas de otros

protocolos o redistribución y backbone que al menos una interfaz pertenece al área 0 (Dordoigne, 2018).

### **2.5.3 Protocolo BGP.**

EL protocolo de puerta de enlace (Border Gateway Protocol, BGP) “se trata de un protocolo externo, es decir, que permite el intercambio de las tablas de enrutamiento entre dos Autonomous System. Funciona basándose en reglas de decisión tomadas a lo largo de los AS cruzados, en lugar de una métrica” (Dordoigne, 2018). Las principales características y beneficios que ofrece el protocolo EGP son descritas a continuación:

- Protocolo de enrutamiento interdominio utilizado para intercambio de información entre sistemas autónomos, específicamente para establecer conectividad a Internet.
- No utiliza las características de estado de enlace ni vector distancia, sino enrutamiento vectorial.
- Soporta CIDR para enviar paquetes basados en prefijos.
- Los términos de uso del protocolo pueden ser interno BGP (iBGP) para adyacencias internas utilizando un mismo sistema autónomo y externo BGP (eBGP) para conexión de adyacencias exteriores usando diferentes sistemas autónomos. La distancia administrativa para rutas iGBP es 200 y eBGP 20 (Velez, 2018).
- Para la selección de rutas utiliza algunos atributos como next-hop, preferencia local, origen, rutas de sistema autónomo, métrica o comunidad (Velez, 2018).
- El peso se puede aplicar a una ruta local o todas las aprendidas a través de un peer, las de mayor asignación establecen prioridad, pero su configuración no es intercambiada en las actualizaciones (Velez, 2018).

## **2.6 Seguridad en redes y sistema de conexión.**

A pesar de establecer modelos de red o tener instalada alguna normativa de seguridad no se puede garantizar una red protegida o evitar a todo intruso de la web, para que esto suceda debería desconectarse el sistema de la red, pero no se

podría acceder al mismo. Sin embargo, se puede garantizar un entorno de seguridad razonable siguiendo las buenas prácticas a continuación descritas:

- **Routers:** con el anuncio de redes proporcionan acceso, por lo que hay que asegurarlos para minimizar la posibilidad de poner en amenaza la red:
  - Bloqueo de acceso remoto por telnet y a través del protocolo SNMP (Simple Network Management Protocol, protocolo de administración de red simple).
  - Control de acceso a través de un servidor AAA (Authentication, Authorization, and Accounting).
  - Registros de los eventos sucedidos (log) con el uso de un servidor (syslog).
  - Desactivación de interfaces y servicios no utilizados.
- **Switches:** se deben tomar ciertas precauciones para evitar riesgos de seguridad tanto en L2 como L3:
  - Desactivar las interfaces que no requieren ser utilizadas.
  - Las VLAN de servicio deben ser únicas y configuradas en las interfaces correspondientes.
  - Configuración de VLAN privadas para filtrar paquetes entre origen y destinos conectados a un switch local.
- **Host:** existen muchas plataformas de sistemas operativos, aplicaciones y hardware, con ello actualizaciones y parches que los hacen visibles en la red. A causa de tal efecto, los hosts son atacados con mayor frecuencia por los hackers y a medida que aumenta la complejidad de los sistemas incrementa la probabilidad de fallos. Se recomienda tener los sistemas actualizados con los parches más recientes, analizando en funcionamiento con los componentes restantes del sistema evaluando antes de implementarlo en un entorno de producción.
- **Redes:** Uno de los ataques más comunes es la denegación distribuida de servicio (Distributed Denial-of-Service, *DDoS*), haciendo que algunas máquinas envíen datos falsos de forma simultánea hacia una dirección IP afectando no solo un host determinado, sino todo el funcionamiento de la red perdiendo solicitudes legítimas. Una de las formas de mitigar es a través del ISP limitando la velocidad en la interfaz asignada para la

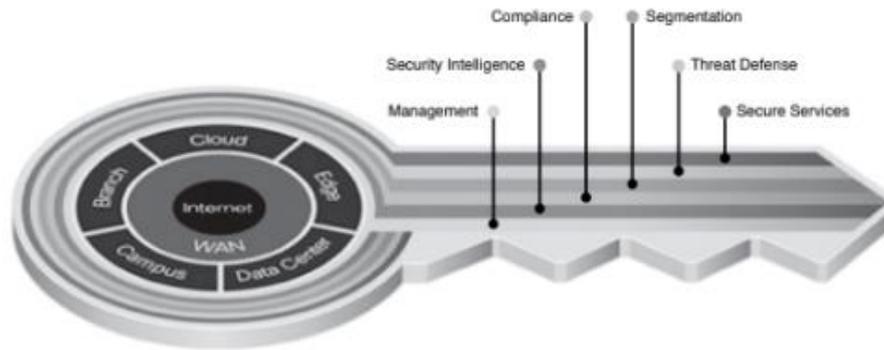
empresa, eliminando la mayor parte de tráfico no deseado cuando supera la velocidad de transmisión disponible.

- **Aplicaciones:** Están sujetas a numerosos errores creando puntos vulnerables en la seguridad donde sistemas como el de detección de intrusos (*Intrusion Detection System*, IDS) los intenta identificar, enviando notificaciones o tomando medidas correctivas de forma automática. Los IDS pueden ser basados en host (HIDS) o en red (NIDS) por lo que se recomienda la utilización de ambos para tener un sistema de detección de intrusos completa. Un NIDS al detectar un ataque de un host puede impedir el acceso a la red durante un determinado tiempo, normalmente debe utilizarse en tráfico TCP para que la probabilidad de un falso positivo sea muy baja por ser más difícil de falsificar.

### **2.6.1 Arquitectura de seguridad para empresas.**

La arquitectura de seguridad mostrada en la figura 2.11, proporciona una guía para la elaboración de diseños e implementación de redes seguras y confiables, mejorando la confidencialidad, integridad y disponibilidad de recursos en actividad de negocios críticos. A continuación, las ventajas de disponer de una arquitectura que simplifica la complejidad de la red al protegerla por áreas:

- Seguridad en los servicios utilizando control de acceso, VPN y encriptación (Bruno & Jordan, 2017).
- Protección contra ataques brindando visibilidad para los cyber ataques o actividades sospechosas (Bruno & Jordan, 2017).
- Seguridad inteligente proporciona detección de malware.
- Mecanismos de segmentación y mitigación de amenazas basados en políticas, creando límites entre usuarios e información (Bruno & Jordan, 2017).
- Administración de sistemas y equipos, llevando gestión de cambio del flujo de trabajo.



**Figura 2.11:** Componentes de arquitectura de seguridad y áreas de protección.  
**Fuente:** (Bruno & Jordan, 2017)

Las soluciones de protección de red avanzada consisten en disponer de appliance de seguridad, router y switch con características de inteligencia integrada:

- **Appliance de Seguridad:** equipo con alto rendimiento a nivel de prevención/detección de intrusos (Intrusion Detection and Prevention, IDP), antivirus, antispam, filtrado de contenido, control de acceso, túneles IPSec VPN y la capa de puertos seguros (Secure Sockets Layer, SSL) integrados en un solo equipo.
- **Router:** equipo que incluya sistemas operativos con características de seguridad, firewall, soporte de VPN a través de IPSec y SSL.
- **Switch:** capaces de soportar ataques como denegación de servicios (Denial Of Services, DoS), hombre en el medio (man-in-the-middle), con integración de módulos de seguridad que proporcionan firewall y conexiones seguras a través de VPN.

### 2.6.2 Seguridad empresarial.

La arquitectura de seguridad proporciona uno de los sistemas más amigables frente a las amenazas de red empresarial, ofreciendo una mejor protección a los distintos requerimientos de las localidades, basados en las siguientes soluciones:

- **Seguridad en matriz:** la seguridad debe ser total con el uso de tecnologías, protocolos, equipos y soluciones implementadas en las capas del modelo de red jerárquico, agrupados en categorías como ilustra la tabla 2.3.

**Tabla 2.3: Categorías de seguridad en matriz.**

<b>Categoría</b>	<b>Soluciones de Seguridad</b>
Identidad y control de acceso	802.1X, ACLs, Firewall
Detección y mitigación de ataques	NetFlow, Syslog, SNMP, RMON, IPS
Protección de infraestructura	AAA, TACACS, RADIUS, SSH, SNMPv3, IGP-EGP MD5, seguridades a nivel L2
Administración de seguridad	CSM, Cisco ISE, ACS

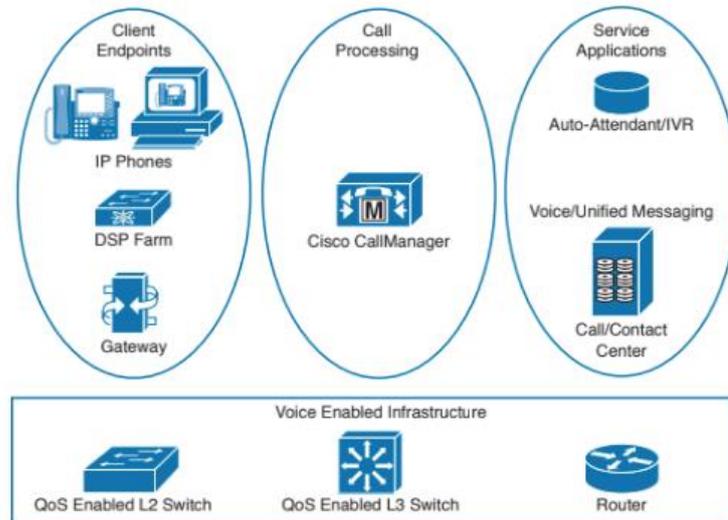
**Nota.** ACL (Access Control List), SNMP (Simple Network Management Protocol), RMON (Remote Network Monitoring), AAA (Authentication, authorization, and Accounting), TACACS (Terminal Access Controller Access Control System), RADIUS (Remote Authentication Dial-In User Service), SSH (Secure Shell), CSM (Cisco *Security Manager*), ISE (*Identity Services Engine*), ACS (*Access Control System*)

**Fuente:** (Bruno & Jordan, 2017)

- **Seguridad en Data Center:** aloja aplicaciones y servidores que pueden contener información crucial para la empresa; por lo cual, no puede verse comprometida y requiere una alta disponibilidad a través del uso de tecnologías y soluciones de protección, considerando el rendimiento (performance), de lo contrario podrían tener riesgos como el acceso no autorizado a información crítica o servidores comprometidos atacando al resto dentro de la red.
- **Seguridad en equipos de borde y red WAN empresarial:** encargados de proporcionar conectividad a la empresa a través de redes públicas o privadas, deben integrar múltiples funcionalidades con opciones de seguridad en las transferencias de información entre localidades y la conexión hacia Internet para prevenir acceso de atacantes que puedan comprometer la confidencialidad e integridad de la información.

## 2.7 Tecnología VoIP

El proceso de convertir la voz en paquetes y enviarlos a través de una red de datos es lo que se conoce como VoIP (Voice over IP), garantizando que los paquetes lleguen a su destino en el tiempo (QoS), con métodos adecuados de codificación y decodificación (códec) brindando la seguridad respectiva, encriptación (Reyes Galarza, 2017). La figura 2.12 ilustra la implementación de esta tecnología con cuatro componentes fundamentales: clientes finales, procesamiento de llamadas, aplicaciones de servicio e infraestructura (Bruno & Jordan, 2017).



**Figura 2.12:** Componentes fundamentales de un sistema VoIP.  
**Fuente: (Bruno & Jordan, 2017)**

### 2.7.1 Codificación de Voz.

La conversión de voz de analógico a digital tiene tres pasos fundamentales que son: filtrado, muestreo, y digitalización. El rango de frecuencia de la voz es de 300 Hz hasta 3400 Hz aproximadamente, pero los codecs han sido configurados para filtrar sobre los 4000 Hz, para tal efecto se muestrea la señal utilizando modulación por amplitud de pulso (Pulse Amplitude Modulation, PAM) para finalmente convertir la amplitud muestreada en códigos binarios a través de la modulación de pulsos codificadas (Pulse Code Modulation, PCM) (Bruno & Jordan, 2017).



**Figura 2.13:** Codificación y decodificación de voz.  
**Fuente: (Bruno & Jordan, 2017, p. 581)**

Cada codec proporciona un nivel de fidelidad al audio original y cierta calidad de voz los cuales son medidos a través del puntaje de opinión promedio (Mean Opinion Score, MOS), la tabla 2.4 muestra un resumen de los estándares más utilizados.

**Tabla 2.4: Estándares de Códec.**

Códec	Tasa de bits	MOS	Descripción
G.711u	64 kbps	4.1	PCM, <i>Mu-law</i> usada en Norte América y Japon.
G.711a	64 kbps	4.1	PCM, <i>A-law</i> usado en Europa y sistemas internacionales.
G.726	16/24/32/40 Kbps	3.85	AD-PCM
G.728	16 kbps	3.61	LD-CELP
G.729	8 kbps	3.92	CS-ACELP
G.723.1	6.3 Kbps	3.9	MPE-MLQ
G.723.1	5.3 Kbps	3.65	ACELP

**Nota.** AD-PCM (Adaptive differential pulse-code modulation), LD-CELP (Low- Delay Code Excited Linear Prediction), CS-ACELP (Conjugate Structure Algebraic Codebook Excited Linear Prediction), MPE-MLQ (Multipulse Excitation–Maximum Likelihood Quantization)

Fuente: (Bruno & Jordan, 2017, p. 581)

### 2.7.2 Protocolos de transporte y control de VoIP.

Los protocolos de transporte en tiempo real (Real Time Protocol, RTP) y de control de transporte (Real Time Control Protocol, RTCP) operan en la cuarta capa del modelo OSI sobre el protocolo sin conexión de datagramas de usuario (User Datagram Protocol, UDP). RTP se encarga de la agregación de marcas de tiempo y el número de secuencias en la información del encabezado, que permiten al receptor ordenar los paquetes y eliminar los leves retrasos para proporcionar una reproducción de audio sin problemas (Vinueza, 2015).

- Las transmisiones RTP funcionan en una dirección, al tratarse de una conversación bidireccional los dispositivos establecerán una por cada dirección, donde es elegido un número de puerto de forma aleatoria incluso UDP desde 16.384 hasta 32.767. En la cabecera de información del protocolo el campo tipo de carga útil (Payload Type) es utilizado para identificar el tipo de tráfico audio o video (Vinueza, 2015).
- El protocolo RTCP es activado al establecer una llamada y su función principal consiste en generar el informe de estadísticas de los dispositivos que participan en la misma tales como paquetes perdidos, conteo, retrasos y sus variaciones (jitter); para tal efecto, es establecida una sesión separada sobre UDP usando un puerto impar del mismo rango desde 16.384 hasta 32.767 (Vinueza, 2015).

### **2.7.3 Protocolo de Señalización SIP.**

El protocolo de inicio de sesión (Session Initiation Protocol, SIP) definido por el grupo de trabajo de ingeniería de internet (Internet Engineering Task Force, IETF), fue desarrollado específicamente para telefonía IP, encargado de iniciar y concluir sesiones multimedia (Bruno & Jordan, 2017). La comunicación entre los miembros de una sesión puede ser a través de tráfico unicast, multicast o una combinación. Adicionalmente incorpora protocolos como:

- Protocolo de transmisión en tiempo real (Real Time Streaming Protocol, RTSP), control de entrega en los medios de transmisión.
- Protocolo de descripción de sesión (Session Description Protocol, SDP), describe las sesiones multimedia.
- Protocolo de anuncio de sesión (Session Announcement Protocol, SAP), publica sesiones multimedia a través de tráfico multicast.
- RTP y RTCP, transportación de datos en tiempo real.
- Protocolo de reservación de recurso (Resource Reservation Protocol, RSVP), reserva el ancho de banda de la red (Bruno & Jordan, 2017).

### Capítulo 3: Levantamiento de Información

Para realizar el levantamiento de información de la infraestructura de red de la empresa Infamotor S.A., fueron utilizados los pasos recomendados de las dos primeras fases del modelo PPDIIO (Preparación, Planificación, Diseño, Implementación, Operación, Optimización) de Cisco que cumple con las diferentes etapas en que puede dividirse el ciclo de vida de una red (Singh, 2017). El enfoque de la metodología consiste en:

- **Identificación de los requerimientos:** radica en el levantamiento de información de las necesidades de los usuarios y empresa, asociado a la fase de Preparación.
- **Características de red existente:** basada en la evaluación del funcionamiento, rendimiento y calidad del servicio de la red, haciendo un análisis de las falencias para determinar la infraestructura necesaria para cumplir con los requerimientos. Este paso está asociado con la fase de Planificación.

#### 3.1 Identificación de los requerimientos

El edificio matriz de la empresa INFAMOTOR S.A., está ubicado estratégicamente al norte de la ciudad de Guayaquil, dispone de una infraestructura de uso de 9 años aproximadamente a partir de su construcción, dedicada principalmente a la comercialización de repuestos automotrices. El crecimiento de la marca, incorporación de más colaboradores y extensión de puntos de ventas han provocado que la red inicial tenga que adaptarse a la demanda de los nuevos requerimientos para la prestación de servicios. Por lo cual, es preciso realizar un análisis que permita determinar la situación actual, seguridad de la información y la exigencia al cambio de infraestructura que garantice el correcto funcionamiento e integración de nuevos recursos.

Para la obtención de los requerimientos fue realizada una entrevista a la jefa de operaciones y analista técnico de la empresa, como resultado de lo cual permitió obtener información con datos confiables referentes a las fortalezas y deficiencias de la infraestructura de red. Para la recopilación se consideraron los siguientes pasos:

- Identificar servicios y aplicaciones de red.
- Definir la meta organizacional de la empresa.
- Definir los objetivos técnicos.
- Determinar las posibles limitaciones técnicas y organizacionales.

### **3.1.1 Identificar servicios y aplicaciones de red.**

Los datos proporcionados en el levantamiento de información junto con el análisis de los procesos internos que involucran la utilización de software para ejecución de tareas en las actividades del día a día, permitieron identificar las aplicaciones actuales, planificadas y la importancia de cada una de ellas sobre los servicios ofrecidos a los clientes internos o externos, clasificándolas en la siguiente distribución:

- Servicios y aplicaciones actuales.
- Servicios y aplicaciones planificadas.

#### **3.1.1.1 Servicios y aplicaciones actuales.**

Los servicios y aplicaciones actuales son las herramientas de cooperación que disponen los usuarios para la ejecución de las tareas o automatización de los procesos. A continuación una breve descripción de los existentes:

- **Servicio DHCP:** facilita la configuración de red de los ordenadores de forma dinámica, la asignación de direcciones IP están fuera de rango y son otorgados por un tiempo determinado (12 horas).
- **Servicio FTP:** es utilizado para el intercambio de archivos, haciendo referencia a carpetas que contienen los manuales de usuario o fichas técnicas (datasheet), las conexiones emplean métodos de autenticación y uso del puerto 21/TCP.
- **Servicio web:** los anuncios de las promociones, productos, catálogos y servicios están disponibles para los clientes mediante el sitio [www.infamotor.com](http://www.infamotor.com) (puertos 80/TCP, 443/TCP) que aprovecha Internet para promocionar la empresa, aumentando la posibilidad de crear nuevos negocios y generando una comunicación 24/7 inclusive con los proveedores.

- **Servicio de correo electrónico:** logra el intercambio de mensajes con envío de texto o archivos digitales que informan a los clientes y usuarios, utilizando Zimbra como agente de transferencia de correo, SMTP como protocolo de transporte con el puerto 465/TCP para el envío/recepción, IMAP (Internet Message Access Protocol) para el acceso a la lista de mensajes de forma remota con el puerto 993/TCP y como método de cifrado SSL.
- **Aplicaciones de Ofimática:** la empresa utiliza el software de Microsoft Office para la ejecución de diferentes tareas y funciones de oficinas con aplicaciones que permiten crear, modificar, organizar, comunicar, entre otras, tales como: Word, Excel, Access, Power Point y Outlook.
- **Aplicación de videoconferencia:** es utilizado Skype como la herramienta para la ejecución de videoconferencia, chat online, compartición de archivos y comunicación a los números móviles o fijos. Está hospedada en los dispositivos de escritorio, tabletas y teléfonos celulares.
- **Software ERP (Enterprise Resource Planning):** los procesos son gestionados de forma conjunta a través del software de Gestión de Recurso Empresarial; en otras palabras: la actividad económica, gestión de bodega, recursos humanos, compras de materiales, gestión de ventas, reportes, analítica, etc., pueden ser administrados de forma íntegra. SAP (Sistemas, Aplicaciones y Productos) proporciona una arquitectura basada en módulos con una gran cantidad de aplicaciones y herramientas conectadas entre sí para el manejo de los bienes de la empresa.
- **Servicio de Internet:** la velocidad de transmisión para edificio matriz es de baja capacidad y para sucursales 1 Mbps con asignación de IP privadas, las cuales utilizan el mecanismo de traducción de direcciones de red (Network Address Translation, NAT) para navegación. El servicio está implementado con tecnología inalámbrica.
- **Servicio de telefonía:** la comunicación telefónica convencional para el edificio matriz incorpora 8 líneas de entrada a una central privada (Private Branch Exchange, PBX), brindando 24 extensiones con características de Fax, llamadas en espera, llamada de conferencia, identificador, bloqueo, etc. Cada una de las sucursales de forma independiente dispone de una línea analógica.

- **Servicio de seguridad:** con soluciones de endpoint para los ordenadores ha sido integrado a Kaspersky como protección, control de aplicaciones, administración y mitigación de amenazas, entre otros aspectos de alta relevancia que brinda el producto. Las licencias están vigentes y fueron adquiridas por cada dispositivo.

La tabla 3.1 proporciona un resumen de los servicios y aplicaciones existentes, obtenidos en el levantamiento de información.

**Tabla 3.1: Resumen de servicios y aplicaciones actuales.**

<b>Servicio / Aplicación</b>	<b>Velocidad de Transmisión</b>	<b>Importancia</b>	<b>Comentario</b>
DHCP	Baja	Alta	Servicio local
FTP	Alta	Alta	
WEB	Alta	Critica	
Zimbra	Media	Alta	Utilización de IMAP
Ofimática	Baja	Alta	Aplicaciones locales
Skype	Media	Baja	
ERP	Alta	Critica	
Internet	Alta	Alta	
Telefonía	-	Media	Líneas analógicas
Kaspersky	Baja	Critica	

Fuente: Autor

### **3.1.1.2 Servicios y aplicaciones planificadas.**

Los servicios y aplicaciones planificadas están enfocados en la integración de herramientas que reduzcan la mano de obra, optimicen el tiempo de ejecución de actividades, sustituyan los procesos manuales, mejoren constantemente los procedimientos, establezcan medidas de seguridad para protección de la información e impulsen el crecimiento de la empresa. Cabe agregar, que el asesoramiento brindado para la identificación de opciones de solución, lograron proyectar las siguientes:

- **Software CRM (Customer Relationship Management):** considerada principalmente para mejorar el nivel de servicio ofrecido a los clientes, logrará crear un valor agregado en las relaciones comerciales (venta, marketing, post-venta) que permitan incrementar la confianza y los

ingresos por ventas. La funcionalidad del ERP asegura la integración con herramienta de gestión empresarial como CRM.

- **Aplicaciones de colaboración:** la innovación tecnológica brinda un sin fin de beneficios, entre los cuales está instar la obtención de resultados haciendo que las reuniones web sean más productivas. Por lo cual, se estima la integración de una solución que permitirá incorporar usuarios desde cualquier dispositivo o lugar, compartiendo información y manteniendo la seguridad de la información.
- **Servicio de Datos:** con el propósito de integrar a las agencias a los servicios y plataforma del edificio matriz, la contratación de enlaces de datos establecerá conectividad hacia las sucursales de forma privada y segura, replicando las políticas de control del edificio matriz, junto con la administración de conexiones de forma centralizada.
- **Servicio VoIP:** el sistema de telefonía IP integrado a soluciones informáticas obtendrá grandes prestaciones que aportarán al crecimiento de ventas, como la incorporación de smartphones, control de calidad en la atención a los clientes, facilidad de crecimiento y ahorro en costos de operación.
- **Servicio de Acceso Remoto:** pensando en la flexibilidad de los usuarios para conexiones seguras a los servicios de la empresa fuera de la jornada laboral o desde cualquier lugar del mundo, las soluciones de acceso remoto a través de VPN ayudarán a mejorar la productividad aportando con el teletrabajo.

**Tabla 3.2: Resumen de servicios y aplicaciones planificadas.**

<b>Servicio / Aplicación</b>	<b>Velocidad de Transmisión</b>	<b>Importancia</b>
CRM	Media	Critica
Colaboración	Media	Alta
Datos	Media	Alta
VoIP	Media	Alta
Acceso Remoto (VPN)	Media	Alta

Fuente: Autor

### 3.1.2 Definir la meta organizacional de la empresa.

En la entrevista realizada a la jefa de operaciones, dió a conocer que la empresa impulsa un proceso de mejora a un corto plazo, gracias al incremento de las ventas en sus productos, proyecta un crecimiento en tamaño y campo de actividad. Entre las modificaciones previstas estarán considerados aspectos cualitativos y cuantitativos como la creación de nuevas áreas que apuntan a tener ventajas competitivas sobre un entorno tan dinámico:

- **Área de gestión de servicio:** tendrá como propósito aumentar la satisfacción del cliente, identificando las necesidades y creando las oportunidades que ayuden a mejorar el servicio. La incorporación de nuevas herramientas como el CRM permitirá conocer, comprender y solventar las carencias de la empresa dando un trato personalizado a los clientes.
- **Área de soluciones:** se enfocará primordialmente en la innovación que dará un valor agregado a los servicios y productos, cubriendo las expectativas de los usuarios, constituyéndose como uno de los factores importantes que fideliza al cliente con la empresa.
- **Sucursales:** tienen como objetivo aumentar las ventas y cobertura en diversos sectores del país, facilitando el acceso y la comodidad a los clientes.

### 3.1.3 Definir los objetivos técnicos.

La innovación tecnológica permitirá promover un cambio en la forma de interactuar con los clientes, creando una red adaptable a las renovaciones continuas y optimizable a los procesos internos de la empresa. Para lograr este propósito, fueron identificadas las necesidades que consiguen determinar los requerimientos técnicos, descritos a continuación:

- Mejorar los tiempos de respuesta entre dispositivos de la red local para evitar retardos en el intercambio de información.
- Disminuir los períodos de falla e inactividad de la red con soluciones de alta disponibilidad respaldadas en niveles de acuerdo de servicio (SLA).

- Gestión de red simplificada con información confiable del funcionamiento de los equipos que permita identificar eventos significativos y establecer mantenimientos preventivos.
- Fácil administración de una red escalable, capaz de soportar una proyección de crecimiento, y adaptable a la mejora continua de la tecnología.
- Mitigar riesgos de acceso a la información mediante dispositivos que brinden una protección eficaz a las amenazas de tráfico malicioso, análisis de los protocolos de intercambio de datos, restricciones de acceso limitadas por usuarios, protección de la información asegurando la continuidad de los servicios, confiabilidad en las conexiones locales y remotas.
- Establecer control de calidad en las llamadas telefónicas con un sistema que permita obtener estadísticas, grabaciones, enrutamientos por horarios de trabajo, abierta a integración de nuevos servicios que incremente la productividad, simplifiquen el trabajo a los usuarios y brinden a la empresa una ventaja competitiva.
- Modernización tecnológica de las plataformas e infraestructura que impulsen la productividad, competitividad en el mercado, generando un mayor valor en los productos y alto grado de diferenciación en los servicios que se ofrecen a los usuarios internos y externos.

#### **3.1.4 Determinar las posibles limitaciones técnicas y organizacionales.**

Las restricciones técnicas y organizacionales pueden contener parámetros que limiten el diseño de una solución técnica, como los identificados a continuación:

- Personal técnico limitado, el headcount de Infamotor S.A. incluye únicamente un analista en el edificio principal, por lo que las sucursales deben tener una solución centralizada.
- Cronograma de trabajo, los permisos de ingreso considerando una fase de implementación serían otorgados únicamente para los fines de semana.
- La velocidad de transmisión actual no admite la integración de nuevas aplicaciones virtualizadas.

## 3.2 Características de la red existente

En la identificación de componentes de red existentes fue realizado un análisis de sus especificaciones técnicas, incluyendo las herramientas utilizadas para monitorear el tráfico de datos de las diferentes áreas de trabajo, así como las ventajas y limitaciones que ofrece la topología implementada. La obtención de la información consideró los siguientes aspectos:

- Información de la infraestructura existente.
- Topología de red existente.
- Herramientas de análisis de tráfico.
- Análisis de la red empresarial existente.

### 3.2.1 Información de la infraestructura existente.

La red de área local conecta una gran cantidad de estaciones de trabajo dentro del edificio matriz, las cuales comparten recursos e intercambian información entre las áreas que constituyen la empresa. Para documentar y determinar el diseño ajustable a las necesidades empresariales debió hacerse una recopilación de datos de la situación actual sobre los siguientes componentes:

- Información organizacional.
- Infraestructura física.
- Infraestructura lógica.

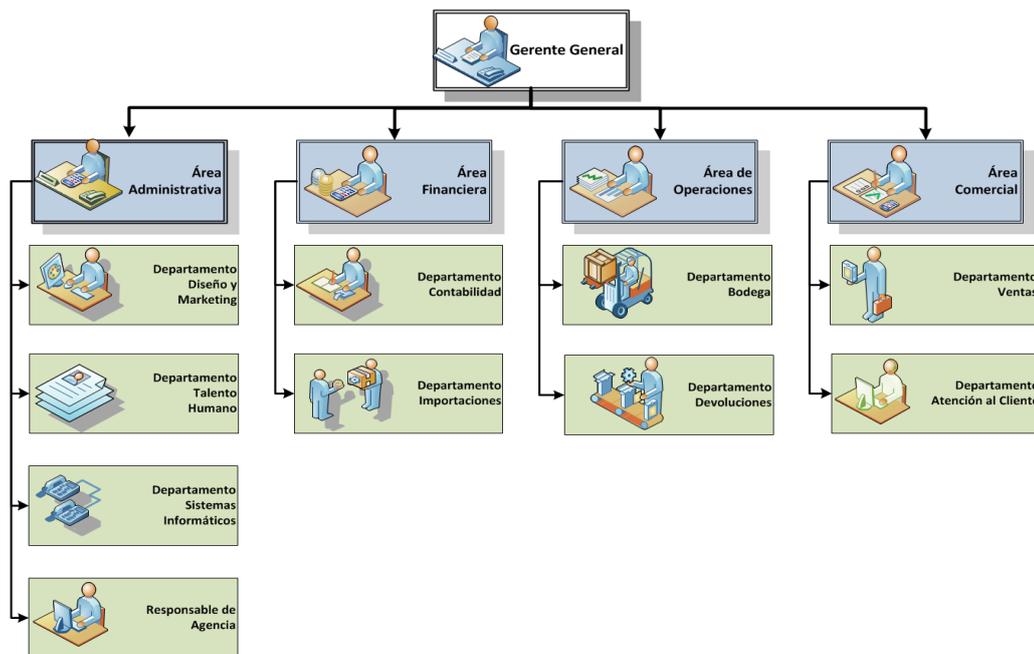
#### 3.2.1.1 Información organizacional.

La información organizacional permitió conocer las funciones que desempeña la empresa, saber cómo está estructurada, entender la relación que existe entre los distintos departamentos en los procesos y definir los niveles de jerarquía. Para el presente estudio fueron recogidos los siguientes datos:

- **Estructura organizacional:** las áreas y departamentos encargados de desarrollar las actividades que desempeña la empresa son detalladas a continuación:
  - Área Administrativa: prioridad alta, entre sus tareas está el control de la documentación de la empresa que engloba actividades de gestión,

marco legal, investigación de mercado, funcionamiento tecnológico de la empresa y demás funciones.

- Área Financiera: prioridad alta, encargados del manejo de los estados financieros, llevando un control de los recursos y cumplimiento con el proceso contable.
- Área de Operaciones: prioridad alta, encargada de almacenar, mantener y despachar los productos, también vela por la calidad, garantía y confianza de los clientes.
- Área Comercial: prioridad alta, engloba las actividades de venta de los productos, identificando las necesidades del mercado y determinar cómo satisfacer las mismas, dando un servicio de calidad a los clientes e impulsando las promociones, constituida como uno de los motores para los ingresos de la empresa.



**Figura 3.1:** Organigrama de la empresa Infamotor S.A.  
**Fuente:** Autor

- **Número de empleados:** en base a la información del INEC (Instituto Nacional de Estadísticas y Censos) sobre las variables de clasificación para definir el tamaño de una empresa, Infamotor S.A. está dentro del grupo Mediano “A” en la actividad económica comercial (Chávez,

Campuzano, & Betancourt, 2018), con un total de 50 empleados distribuidos de acuerdo a las áreas existentes, tal como detalla la tabla 3.3.

**Tabla 3.3: Distribución de número de empleados.**

<b>Número de Empleados</b>		
<b>Área</b>	<b>No Mujeres</b>	<b>No Hombres</b>
Administrativa	7	5
Financiera	5	4
Comercial	5	10
Operaciones	2	12
<b>Total 50 Empleados</b>		

Fuente: Autor

### 3.2.1.2 Infraestructura física de red.

La infraestructura de red está conformada por un conjunto de materiales conductores, que son el transporte de señales eléctricas u ópticas, conectados a los dispositivos de red que hacen posible el intercambio de información. Posteriormente están listados los componentes identificados en la solución existente:

- **Tipos de cables:** entre los cables utilizados como medio de transmisión para los servicios de telecomunicaciones de la empresa, resaltan los siguientes:
  - Cable UTP categoría 3 de dos pares utilizado para el servicio de telefonía analógica.
  - Cable UTP categoría 6 de cuatro pares utilizado para el servicio de transmisión de Datos, Internet y para el sistema de CCTV (Circuito Cerrado de Televisión).

**Tabla 3.4: Detalle del total de puntos de red de datos y telefonía.**

<b>Puntos de Red Datos - Telefonía</b>			
<b>Ubicación</b>	<b>Departamento</b>	<b>Cat. 3</b>	<b>Cat. 6</b>
Segundo Piso	Contabilidad	1	6
	Talento Humano	1	2
	Importaciones	1	2
	Ventas	1	4
	Bodega	1	2
Planta Baja	Sistemas Informáticos		1
	Diseño - Marketing		1
	Atención al Cliente	1	1
	Devoluciones		1
Exterior	Sucursales	2	5
<b>Total</b>		<b>8</b>	<b>25</b>

Fuente: Autor

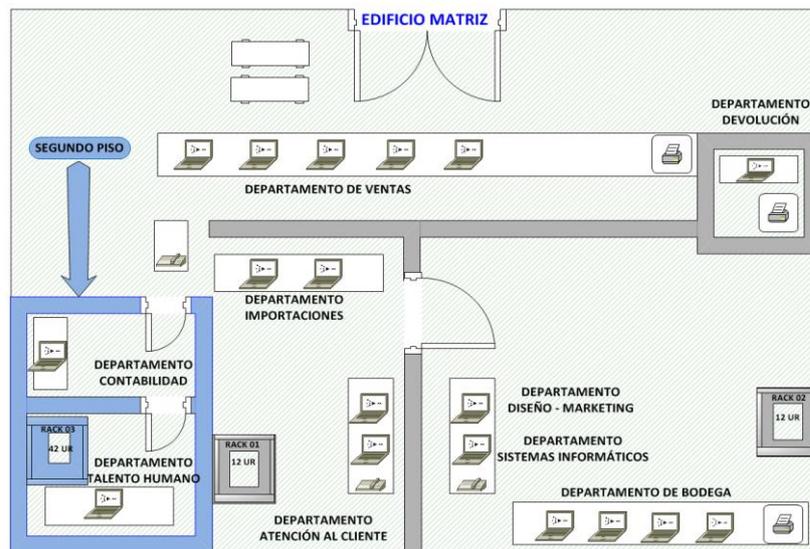
- **Dispositivos de red:** los equipos implementados que permiten la conexión de los dispositivos de usuario final (computadoras, impresoras, teléfonos, etc.) a la red son los siguientes:
  - Hub: fueron identificados algunos modelos de equipos, colocados en cascada para interconectar la red local como: 3Com SuperStack de 24 interfaces eléctricas, TP-LINK de 8 y 16 interfaces eléctricas.
  - Router: para la conexión con las redes externas está implementado un router Mikrotik que dispone 5 interfaces eléctricas 10/100 Base T.
  - Central telefónica: la comunicación telefónica de la empresa es llevada a cabo con una central analógica Panasonic KX-TES824 que soporta hasta 8 líneas y 24 extensiones.
  - Router Inalámbrico: la conexión WiFi es proporcionada por un equipo TP-LINK dual-band, es decir, frecuencias de 2.4 y 5 GHz cumpliendo con los estándares 802.11 b/g/n.
  - Servidores: las aplicaciones y servicios están implementadas en servidores ProLiant de HPE (Hewlett Packard Enterprise) muy eficiente en sus funciones con una alta capacidad de procesamiento.

**Tabla 3.5: Dispositivos de red activos.**

Ubicación	Cantidad	Dispositivo	Marca	Descripción
Segundo Piso	1	Hub	3Com SuperStack	24 interfaces eléctricas
	1	Hub	TP-LINK	8 interfaces eléctricas
	1	Router	Mikrotik	5 interfaces eléctricas
	1	Server	HPE ProLiant	procesadores Intel Xeon
	1	Server	HPE ProLiant	procesador Intel Xeon
	1	Server	HPE ProLiant	procesador Intel Xeon
Primer Piso	2	Hub	3Com SuperStack	24 interfaces eléctricas
	5	Hub	TP-LINK	8 interfaces eléctricas
	1	Router	TP-LINK	WiFi dual-band, 802.11 b/g/n
	1	Central Telefónica	Panasonic	soporta hasta 8 líneas y 24 extensiones
Sucursales	2	Router	Mikrotik	5 interfaces eléctricas
	2	Hub	TP-LINK	16 interfaces eléctricas
<b>Total 19 Dispositivos</b>				

Fuente: Autor

- **Proveedor de servicio:** el proveedor utiliza la tecnología inalámbrica como red WAN en banda no licenciada de 5 GHz para el servicio de Internet tanto para matriz como para las agencias, con enlaces punto a punto totalmente independientes. Los equipos implementados son marca Ubiquiti en modo de operación access point, con una velocidad de transmisión simétrica sin compartición.
- **Ubicación del rack:** el edificio principal tiene un total de tres racks para alojamiento de equipos como muestra la figura 3.2, distribuidos por pisos: en la planta baja se encuentran dos de pared (Rack 01, Rack 02) con 12 UR y en la segunda planta uno de piso (Rack 03) con 42 UR. Cada uno de las estructuras alberga panel de conexión (patch-panel), regletas eléctricas y los dispositivos de la infraestructura de red existentes.



**Figura 3.2:** Dispositivos de red activos.

**Fuente:** Autor

### 3.2.1.3 Infraestructura lógica de red.

La información de infraestructura lógica hace referencia a las configuraciones que utilizan los usuarios para estar comunicados a través de los dispositivos que forman parte de la red local implementada, entre las más relevantes fueron verificadas las siguientes:

- **Direccionamiento IPv4:** con la utilización del enmascaramiento de direcciones IPv4 como una de las funciones del mecanismo NAT, la red

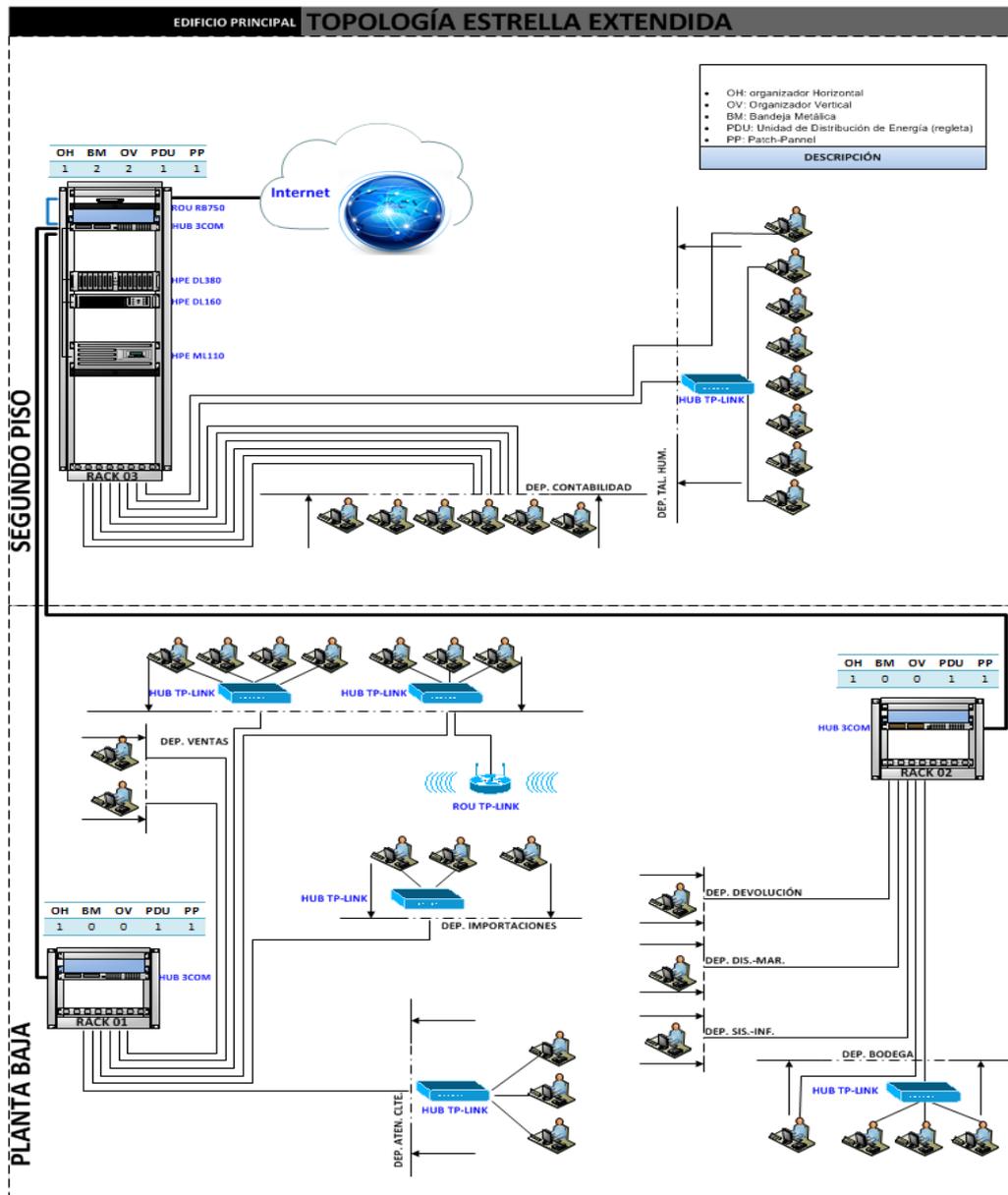
interna del edificio principal tiene configurado un segmento de red privado correspondiente a una clase C, el cual está representado por la red 192.168.10.0/24 distribuido de forma dinámica hacia cada usuario mediante el servicio que ofrece el protocolo DHCP configurado en el router Mikrotik.

- **Tipo de enrutamiento:** las redes de área local del edificio matriz y sucursales tienen únicamente salida a Internet de forma independiente, por lo cual utilizan rutas estáticas en cada uno de sus equipos de enrutamiento (ruta por defecto).
- **Listas de control de acceso:** la denegación o el permiso del flujo de tráfico está dado por privilegios que permiten tener acceso a determinados objetos (puertos, redes, dominios, etc.) a través de reglas definidas en seguridad informática.
- **Tráfico de red:** la transmisión de datos y video convergen en la infraestructura de red, compartiendo el mismo dominio de broadcast y colisión.

### 3.2.2 Topología de red existente.

Con la infraestructura de red existente en el edificio principal la topología de red pudo diferenciarse en dos aspectos: física, representa el esquema de conexión de dispositivos; y lógica, la forma en la que fluye la información. Los tipos a los cuales corresponden son descritos a continuación:

- **Topología física:** es tipo estrella extendida debido a que existe un concentrador central que enlaza a otros que tienen dispositivos directamente conectados, ilustrados en la figura 3.3.
- **Topología lógica:** es un tipo Bus dado que la información que emite un dispositivo de red es replicada por el concentrador a todos los que se encuentran conectados, es decir, el flujo de información actúa como si estuvieran conectados a través de un mismo medio.



**Figura 3.3:** Topología física de dispositivos en edificio principal.

**Fuente:** Autor

### 3.2.3 Herramientas de análisis de tráfico.

La herramienta utilizada para análisis de desempeño de red y monitoreo es Cacti, encargado en la medición de velocidades de subida (upstream) y bajada (downstream) de información, con la generación de gráficos obtenidos de la recopilación de datos del equipo de enrutamiento a través del protocolo SNMP, la cual ha permitido tener un enfoque general para determinar que la capacidad adquirida requiere mejoras.

### **3.2.4 Análisis de la red empresarial existente.**

Una vez conocidas las condiciones actuales de la red empresarial, se busca identificar los requerimientos tecnológicos necesarios para el crecimiento continuo de Infamotor S.A., determinando que conservar, mejorar y eliminar sobre la infraestructura existente. A continuación, se dan a conocer los aspectos más importantes considerados para el análisis:

- Análisis de objetivos comerciales.
- Análisis de la infraestructura de red.
- Análisis del rendimiento de la red.
- Análisis de seguridad de red.

#### **3.2.4.1 Análisis de objetivos comerciales.**

La empresa Infamotor S.A. busca a través de la tecnología de la información aumentar la productividad, los ingresos económicos, el indicador de liquidez y su participación en el mercado. Tiene como enfoque crear un entorno abierto y colaborativo, fomentando una relación interactiva online de clientes, proveedores, vendedores y usuarios internos, para de este modo, reducir el tiempo de atención a los requerimientos.

Uno de los grandes propósitos de la empresa en análisis es proteger a la organización de actividades ilegales de los usuarios por el mal uso de los servicios de TI, acogiéndose a estándares y procesos que ayudarán a garantizar la prestación efectiva de los mismos, preservando la divulgación involuntaria de datos privados que puedan causar impacto en las operaciones comerciales.

El departamento gerencial de Infamotor S.A. requiere características de alta disponibilidad y resiliencia que avalen el éxito empresarial con la continuidad de operaciones de la fuerza de ventas, siendo esta el área más crítica para el desarrollo del negocio.

Por lo anteriormente expuesto, pueden listarse los objetivos comerciales principales que deben ser considerados en el diseño de red:

- Expandir el negocio a nuevos mercados.
- Incrementar las ventajas competitivas en el segmento.

- Aumentar la productividad de los dependientes.
- Actualizar las tecnologías obsoletas.
- Evitar la interrupción de las operaciones por temas de seguridad con resiliencia ante desastres naturales.
- Ofrecer nuevos servicios y reducir los tiempos de atención.
- Hacer que el centro de datos sea más eficiente en el uso de recursos.

Para determinar la viabilidad del diseño de una solución que cumpla con los requerimientos comerciales, fueron evaluados los recursos vinculados con la situación actual: técnicos, operacionales y financieros.

- **Factibilidad técnica:** la infraestructura tecnológica que permite llevar a cabo la actividad de la empresa tiene componentes tan diversos que han superado el tiempo de vida promedio como enrutadores y concentradores (hub) sin un modelo de red jerárquico, si bien han sostenido múltiples procesos no podrán soportar la tendencia de crecimiento operativo. Por lo tanto, debe considerarse la adquisición de nuevo equipamiento con una arquitectura de red que permita mejorar los procesos y cumpla con las exigencias de la empresa.
- **Factibilidad operacional:** de considerarse la implementación de la propuesta de mejora tecnológica, tendría que llevarse a cabo una serie de actividades operativas que implicaría: cambios en la topología de red, integración de nueva infraestructura, modificación en las configuraciones de protocolos, desarrollo de nuevas políticas de seguridad de información, control y mantenimiento de red de las sucursales, entre otras. Sin embargo, en un mercado tan competitivo las propuestas de los proveedores ofrecen métodos y opciones que abarcan la puesta en funcionamiento; por lo cual, el analista de red existente está calificado para seguir llevando a cabo sus actividades integrando nuevas funciones de monitoreo, gestión de las plataformas y controles de acceso, lo que califica este recurso como viable.
- **Factibilidad financiera:** la empresa es sostenible y rentable lo que hace que la probabilidad de factibilidad incremente, aún más con la incorporación de nuevas tecnologías que permitan fortalecer la estrategia de negocio, automatizar los procesos y medir indicadores que agilicen la

toma de decisiones. Para la puesta en marcha, deberá existir una aprobación de presupuesto por parte de la gerencia destinado a un plan de mejora tecnológico (compra de equipos, licencias de software, mantenimientos, capacitaciones, horas de consultoría y soporte) que dentro de sus beneficios aportará con el cumplimiento de los objetivos comerciales.

En consecuencia, el presente estudio propone un diseño de solución que aborda las necesidades empresariales con un enfoque modular para que exista un límite al acceso externo, manejo de información segura, teniendo un centro de datos eficiente que dispersa las funciones críticas considerando recuperación ante desastres y la continua convergencia de las redes.

#### **3.2.4.2 Análisis de la infraestructura de red.**

Al realizar un análisis de los componentes que permiten la comunicación entre los dispositivos de los usuarios de forma interna y externa a la empresa Infamotor S.A., fueron detectadas las siguientes condiciones:

- Las características técnicas de los dispositivos de red que tienen como función principal brindar conectividad a los usuarios están obsoletas, incapaz de responder a la evolución tecnológica mostrando incompatibilidad, limitaciones y desactualizaciones. Esto retrasa el trabajo, dificultando la adaptación a las necesidades y exigencias de mercado.
- La red de cable telefónico, conectores y canaletas que conforman el sistema de cableado estructurado corresponde a categoría 3, el mismo que presenta ciertas desventajas a la integración de la tecnología VoIP.
- La red de cable de datos, conectores y canaletas que conforman el sistema de cableado estructurado corresponde a categoría 6, capaz de responder a los avances tecnológicos (redes convergentes) especialmente por la capacidad de velocidad de transmisión que pueda soportar.
- Tomando como referencia la norma ANSI/TIA/EIA 568-C.1 para el componente de distribución horizontal de cableado estructurado que conecta las áreas de trabajo con los repartidores horizontales (ubicados en el armario de telecomunicaciones) en rutas planas (Mariño, 2017), el resultado del análisis fue el siguiente:

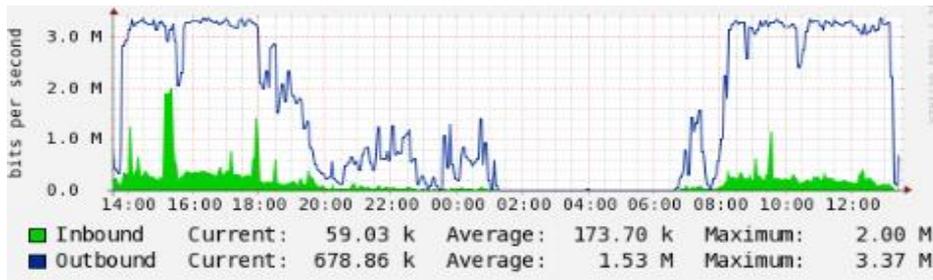
- El cielorraso tiene un sistema de distribución para transportar los cables horizontales, esto facilita el mantenimiento, reubicación de puntos de red y evita colocar los cables cerca de fuentes de emisiones electromagnéticas.
  - La estructura del cableado sigue una topología estrella hacia los determinados puntos de convergencia identificados por piso.
  - La distancia horizontal de los puntos está dentro de los parámetros permitidos, es decir no excede los 90 m desde el panel de conexiones hasta las salidas en el área de trabajo (faceplate).
- Tomando como referencia la norma ANSI/TIA/EIA 568-C.1 para el componente de distribución central de cableado estructurado que interconecta los armarios de telecomunicaciones con la sala de equipos en rutas troncales (Mariño, 2017), el resultado del análisis fue el siguiente:
- El tendido del cableado troncal cumple una topología estrella con cables UTP categoría 6, presentando un solo nivel de interconexión hasta la sala de equipos lo que reduce puntos de falla y simplificación en los mantenimientos.
  - No existen empalmes en el cableado vertical, lo cual cumple con las recomendaciones de la normativa.
  - Existe un sistema de distribución vertical que evita las emisiones electromagnéticas o protección al cableado a lo largo del recorrido.
  - La distancia máxima del cableado vertical está dentro de los valores permitidos por la norma.
- Siguiendo con las recomendaciones de la norma ANSI/TIA/EIA 568-C.1 para los componentes de repartidores horizontales, distribuidor principal (sala de equipos) y áreas de trabajo (Mariño, 2017), las condiciones de la infraestructura del edificio son las siguientes:
- El cableado horizontal que converge en los repartidores horizontales termina en un patch-panel con elementos de interconexión adecuados.
  - Los equipos activos colocados en los repartidores horizontales y distribuidor principal no disponen de los cables de interconexión o patch-cords adecuados.
  - Las tomas en las áreas de trabajo no superan la distancia de 5m, desde el faceplate hasta el equipo, recomendada para el cable de conexión.

- Los cables UTP en las áreas de trabajo terminan en conectores “jacks”.
- Siguiendo las recomendaciones de las normas de puesta a tierra para los sistemas de telecomunicaciones en edificios comerciales, TIA-607-B-1 (Mariño, 2017), las condiciones fueron las siguientes:
  - Cumple con la disponibilidad de un conductor de tierra desde el aterramiento principal del edificio hasta la barra de tierra para telecomunicaciones en el cuarto de equipos, colocado de forma directa e independiente, es decir, está aislado sin compartir el uso de canaletas metálicas.
  - Las características de cable están bajo normativa con la dimensión 6 AWG (American Wire Gauge), cubierta de color verde y colocación adecuada de etiquetas.
  - La barra de tierra para telecomunicaciones o RGB (Rack Grounding Bussbar) sigue la norma con las medidas mínimas: espesor de 6 mm, ancho 50 mm y de largo 482,6 mm.
  - Carece de conductores de tierra que conecten los equipos de telecomunicaciones a la RGB.
- Disponibilidad de un sistema de energía ininterrumpida ante posibles eventualidades que puedan provocar pérdida de información o retardos en la ejecución de las actividades operativas de la empresa.

### 3.2.4.3 Análisis del rendimiento de la red.

El análisis del rendimiento de la red fue abordado de manera práctica, determinando los umbrales de consumo y escalabilidad de la empresa en su infraestructura actual. Los factores considerados para el estudio fueron los siguientes:

- **Utilización:** define la medida de cuanto ancho de banda para navegar por internet es utilizado durante un tiempo específico, expresada en porcentaje establece como recomendación no superar el 70%. Sin embargo, la red en análisis tiene un valor del 100% verificando una saturación del valor contratado (3 Mbps) durante las horas de jornada laboral, demostrado en la figura 3.4.



**Figura 3.4:** Tráfico de navegación por Internet.

**Fuente:** Autor

- **Rendimiento (Throughput) de los equipos:** determina la cantidad de datos que pueden ser transmitidos por unidad de tiempo, es decir, los paquetes por segundo (pps) que debe procesar un dispositivo de red. Las características de throughput del router son capaces de soportar el ancho de banda contratado; no obstante, a medida que la velocidad incrementa los paquetes empiezan a descartarse, lo cual reduce la tasa de transferencia que debería incrementar linealmente con la carga ofrecida, esto debido al producto de la integración de algunos dispositivos de red que no cumplen con las características técnicas que requiere la demanda.
- **Eficiencia:** representa una forma útil de medir el rendimiento de la red a través de la efectividad al realizar el envío de tráfico. El presente caso de estudio muestra una topología lógica de bus con un único dominio de colisión, es decir, las tramas (unidad de datos de L2) entre dispositivos conectados a la red son emitidas de forma simultánea provocando choques (colisiones), también se presenta un solo dominio de broadcast en la que un paquete identificado con una dirección IP específica es emitido a cada host, lo que ocasiona deficiencia en la red por consumo inapropiado de los recursos y la sobrecarga que se genera para obtener el resultado deseado.
- **Retraso (delay):** las aplicaciones de audio/video experimentan interrupciones debido a las fluctuaciones de tiempo en las transmisiones, fundamentalmente por la baja tasa de transferencia de datos y de la latencia acumulada en conmutación y enrutamiento de paquetes que depende de las características técnicas de los dispositivos (arquitectura, circuitos, software, CPU y memoria RAM), sin considerar el efecto que tendrían las funcionalidades de QoS, IPSec, listas de control de acceso, etc.

- **Tiempo de respuesta:** es el más notorio por los usuarios, dado que experimentan lentitud al abrir las páginas web o en descarga de correo electrónico, al superar el umbral de los 100 ms utilizado para aplicaciones interactivas y temporizador para retransmisión de datos para protocolos en la capa de transporte.

#### **3.2.4.4 Análisis de seguridad de la red.**

La seguridad de la información establece el equilibrio de una empresa; por lo tanto, una alteración, pérdida o mal uso puede producir pérdidas significativas. Razón por la cual, deben tomarse medidas de protección mediante la combinación de diversas tecnologías que logren conservar la confidencialidad e integridad de la misma. Realizando un análisis general de seguridad, las condiciones de la red existente son las siguientes:

- La asignación de direcciones IP, segmento 192.168.10.0/24, es dinámica sin la existencia de un plan de direccionamiento o una distribución por departamentos, generando lentitud en el troubleshooting, conflictos de IP, problemas con las impresiones y falta de control de acceso de dispositivos a la red.
- Los ordenadores tienen protección Antivirus, detección de amenazas y antimalware a través de Kaspersky, con licencias activas.
- El acceso a los sitios web carece de políticas que controlen el acceso a categorías de sitios inadecuados, para que protejan a los usuarios mientras navegan.
- Las interfaces de red no tienen implementadas funciones que limiten la conexión de equipos previo registro de dirección de control de acceso al medio (Media Access Control, MAC).
- Existe periodicidad en la ejecución de respaldos o copias de seguridad, evitando que la información quede expuesta a una pérdida por agentes como infecciones de virus, apagado repentino de los ordenadores, defecto del hardware, etc.
- Los componentes de hardware y software no tienen implementado un sistema de monitoreo que permita adquirir datos, analizar, supervisar e informar el estado de la infraestructura de red. Por lo cual, impide tomar

medidas preventivas en el aprovisionamiento de recursos, entre los principales parámetros de medición están los siguientes:

- Uso de los recursos de servidores y ordenadores (memoria, CPU, flash, sesiones activas, etc.).
  - Disponibilidad de los servicios, tráfico de red y consumo de ancho de banda.
  - Notificar alertas, amenazas a la seguridad y estadísticas de filtrado de contenido.
- La red no tiene una administración centralizada de los usuarios para el control del uso de los dispositivos y estandarización de perfiles.

## Capítulo 4: Desarrollo de la propuesta

Para realizar la elaboración del diseño de solución que permita la innovación tecnológica, fueron utilizadas las recomendaciones de la tercera fase del modelo PPDIOO (Preparación, Planificación, Diseño, Implementación, Operación, Optimización) de Cisco que cumple con las diferentes etapas en que puede dividirse el ciclo de vida de una red (Singh, 2017). El enfoque de la metodología en la fase de diseño tiene como propósito cumplir los requerimientos técnicos para alcanzar las metas empresariales y realizar el cierre de brechas identificadas, encaminadas a una proyección de crecimiento continuo.

La recopilación de datos significativos sobre el giro de negocio de la empresa, topología de red, limitaciones técnicas, utilización de direcciones IP, plataforma del sistema transaccional, características de los dispositivos de red, tipos de usuarios, protocolos de enrutamiento, servicios de telecomunicaciones implementados, incluso los procesos de atención de requerimientos obtenidos en las fases previas de estudio, permitieron identificar las características técnicas, funcionales y de rendimiento que debe contemplar el diseño de la solución, distribuyéndolo en tres secciones:

- **Modelo de arquitectura de red:** define el modelo de arquitectura empresarial a utilizar para el diseño de red, basado en el levantamiento de información y análisis realizado.
- **Selección de infraestructura de red:** dimensiona los equipos y determina las especificaciones técnicas mínimas para el cumplimiento de los requerimientos.
- **Diseño de redes de comunicación:** lleva a cabo el diseño de la red de datos y esquema de conexión propuestos como solución a los servicios de telecomunicaciones de Infamotor S.A.

### 4.1 Modelo de arquitectura de red.

Con el incremento de demanda en los negocios, la evolución tecnológica y la expansión de redes en las empresas, éstas se volvieron más complejas viendo la necesidad de modificar las soluciones tradicionales por un enfoque modular,

donde cada módulo divide a la red en áreas específicas facilitando el control y la resolución de problemas.

Considerando las características técnicas de los equipos existentes y la proyección de crecimiento en la red de Infamotor S.A., fue seleccionado el **modelo de arquitectura empresarial de Cisco** (Gómez & Yagual, 2018), para diseñar una solución escalable que abarque las necesidades operacionales, determinando las funciones que ejecutará la infraestructura actual y nueva a través de los módulos a continuación propuestos:

- Módulo Campus Empresarial.
- Módulo Borde Empresarial.
- Módulo Proveedor de Servicios de Borde.
- Módulo Funcional Remoto.

#### **4.1.1 Módulo Campus Empresarial.**

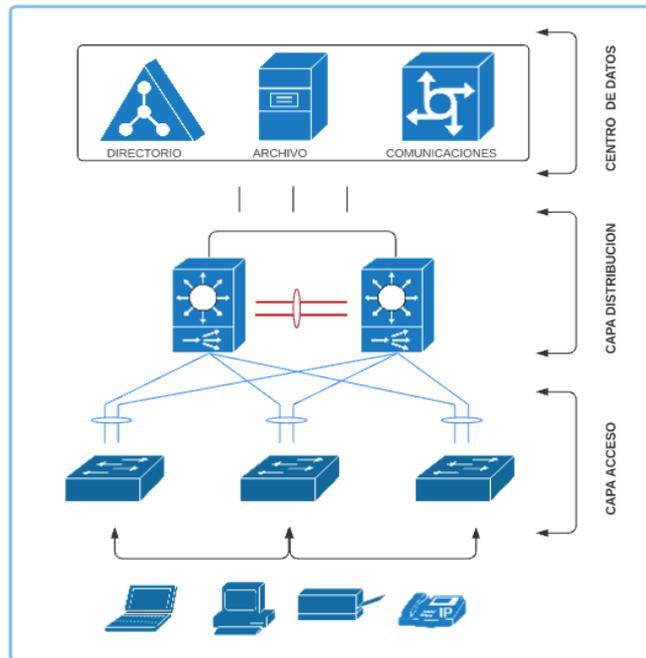
El módulo campus empresarial abarcará geográficamente al edificio matriz donde se desarrollarán las operaciones principales de la empresa, utilizando un enfoque jerárquico y modular para que los servicios de telecomunicaciones aborden las necesidades corporativas.

Considerando el tamaño de la empresa (mediana A), las secciones del modelo que se aplicarían para simplificar la interconexión de las redes del edificio matriz de Infamotor S.A., figura 4.1, serían las siguientes:

- **Capa de acceso del edificio matriz:** será la encargada de integrar los terminales de los usuarios tales como ordenadores, impresoras, teléfonos IP y dispositivos inteligentes. Este submódulo marcará la primera línea de equipos de conmutación (switch L2) que operan en la capa de enlace del modelo OSI, dimensionados en función de la cantidad de puertos necesarios y características técnicas calculadas en base a las actividades de la empresa.
- **Capa de núcleo-distribución colapsado del edificio matriz:** por el tamaño de la empresa el diseño jerárquico en los niveles de núcleo y distribución colapsan en una sola capa. Dentro de las funciones primordiales que cumplirá, pueden resaltarse: garantizar la alta

disponibilidad de los servicios, proporcionar el acceso a los servicios de telecomunicaciones y facilitar la conexión con las diferentes áreas de la empresa Infamotor S.A. En este punto se marcará la segunda línea de equipos de conmutación (switch L2) que operan en la capa de enlace del modelo OSI.

- **Centro de Datos:** aportará en el diseño de la solución agrupando a los equipos informáticos que tienen un alto recurso de cómputo, los cuales alojarán localmente a servicios/aplicaciones existentes y planificados que fueron identificados en el levantamiento de información. Para esto, se consideraron algunos factores como latencia, capacidad de ancho de banda, escalabilidad al crecimiento de necesidades y la reutilización del hardware existente. Posteriormente, es presentada una descripción breve del equipamiento seleccionado:
  - Servidor de comunicaciones: contemplado dentro de los servicios planificados, será un nuevo recurso que permitirá brindar el servicio de telefonía IP junto con los beneficios y herramientas que la misma ofrece, tales como: chat, videoconferencia, redirección y distribución de llamadas, etc.
  - Servidor de directorio: forma parte de los servicios planificados, sus funcionalidades contribuirán con el control de la red potencializando la seguridad, así como también la administración de los usuarios/grupos y ordenadores, otorgando los permisos necesarios para el acceso a los recursos empresariales.
  - Servidor de archivo: pertenece a la categoría de los servicios existentes, el cual es utilizado para el almacenamiento de información (servicio FTP) y tendrá como función complementaria la administración centralizada de datos de la empresa, permitiendo o denegando el acceso a los usuarios para que puedan extraer o compartir la misma.



**Figura 4.1:** Secciones aplicadas del Módulo Campus empresarial.

**Fuente:** Autor

#### 4.1.2 Módulo Borde Empresarial.

Dentro del entorno tecnológico de Infamotor S.A., el módulo de borde empresarial corresponde a la infraestructura de red que actuará como puerta de enlace a los servicios de telecomunicaciones, donde serán ejecutadas las políticas de seguridad para que la información no quede expuesta, permitiendo la interconexión con los diversos ambientes como sucursales (branch office), servicio en la nube (cloud services) o teletrabajadores (teleworkers) a través de redes privadas virtuales (VPN), otorgando el acceso remoto de conformidad con las necesidades que demande la empresa.

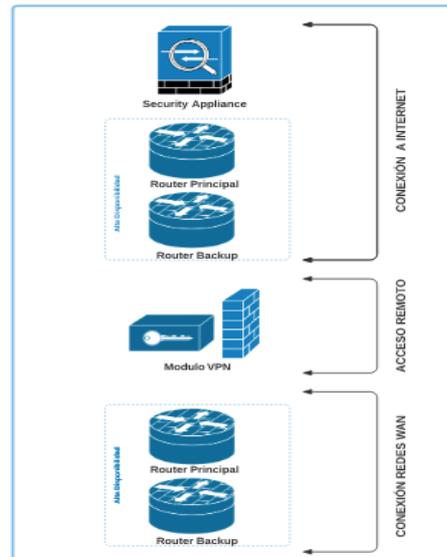
La sección de borde de Infamotor S.A., tendrá como propósito fundamental preservar la privacidad de los datos, minimizando el riesgo de ataques informáticos con el uso de herramientas que analicen, filtren y bloqueen contenido malicioso, proporcionando niveles adecuados de protección para evitar el acceso no autorizado de intrusos cibernéticos que puedan comprometer la operación de la organización.

El módulo mostrado en la figura 4.2 está conformado con diferentes dispositivos que garantizarán la disponibilidad de los servicios por medio de conexiones y configuraciones basadas en la actividad que desarrolla la empresa.

También cumplirá el rol de vínculo con las redes externas e internas de la organización que incluirán las siguientes funcionalidades principales:

- **Conexión a Internet:** el acceso que tendrá la red empresarial a Internet estará caracterizada por dos aspectos fundamentales:
  - Alta disponibilidad con enlaces redundantes (multihoming), que proporcionarán tolerancia a fallas asegurando de forma ininterrumpida las operaciones corporativas. Entre las alternativas de multihoming existentes y fundamentado en la experiencia, la mejor opción como solución es doble router y doble enlace hacia un mismo ISP; por lo tanto, tendrá la capacidad de identificar un fallo y recuperarse de forma efectiva garantizando un servicio activo.
  - Protección en un entorno de perímetro difuso, corresponde al recurso tecnológico que formará parte de la línea de defensa que procurará minimizar significativamente las amenazas cibernéticas en el borde de la red, incorporará herramientas de inspección de alto rendimiento que respondan a la evolución del comportamiento de los usuarios, utilizando tecnologías de la información adaptables a los nuevos procesos de negocios y cambios en los mecanismos de ataques que comprometan a la información. Estas estrategias de protección se efectuarán de forma centralizada a través de un equipo de seguridad (security appliance) que da una solución orientada a entornos empresariales como las PyME, complementando las políticas locales definidas para mantener la integridad, privacidad y control de los datos de Infamotor S.A.
- **Conexión de acceso remoto:** brindará el servicio de acceso a recursos corporativos y aplicaciones de la empresa a los teletrabajadores a través de redes privadas virtuales (VPN), las cuales protegerán los datos con un alto nivel de cifrado y garantizarán la navegación web desde cualquier red pública. Este módulo de configuración estará integrado a las funciones del security appliance de protección del perímetro difuso junto con la arquitectura sito-a-sitio (site-to-site) que permitirá crear túneles vía Internet para la administración de las plataformas remotas, considerando los requerimientos técnicos del levantamiento de información.

- **Conexión a redes WAN:** como funcionalidad, permitirá la conectividad con las tecnologías de transporte que ofrecen los distintos proveedores para la transmisión de datos, video y voz. Por lo que, serán dimensionados equipos de enrutamiento (principal, backup) capaces de soportar el ancho de banda que demandan las necesidades de los usuarios, con protocolos que permitan obtener una alta disponibilidad a las aplicaciones en red, escalabilidad, accesibilidad y facilidad de implementación.



**Figura 4.2:** Secciones aplicadas del módulo borde empresarial.  
**Fuente:** Autor

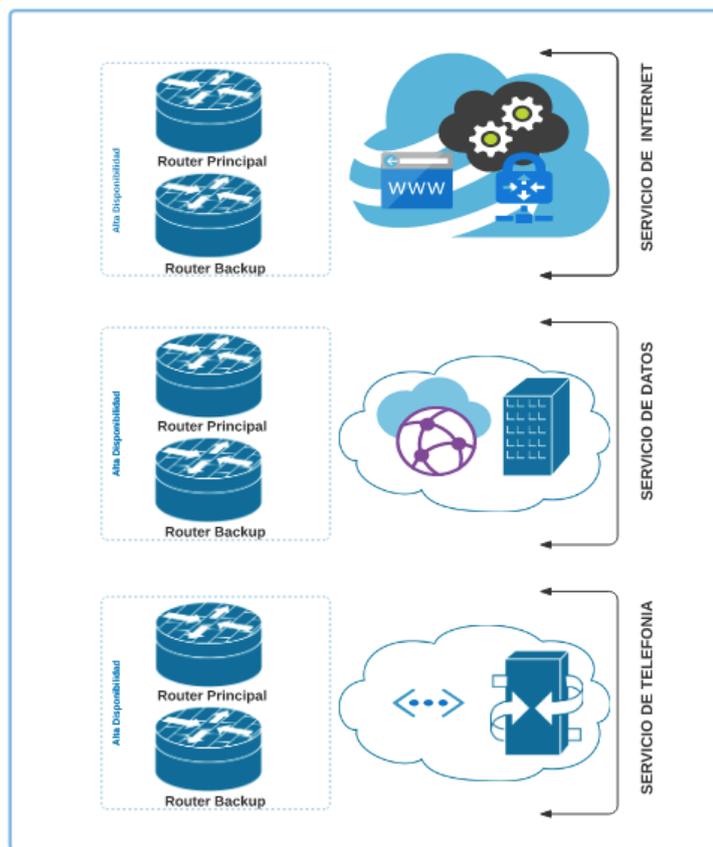
#### 4.1.3 Módulo Proveedor de Servicios de Borde.

Para la infraestructura física de red del edificio principal de Infamotor S.A. el presente módulo determinará el punto de demarcación con los proveedores de servicios, los cuales ofrecerán soluciones tecnológicas con diversas prestaciones como servicios fijos, servicios en la nube (cloud computing) y servicios gestionados en función de las necesidades de la empresa.

El cambio tecnológico integrará soluciones de colaboración que aporten con ventajas competitivas a las estrategias de ventas, asimismo buscará garantizar la alta disponibilidad de sus aplicaciones. En atención a lo cual, deberán considerarse los siguientes factores claves a cumplir en las propuestas técnicas de los proveedores:

- **Acuerdo de nivel de servicio (SLA):** describirá los objetivos de desempeño de red y disponibilidad de los servicios a contratar (Datos, Internet, Telefonía), conociendo los alcances, limitaciones y responsabilidades que deben tener ambas partes. El SLA permitirá establecer las condiciones de servicio en cuanto al tiempo de instalación, tipo de interfaces a utilizar, aspectos de confidencialidad (costos, topología, protocolos, etc.), procesos de reporte de problemas, calidad de enlace (ancho de banda, latencia, pérdidas permitidas, etc.) y niveles de escalamiento.
  
- **Portafolio de servicios:** es importante que el proveedor de servicios pueda ofrecer un amplio portafolio de soluciones tecnológicas, que puedan aportar para el crecimiento futuro.
  
- **Costos y puntos de presencia:** los costos de implementación de las redes de acceso y las tarifas mensuales de los servicios a contratar deberán estar dentro de los valores asequibles para la empresa; sin embargo, a la hora de elección del proveedor, este aspecto será establecido como el último factor determinante, dado que el análisis se basará en el cumplimiento de las exigencias técnicas. El proveedor de servicios tendrá que disponer de diversos puntos de presencia con acceso a las ciudades principales con el propósito de brindar conectividad a las sucursales de la empresa Infamotor S.A.

Del mismo modo, entre las diversas opciones de conectividad de la red de acceso o última milla que ofrecen los proveedores para los servicios fijos de internet, telefonía y datos, deberán disponer de una arquitectura backbone de alto performance como MPLS a nivel de transporte, con redundancia de al menos tres salidas internacionales (Tier-1), incluyendo soluciones L3VPN (Layer 3 Virtual Private Network) que proporcionen separación de tráfico y calidad de servicio.



**Figura 4.3:** Módulo proveedor de servicios de borde.

**Fuente:** Autor

#### 4.1.4 Módulo funcional remoto.

La estructura del módulo funcional remoto facilitará al personal de Infamotor S.A., tener flexibilidad de trabajar desde sus hogares (teleworker), al establecer conexiones seguras con la utilización de una red privada virtual (VPN) que brindará una solución de acceso a la información y aplicaciones empresariales.

Asimismo, los requerimientos para los servicios y aplicaciones planificadas descritas en el análisis previo estarían albergados en el submódulo Data Center con las características principales que ofrecen de disponibilidad y seguridad de la información a nivel físico y lógico.

Por otra parte, también se integrarán los servicios de telecomunicaciones de las sucursales existentes, junto con el despliegue de nuevas dependencias, a través de soluciones tecnológicas que ayudarán a cumplir las exigencias que demandan las nuevas herramientas de colaboración, mejorando la capacidad de visibilidad y

control de la red. A continuación, un breve resumen de los componentes del módulo:

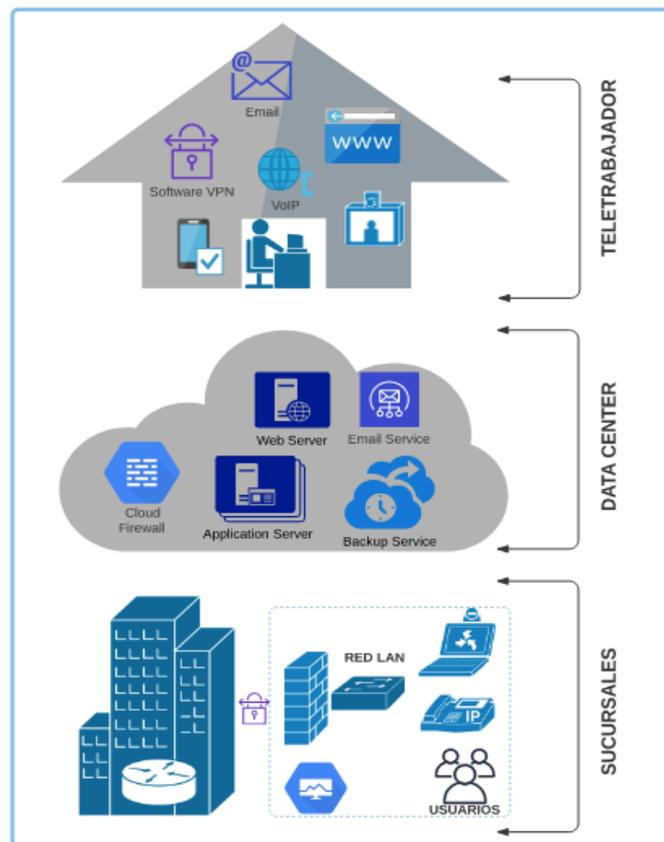
- **Teletrabajador:** aportará con el cumplimiento de los requerimientos considerados para promover el crecimiento de la empresa, brindando al staff las facilidades de acceso remoto (VPN) a los recursos empresariales desde cualquier ubicación conectada a Internet, con la utilización de herramientas que lograrán al usuario acercarlo a un entorno de oficina típico. Entre los mecanismos más utilizados están los siguientes:
  - **Un sistema de telefonía empresarial** permitirá realizar llamadas VoIP a través de una aplicación de software (app) móvil o desde un ordenador.
  - **Una herramienta fiable de colaboración visual** contribuirá en la coordinación de reuniones virtuales brindando funciones de compartición de contenido y protección de la información que impulsen la productividad.
  - **Software de cliente VPN**, utilizará Internet para acceder a la red corporativa estableciendo una conexión con protocolos de seguridad que cifren la información, conserven la integridad de los datos e incorporen políticas de acceso a las plataformas empresariales (ERP, CRM, base de datos, entre otras).
  - **Servicio de correo corporativo**, estará gestionado por el software de ofimática empresarial y podrá utilizarse como una forma de comunicación con clientes o proveedores. A su vez, ayudarán a consolidar la imagen de la empresa al proyectar confianza, seriedad y seguridad.
- **Data Center:** el centro de datos o informática en la nube definido por (Blanco, 2016) como: “Un modelo tecnológico que permite el acceso de red ubicuo, adaptado y bajo demanda en red a un conjunto compartido de recursos de computación configurables compartidos (redes, servidores, equipos de almacenamiento, aplicaciones y servicios...), que pueden ser rápidamente aprovisionados y liberados con un esfuerzo de gestión reducido o interacción mínima con el proveedor de servicios (Blanco, 2016).

A todo esto, impulsará la transformación digital e innovación empresarial, brindando simplicidad al crecimiento de capacidades, incrementando los beneficios y productividad con facilidades de expandirse. A continuación, los servicios categorizados para el cloud computing:

- **Servidor Web:** corresponde a los servicios existentes de almacenamiento de información web, implementado en la nube pública y encargado de alojar el sitio [www.infamotor.com](http://www.infamotor.com), con la seguridad correspondiente para responder las peticiones de acceso a la página de los usuarios.
  - **Servidor de Correo:** integrado a los métodos de comunicación corporativa existente, está implementado en la nube pública con la función de administrar todas las cuentas de correo electrónico de la empresa y las funcionalidades
  - **Servicio de Colaboración Web:** considerado dentro de los servicios proyectados de aplicaciones en la nube (cloud applications), facilitará de manera ágil la coordinación de reuniones desde cualquier dispositivo con acceso a internet, incorporando funciones de mensajería instantánea, audio, video y compartición de archivos con los participantes de cada sesión: proveedores, clientes, empleados o socios.
  - **Servicio de respaldo:** planificará con anticipación la continuidad de las operaciones con la recuperación ante desastres en la nube, al disponer de réplicas de las aplicaciones críticas de la empresa, minimizando el tiempo de inactividad que reforzará la confianza con los clientes y su reputación.
  - **Servicio de infraestructura en la nube:** permitirá la migración del sistema ERP existente al data center virtual (nube privada), garantizando la protección de los datos del software de gestión y automatización de los procesos empresariales de Infamotor S.A. Por otra parte, estaría integrado al CRM como una las aplicaciones proyectadas para dar atención personalizada y rápida a los clientes.
- **Sucursales de la empresa:** una de las metas que sigue la empresa es la apertura a nuevos canales de venta de los productos y servicios automotrices que ofrece a la ciudadanía. Para esto, las sucursales

alcanzarán el mismo nivel de sofisticación de las plataformas tecnológicas que dispondrá la matriz principal, apuntando a la innovación y mejora de productividad en los empleados. De modo que, demandan la utilización de herramientas de colaboración, sistemas y aplicaciones alojadas en la nube, resaltando la consideración de algunos aspectos para la obtención de los resultados esperados, tales como:

- Ofrecer una infraestructura de red con capacidad de ampliación.
- Proteger los dispositivos locales e incrementar la seguridad en las conexiones hacia los servicios en la nube.
- Adquirir soluciones de control y visibilidad de la red que impulsen la confianza a nuevos servicios.
- Incorporar socios tecnológicos que contribuyan en proyectos innovadores, agregando valor y beneficios en las comunicaciones.



**Figura 4.4:** Módulo funcional remoto.

**Fuente:** Autor

## **4.2 Selección de la infraestructura de red.**

Para el dimensionamiento de infraestructura fueron tomados los datos del levantamiento de información a fin de determinar soluciones que proporcionen escalabilidad, fiabilidad y beneficios a un crecimiento futuro. De forma general, estuvieron considerados los roles que desempeñarán los equipos, características de las aplicaciones de red que demandan un tiempo mínimo de respuesta, alta disponibilidad o gran consumo de ancho de banda. Por lo que, el equipamiento en estudio quedó distribuido en:

- Infraestructura de acceso LAN alámbrica e inalámbrica.
- Plataformas de Seguridad de Red.
- Plataformas de Soluciones para Reuniones (Meeting).
- Infraestructura de nuevas aplicaciones y servicios.

### **4.2.1 Infraestructura de acceso LAN alámbrica e inalámbrica.**

La selección de equipos para las soluciones en infraestructura de red de acceso LAN para campus y sucursales, está fundamentada en la investigación de la empresa Gartner, como una herramienta que permite identificar a los proveedores posicionados para cumplir con las exigencias de un mercado cambiante a la conectividad.

El Magic Quadrant de Gartner contiene los proveedores que destacan como Líderes en innovación, demostrando la capacidad de tener relaciones sólidas y el cumplimiento de una variedad de requisitos de los clientes. Con un amplio portafolio de equipos de conmutación por cable (wired switching), productos Wireless LAN, aplicaciones y servicios de red, la empresa Cisco continúa sobresaliendo en soluciones de infraestructura de acceso (Gartner, 2019). En Ecuador se disponen de varios canales de distribución de la marca, que facilitarán una futura adquisición, garantía y soporte técnico.

El modelo de arquitectura empresarial propuesto está compuesto por secciones que contienen wired switches y puntos de acceso inalámbrico (wireless access points), los mismos que serán analizados tomando como referencia la marca Cisco para determinar sus características técnicas:

- Dispositivos de conmutación capa de acceso.

- Dispositivos de conmutación capa de núcleo-distribución colapsado.
- Dispositivos de conmutación sucursales.
- Dispositivos de puntos de acceso inalámbrico.

#### 4.2.1.1 Dispositivos de conmutación capa de acceso.

Al determinar las características de los dispositivos de conmutación de la capa de acceso como punto de partida, fue determinado el número de puertos requeridos, conformado por la suma actual de trabajadores de las áreas del edificio matriz, dispositivos periféricos (impresora, escáner) y la proyección de crecimiento de ambos. Como resultado del análisis, la tabla 4.1 muestra el total de interfaces según la distribución de convergencia por rack de los puntos de red, estableciendo equipos de conmutación de 24 puertos que suministren alimentación eléctrica (PoE) amparados en los estándares IEEE 802.3af/at.

**Tabla 4.1: Criterio para determinar el total de interfaces en equipos de acceso.**

<b>ID Rack</b>	<b>No Actual Usuarios</b>	<b>No Dispositivos</b>	<b>Proyección Usuarios</b>	<b>Proyección Dispositivos</b>	<b>Total Interfaces</b>
PB-01	18	2	10%	5%	<b>22</b>
PB-02	17	3	10%	5%	<b>22</b>
P2-03	10	2	0%	5%	<b>13</b>

Fuente: Autor

La realización del cálculo que determina las capacidades mínimas de las características técnicas relevantes que deben disponer los equipos en mención forma parte del anexo 1, como resultado la tabla 4.2 resume las especificaciones a cumplir, consideradas como clave para el éxito del diseño.

**Tabla 4.2: Capacidades mínimas de los equipos de acceso.**

<b>ID Rack</b>	<b>No de Puertos Usuarios</b>	<b>No de Puertos SFP Uplink</b>	<b>Switching bandwidth</b>	<b>Cantidad de Switches</b>
PB-01	24 GE	2 TE	88 Gbps	1
PB-02	24 GE	2 TE	88 Gbps	1
P2-03	24 GE	2 TE	88 Gbps	1
Total de equipos de acceso en edificio matriz				<b>3</b>

**Nota.** Cálculo de capacidades detallada en el anexo 1.

Fuente: Autor

La empresa Cisco ofrece una herramienta web que permite identificar de forma ágil el equipo de conmutación adecuado a las necesidades, llamada Switch

Selector: <https://www.cisco.com/c/en/us/products/switches/index.html>. El modelo escogido corresponde a la nueva generación Catalyst de la serie 9200 con características de simplicidad, administración inteligente y alta seguridad, tal como se muestra a continuación en la tabla 4.3.

**Tabla 4.3: Recomendación modelo de equipo para capa de acceso.**

Ubicación	Modelo	Puertos Ethernet 10/100/1000	Interfaces Uplink	Consumo de Energía	Switching Bandwidth
PB-01	C9200L-24P-4X	24 PoE+	4 SFP+	0.57 KVA	128 Gbps
PB-02	C9200L-24P-4X	24 PoE+	4 SFP+	0.57 KVA	128 Gbps
P2-03	C9200L-24P-4X	24 PoE+	4 SFP+	0.57 KVA	128 Gbps

Fuente: Autor

#### 4.2.1.2 Dispositivos de conmutación capa de núcleo-distribución colapsado.

Para realizar el dimensionamiento, fue cuantificado el total de interfaces requeridas, tomando en consideración la cantidad de conexiones con los servidores del submódulo centro de datos, vinculación de los switches de la capa de acceso con enlaces redundantes, proyección de crecimiento, interconexión con los equipos del módulo de borde y proveedores de servicio.

La convergencia de las conexiones en este nivel radica en garantizar la alta disponibilidad, en atención a lo cual fueron contemplados dos equipos núcleo-distribución a través de técnicas redundantes multicapas y distribución de carga. Como resultado del análisis la tabla 4.4 presenta la cantidad obtenida.

**Tabla 4.4: Criterio para determinar interfaces en equipos núcleo-distribución.**

ID	No Conex. Eq. Acceso	No Conex. Cen. Datos	No Conex. Mod. Borde	No Conex. Pro. Serv.	Proyección Crecimiento
DP2-01	3 SFP+	3 1000 Base-T	2 1000 Base-T	2 1000 Base-T	5%
DP2-02	3 SFP+	3 1000 Base-T	2 1000 Base-T	2 1000 Base-T	5%

Fuente: Autor

El anexo 2 muestra el cálculo realizado para definir las capacidades mínimas que deben incluir los equipos núcleo-distribución en sus especificaciones técnicas, agregando la propiedad de apilamiento (stacking) que contribuirá al cumplimiento de las funciones establecidas. La tabla 4.5 a continuación consolida los resultados obtenidos.

**Tabla 4.5: Capacidades mínimas de los equipos de núcleo-distribución.**

ID	Puertos GE	Puertos Ten GE	Capacidad Stacking	Switching Bandwidth	Cantidad de Switch
DP2-01	24	4 SFP+	128 Gbps	204 Gbps	1
DP2-02	24	4 SFP+	128 Gbps	204 Gbps	1
Total de equipos de núcleo-distribución colapsado					<b>2</b>

**Nota.** Cálculo de capacidades detallada en el anexo 2.

Fuente: Autor

A causa de la diversidad de características que se asocian para las soluciones de servicios de telecomunicaciones, la elección de los equipos puede resultar compleja. Sin embargo, fueron tomados en consideración principalmente los aspectos de eficiencia, rendimiento y proyección de crecimiento. Con la herramienta Cisco Selector el modelo escogido corresponde a la serie 9300, mostrado en la tabla 4.6, como una plataforma optimizada para alta densidad, capacidad avanzada de seguridad, gestión unificada virtualización, administración inteligente y segmentación de red.

**Tabla 4.6: Recomendación modelo de equipo para capa núcleo-distribución.**

ID	Modelo	Cantidad Interfaces	Consumo de Energía	Capacidad Stacking	Switching Bandwidth
DP2-01	C9300L-24T-4X	24 GE / 4 SFP+	0.10 KVA	320 Gbps	448 Gbps
DP2-02	C9300L-24T-4X	24 GE / 4 SFP+	0.10 KVA	320 Gbps	448 Gbps

Fuente: Autor

#### 4.2.1.3 Dispositivos de conmutación sucursales.

En el dimensionamiento de equipos de conmutación de las sucursales, los datos obtenidos en el levantamiento de información como dispositivos periféricos, número de usuarios y proyección de crecimiento, permitieron cuantificar las interfaces requeridas. Del mismo modo, la referencia de velocidad de las interfaces calculadas en el anexo 1, junto con la utilización de Cisco Selector lograron escoger un modelo asociado a la serie 2960, tabla 4.7, diseñado para las branch offices brindando características de seguridad mejorada, suministro de alimentación eléctrica (PoE), confiabilidad, administración inteligente y soportable para internet de las cosas (Internet of Things, IoT).

**Tabla 4.7: Recomendación modelo de equipo para sucursales.**

ID	Modelo	Puertos Ethernet 10/100/1000	Interfaces Uplink	Consumo de Energía	Switching Bandwidth
SUC01	C2960L-8PS-LL	8 PoE+	2 SFP	0.11 kVA	20 Gbps
SUC02	C2960L-8PS-LL	8 PoE+	2 SFP	0.11 kVA	20 Gbps

Fuente: Autor

**4.2.1.4 Dispositivos de puntos de acceso inalámbrico.**

El edificio principal se caracteriza por tener una infraestructura de red alámbrica con puntos de conexión por usuario; sin embargo, la transformación digital de las empresas incorpora avances tecnológicos como IoT y los desafíos asociados con traer su propio dispositivo (Bring Your Own Device, BYOD), exigiendo soluciones inalámbricas que brinden visibilidad, políticas de control, flexibilidad y confiabilidad a través de puntos de acceso seguro.

A su vez, como valor agregado a la experiencia de visita al establecimiento se busca ofrecer WiFi a los clientes, proporcionando conexiones seguras y de calidad. Para esto, la solución como fase inicial debe contemplar dispositivos dirigidos a un pequeño segmento de usuarios concurrentes, admitiendo el funcionamiento mediante PoE/PoE+, soportado por los estándares inalámbricos IEEE 802.11 a/b/g/n/ac, simplicidad en la implementación, incorporación a sistemas de autenticación, operatividad de forma autónoma o controlada.

La empresa Cisco, manteniéndose a la vanguardia de la tecnología ofrece también una herramienta web que permite seleccionar los equipos de acceso inalámbrico según las necesidades empresariales, llamada Wireless Selector: <https://explore.cisco.com/dna-wireless/cisco-wireless-selector>. El modelo escogido corresponde a la nueva generación Aironet de la serie 1800 con la capacidad de cumplir las funcionalidades de alto rendimiento que demanda el entorno empresarial, las características relevantes son presentadas en la tabla 4.8.

**Tabla 4.8: Recomendación punto de acceso inalámbrico.**

Modelo	Puerto Ethernet	Número de Radios	Máx. Usuarios Concurrentes	Tecnología Multiplex.	Consumo de Energía
Aironet 1815i	1x10/100/1000 PoE	Dual 2.4/5 GHz	200 por Radio WiFi	2x2:2 MU/SU-MIMO	8.3 W

Fuente: Autor

#### **4.2.2 Plataformas de Seguridad de Red.**

Cuando surgieron los primeros criterios de seguridad se encontró al firewall como un hardware que brinda protección a la red contra intrusos cibernéticos, actualmente han surgido muchas generaciones e incorporación de características (features) a la vigente solución. Sin embargo, la evolución tecnológica en el mundo de Internet como un recurso accesible a las personas y el comercio electrónico, como oportunidad para llegar a nuevos mercados, hicieron que surjan nuevos desafíos de seguridad, exigiendo mejoras para la protección de información e incremento de seguridad en las empresas.

De modo que, tuvo origen un nuevo concepto en seguridades: Gestión de Amenazas Unificadas (UTM, Unified Threat Management), tecnología de protección de información centralizada a través de un único appliance. El UTM incorpora inspección de tráfico en la capa de aplicaciones con nuevos features que centralizan funcionalidades, entre otras, filtrado de contenido, VPN, anti-virus, anti-spam, políticas de control de acceso, IDP y detección/prevenición de anomalías (Anomaly Detection Prevention, ADP) como solución orientada a entornos poco exigentes en rendimiento como las PyME.

Luego, con el movimiento de clientes hacia redes híbridas, demanda de soluciones virtuales con soporte a plataformas públicas (Infraestructure as a Software, IaaS), incorporación de redes WAN definidas por software (Software-Defined, SD-WAN), detección avanzada de malware, capacidad de automatización e integración de otros componentes de defensa, surgen las plataformas de seguridad de red conformada por soluciones de firewall virtuales y físicas (appliance) de nueva generación (New Generation Firewall, NGFW), con multifuncionalidades que brindan escalabilidad para ambientes que requieren capacidades dinámicas.

El presente caso de estudio demanda requisitos que deben ser abordados por los productos de seguridad que ofrecen los proveedores, entre otros, destacan los siguientes:

- Alto rendimiento y mejor visibilidad para las aplicaciones de negocio consideradas como críticas.

- Reducción de latencia para la conexión de usuarios a las aplicaciones en la nube.
- Protección contra ataques maliciosos producidos desde el exterior (Internet) e interior de la red (LAN).
- Establecimiento de políticas de control de acceso a aplicaciones e inspección profunda de paquetes.
- Restricción de acceso de usuarios no autorizados y control de navegación a páginas inapropiadas.
- Operación de un sistema de administración centralizada de los productos de seguridad propuestos.
- Utilización de IPSec/SSL para la creación de VPN Site-to-Site (mínimo 5) y conexión remota de usuarios (mínimo 25).
- Dimensionamiento para la conexión máxima de 50 usuarios en edificio matriz con un promedio de 200 sesiones concurrentes por cada uno.
- Dimensionamiento para la conexión máxima de 10 usuarios por sucursal con un promedio de 200 sesiones concurrentes por cada uno.
- Integración con el directorio activo para reconocer el origen del acceso aplicaciones, páginas web, etc.

La selección de equipos para las soluciones de seguridad está fundamentada en la investigación de la empresa Gartner, como una herramienta que permite identificar los proveedores que han liderado el mercado en innovación, protegiendo a las empresas a medida que avanzan hacia nuevos factores de forma de infraestructura (Gartner, 2019). El Magic Quadrant de Gartner define criterios de evaluación e integración de características adicionales que mejoran la experiencia del usuario, consolidando a las marcas Palo Alto, Fortinet, Check Point y Cisco que destacan como líderes.

Considerando como fundamentales las soluciones SMB (Small Business) firewall, bajo costo de operación en sucursales, satisfacción a los clientes con productos que han alcanzado madurez, integración de SD-WAN por la alta demanda de consumo de ancho de banda y disponibilidad de varios canales de distribución con soporte 24/7, la marca **Fortinet** ha sido utilizada como referencia para el dimensionamiento de los equipos de seguridad. A continuación, la tabla 4.9 ilustra un cuadro comparativo de capacidades entre los diferentes proveedores.

**Tabla 4.9: Cuadro comparativo de capacidades con los diversos proveedores.**

				
Gestión de panel único.	↑	↑	↑	×
Garantía de seguridad verificada por thrid-party.	↑	↑	×	×
Diseño con segmentación adaptable.	↑	↔	×	↑
Visibilidad end-to-end e inteligencia sobre ataques.	↑	↔	↔	×
Mayor protección, relación costo/rendimiento.	↑	×	×	×
				

Fuente: Autor

La marca Fortinet en su guía de diseño rápida para SMB, propone como soluciones de firewall los modelos **FortiGate 80E** para el edificio matriz y **FortiGate 30E** para las sucursales (Fortinet, 2020), con especificaciones técnicas detalladas en la tabla 4.10, las cuales cumplirán con las necesidades empresariales de garantizar la alta disponibilidad de aplicaciones críticas, reducir los costos de contratación de ancho de banda y el control de amenazas.

**Tabla 4.10: Especificaciones técnicas equipos FortiGate 30E/80E.**

Especificaciones	FortiGate 30E	FortiGate 80E
Rendimiento NGFW	200 Mbps	360 Mbps
Rendimiento IPS	300 Mbps	450 Mbps
Rendimiento ATP	150 Mbps	250 Mbps
Rendimiento Firewall	900 Mbps	4 Gbps
Rendimiento Inspección SSL	125 Mbps	135 Mbps
Sesiones Concurrentes	900,000	1,300,000
Latencia	130 μs	3 μs
Número de Usuarios	1-10	20-60
Usuarios IPsec-VPN	250	2500
Usuarios SSL-VPN	100	200
Túneles IPsec VPN STS	200	200
Dominios Virtuales	5	10
Interfaces GE	4	14
Corriente Máxima	100V AC / 0.6A	100V AC / 0.25A
Consumo Máximo de Energía	15 W	25 W
Temperatura de Funcionamiento	0-40°C	0-40°C

Fuente: Autor

Para la protección de punto final (endpoint), los sistemas operativos de ordenadores integran a **Microsoft Defender**, considerada por Gartner dentro del cuadrante de líderes como una solución competitiva para los EPP (Endpoint Protection Platform) (Gartner, 2019), fortaleciendo principalmente la detección de ataques avanzados, capacidad para responder y remediar incidencias de seguridad asistidos por una arquitectura en la nube. También, dentro de la infraestructura existente la empresa dispone del antivirus **Kaspersky** con sus fuertes capacidades de detección y prevención de amenazas que reforzarían (hardening) las políticas de control en los dispositivos de comunicación final.

#### **4.2.3 Plataformas de Soluciones para Reuniones (Meeting).**

La utilización de Microsoft Skype como herramienta de elaboración de video conferencias en Infamotor S.A., permitió solventar requerimientos poco exigentes en escenarios de negocios que eran complementados con reuniones presenciales. Sin embargo, con la llegada de la pandemia del COVID-19 ha sido indispensable adquirir una solución que combine colaboración, comunicación e intercambio de contenido para la realización de reuniones desde cualquier lugar.

Las nuevas soluciones para reuniones empresariales y trabajo remoto abordarán las necesidades de interacción de los participantes en presentaciones con intercambio de contenido que mejoren las actividades diarias, brinden movilidad sin importar la ubicación geográfica, integren la plataforma telefónica existente (Public Switched Telephone Network, PSTN), faciliten el entrenamiento de nuevos productos, seminarios web de marketing, optimicen recursos con asistencias virtuales y fortalezcan la profilaxis frente a la emergencia sanitaria que vive el mundo.

Para seleccionar la mejor opción entre las alternativas de soluciones disponibles para reuniones, la misma fue sustentada en el estudio de Gartner, estableciendo en su cuadrante de líderes a proveedores como Cisco, Zoom, Microsoft y LogMein (Gartner, 2019). De modo que, al realizar un cuadro comparativo de las dos herramientas de colaboración más utilizadas, Microsoft Teams sobresale al cumplir uno de los requerimientos empresariales tan

relevantes como es la experiencia de llamadas colaborativas con la conexión de diversas plataformas telefónicas, tabla 4.11.

**Tabla 4.11: Cuadro comparativo de Cisco Webex y Ms Teams.**

<b>Características</b>	<b>Cisco Webex</b>	<b>Ms Teams</b>
Automatización de tareas en la planificación de reuniones de seguimiento.	☑	☑
Integrar a participantes mientras viajan (reuniones móviles).	☑	☑
Creación de reuniones rápidas en salas personales.	☑	☑
Unirse desde cualquier navegador o dispositivo de elección del participante.	☑	☑
Compartir escritorio o contenido con los participantes.	☑	☑
Compartir pantalla de un navegador, dispositivo Android o IOS.	☑	☑
Alta calidad de audio, optimización de micrófono y eliminación de ruido.	☒	☑
Silenciar o activar simultáneamente el audio de los participantes.	☑	☑
Grabación, edición y reproducción de reuniones	☑	☑
Analítica avanzada sobre detalles de llamadas o reuniones	☑	☑
Facilidad de implementación y escala al ser un servicio implementado en la nube.	☑	☑
Autenticación multi-factor e inicio de sesión con un servidor de directorio.	☑	☑
Variedad de idiomas admitidos.	☑	☑
Chat de forma pública o privada con los participantes.	☑	☑
Integración con diversas plataformas telefónicas empresariales (PSTN).	☒	☑
Incorporación con diversos proveedores de dispositivos telefónicos IP y <i>Softphone</i> .	☒	☑

Fuente: Autor

Tomando como factores claves a la madurez del producto, estabilidad por algunos años consecutivos, destacando resultados de innovación, eficiencia operacional, facilidad de uso y sensibilidad de costos, **Microsoft Teams** será elegida como una solución única capaz de satisfacer las necesidades empresariales de Infamotor S.A.

#### **4.2.4 Infraestructura de nuevas aplicaciones y servicios.**

La incorporación de aplicaciones y herramientas proyectadas en el modelo de arquitectura empresarial proporcionarán un valor agregado a la seguridad de la red, escalabilidad en comunicación de voz, además de una alta disponibilidad a través de enlaces redundantes. De modo que, deberán considerarse varios aspectos relevantes para evaluar y seleccionar al proveedor adecuado según los siguientes servicios:

- Servidor de directorio.
- Servidor de comunicaciones.
- Especificaciones técnicas de servicios fijos: Datos, Internet y Telefonía.
- Especificaciones técnicas de servicios Datacenter.

#### 4.2.4.1 Servidor de Directorio.

También conocido como directorio de dominio, cumplirá con uno de los roles más importantes que es potenciar la seguridad de la red. Estará encargado de administrar los usuarios, grupos y máquinas de escritorio, otorgando los permisos y acceso a la información de forma centralizada. Entre algunos de los servicios de directorio ofrecidos por los proveedores están los siguientes:

- **Active Directory Windows Server:** contiene información sobre la ubicación y características de los diferentes tipos de recursos gestionados dentro de la red, como ventaja utiliza el protocolo LDAP (Lightweight Directory Access Protocol, protocolo simplificado de acceso a directorio) que permite acceder a la base de datos de objetos del directorio para un determinado dominio o varios dominios creando un bosque (contenedor lógico de varios dominios interconectados) reduciendo la complejidad y facilitando el control de toda la red (Francis, 2019).
- **Open Directory MAC OS:** es el servicio de directorio de Apple Inc. que organiza y almacena información de los objetos de red, se basa en estándares compatibles con otros entornos de directorios activos de Windows o Linux, incluyendo al protocolo LDAP. Además, integra una autenticación robusta Kerberos (protocolo de autenticación que permite una comunicación segura entre dispositivos a través de la criptografía de claves) y replicación del servicio de directorio (Dreyer & Karneboge, 2019).
- **Novell eDirectory:** es un servicio de directorio que ofrece una solución de administración de identidad segura, capaz de ejecutarse en múltiples plataformas (Windows, Linux, Solaris) brindando escalabilidad y alto rendimiento. Almacena y administra objetos de forma centralizada sirviendo como repositorio para la información del usuario y otras aplicaciones que pueden ser accedidas a través del protocolo LDAP.

La elección del servicio de directorio para el diseño de la presente solución tecnológica contempla uno de los sistemas más utilizados en el ambiente Microsoft disponible en los recursos empresariales existentes con Windows Server 2016, como lo es el directorio activo o **Active Directory**. Tendrá como propósito almacenar la información de seguridad de la empresa en una base de datos que es capaz de expandirse con otros componentes de dominio (portal cautivo, acceso VPN, Exchange, etc.), ofreciendo mejoras en el rendimiento del sistema, aprovechando un mayor control sobre los equipos y fortaleciendo las políticas de acceso de usuarios a la red.

#### 4.2.4.2 Servidor de comunicaciones.

La solución de comunicaciones inteligentes logrará cumplir las necesidades empresariales al permitir la integración de las mismas de manera unificada, optimizando recursos con un sistema de gestión simplificada que ofrece un servicio de calidad y competitividad en el mercado. A continuación, la descripción de algunas de las plataformas más utilizadas:

- **Asterisk:** es una solución de software libre (open source), flexible, compatible con los estándares de telefonía y una herramienta relevante para el giro de negocio de las empresas, desarrollado por Mark Spencer (Digium, compañía tecnológica EE.UU.) que opera sobre Linux (Meggelen, Madsen, & Bryant, 2019), en Guayaquil la empresa Palo Santo es especializada en proveer servicios de soporte técnico en sus configuraciones. La arquitectura de Asterik está conformada por módulos, los cuales a su vez proporcionan específicas funcionalidades como resume la tabla 4.12, capaz de integrar la telefonía tradicional o IP con la utilización de protocolos de señalización como SIP, IAX (Inter-Asterisk Exchange Protocol) y H.323. Para la integración con Microsoft Teams requiere de un controlador de sesión de borde (Session Border Controller, SBC) como interfaz de comunicación con la plataforma.

**Tabla 4.12: Módulos y funcionalidades de Asterik.**

Módulo	Funcionalidades
Aplicaciones	- Varias de las acciones aplicadas en una llamada: Dial (), Directorio (), Playback (), Playtones (), Queu (), Record (), Transfer (), Voicemail (), etc.

Bridging	- Utilizado por la aplicación confbridge para conferencias (múltiples participantes).
Registro de llamada detallada (CDR)	- Facilita varios métodos de grabación de llamadas como archivos, base de datos, syslog, etc.
Registro de eventos del canal (CEL)	- Proporciona mayor control sobre el reporte de actividad de llamadas.
Controladores de Canal	- Permite la ejecución y recepción de llamadas, de acuerdo al protocolo o tipo de canal: SIP, ISDN, etc.
Traductores de Codec	- Convertidor de varios codecs: G729, G711, G722, etc.
Intérpretes de Formato	- Trabaja sobre archivos grabados en wav, gsm, jpeg, etc., determinando el formato adecuado a utilizar para reproducir la grabación
Funciones de Dialplan	- Complementan las funcionalidades del módulo de aplicaciones como blacklist (), dialgroup (), callerid (), etc.
Módulos de Recursos	- Integración con recursos externos: sistemas de calendario, directorio activo (LDAP), base de datos (ODBC), etc. - Complementa las funcionalidades de los demás módulos: SNMP (), fax (), crypto (), log (), etc.
Módulos Add-on	- Hacer y recibir llamadas VoIP utilizando el protocolo H.323. - Permite reproducir archivos en MP3.

Fuente: Autor

- **Denwa Technology:** las soluciones tecnológicas que ofrece integran las comunicaciones de forma unificada, permitiendo simplificar la gestión, optimizar los recursos y brindar respuestas a las necesidades de la empresa con un alto grado de calidad de servicio (Denwa, 2019), en Guayaquil algunos de los proveedores principales que proveen la marca son Intcomex y Telered. Las funcionalidades posibilitan la movilidad de los usuarios, asegurando y optimizando las comunicaciones sobre internet con tipos de instalaciones en el local del cliente appliances o cloud. La tabla 4.13 presenta un resumen de las características principales que provee Denwa, considerando que para la integración con Microsoft Teams requiere de un SBC como interfaz de comunicación con la plataforma.

**Tabla 4.13: Funcionalidades principales de la tecnología Denwa.**

Funcionalidad	Descripción
IVR o recepcionista digital	- Permite que las llamadas externas sean atendidas automáticamente, logrando que interactúen con el sistema telefónico a través de un menú de navegación.
Buzón de voz	- En caso de requerirse, cada extensión podrá disponer de un buzón de voz para llamadas que no hayan podido ser contestadas.
Softphone	- Software desarrollado en Denwa que permite comunicar una computadora ofreciendo funciones

	similares a los dispositivos de telefonía IP.
Grabación de llamadas	- Realiza la grabación de llamadas entrantes y salientes de las extensiones.
Salas de conferencia	- Permite realizar reuniones virtuales entre varios usuarios internos o con llamadas externas a través de la digitación de un prefijo.
Enrutamiento de menor costo	- O enrutamiento inteligente, direcciona las llamadas por la troncal en la cual los minutos generen menos costos.
Estadísticas y reportes	- Obtiene reportes detallados de las llamadas realizadas por los usuarios como tiempo de duración, fecha, número destino, etc.
Billing	- Administra un centro de costos, definiendo valores por conexión y duración de las llamadas en base a la numeración de destino.
Roaming de extensiones (Movilidad)	- Permite el registro de usuarios en la central desde un sitio remoto (fuera de oficina o país) y que reciban llamadas como si estuvieran en su lugar de trabajo.
Directorio	- Administra extensiones, contactos personales o empresariales, guía telefónica, integración con google maps y LDAP.

Fuente: Autor

- **Yeastar:** aportando al mercado de las telecomunicaciones desde el año 2006, ha convertido la telefonía IP en una tecnología asequible al sector PYME, ofreciendo innovadoras soluciones de comunicaciones unificadas interoperables con los distintos fabricantes como la integración de Microsoft Teams, mejorando el rendimiento y competitividad de las empresas frente al entorno cambiante. Dentro del portafolio de productos diseñados para las necesidades de comunicación de voz está S-Series VoIP PBX junto con la aplicación de Linkus UC disponible para los sistemas operativos más comunes, ofreciendo funcionalidades que permiten movilidad, gran flexibilidad y confiabilidad desde una misma plataforma, resumidas en la tabla 4.14. En Guayaquil una de las empresas reconocidas en el medio que trabaja con la marca es Totaltek.

**Tabla 4.14: Funcionalidades principales de la tecnología Yeastar.**

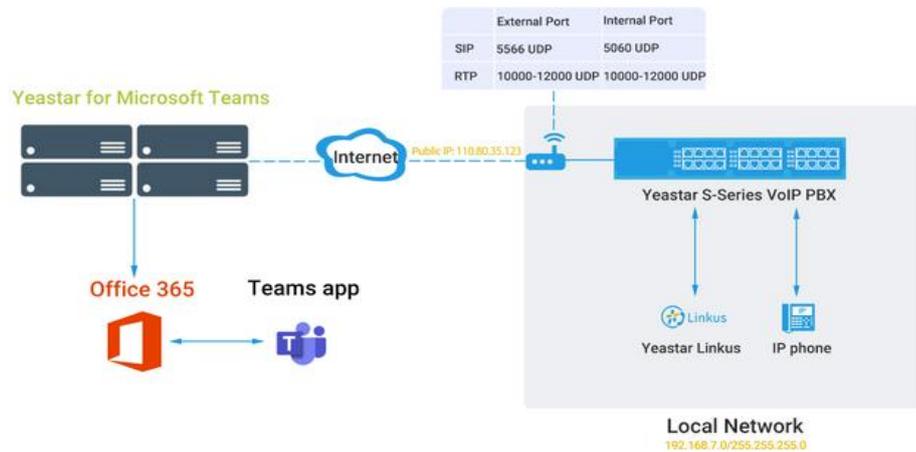
Funcionalidad	Descripción
Llamadas entrantes	- Los beneficios que ofrece permiten redirigir una llamada a otro dispositivo, enrutamiento según las reglas especificadas a cada extensión, parqueo de llamadas, atención según prioridad, condición de tiempo para enrutamiento de llamadas, identificación, entre otras. Con la utilización de features como: AutoCLIP, Call Forwarding, Call Parking, Call Pickup, Call Routing, Call Waiting, Caller ID, Dial by Name, Follow Me, Queue, Ring Group, Time Conditions, etc.

Llamadas salientes	<ul style="list-style-type: none"> <li>- Ofrece funciones que posibilitan realizar consultas de disponibilidad de extensiones antes de enrutar, devolución de llamadas, música de espera, acceso rápido con Linkus, muestra del estado de otras extensiones, marcado de números cortos, número de emergencia, entre otras. A través de los features: Attended Transfer, BLF Support, Blind Transfer, Callback, Emergency Number, Music On Hold, Speed Dial, Linkus Click to Call.</li> </ul>
Negocios	<ul style="list-style-type: none"> <li>- Realiza la grabación de llamadas entrantes y salientes de las extensiones, colocación de números en listas negras, grabación de propio mensaje de voz, atención de llamadas de forma automática, asignación de PIN, extensiones móviles, integración con otras plataformas, supervisión de llamadas, marcación de varias extensiones con una llamada, clientes Linkus, anuncios a través del altavoz, entre otras. Mediante los features Blacklist, Call Monitor, Call Recording, Custom Prompts, IVR (Interactive Voice Response), Linkus Mobile&amp;Desktop, Paging/Zone Paging, PIN List, Whitelist, Mobility Extension, SIP Forking, Remote Management, CRM Integration, etc.</li> </ul>
Colaboración	<ul style="list-style-type: none"> <li>- Permite realizar reuniones virtuales con Linkus , conferencias, video llamadas, llamadas tripartitas, entre otras. Utilizando features como: Conference, Instant Meeting on Linkus, Three-way Calling, Video Calls, Linkus Cloud Service, Contacts.</li> <li>- Obtiene reportes detallados de las llamadas realizadas por los usuarios, registra log de eventos, administra extensiones, contactos personales o empresariales, integración con LDAP, soporte de SNMP, VPN, alta disponibilidad, monitoreo del estado de las líneas, entre otras. Al utilizar los features App Center, CDR (Call Detail Records), Event Notification, Event Logs, Exporting/Importing Extension, Hot Standby, LDAP, PBX Monitor, SLA (Shared-Line-Appearance), SNMP, etc.</li> </ul>
Administración	<ul style="list-style-type: none"> <li>- Firewall Interno, con soporte TLS y SRTP, bloqueo de direcciones IP</li> </ul>
Seguridad	<ul style="list-style-type: none"> <li>- Integración con Ms Teams sin incorporar hardware o software adicional en las instalaciones del cliente</li> </ul>
Comunicaciones Unificadas	<ul style="list-style-type: none"> <li>- Incorpora la app Linkus Softphone facilitando la comunicación empresarial desde un dispositivo móvil o desktop.</li> </ul>
Softphone	<ul style="list-style-type: none"> <li>- Agrega módulos con interfaces FXS, FXO, ISDN BRI, GSM/3G o E1/T1/PRI.</li> </ul>
Expansión	

Fuente: Autor

Las marcas mencionadas contienen funcionalidades con la capacidad de cumplir los requerimientos y expectativas que demanda la solución de las comunicaciones de voz regulares de un PBX. Sin embargo, la innovación tecnológica que ofrece **Yeastar** con el módulo de seguridad, colaboración y comunicaciones unificadas al integrar Ms Teams sin dispositivos adicionales, mostrado en la figura 4.5, establecen las ventajas que harán de Infamotor S.A., incrementar los niveles de productividad de los usuarios, agilizando la resolución

de problemas con las opciones de comunicación y el seguimiento en las operaciones. Considerando el número de personas que integran la empresa el modelo de referencia utilizado fue S-100 VoIP PBX (capacidad hasta de 100 usuarios).



**Figura 4.5:** Esquema de integración de Yeastar con Ms Teams.  
**Fuente:** (Yeastar, 2020)

#### 4.2.4.3 Especificaciones técnicas de servicios fijos: Datos, Internet y Telefonía

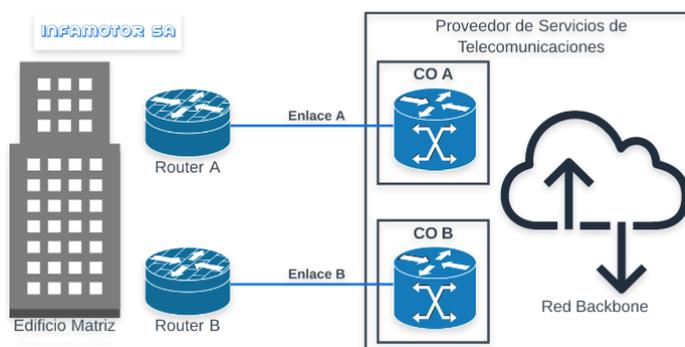
Los proveedores de servicios de telecomunicaciones ofrecen muchas opciones de conectividad para el acceso a internet, datos o telefonía, sin embargo, para poder seleccionar el adecuado a los requerimientos empresariales de Infamotor S.A., deben analizarse factores claves como la experiencia en el mercado, despliegue de infraestructura tecnológica, tiempos de respuesta ante fallos y disponibilidad, principalmente establecidos con un acuerdo de nivel de servicio (SLA). Por lo cual, han sido resumidas las características mínimas a cumplir en el presente diseño:

- **Disponibilidad:** es el porcentaje de tiempo que el servicio de datos y/o internet es utilizable para los usuarios, será medido mensualmente con un valor del 99.8%, en caso de no cumplirse el proveedor aplicará el respectivo descuento que determine el costo a cancelar, y estará calculado de acuerdo a la siguiente expresión (CNT, 2020):

$$D = \left( \frac{TD + TM}{TT} \right) \times 100 [\%]$$

- D (%): Disponibilidad, porcentaje de disponibilidad mensual del enlace.

- TD (horas): Tiempo Disponible, tiempo en el que el servicio estuvo disponible durante el mes.
  - TT (horas): Tiempo Total, tiempo de operatividad del servicio durante el mes, valor fijo detallado en horas: 672 (28 días), 696 (29 días), 720 (30 días) y 744 (31 días).
  - TM (horas): Tiempo de Mantenimiento, tiempo en el cual el enlace estuvo fuera de servicio por mantenimientos preventivos planificados por el proveedor y aceptados por Infamotor S.A.
- **Redundancia:** para garantizar la conectividad de los servicios frente a cualquier eventualidad que pueda surgir, el proveedor deberá implementar un sistema redundante con enlaces que trabajen en modo activo-pasivo, siguiendo el tipo de conexión Multihoming (tercera opción: dual routers, dual link to one ISP), esto es, dos conexiones de última milla al mismo ISP utilizando enrutadores independientes por cada enlace y bajo la configuración de un protocolo de alta disponibilidad, ilustrado en la figura 4.6.



**Figura 4.6:** Tipo de conexión Multihoming tercera opción.

**Fuente:** Autor

- **Redes de acceso:** las soluciones tecnológicas de redes de acceso que planteen los proveedores de servicio deberán incluir dos enlaces (principal, backup) con rutas de implementación hacia centrales de convergencia distintas, que posean características tales como inmunidad a la interferencia estática, inmunidad a la diafonía, mayor resistencia a las condiciones ambientales, baja latencia, escalabilidad a incrementos de velocidad de transmisión, garantizando una red confiable y de alto

rendimiento. Entre los medios de acceso más utilizados, sobresale la fibra óptica con sus ventajas técnicas como mejor alternativa de utilización.

- **Equipos de Enrutamiento:** Los equipos estarán asociados con las tecnologías de vanguardia y dimensionados con las capacidades requeridas por los servicios empresariales, disponiendo de características idénticas en funcionalidades que garanticen la alta disponibilidad, minimicen de forma considerable los riesgos de seguridad, así como también optimicen las operaciones.

La topología WAN de los proveedores tendrá que ser adaptable a las tecnologías futuras sin la necesidad de realizar grandes cambios en hardware/software con la infraestructura colocada en las instalaciones empresariales, asegurando la continuidad de los servicios. Por otra parte, la gestión y soporte de la red son aspectos a considerar dentro de la rentabilidad de la solución, así como también aspectos relevantes que determinarán la calidad de los enlaces, descritos a continuación:

- **Tiempo de respuesta:** mide el tiempo entre la solicitud de un usuario y la respuesta hacia un host destino que puede ser local, interurbano o internacional. Por ejemplo, la solicitud de una página web (HyperText Markup Language, HTML) tiene un límite en cuanto al tiempo de espera, que para los usuarios es reflejada en la rapidez en la que se actualiza la pantalla, dependiendo del tipo de aplicaciones o uso se consideran valores promedios de retardo (delay). De modo que, será tomado como referencia para la medición el protocolo ICMP mediante la herramienta de diagnóstico PING en un canal sin carga, con un tamaño de 64 bytes (defecto) y 1000 repeticiones:
  - Enlaces locales: delay < 30 ms, pérdidas menores al 2% que no afecten la calidad de los canales de voz.
  - Enlaces Interurbanos: delay < 90 ms, pérdidas menores al 2%.
  - Enlaces Internacionales: delay < 100 ms, pérdidas menores al 3%.
  - Satelitales: delay < 850 ms.
- **Velocidad de transmisión:** también conocido como ancho de banda, estará garantizada y definida por el proveedor en conjunto con el

departamento técnico de Infamotor S.A., considerando las capacidades necesarias para satisfacer las necesidades de los servicios de datos e internet que implican intercambio de archivos, tráfico interactivo, así como también la práctica innovadora de las aplicaciones (apps) de colaboración empresarial en tiempo real. Con lo que respecta al servicio de telefonía, la capacidad estará relacionada directamente con el códec a utilizar y la cantidad de llamadas simultáneas, evitando saturar el enlace.

- **Errores:** para las propuestas de solución con redes de transmisión en tecnologías SDH/DWDM a través de un clear-channel, donde es factible la medición, el proveedor garantizará una tasa de error de bit (BER) inferior a  $1 \times 10^{-8}$  medidos durante un período no menor a 24 horas, al momento de la instalación.
- **Pérdida de paquetes:** los servicios a contratar dispondrán de una pérdida de paquetes  $< 1\%$ .

Finalmente, las propuestas técnicas de los proveedores para el servicio de telefonía deberán incluir arquitecturas de nueva generación, con la utilización principal de protocolos como SIP/IP/MPLS que permitirán la convergencia de las redes de datos y voz a través de un mismo medio, reduciendo costos de inversión empresarial en implementación de varias redes de acceso en los servicios contratados. También brindará flexibilidad para el incremento de canales de voz en base a las necesidades de crecimiento, agregando una serie numérica de fácil recordatorio y un SLA que estará medido de forma mensual por el ASR (Answer Seizure Ratio), el cual determinará la calidad mediante el porcentaje de llamadas respondidas con respecto al total de llamadas realizadas, aplicable para todas las llamadas (locales, nacionales, internacionales y móviles).

#### **4.2.4.3 Especificaciones técnicas de servicios Datacenter**

Antes de la contratación de los servicios de cloud computing, el poder realizar una prueba de calidad gratis (demo) permitirá familiarizarse con las herramientas/plataformas y conocer si el proveedor solventará las necesidades empresariales. Asimismo, la reputación, confianza, expectativas generadas en las soluciones informáticas a sus clientes e información sobre la localización del centro de datos donde se alojará la información, agrupan algunos de los factores a

considerar en la selección del proveedor. A continuación, están consideradas las características de infraestructura y operación que un Datacenter deberá ofrecer:

- Alta disponibilidad con un estándar de infraestructura TIER III o IV, medido en horas y calculado de forma anual con un valor del 99.982%, de acuerdo a la siguiente expresión (CNT, 2020):

$$D = \left( \frac{TD}{TT - TM} \right) \times 100 \text{ [%]}$$

- D (%): Disponibilidad, porcentaje de disponibilidad anual del servicio.
  - TD (horas): Tiempo Disponible, tiempo en el que el servicio estuvo disponible durante el año.
  - TT (horas): Tiempo Total, tiempo de operatividad del servicio durante el año, valor fijo detallado en horas: 8760 (365 días).
  - TM (horas): Tiempo de Mantenimiento, tiempo en el cual el enlace estuvo fuera de servicio por mantenimientos preventivos planificados por el proveedor y aceptados por Infamotor S.A., o a cualquiera de los motivos considerados como casos fortuitos o de fuerza mayor.
- Agilidad en la implementación de servicios con las opciones de SaaS (Software as a Service), IaaS (Infrastructure as a Service) y PaaS (Platform as a Service).
  - Tiempo de recuperación ante fallas (Mean Time to Recovery, MTTR) del Datacenter máximo de 3 horas al año.
  - Los niveles de servicio para el soporte técnico estarán categorizados de acuerdo a su severidad, bajo la definición de prioridades en modalidad 7x24x365 mostrados en la tabla 4.15.
  - Escalabilidad para aumento o disminución de capacidades con alternativas de almacenamiento público, privado o híbrido.
  - Accesibilidad de gestión con cifrado de información, servicios de seguridad proporcionando protección a datos y aplicaciones.
  - Actualizaciones tecnológicas (software, plataformas) de forma periódica.
  - Monitoreo continuo de la actividad de red, nivel de consumo y rendimiento de los recursos.
  - Valor agregado con infraestructura hiperconvergente y soluciones de recuperación ante desastres.

- Firewall virtual que permita realizar un análisis de tráfico, control, bloqueo, escaneo, entre otras acciones más, para garantizar la seguridad de la información y aplicaciones empresariales.

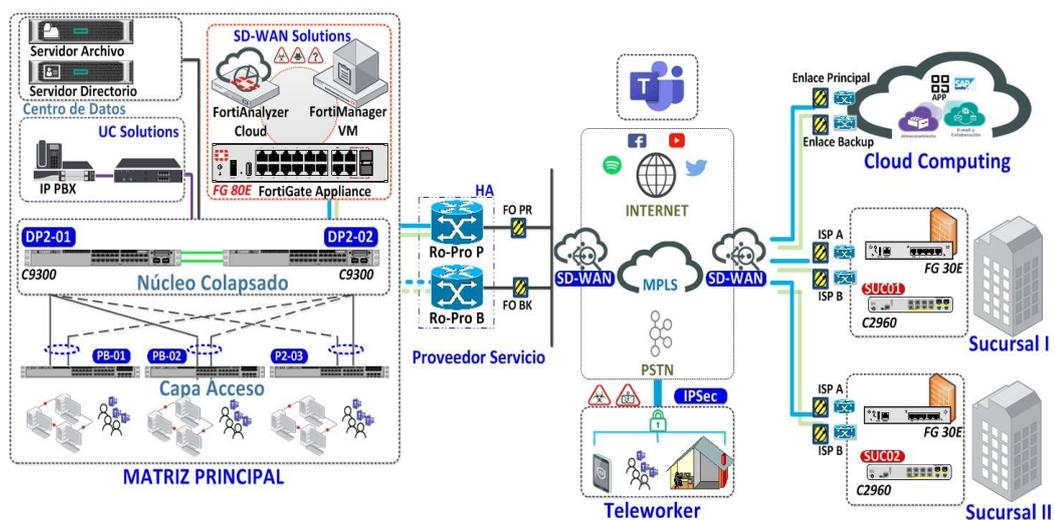
**Tabla 4.15: Niveles de Servicio Datacenter.**

Prioridad	Tiempo de Respuesta	Modalidad de comunicación	Tiempo máximo de diagnóstico inicial	Tiempo de solución / cambio de repuestos
<b>Clase A</b>	15 minutos	Telefónica y/o e-mail.	1h posterior a la comunicación.	4h posteriores al resultado del diagnóstico
<b>Clase B</b>	15 minutos	Telefónica y/o e-mail.	2h posteriores a la comunicación.	8h posteriores al resultado del diagnóstico
<b>Clase C</b>	15 minutos	Telefónica y/o e-mail.	4h posteriores a la comunicación.	16h posteriores al resultado del diagnóstico

Fuente: Autor

### 4.3 Diseño de redes de comunicación

La selección del modelo de arquitectura empresarial para el diseño de solución tecnológica de Infamotor S.A., tendrá la capacidad de cumplir con los requerimientos actuales y futuros que demandan las operaciones en el giro del negocio. La segmentación por módulo ofrecerá principalmente simplicidad para el administrador de red en la ejecución de soporte técnico (troubleshooting), visibilidad de toda la infraestructura, administración centralizada de las soluciones de comunicación, registro único de eventos o alarmas de los sistemas, habilidad de la red para reaccionar y adaptarse a los cambios de evolución.



**Figura 4.7:** Esquema de conexión del diseño de solución tecnológica.

Fuente: Autor

La figura 4.7 presenta el esquema de conexión de los módulos del modelo de arquitectura empresarial propuesto para Infamotor S.A., con características técnicas y de funcionamiento que cumplirán con la demanda de rendimiento, automatización o simplificación de los procesos, organizadas en los siguientes criterios:

- Infraestructura de red LAN
- Seguridad de la red empresarial
- Solución de integración con proveedores
- Solución SD-WAN con administración centralizada
- Solución de Comunicaciones Unificadas (UC)

#### **4.3.1 Infraestructura de red LAN**

La solución tecnológica con enfoque modular principalmente permitirá implementar características de seguridad por sección, evaluando la relación con los distintos bloques funcionales de la red que tendrá las siguientes propiedades a nivel LAN:

- Los equipos de la capa de acceso dimensionados corresponden al modelo Cisco 9200, como la nueva evolución de Switch Catalyst que reemplaza a la serie 2960, estarán distribuidos en los rack (PB-01, PB-02, P2-03) donde convergen los puntos de red de usuarios en el edificio matriz.
- Los equipos de la capa núcleo-colapsado dimensionados corresponden al modelo Cisco 9300 como la nueva evolución de Switch Catalyst que reemplaza a la serie 3850, estarán colocados en el rack P02-03 del cuarto de equipos del edificio matriz.
- Las interfaces de Uplink de los Cisco 9200 estarán conectados a la capa superior físicamente con una red de acceso de fibra óptica y lógicamente con la utilización del protocolo EtherChannel, brindando alta disponibilidad e incremento en la velocidad de transmisión, esto eliminaría el uso del protocolo STP agregando simplicidad a la operación de la red.
- La funcionalidad de stacking switches que ofrece Cisco con la serie 9300 proporciona una característica de alta disponibilidad que permitirá obtener un solo equipo virtual en la capa de núcleo-colapsado, optimizando la

administración y control de las interfaces. Las interfaces de Uplink estarán distribuidas para la conexión con los equipos de acceso C9200.

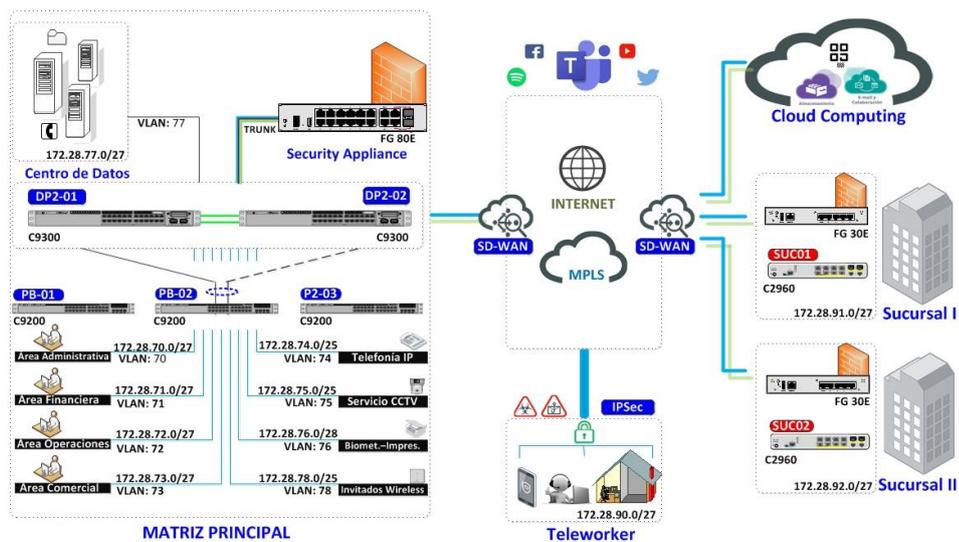
- El paquete de licenciamiento de los equipos correspondería a la opción de suscripción de la arquitectura de red digital de Cisco (Digital Network Architecture, DNA) Advantage como un modelo flexible de protección de inversión que incluye principalmente: segmentación de red (VRF), visibilidad (NetFlow), integración de IoT, mecanismos de seguridad, funcionalidades fundamentales (VLAN, VRRP, PBR, CDP, QoS) y avanzadas de conmutación (BGP, EIGRP, HSRP, IS-IS, IP SLA, OSPF).
- Utilización de la tecnología de segmentación de VLAN privada (PVLAN) que logrará limitar la comunicación de una interfaz directamente con otras, introduciendo múltiples dominios de broadcast que dividirán el tráfico para mejorar la seguridad y rendimiento en los equipos de conmutación.
- Los puertos de los equipos Cisco 9200 asignados a los hosts estarán configurados sin etiquetar (untagged), utilizando el comando “switchport mode access” con la VLAN de datos del grupo correspondiente, adicional tendrán la integración de la telefonía IP mediante el comando “switchport voice vlan” para optimizar sobre un mismo punto de red la operatividad de ambos servicios. La tabla 4.16 presenta el plan de direccionamiento IP propuesto que tendrá la capacidad de cumplir los requisitos actuales o de crecimiento futuro, estableciendo una asignación dinámica de dirección para los usuarios y estática para los dispositivos.

**Tabla 4.16: Plan de direccionamiento IP.**

<b>Grupo</b>	<b>VLAN ID</b>	<b>Segmento de Red</b>	<b>Default Gateway</b>
Área Administrativa	70	172.28.70.0/27	172.28.70.1/27
Área Financiera	71	172.28.71.0/27	172.28.71.1/27
Área de Operaciones	72	172.28.72.0/27	172.28.72.1/27
Área Comercial	73	172.28.73.0/27	172.28.73.1/27
Servicio Telefonía IP	74	172.28.74.0/25	172.28.74.1/25
Servicio CCTV	75	172.28.75.0/25	172.28.75.1/25
Sistema Biométrico - Impresoras	76	172.28.76.0/28	172.28.76.1/28
Servidores de Aplicaciones	77	172.28.77.0/28	172.28.77.1/28
Invitados Wireless	78	172.28.78.0/25	172.28.78.1/25
Administración de equipos	100	10.28.100.0/27	10.28.100.1/27
Conexión VPN (Teleworker)		172.28.90.0/27	
Sucursal I	20	172.28.91.0/27	172.28.91.1/27
Sucursal II	30	172.28.92.0/27	172.28.92.1/27

Fuente: Autor

- Las interfaces no utilizadas en los equipos de conmutación serán desactivadas, con la finalidad de impedir la conexión de usuarios no autorizados con el resto de la red.
- Los equipos Cisco 9200 de la capa de acceso cumplen con el estándar PoE IEEE 802.3af con una potencia máxima de 15.4 W que permitirá la alimentación de los teléfonos IP y 802.3at (30.0 W) para la conexión de los puntos de acceso (AP), el suministro a cada dispositivo será determinado automáticamente por medio de la auto negociación, consiguiendo de esta manera reducir costos de implementación en cableado de energía eléctrica.
- La figura 4.8 muestra los componentes de la infraestructura de red que formarán una topología lógica tipo estrella, estableciendo como punto de convergencia los equipos de la capa núcleo-colapsado.



**Figura 4.8:** Topología lógica tipo estrella de Infamotor SA.  
Fuente: Autor

- Los equipos de red establecerán mecanismos de seguridad como: bloqueo de acceso por telnet, desactivación de los servicios no necesarios, registro apropiado del nivel de privilegio de los usuarios y restricción al protocolo SNMP.
- Los equipos de red tendrán sincronizados los relojes con la utilización del protocolo de tiempo de red (Network Time Protocol, NTP) para

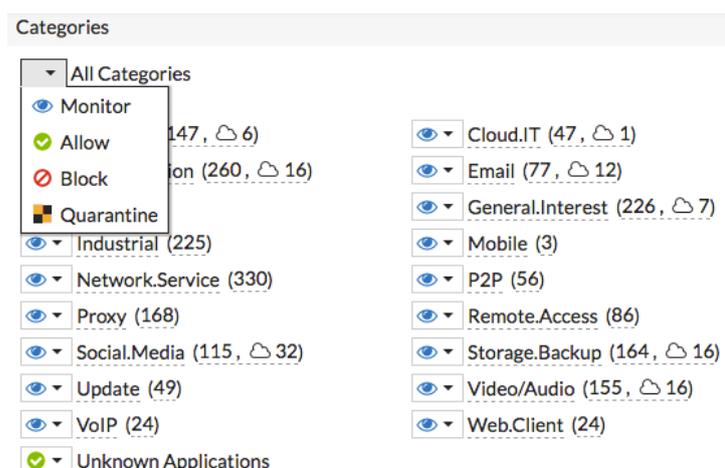
simplificar la gestión y generación de informes, útiles para solucionar problemas de red o amenazas de seguridad.

- Las interfaces de los equipos Cisco 9200 de la capa de acceso utilizarán el mecanismo de seguridad port security mediante la línea de comando “switchport port-security maximum 2” para limitar el registro de direcciones MAC por puerto, restringiendo la conexión de dispositivos no autorizados o el ataque de seguridad por inundación de la tabla de memoria de contenido direccionable (Content Addressable Memory, CAM), conocido como MAC flooding attack.

### 4.3.2 Seguridad de la red empresarial

El diseño de la presente solución fue considerado para un ambiente empresarial PyME, contemplando al NGFW principalmente para la mitigación de riesgos, detección de ataques y protección de la información, entre sus funcionalidades destacan las siguientes:

- **Control de aplicaciones:** la utilización de la red estará controlada mediante la administración de aplicaciones, al identificar y categorizar las mismas en mensajería instantánea, peer-to-peer, VoIP, streaming, etc., dando prioridad a las de alta relevancia lo que logrará optimizar el ancho de banda con opciones de bloqueo, permiso, monitoreo o colocación en cuarentena.



**Figura 4.9:** Categorías de las aplicaciones del NGFW FG-80E.

**Fuente:** Autor

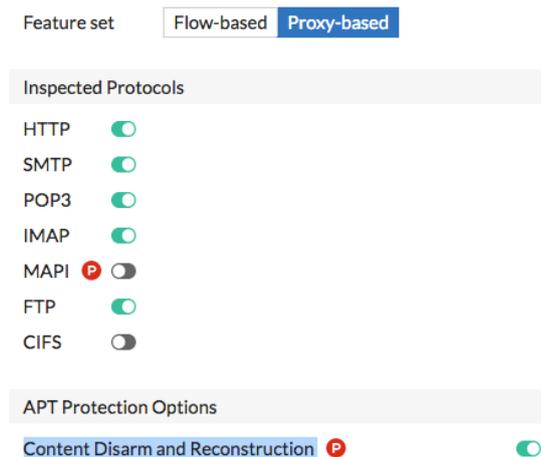
- **Filtrado Web:** con la funcionalidad de filtrado web cada departamento tendrá configurado un perfil de navegación según el rol que desempeñe en

la empresa, con las opciones de autorización o denegación de acceso a las páginas distribuidas en categorías de contenido adulto, sitios web ilegales, sitios web peligrosos, entretenimiento, redes sociales o sitios no categorizados.

Name	Action
Potentially Liable 9	
Adult/Mature Content 15	
Bandwidth Consuming 6	
Security Risk 6	
General Interest - Personal 35	
General Interest - Business 15	
Unrated 1	

**Figura 4.10:** Filtrado Web basado en categorías.  
**Fuente:** Autor

- **Anti-Virus:** la funcionalidad del anti-virus actuará como la primera línea de protección de la red empresarial contra alguna amenaza potencial, malware o virus inusual, al realizar la inspección de protocolos como HTTP, HTTPS, FTP, SMTP y POP3 con una base de datos de firmas actualizadas. La configuración utilizaría el modo proxy que incorpora la característica de desarmado y reconstrucción de contenido (Content Disarm and Reconstruction, CDR), para la prevención de archivos en formato de compresión zip con documentos de Office maliciosos.



**Figura 4.11:** Configuración Anti-virus opción CDR en modo proxy.  
**Fuente:** Autor

- **Prevención de intrusos:** proporcionará una inspección a fondo de paquetes del tráfico entrante/saliente para detectar y bloquear mediante la comparación de firmas de amenazas conocidas los ataques de red. Las funcionalidades de IPS incorporarán bloqueo de conexiones a dominios botnet (redes de robots informáticos), registro de eventos y notificaciones al administrador de red en el momento que ocurre un incidente, estableciendo una protección más confiable a los sistemas operativos y las aplicaciones web.
- **Filtrado de correo:** la red empresarial de Infamotor S.A., dispondrá de la funcionalidad de filtrado de correo para protección contra spam (correo no deseado) y ataques de phishing, que hoy en día el mayor porcentaje integra algún tipo de malware. Las configuraciones permitirán la creación de reglas de control para el bloqueo o autorización de fuentes específicas (servidores SMTP y POP3), filtrado de direcciones IP una vez detectado el origen del spam y defensa contra ataques zombie (sistema informático comprometido que es controlado remotamente para envío de spam).

Las configuraciones básicas recomendadas para la puesta en operación de los equipos NGFW que conforman la solución tecnológica (FG-80E/30E) de la red empresarial de Infamotor S.A., serían las siguientes:

- Configuración de reglas en Web Filtering, mediante la selección de categorías y definición de grupos de usuarios, por ejemplo: VIP, General e Invitados.
- Configuración de interfaces y zonas de seguridad para los tipos de redes las LAN, WAN, DMZ y SD-WAN.
- Configuración de perfiles y políticas en la funcionalidad de control de tráfico (Traffic Shaping).
- Configuración de al menos un perfil de la funcionalidad de Anti-virus.
- Configuración de perfiles de la funcionalidad control de aplicaciones, definidos por el rol de cada departamento.
- Configuración de al menos un perfil de la funcionalidad IPS.
- Creación de objetos de red y la vinculación con las políticas de firewall.
- Configuración de un perfil de la funcionalidad VPN SSL para el acceso remoto seguro de los usuarios a los recursos empresariales.

- Integración con el servidor de directorio activo a través de LDAP.

### 4.3.3 Solución de integración con proveedores

Para la integración de servicios de telecomunicaciones los equipos Cisco 9300 con sus especificaciones técnicas de alto rendimiento en enrutamiento IP, actuarán como equipos de borde soportando protocolos estándares o propietarios según la marca de equipos que instalen los proveedores. Por lo que, el diseño de solución propuesta contiene las siguientes características que garantizarán la alta disponibilidad:

- **Topología:** los servicios de datos mantendrán una topología lógica hub-and-spoke (estrella), al establecer el edificio matriz como punto principal de convergencia con conexiones a las sucursales mediante la tecnología WAN MPLS. La red brindará beneficios como disminución de costos de implementación, reducción de enlaces punto a punto, incremento de disponibilidad con la implementación de un enlace backup en la matriz, administración centralizada y simplificada.
- **Soporte para crecimiento:** las sucursales deberán configurarse con el protocolo de enrutamiento dinámico EIGRP propietario de los equipos Cisco 9300 o estándar como OSPF, con una tecnología WAN capaz de soportar los requerimientos actuales y la expansión de red empresarial a futuro. El propósito fundamental de los protocolos es reducir la complejidad operacional y mantenimiento de red, al determinar de forma dinámica la mejor ruta para alcanzar un destino sin intervención del analista técnico de TI.
- **Segmentación de red:** los servicios de telecomunicaciones estarán segmentados lógicamente independientes a través de una misma infraestructura física. Cada servicio administrará sus propias políticas de seguridad, tablas de enrutamiento y reglas de QoS, utilizando la tecnología de virtualización VRF implementada en entornos MPLS.
- **Calidad de servicio:** la operatividad de los servicios de telecomunicaciones a través de un mismo medio físico junto con el crecimiento de demanda de las aplicaciones de voz y video exigirá que los

proveedores en su propuesta técnica incluyan tecnología confiable, calidad de servicio e ingeniería de tráfico.

- **Alta disponibilidad:** los servicios de telecomunicaciones en la matriz de convergencia dispondrán de un enlace de backup que incrementará la disponibilidad, convirtiéndolo en un factor importante para garantizar la continuidad del negocio. Los enlaces de datos utilizarán el protocolo de enrutamiento dinámico para la conmutación automática, seleccionando la mejor ruta hacia un destino conforme a los parámetros que definen la métrica: número de saltos, ancho de banda, costo, carga, retraso y confiabilidad. Por otra parte, las conexiones de los servicios Internet y Troncal SIP utilizarían rutas estáticas definiendo la prioridad por la distancia administrativa del enlace principal, configuradas con el mecanismo de monitoreo del host destino track (rastreo) que estará vinculado a la tecnología IP SLA de Cisco, en caso de pérdida de conectividad la ruta quedará inactiva y el tráfico será enrutado al enlace de backup.
- **Seguridad:** los equipos locales del cliente (Customer Premises Equipment, CPE) y de borde de la red empresarial, establecerán políticas de seguridad para control de acceso no autorizado a subredes específicas. Por otra parte, con el servicio de internet serán establecidas conexiones VPN site-to-site compuestas por IPSec en modo de transporte, empleando encapsulación ESP (Encapsulated Security Payload) y los parámetros de configuración por fase descritos en la tabla 4.17.

**Tabla 4.17: Parámetros de configuración por fase para VPN Site-to-Site.**

	Propiedades del túnel	Información de configuración
<b>Fase 1</b>	Método de Autenticación	PRE-SHARED KEY
	Esquema de Cifrado	IKE
	Grupo Diffie-Hellman	GRUPO 5
	Algoritmo de Cifrado	AES256
	Algoritmo de Hashing	SHA-1
	Modo Main o Agresivo	MAIN
	Lifetime	86400 S
<b>Fase 2</b>	Encapsulación	ESP
	Algoritmo de Cifrado	AES256
	Algoritmo de Autenticación	SHA-1
	Perfect Forward Secrecy	NO PFS
	Lifetime	3600 S

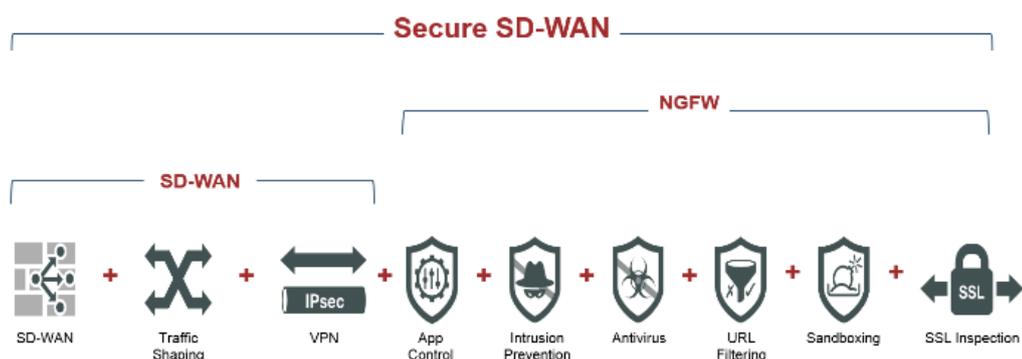
Fuente: Autor

#### 4.3.4 Solución SD-WAN con administración centralizada

Para establecer comunicación hacia las sucursales o los servicios de cloud computing existen varias soluciones a nivel WAN disponibles por los proveedores de servicios, sin embargo, están presentes los problemas en las redes como: alta latencia, pérdida de paquetes o saturación de enlace. SD-WAN es uno de los avances tecnológicos que permite solventar estos inconvenientes al incorporar calidad de servicio con una selección dinámica de enlaces.

SD-WAN es una interfaz virtual que asocia todas las interfaces que pueden estar conectadas a diferentes tipos de enlaces, simplificando la configuración al establecer un solo grupo de políticas de enrutamiento y control de acceso aplicable a todos los miembros. Cabe agregar, la selección de enlace definido acorde al tipo de tráfico o el uso de algoritmos de balanceo (load balanced) de carga para el incremento de disponibilidad.

Fortinet como la marca citada para la solución de la capa de seguridad en el presente caso de estudio, ofrece **SD-WAN Seguras** que integra las funcionalidades de los NGFW. De modo que, permitirá la comunicación en el escenario existente de la empresa Infamotor S.A., incorporando visibilidad, escalabilidad, así como también calidad de servicio entre matriz principal, sucursales, nube privada y centro de datos on premise.

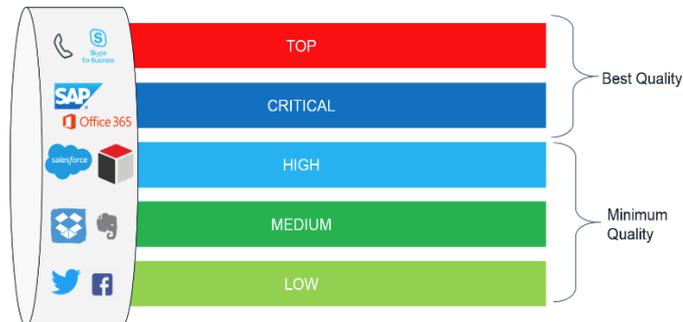


**Figura 4.12:** Solución SD-WAN seguras de Fortinet.

**Fuente:** Autor

El control de las aplicaciones podrá determinarse con criterios que miden la calidad del enlace en los distintos tipos de tecnología WAN. La figura 4.13 muestra cómo están categorizadas las aplicaciones según la recomendación de Fortinet, definiendo entonces, bajo los servicios proyectados en la arquitectura de

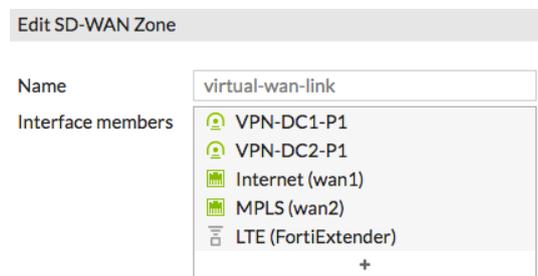
red empresarial a la conexión de Internet con la utilización de VPN IPsec como la ruta para **aplicaciones no críticas** (baja calidad) y la red de Datos mediante el protocolo MPLS para **aplicaciones críticas (alta calidad)**.



**Figura 4.13:** Categoría de las aplicaciones determinada por Fortinet.  
**Fuente: (Fortinet, 2020)**

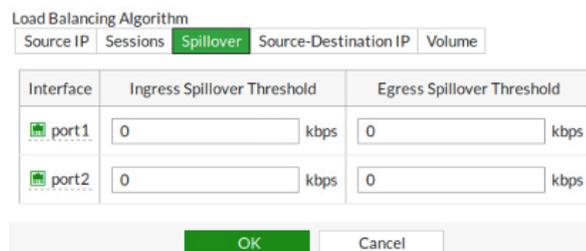
Las configuraciones de SD-WAN estarían realizadas en los modelos Fortigate considerados en el diseño de solución (FG 80E - 30E), siguiendo las siguientes recomendaciones:

- Asociación de las interfaces declaradas a nivel WAN para comunicación con las distintas localidades (Internet, MPLS, VPN IPsec, etc.) con la interfaz SD-WAN.



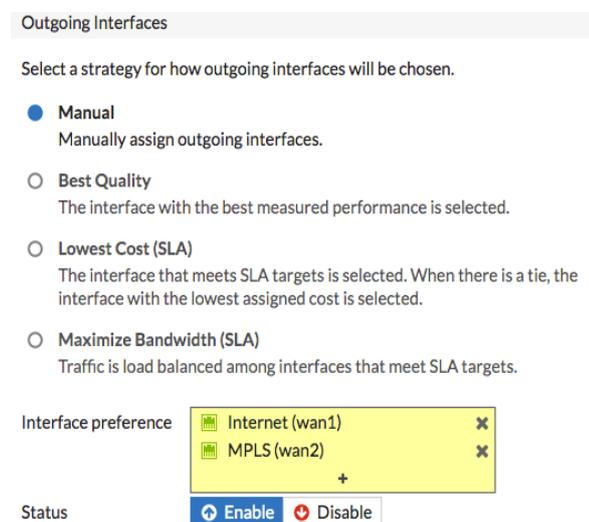
**Figura 4.14:** Ejemplo de configuración de interfaz SD-WAN.  
**Fuente: Autor**

- Configuración de condiciones para las opciones de load balanced, relacionados con la definición de categoría establecidas a las aplicaciones.



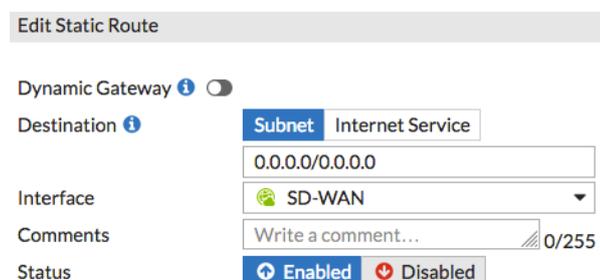
**Figura 4.15:** Ejemplo de configuración de criterios de load balanced.  
**Fuente: Autor**

- Configuración de las reglas de control de acceso SD-WAN, de acuerdo a la prioridad que requieren las aplicaciones:
  - **Manuales:** a criterio del administrador de la red.
  - **Mejor Calidad:** determina los criterios de rendimiento de enlace como latencia, jitter, pérdida de paquetes y capacidad de descarga.
  - **Menor costo:** selección de condición asignado a las interfaces en las configuraciones de load balanced (SLA)
  - **Umbral de Ancho de Banda:** selección de condición a los valores definidos como umbrales de tráfico en las configuraciones de load balanced (SLA).



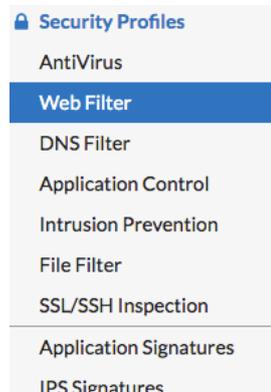
**Figura 4.16:** Opciones para configuración de reglas de SD-WAN.  
**Fuente:** Autor

- Configuración de ruta por defecto a la interfaz SD-WAN, Fortigate asociará a cada una las interfaces miembros.



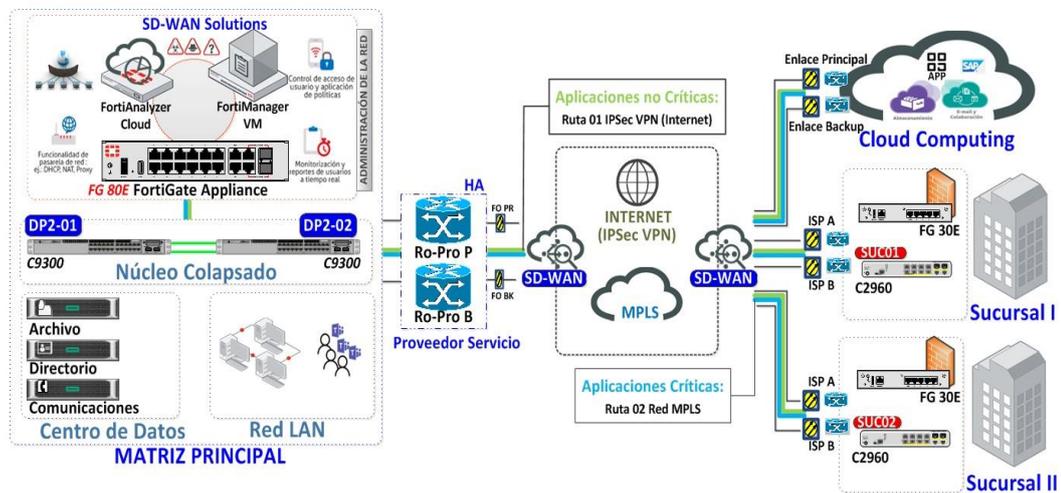
**Figura 4.17:** Ejemplo de configuración de ruta por defecto SD-WAN.  
**Fuente:** Autor

- Configuración de seguridad a nivel de aplicaciones: IPS, AppCtrl, políticas control de acceso (Firewall), AV, Sandboxing, Filtrado web y autenticación con AD.



**Figura 4.18:** Configuración de seguridad a nivel de aplicaciones.  
**Fuente:** Autor

Con la arquitectura de red empresarial definida para el presente caso de estudio, la integración de la solución SD-WAN segura con administración centralizada, quedaría esquematizada según la representación de la figura 4.19, utilizando las conexiones de alta disponibilidad que ofrecen los proveedores para los servicios de Internet y datos.

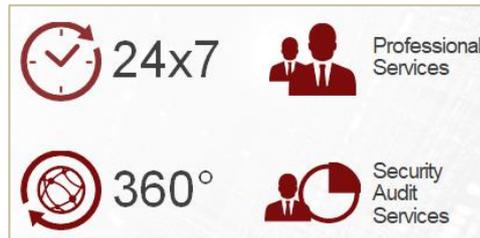


**Figura 4.19:** Diseño de solución SD-WAN con administración centralizada.  
**Fuente:** Autor

#### 4.3.4.1 Licenciamiento de equipos Fortigate

Las soluciones de SD-WAN seguro incluyen servicios de soporte con FortiCare y seguridad con FortiGuard que tienen una vigencia de licenciamiento de 12, 24 o 36 meses, establecidas según los requerimientos de aplicación.

- **FortiCare:** el servicio de atención al cliente que proporciona asistencia técnica global para todos los productos Fortinet, con soporte en las Américas, Europa, Medio Oriente y Asia.



**Figura 4.20:** Servicio de Soporte FortiCare.  
**Fuente:** (Fortinet, 2020)

- **FortiGuard:** servicio de seguridad de Fortinet que incluye el licenciamiento de los módulos IPS, Antivirus, Filtrado Web, Control de Aplicaciones, FortiSandbox Cloud, Data Loss Prevention, AntiSpam, actualizaciones de las firmas de ataques globales y de día cero.

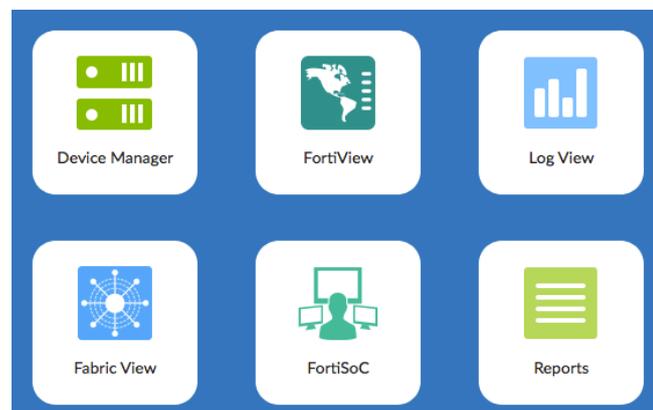


**Figura 4.21:** Servicio de seguridad FortiGuard.  
**Fuente:** (Fortinet, 2020)

#### 4.3.4.2 Componentes adicionales

Para gestionar todo el entorno SD-WAN desde un único punto central, controlando los túneles IPSec, estado de los enlaces, amenazas avanzadas, incidencias de red, gestión de alarmas, análisis y recopilación de eventos, entre otros, Fortinet ofrece los siguientes componentes adicionales para una completa visibilidad en tiempo real e informes personalizados:

- **FortiAnalyzer:** es un servicio gestionado en la nube de Fortinet que permitirá recopilar, analizar y correlacionar datos de registro de la red distribuida por los equipos Fortigate (FG 80E, FG 30E) desde una ubicación central. Simplificará la complejidad de monitoreo proporcionando información detallada sobre amenazas a través de la orquestación y automatización en un solo panel de visualización, reduciendo riesgos de ataques e incrementando la seguridad de Infamotor S.A. Los beneficios adicionales que brindará la herramienta son descritos a continuación:
  - Detección/correlación de amenazas avanzadas para identificar y responder de forma inmediata a los ataques de seguridad.
  - Automatización de los flujos de trabajo y generación de informes.
  - Recopilación, gestión de registro en tiempo real e histórico de eventos en los equipos Fortigate.
  - Búsqueda centralizada e intuitiva que informará sobre tráfico de red, amenazas y actividades.
  - Resumen de aplicaciones, fuentes, destinos, sitios web, amenazas de seguridad, modificaciones administrativas y eventos del sistema.



**Figura 4.22:** Centralización de eventos y reportes con FortiAnalyzer.  
**Fuente:** Autor

- **FortiManager:** es un servicio on premise que logrará administrar de forma centralizada los dispositivos FortiGate y FortiAnalyzer desde una misma consola, con una visibilidad completa y gestión de seguridad sofisticada para la protección de amenazas avanzadas a la red empresarial

de Infamotor S.A. Los beneficios adicionales que brindará la herramienta son descritos a continuación:

- Orquestar dispositivos y sistemas optimizando el aprovisionamiento de red, políticas de seguridad o gestión de cambios.
- Automatizar los procesos de control y cambio, reduciendo las tareas administrativas.
- Visibilidad centralizada de toda la superficie de ataque digital con funciones de detección precisa, correlación automatizada y rápida respuesta.



**Figura 4.23:** Ejemplo de integración de herramientas en FortiManager.

**Fuente:** Autor

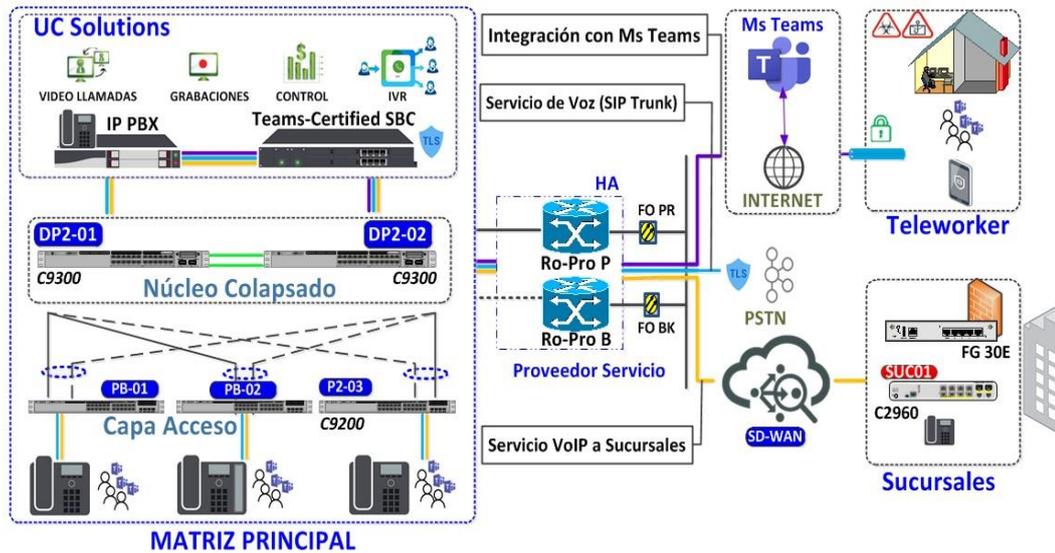
#### 4.3.5 Solución de Comunicaciones Unificadas (UC)

La empresa Infamotor S.A., dentro de sus servicios dispone de la telefonía tradicional para comunicación de voz y uno de los planes empresariales más completos de productividad que ofrece Office 365 como Enterprise E5. Para esto, el diseño de innovación tecnológica propuesto con la solución de comunicaciones unificadas permitirá la integración de ambos, al tener una plataforma única y de colaboración con Microsoft Teams. Las conexiones de Microsoft pueden realizarse con las siguientes opciones:

- Adquiriendo un plan de llamadas de Microsoft (nacional e internacional).
- Utilizando la infraestructura telefónica on premise a través de **Phone System Direct Routing**.

La opción de adquisición del plan de llamadas que ofrece Microsoft con el servicio de Teams no está disponible para Ecuador, por lo tanto la solución de comunicaciones unificadas considerada a utilizar es Direct Routing que integra el servicio de telefonía con los proveedores locales.

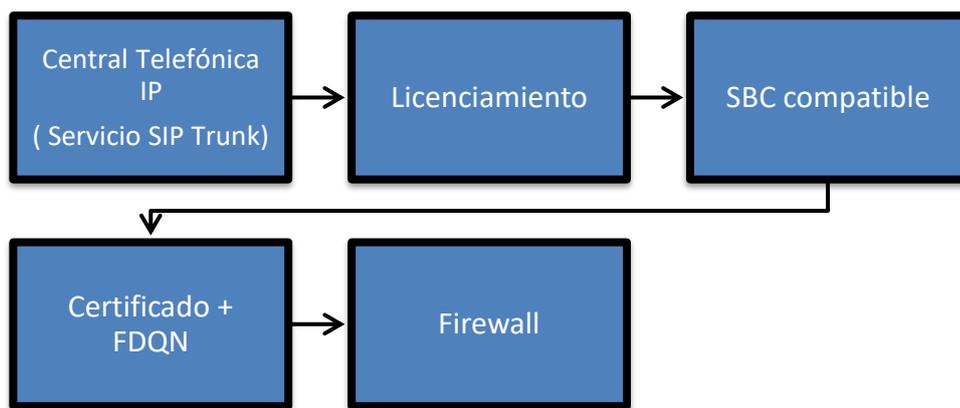
La figura 4.24 muestra el diseño de solución con el que los usuarios de Infamotor S.A., dispondrán de la interoperabilidad de la telefonía empresarial con la plataforma de Microsoft Teams ofreciendo las funcionalidades de chat, creaciones de grupos de trabajo, realización de reuniones o conferencias, conectividad a la PSTN para realizar y recibir llamadas, entre las principales.



**Figura 4.24:** Diseño de solución de comunicaciones unificadas.

**Fuente:** Autor

Los requisitos de infraestructura para la solución de comunicaciones unificadas considerados para la interoperabilidad de Direct Routing entre los usuarios de la red empresarial local y externa son los siguientes:



**Figura 4.25:** Requisitos de infraestructura de comunicaciones unificadas.

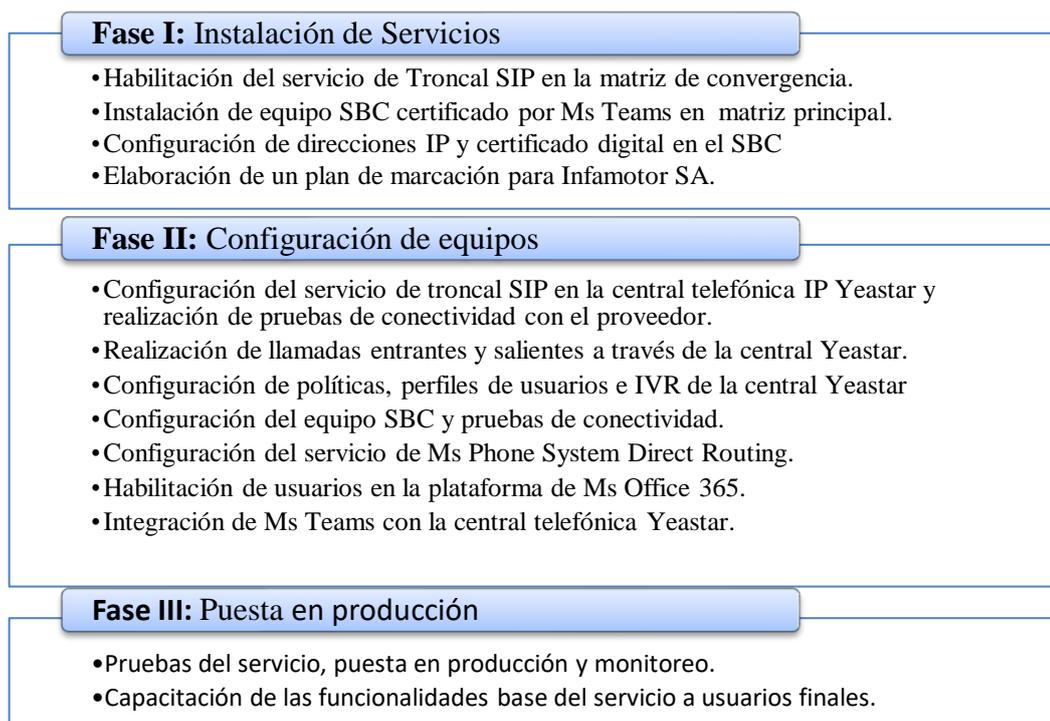
**Fuente:** Autor

- **Central Telefónica IP:** en el diseño de la presente solución tecnológica fue considerada la central telefónica Yeastar modelo S-100 VoIP PBX como una herramienta que permitirá aprovechar los recursos de comunicación de voz para mejorar la productividad de los usuarios, al aportar con beneficios tales como:
  - Reducción de costos de comunicación con sucursales al utilizar las redes WAN junto a políticas de QoS, transmitiendo voz, datos y videos sobre una misma infraestructura que ofrecerá enrutamiento de tráfico eficaz con SD-WAN.
  - Reducción de costos de cableado estructurado aprovechando el mismo punto de conexión de datos para la comunicación de la telefonía IP.
  - Flexibilidad y reducción de costos en los cambios de ubicación (traslados de oficinas), dado que no requieren ninguna reconfiguración en el servicio conservando la serie numérica contratada y el número de extensiones asignadas a los usuarios.
  - Instalar software a los sistemas operativos de las computadoras que funcionen como teléfono, softphone, con aplicaciones de correo electrónico, video llamadas, mensajería instantánea y lista de contactos.
  - Incrementar la productividad configurando saltos de llamadas con criterios cíclicos o jerárquicos que ayudaran de forma eficaz a atender una llamada que una extensión no pueda atender en un determinado momento antes de ser enviado al buzón de voz.
  - Control de calidad a través de la información que se puede extraer de la plataforma que permitirá identificar número de llamadas entrantes, determinación de horas pico, grabación de audio, porcentaje de llamadas contestadas en comparación con el total de realizadas, entre otras.
  - Integrar dispositivos de diferentes fabricantes por ser una plataforma abierta compatible con los estándares de VoIP.
  - Control de los usuarios para determinar el tipo de llamadas que podrán realizar de acuerdo al plan de marcación (dialplan).

- Centralizar el ingreso de usuarios con la integración del servidor de directorio empresarial (AD), incrementando la seguridad en el aprovisionamiento.
  - Asignación automática de direcciones IP a los teléfonos de matriz principal con el servicio de DHCP.
  - Integración con el servidor de correo empresarial para envío de notas de voz a los usuarios con cuentas registradas, aplicable en los escenarios que no sea posible la atención de llamadas y dejen mensajes en el buzón.
- **Licenciamiento:** el licenciamiento requerido por Ms Teams para alojar los usuarios está incluido en el plan empresarial de Office 365 Enterprise E5 o como un servicio complementario (add-on) para E1, E3 y E4.
  - **SBC compatible:** el dispositivo SBC deberá pertenecer a un proveedor aprobado por Microsoft, entre las marcas conocidas en el medio están Audicodes, Cisco, Avaya y Ribbon Communications. Entre las funcionalidades más relevantes que incorporará a la solución están las siguientes:
    - Agregar una capa de seguridad con protección perimetral para prevención de ataques VoIP maliciosos y fraudes telefónicos, al actuar como firewall de tráfico multimedia.
    - Interoperabilidad de la central telefónica Yeastar S-100 VoIP PBX con Ms Teams, al establecer sesiones con elementos de la red interna y externa con protocolos de señalización distinta.
    - Transcoding, para optimización del ancho de banda y adaptación de codecs en caso de que no coincidan los utilizados por las sesiones interna o externa.
    - Controlar y gestionar mediante políticas el número de sesiones establecidas para no sobrepasar el límite soportado.
  - **Certificado digital y FQDN:** el certificado digital deberá emitirse por las entidades calificadas y el nombre de dominio completo (Full Qualified Domain Name, FQDN) del SBC corresponderá a un nombre registrado en los dominios del cliente.
  - **Firewall:** la seguridad de red con los equipos dimensionados deberá permitir el acceso a la dirección IP pública, uso del puerto lógico para

señalización de cifrado de datos multimedia con el protocolo SRTP y encriptación de tráfico de establecimiento de llamadas con TLS.

Las actividades de configuración e instalación recomendadas para la implementación de la solución de comunicaciones unificadas pueden resumirse en las fases descritas en las figura 4.26.



**Figura 4.26:** Fases de configuración e instalación de la solución de UC.

**Fuente:** Autor

## Conclusiones

- Las estaciones de trabajo de Infamotor SA están conectadas a equipos de conmutación que forman una topología de red estrella extendida, estableciendo como punto de convergencia al router de borde, encargado de las políticas de control de acceso y permisos de navegación con un sistema de comunicación autónoma por cada sucursal.
- Los equipos que conforman la red empresarial de Infamotor SA presentan limitaciones en sus características técnicas, ocasionando un bajo rendimiento con una red inestable que no responde a las necesidades del negocio, condicionada de incorporar nuevos servicios y de soportar el incremento de tráfico por el uso de aplicaciones.
- Con la solución SD-WAN de Fortinet la comunicación hacia las sucursales de Infamotor SA tendrán automatización en el enrutamiento de tráfico que prioriza las aplicaciones críticas mediante el rendimiento de los enlaces, incorporando las funcionalidades de un dispositivo NGFW con una administración centralizada que brindarán los componentes FortiAnalyzer y FortiManager.
- La solución de comunicaciones unificadas logrará la interoperabilidad de la telefonía tradicional, integrando la central telefónica IP con el servicio de SIP Trunk e incorporando las funcionalidades de la herramienta Ms Teams que brinda recursos para reuniones o conferencias, que mejorarán la productividad de los usuarios y los tiempos de atención al cliente.
- La capa de seguridad del módulo de borde empresarial mejorará la protección del entorno corporativo contra las amenazas internas (LAN) y externas (Internet), al reducir las vulnerabilidades de la red, logrando visibilidad, control de acceso y análisis de eventos con múltiples mecanismos de detección como filtrado web, sistema de prevención de intrusos, antivirus o antispam.
- Se logró diseñar un modelo de arquitectura empresarial que segmenta la red de Infamotor SA en módulos que contienen una infraestructura de alto rendimiento, estableciendo un sistema de comunicación flexible para la integración de nuevos servicios, alineados a las necesidades de mercado y mejora continua en la experiencia de usuario, con tecnologías que lograrán disponer de una administración centralizada, visibilidad, monitoreo, así como también control para el aprovisionamiento de recursos.

## **Recomendaciones**

- En la implementación del diseño propuesto es recomendable adquirir los modelos de equipos dimensionados para garantizar la alta disponibilidad, escalabilidad y rendimiento de la red, manteniendo las operaciones de negocio de Infamotor SA sin interrupciones.
- Mantener activas las licencias de los equipos de seguridad Fortinet y Cisco en networking, esenciales para proteger la información empresarial, manteniendo una base de datos actualizada que permite identificar amenazas, sitios potencialmente peligrosos y ataques de día cero.
- Establecer un plan anual estratégico de mantenimiento preventivo a la infraestructura de red para evitar eventualidades o futuras fallas que puedan ocasionar un impacto en el funcionamiento, rendimiento y conservación de los equipos.
- Para proteger los archivos es recomendable utilizar la regla backup 3-2-1 (3 o más copias, 2 o más sistemas, 1 o más localizaciones) con un plan de recuperación ante desastres que incorpore seguridad, simplicidad y actualización constante de las copias de aplicaciones a través de máquinas virtuales.

## Bibliografía

- Ariganello, E. (2016). *REDES CISCO* (4ta ed.). Madrid, España: Grupo Editorial RA-MA.
- Ariganello, E. (2017). *REDES CISCO*. Madrid: Sextil Online SA.
- Armijos, C. A. (2019). *Rediseño e implementación de la red LAN para la locación “La Palma” de la Corporación Eléctrica del Ecuador CELEC EP, Unidad de Negocio Hidrotoapi*. Quito: Escuela Politécnica Nacional.
- Baque, S. (2019). *Implementación de un módulo didáctico para la administración y seguridad en redes de datos WLAN aplicado a la asignaturade redes inalámbricas de la carrera de ingeniería en computación y redes*. Jipijapa: Universidad Estatal del Sur de Manabí.
- Bernal, C. (2006). *Metodología de la investigación: para administración, economía, humanidades y ciencias sociales*. México: Pearson Educación.
- Blanco, F. (2016). *Oportunidades: emprendimiento verde, social y tecnológico*. Madrid, España: ESIC Editorial.
- Bruno, A., & Jordan, S. (2017). *CCDA 200-310 Official Cert Guide*. Indianapolis, USA: Cisco Press.
- Cabeza, G. (2018). *Análisis e implementación del servicio de outernet por medio de micro satélite para la recepción de información en el laboratorio de microondas y comunicaciones de la facultad de informática y electrónica*. Riobamba: Escuela Superior Politécnica de Chimborazo.
- Campo, J. (2019). *Diseño de red de ARCOTEL utilizando el modelo de arquitectura empresarial jerárquica de CISCO*. UNIVERSIDAD POLITÉCNICA SALESIANA. Quito: Universidad Politécnica Salesiana.
- Chávez, G., Campuzano, J., & Betancourt, V. (2018). Las micro, pequeñas y medianas empresas. clasificación para su estudio en la carrera de ingeniería en contabilidad y auditoría de la Universidad Técnica de Machala. *Universidad & Diversidad(1990-8644)*, 417. Revista Conrado.
- Cisco Systems, I. (2018). *Bandwidth Planning in your Cisco Webex Meetings Environment*. San Jose, CA: Cisco.
- Cisco Systems, I. (2020). *Cisco Annual Internet Report (2018–2023)*. CA: Cisco.
- CNMC. (2018). *COsumo de Banda Ancha por usuario*. Madrid.
- CNT. (2020). *SLA Datacenter*. Corporacion Nacional de Telecomunicaciones EP. Quito: CNT EP.

- CNT. (2020). *SLA Servicios Fijos CNT EP Disponibilidad 99.8%*. Quito: CNT EP.
- Cubillos, J., & Manrique, O. (2019). *Diseño de una red jerárquica para la empresa SIFAP tecnología, implementando estándares ieee 802.1 y 802.1q*. Bogotá: Universidad Cooperativa de Colombia.
- De Anda, G. (2018). *Implementación de solución de datos y seguridad con tecnología Cisco y Fortinet*. Universidad de Quintana Roo. Chetumal: Universidad de Quintana Roo.
- Denwa. (02 de 04 de 2019). *Denwa UCC Standard Line*. Recuperado el 20 de 07 de 2020, de Denwa Switching your life: <https://www.denwaip.com>
- Dordoigne, J. (2018). *Redes Informáticas*. Barcelona: Ediciones ENI.
- Dreyer, A., & Karneboge, A. (2019). *macOS Support Essentials 10.14* (Vol. 1). California: Peachpit Press.
- Fortinet, I. (2020). *Next-Generation Firewall (NGFW)*. Recuperado el 15 de Agosto de 2020, de Fortinet: <https://www.fortinet.com>
- Francis, D. (2019). *Mastering Active Directory* (Vol. 2). Birmingham, Inglaterra: Packt Publishing Ltd.
- García, C. (2019). *Diseño de un clúster de telecomunicaciones vía microondas para transferir servicio de internet a las localidades con múltiples necesidades del distrito de Chota*. Facultad de Ciencias. Piura: Universidad Nacional de Piura.
- Gartner, I. (2019). *Magic Quadrant for Endpoint Protection Platforms*. Gartner, Inc.
- Gartner, I. (2019). *Magic Quadrant for Meeting Solutions*. Gartner, Inc.
- Gartner, I. (2019). *Magic Quadrant for Network Firewalls*. Gartner, Inc.
- Gartner, I. (24 de Septiembre de 2019). *Magic Quadrant for Wired and Wireless LAN Access Infrastructure*. Gartner, Inc. Obtenido de Magic Quadrant for Wired and Wireless LAN Access Infrastructure: <https://www.gartner.com/doc/reprints?id=1-10JQSWP0&ct=190927&st=sb&elqTrackId=42606cbcc680450cad152ff6ccbf854&elq=8fbda4d87eab4e428440000c4262ff7f&elqaid=17388&elqat=1&elqCampaignId=>

- Gómez, G. (2019). *Mejora de la eficiencia espectral en las redes DWDM a 40 Gbps a través de los formatos de modulación avanzados DPSK y DQPSK*. Universidad del Cauca. Popayán: Universidad del Cauca.
- Gómez, L., & Yagual, L. (2018). *Análisis y propuesta de un diseño óptimo para la mejora de las redes LAN y WLAN de la Unidad Educativa Dr. Leonidas Ortega Moreira por medio de Cisco Safe*. Guayaquil: Universidad de Guayaquil.
- León, T. (2017). *Análisis del desempeño de redes alámbricas e inalámbricas utilizando enrutadores con tecnología MPLS*. Guayaquil: Universidad Católica de Santiago de Guayaquil.
- López, R. (2018). *Administración y Seguridad en Redes*. Bogotá D.C., Colombia: Fundación Universitaria del Área Andina.
- Mariño, J. (2017). *Análisis y diseño del cuarto de equipos y re categorización del cableado estructurado de la empresa "CIASEG SA" mediante la utilización de certificación EIA/TIA 568B y IEEE 802.11 - 802.12 para una administración eficiente, segura y confiable*. Universidad de las Américas , Facultad de Ingeniería y Ciencias Agropecuarias. Universidad de las Américas.
- Martínez, D., Amortegui, J., & Murillo, S. (2018). *Rediseño de redes LAN para tarjeta Tuya en almacenes Éxito de Bogotá*. Bogotá: Universidad Cooperativa de Colombia.
- Meggelen, J. V., Madsen, L., & Bryant, R. (2019). *Asterisk: The Definitive Guide*. O'Reilly Media, Inc.
- Mejía, E. (2016). *Estudio y diseño de una red inalámbrica entre el Gobierno Autónomo Descentralizado Municipal de Putumayo y la Comunidad Silvayaku para dotar de servicios de telecomunicaciones*. Pontificia Universidad Católica del Ecuador, Facultad de Ingeniería. Quito: Pontificia Universidad Católica del Ecuador.
- Patricio, R. (2018). *Diseño de un Sistema de Monitoreo para Identificar la Fuente de Ruido en Canales Ascendentes para una Red Hybrid Fiber Coaxial (HFC) Implementada Con DOCSIS 3.0*. Villa El Salvador: Universidad Nacional Tecnológica de Lima Sur.

- Pomar, R. (2019). *Implementación de una red privada virtual de software libre en una empresa*. Universitat Oberta de Catalunya. Cataluña: Universitat Oberta de Catalunya.
- Prende, E., & Castillo, K. (2019). *Propuesta de rediseño para la optimización de la red de datos del Colegio Réplica Simón Bolívar, utilizando principios de la arquitectura safe de CISCO y aplicando procedimientos DRP a la infraestructura tecnológica*. Guayaquil: Universidad de Guayaquil.
- Press, C. (2016). *Switched Networks*. United States of Americas : Cisco Systems.
- Rao, K., Bojkovic, Z., & Milovanovic, D. (2018). *Wireless Multimedia Communications: Convergence, DSP, QoS, and Security*. (C. Press, Ed.) Boca Raton, USA.
- Reyes Galarza, D. Y. (2017). *Estudio de Factibilidad de VoIP en la Facultad de Administración, Finanzas e Informática*. Babahoyo: Universidad Técnica de Babahoyo.
- Reyes, L. (2017). *Rediseño de la red LAN de acceso a la información de la Caja Nacional de Salud Regional Potosí*. La Paz: Universidad Mayor de San Andres.
- Río, M. D. (2016). *Tecnologías de Virtualización*. IT Campus Academy.
- Singh, H. (2017). *Implementing Cisco Networking Solutions*. Birmingham, Inglaterra: Packt Publishing Ltd.
- Vásquez, G., & Triviño, M. (2019). *Diseño y desarrollo de una red LAN jerárquica y un prototipo de sistema web con módulos de: turnos, citas previas y seguridad perimetral de la red para la sociedad ecuatoriana pro-rehabilitación de los lisiados (SERLI)*. Guayaquil: Universidad de Guayaquil.
- Vega, H. (2017). *Desarrollo de una guía técnica para la certificación de instalación de redes GPON FTTH*. Univerddidad De Las Americas. Quito: Univerddidad de Las Americas.
- Velez, D. (2018). *Diseño y simulacion en GNS3 de una red multiservicios MPLS para medianas empresas en el Ecuador*. Guayaquil: Universidad Catolica Santiago de Guayaquil.
- Vera, J. (2018). *Estudio de cobertura de redes inalámbricas con frecuencias 2.4 y 5.0 Ghz en las carreras de ingeniería en sistemas computacionales y*

*tecnología de la información de la Universidad Estatal del Sur de Manabí.*  
Jipijapa: Universidad Estatal del Sur de Manabí.

Vinueza, M. (2015). *Estudio detallado del uso RTP/RTCP y servicios de QoS y QoE en internet para la VoIP.* Escuela Superior Politecnica del Litoral, Facultad de Ingeniería en Electricidad y Computación. Guayaquil: Escuela Superior Politecnica del Litoral.

Yeastar. (2020). *Integrate Yeastar S-Series VoIP PBX with Microsoft Teams.* (S.-S. PBX, Productor) Recuperado el 14 de Agosto de 2020, de Yeastar: <https://www.yeastar.com/>

Zevallos, J. (2018). *Diseño de un nuevo sistema de red para mejorar la productividad en la empresa Corporación GTM del Perú.* Universidad Nacional José Faustino Sánchez Carrión. Huacho: Universidad Nacional José Faustino Sánchez Carrión.

Zyxel. (2020). *Firewall de Seguridad.* Recuperado el 23 de Agosto de 2020, de Zyxel: <https://www.zyxel.com>

## Anexos

### Anexo No 1. Criterios técnicos para la elección de los equipos de acceso

**Velocidad de los puertos:** para determinar el tipo de puerto a utilizar se realizó una estimación de consumo de velocidad de transmisión de las aplicaciones, navegación a Internet y servicios por usuario, con la utilización de una herramienta de supervisión de tráfico, PRTG, instalada en algunos ordenadores durante una semana.

Cabe resaltar, que los valores mostrados para telefonía IP fueron calculados con la utilización de códec G.711 junto con el protocolo SIP, propuesta proporcionada por los proveedores de servicio, a través de la herramienta web que ofrece Asterik [https://www.asteriskguru.com/tools/bandwidth\\_calculator.php](https://www.asteriskguru.com/tools/bandwidth_calculator.php), asimismo la capacidad requerida para la herramienta de colaboración la recomienda Cisco para un escenario clásico de 5 participantes con una pantalla compartida y la incorporación de un audio (Cisco Systems, 2018).

Por otra parte, fue integrado el pronóstico de consumo de Internet en tres años (2023) que propone Cisco en su análisis global que evalúa la transformación digital del segmento empresarial (Cisco Systems, 2020).

#### Cálculo del consumo de tráfico IP

Aplicaciones/Servicios	Capacidad (Mbps)
<b>Demanda de tráfico existente</b>	
Actualizaciones del Sistema Operativo ( <i>patch, service packs</i> )	0.5
Actualización de Antivirus	0.5
Correo Electrónico ( <i>POP3, SMTP</i> )	1
Acceso al sistema ERP	0.1
Información compartida ( <i>Intranet</i> )	20
Navegación por Internet	1.55
Aplicación Interna de registro de inventario	5
<b>Demanda de tráfico planificado</b>	
VoIP con códec G.711	0.08
Acceso a aplicaciones en la nube ( <i>CRM</i> )	0.51
Utilización de Herramientas de colaboración ( <i>Meetings</i> )	1.9
Conferencia Múltiple ( <i>4 participantes</i> )	0.31
Integración nuevo sistema de inventario empresarial	20
<b>Crecimiento de demanda 2023</b>	
Promedio de consumo Internet por usuario ( <i>IoT, APP, IPTv, UCC</i> )	59.3
<b>Total</b>	<b>110.75</b>

Fuente: Autor

La estimación de utilización de velocidad de transmisión por usuario establece un total de 110.75 Mbps, dado que no se disponen puertos de estas capacidades, entonces las características técnicas de las interfaces de los equipos de acceso son de 1000Base T (1 Gbps/RJ45), de acuerdo al estándar IEEE 802.3ab.

**Interfaz Uplink:** para determinar la capacidad de la interfaz *uplink* fue utilizado el parámetro de sobresuscripción de los puertos, estableciendo una relación de 20:1 por tratarse de una red de tráfico medio (Armijos, 2019, p. 59). Por lo que, el cálculo de velocidad quedó reflejado a través de la siguiente ecuación:

$$10 \leq \frac{\text{Número de Interfaces} * \text{Velocidad de puertos}}{\text{Velocidad del puerto Uplink}} \leq 20 \quad (1)$$

Para la obtención del resultado, es importante tomar en consideración el escenario de transferencia simultánea de información (ambas direcciones) de todos los puertos (Armijos, 2019).

$$\frac{48 \text{ Gbps}}{20} \leq \text{Velocidad del puerto Uplink} \leq \frac{48 \text{ Gbps}}{10} \quad (2)$$

Al realizar la operación de la ecuación 2, el resultado obtenido es el siguiente:

$$2.4 \text{ Gbps} \leq \text{Velocidad del puerto Uplink} \leq 4.8 \text{ Gbps} \quad (3)$$

Por lo tanto, la capacidad de la interfaz *Uplink* está en el rango de 2.4 – 4.8 Gbps, lo que refleja características técnicas a través del estándar IEEE 802.3ae 10 Giga Ethernet. Para garantizar la alta disponibilidad a través de conexiones redundantes fueron cuantificadas dos interfaces SFP (*small form-factor pluggable*) por equipo.

**Switching bandwidth:** conocida también como capacidad de conmutación, es la velocidad a la cual el *hardware* puede conmutar el tráfico en la red, medida en bps (bit por segundo). Los parámetros empleados para el cálculo corresponden a

la velocidad de los puertos, modo de transmisión y número de interfaces *uplink*.  
Por consiguiente, se muestra la relación para la obtención del valor:

$$\mathbf{Switch\ B} = [(Vel.Puerto * No. Puerto) + (Vel.Uplink * No.de Uplink)] * Full\ Dúplex \quad (4)$$

En consecuencia, los equipos de acceso tendrán como mínimo una capacidad de conmutación de 88 Gbps.

## Anexo No 2. Criterios técnicos para la elección de los equipos de núcleo-distribución colapsado

**Apilamiento:** disponer de una solución de apilamiento (*stacking*) logrará tener simplicidad y flexibilidad al disminuir la cantidad de equipos a administrar, consiguiendo un solo plano de datos unificado. El número de interfaces soportadas por los estándares 802.3ab (8 Giga Ethernet) y 802.3ae (3 Ten Giga Ethernet) definen la utilización de equipos de conmutación no expandible de 24 puertos, obteniendo una capacidad mínima a soportar de 128 Gbps, reflejada en la siguiente ecuación (Armijos, 2019, p. 61):

$$Cap.Stack = \left[ \left( \frac{No\ total}{de\ Int.\ Elec.} \right) * \left( \frac{Vel. de}{Int. Elec.} \right) \right] * FD + \left[ \left( \frac{No\ total}{de\ Int.\ Opt.} \right) * \left( \frac{Vel. de}{Int. Opt.} \right) \right] * FD \quad (5)$$

**Switching bandwidth:** los parámetros empleados para el cálculo corresponden a la velocidad de los puertos a utilizar, modo de transmisión y capacidad de stacking. Por consiguiente, se muestra la relación para la obtención del valor mínimo a requerir (Armijos, 2019, p. 61):

$$Switch\ B = [ (Vel. PuertosGE * No. PuertosGE) + (Vel. Puertos TenGE * No Puertos TenGE) ] * Full\ Dúplex + Cap.Stack \quad (6)$$

En consecuencia, los equipos de distribución tendrán como mínimo una capacidad de conmutación de 204 Gbps.

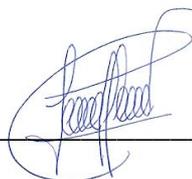
## DECLARACIÓN Y AUTORIZACIÓN

Yo, **Leandro Danilo Macias Loza**, con C.C: # **0923602098** autor/a del trabajo de titulación: **Análisis y diseño de red de la empresa INFAMOTOR S.A. para innovación tecnológica de los servicios de telecomunicaciones con una administración centralizada, ofreciendo alta disponibilidad, flexibilidad y confidencialidad de la información con sus sucursales**, previo a la obtención del título de **Magíster en Telecomunicaciones** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 19 de noviembre de 2020



---

**Leandro Danilo Macias Loza**

**C.C: 0923602098**

**REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA**

**FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN**

<b>TÍTULO Y SUBTÍTULO:</b>	Análisis y diseño de red de la empresa INFAMOTOR S.A. para innovación tecnológica de los servicios de telecomunicaciones con una administración centralizada, ofreciendo alta disponibilidad, flexibilidad y confidencialidad de la información con sus sucursales		
<b>AUTOR(ES)</b>	Leandro Danilo Macias Loza		
<b>REVISOR(ES)/TUTOR</b>	MSc. Edgar Quezada Calle; MSc. Luis Córdova Rivadeneira / MSc. Manuel Romero Paz		
<b>INSTITUCIÓN:</b>	Universidad Católica de Santiago de Guayaquil		
<b>FACULTAD:</b>	Sistema de Posgrado		
<b>PROGRAMA:</b>	Maestría en Telecomunicaciones		
<b>TITULO OBTENIDO:</b>	Magister en Telecomunicaciones		
<b>FECHA DE PUBLICACIÓN:</b>	<b>Guayaquil,</b>	<b>19</b>	<b>de</b>
	<b>noviembre de 2020</b>		<b>No. DE PÁGINAS: 132</b>
<b>ÁREAS TEMÁTICAS:</b>	Red LAN, Redes inalámbricas, Estándares, Protocolos, Seguridad, Tecnología VoIP		
<b>PALABRAS CLAVES/ KEYWORDS:</b>	LAN, EIGRP, OSPF, BGP, VoIP, SIP, SD-WAN		

**RESUMEN:** La evolución de las Tecnologías de la Información y la Comunicación (TIC) han revolucionado el mundo y su forma de hacer negocios. Actualmente, es difícil imaginar que las empresas desarrollen sus actividades y se mantengan en el mercado sin utilizar los recursos de las telecomunicaciones como telefonía, internet, entre otros. INFAMOTOR S.A es una empresa dedicada a satisfacer las necesidades del mercado automotriz mediante la importación, comercialización y distribución de repuestos y accesorios para vehículos de casi todas las marcas. Gracias a la dedicación de su fundador, Sr. Julio Infante Campoverde, la empresa ha crecido considerablemente, logrando establecer sucursales en varias ciudades del país, las mismas que mantienen comunicación permanente a través de internet. Gracias a la apertura del líder de la oficina matriz de la empresa en estudio, y con el afán de diseñar una solución tecnológica de red que permita gestionar los servicios de telecomunicaciones de INFAMOTOR S.A de forma centralizada, se procedió a analizar la infraestructura de red existente. Para tal efecto, fueron aplicados métodos y técnicas investigativas que, junto a la información de importantes autores y a la experiencia del autor, permitieron obtener un diseño que garantice alta disponibilidad, flexibilidad y confidencialidad de la información con sus sucursales. El diseño propuesto aborda las necesidades de la empresa en análisis con un enfoque modular, limitando el acceso externo y brindando seguridad en el manejo de información.

<b>ADJUNTO PDF:</b>	<input checked="" type="checkbox"/> SI	<input type="checkbox"/> NO
<b>CONTACTO AUTOR/ES:</b>	<b>Teléfono:</b> +593-989779099	<b>E-mail:</b> liandru17@gmail.com
<b>CONTACTO CON LA INSTITUCIÓN (COORDINADOR DEL PROCESO UTE):</b>	<b>Nombre:</b> Romero Paz Manuel de Jesús	
	<b>Teléfono:</b> +593-994606932	
	<b>E-mail:</b> manuel.romero@cu.ucsg.edu.ec	

**SECCIÓN PARA USO DE BIBLIOTECA**

<b>Nº. DE REGISTRO (en base a datos):</b>	
<b>Nº. DE CLASIFICACIÓN:</b>	
<b>DIRECCIÓN URL (tesis en la web):</b>	