FACULTAD DE INGENIERÍA

CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

"PROPUESTA DE UNA RED PRIVADA VIRTUAL PARA MEJORAR EL SERVICIO DE COMUNICACIÓN EN LAS TIENDAS MASS PARA LA EMPRESA SUPERMERCADOS PERUANOS S.A."

PARA OBTENER EL TÍTULO DE

INGENIERO DE SISTEMAS

AUTOR

CÉSAR RENATO ESPINOZA CHIPANE

ASESOR

MG. JOSE LUIS HERRERA SALAZAR

LIMA, PERÚ, FEBRERO 2018

DEDICATORIA

Dedico este trabajo a Dios, por darme la vida, guiarme y fortalecerme a lo largo de todos estos años que pasé, a mis seres queridos que hoy no están conmigo en cuerpo presente, pero que desde el cielo me protegen. De igual forma, dedico esta tesis a mi Madre y Hermano los cuales son el motivo de seguir avanzando en la vida.

A mi compañera de vida, por su apoyo incondicional por estar a mi lado en los buenos y malos momentos.

AGRADECIMIENTO

A mis familiares por sus recomendaciones y palabras de aliento constante. A mis profesores, quienes contribuyeron en mi camino profesional para poder llegar a estas instancias.

RESUMEN

El presente proyecto de investigación tiene como objetivo proponer una solución de Red Privada Virtual para mejorar el servicio de comunicación en las tiendas Mass para la empresa Supermercados Peruanos S.A.

Esta investigación fue realizada en base a la metodología PPDIOO (Preparar, Planificar, Diseñar, Implementar, Operar, Optimizar) de Cisco Systems, lo cual nos proporcionará los procesos, habilidades, técnicas necesarias para llevar acabo la propuesta de implementación.

La mejora del Servicio de Comunicación en las tiendas Mass se podrá constatar en el enlace virtual para enlazar dos o más sucursales geográficamente distanciadas.

Se usó como referencia el Modelo OSI para la interpretación de capas de Red.

Nivel 3 (Red): Tiempos de respuesta del enlace: Se verá reflejada en milisegundos, se denotará un notorio tiempo de repuesta mucho más bajo con el actual enlace que poseen 3G o Radio enlaces, se observará realizando un ping desde la PC origen hacia el destino.

Saltos que realiza el paquete para llegar al destino: Esto se verá reflejada en la disminución de saltos al momento de realizar un tracert desde la PC origen hacia el destino, por consiguiente, el paquete llegará mucho más rápido y la transmisión será en menos tiempo.

Nivel 4 (Transporte): La utilización del TCP (Transmission Control Protocol): la solución será orientado a la conexión, esto es importante al momento de transmitir los datos a través de la Red.

Nivel 7 (Aplicación): La velocidad de transmisión: Se denotará significativamente la rapidez y fluidez con la que converge los sistemas informáticos, mejorando la productividad del negocio.

Palabras clave: Redes Privadas Virtuales (VPN), Multiprotol Layer Switching (MPLS), enlaces de Datos, Servicio de comunicación de las tiendas Mass.

ABSTRACT

The present research project aims to propose a Virtual Private Network solution to improve the cmmunication service in Mass stores for the company Supermercados Peruanos S.A. This research was carried out based on the PPDIOO (Prepared, Plan, Design, Implement, Operate and Optimize) methodology developed by Cisco Systems, which will provide us with the necessary processes, skills and techniques to carry out the implementation proposal.

In this proposal of improvement for the communication service in Mass stores, the virtual link can be verified to link two or more geographically distant branches, based on the layers of the OSI (Open Systems Interconnection) model:

Level 3 (Network): Response times of the link: It will be reflected in milliseconds, it will denote a notorious response time much lower with the current link that have 3G or Radio links, will be observed pinging from the originating PC towards the destination. Jumps made by the packet to reach the destination: This will be reflected in the decrease of jumps when performinga tracer from the source PC to the destination, therefore the packet will arrive much faster and the transmission will be in less time.

Level 4 (Transport): The execution of the Transmission Control Protocol (TCP): the solution will be oriented to the connection, this is important when transmitting the data through the Network.

Level 7 (Application): Speed: You will see an improvement when entering, sending or processing some information that the user performs, therefore the level of user satisfaction will improve significantly.

Keywords: Virtual Private Networks (VPN), Multiprotocol Layer Switching (MPLS), Data links, Communication service Mass stores.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

Este proyecto como tal, es una propuesta de implementación de una Red Privada Virtual, cuyo objetivo principal es mejorar la comunicación en las tiendas Mass para la empresa Supermercados Peruanos S.A. Esto conlleva a múltiples objetivos específicos, tales como mejorar el tiempo de latencia del Servicio de Comunicación, disminuir los incidentes por lentitud o intermitencia de la Red, proporcionar a la Red de datos escalabilidad, disminuir costos por el Servicio de Comunicación entre otros.

Por tal motivo esta investigación pretende dar a conocer una solución alterna a los servicios de datos dedicados que se arrienda con un proveedor ISP, el Internet. Con el propósito de hacer más entendible la presente investigación, ha sido dividas en cinco capítulos, cuyos contenidos son los siguientes:

Capítulo I: Planeamiento Metodológico. - Se define la realidad problemática del tema de investigación, el tipo y nivel de investigación, los objetivos generales y específicos, la justificación e importancia, las variables de investigación, además de las técnicas de recolección de datos; y las limitaciones de la investigación.

Capítulo II: Marco Referencial. - Presenta los antecedentes de estudio sustentada por tesis, investigaciones, y la definición de las bases teóricas y científicas que hacen referencia a la investigación.

Capítulo III: Desarrollo de la propuesta de Implementación VPN. – En este capítulo se definen las generalidades, el estudio de factibilidad, además de los requerimientos y se puede apreciar cómo se aplicará las fases de la Metodología que aplicaremos PPDIOO de Cisco Systems.

Capítulo IV: Análisis de Resultados y Contrastación de la Hipótesis. - Se define la población y la muestra utilizadas para la presente investigación. Además, se detalla el análisis y procesamiento de la información de las dos variables de estudio con las pruebas de hipótesis y se da la discusión de los resultados obtenidos.

Capítulo V: Conclusiones y Recomendaciones. - Se muestra las conclusiones y recomendaciones respecto a los resultados obtenidos sobre la presente investigación.

Al final se presenta las referencias bibliográficas y los anexos que intervienen en la investigación. El desarrollo de la presente investigación se espera que sirva como base de futuras investigaciones.

El autor.

CAPÍTULO I

PLANTEAMIENTO METODOLÓGICO

1.1. EL PROBLEMA

1.1.1. Descripción de la Realidad problemática

Realidad Mundial

El mundo ha cambiado mucho en los pares más recientes de las décadas. En vez simplemente de ocuparse de las preocupaciones locales o regionales, muchos negocios ahora tienen que pensar en los mercados globales y la logística. Muchas compañías hacen que los recursos se separen hacia fuera en todo el país, o aún en todo el mundo. Pero hay una cosa que todas las compañías necesitan: una manera de mantener rápidamente, seguro, y comunicaciones confiables dondequiera que se localicen sus oficinas. Hasta hace poco tiempo, la comunicación confiable ha significado el uso de las líneas arrendadas de mantener un Red de área ancha (WAN). WAN tiene ventajas obvias sobre una red pública como Internet cuando se trata de la confiabilidad, del funcionamiento, y de la Seguridad; pero mantener WAN, determinado al usar las líneas arrendadas, puede llegar a ser muy costoso (él a menudo las subidas del coste como la distancia entre los aumentos de las oficinas). Además, las líneas arrendadas no son una solución viable para las organizaciones donde está muy móvil (como en el caso del equipo de comercialización) y pudo necesitar con frecuencia la parte de la fuerza de trabajo conectar con la red corporativa remotamente y acceder los datos vulnerables.

Mientras que el renombre de Internet ha crecido, los negocios han dado vuelta a él como medio para extender sus propias redes. Primero vinieron los intranets, que son sitios diseñados para el uso solamente por los empleados de la compañía. Ahora, muchas compañías crean su propio Redes privadas virtuales (VPN) para acomodar las necesidades de los empleados remotos y de las oficinas lejanas.

Un VPN típico pudo tener una red de área local (LAN) principal en las oficinas principales de la compañía de una compañía, otros LAN en las oficinas remotas o los recursos, y los usuarios individuales que conectan hacia fuera adentro del campo. Un VPN es una red privada que utiliza una red pública (generalmente Internet) para conectar los sitios remotos o a los usuarios juntos. En vez de usar una conexión dedicada, del mundo real, tal como línea arrendada, un VPN utiliza las conexiones “virtuales” ruteadas a través de Internet de la red privada de la compañía al sitio remoto o al empleado. (Cisco Systems, 2008).

Realidad Nacional

Las empresas peruanas tienen su objetivo claro: acelerar la transformación digital. Se trata de sobrevivir en un mundo cada vez más rápido y competitivo. Para ello, es importante que las compañías tengan claro que se trata del aprovechamiento de la nueva tecnología para vender más y con mayor satisfacción a los clientes.

Para Luis Jesús Pintado, director IT Solutions & Services de Everis, en el Perú existe una brecha entre algunos sectores. “La banca peruana está apostando a tope con la transformación digital, y no solo a nivel de los sistemas informáticos, sino también a nivel integral, a la forma cómo trabajan los equipos. En ese sentido la banca peruana no tiene nada que envidiar a la banca española”, sostuvo el ejecutivo. (Gestión, 2017).

Sin embargo, resaltó Pintado, no pasa lo mismo en el sector de las telecomunicaciones, que tras hacer importantes inversiones en líneas de comunicación 3G y 4G, se han dado cuenta que el valor no está en la línea, sino en los servicios para los que utilizan la línea. “Al final el dinero se lo lleva Facebook, que no ha hecho esas inversiones. Por ese motivo estas empresas están pasando por un momento económico complicado. Son conscientes de la necesidad de transformación digital, pero la situación es difícil”, añadió. (Gestión, 2017).

Por otro lado, Luis Ladera, gerente de Datos e Internet en CenturyLink (antes Level 3), señala que la transformación digital es interés de todos los sectores. “En la medida que pasa el tiempo y las economías se van globalizando a través de las telecomunicaciones, se hace necesario que las empresas tengan estrategias orientadas a competir no solo en el ámbito local, sino en el ámbito global”, dijo. Para Ladera, el Perú es un país que ha tenido una oportunidad enorme de avanzar gracias a las políticas económicas que se han implementado en los últimos 20 años, algo que se refleja en su crecimiento. “En este momento Perú está a la vanguardia de lo que es la adopción de nuevas tecnologías frente a otros países de Latinoamérica. Pienso que el empresariado peruano está tomando muy en serio la transformación digital”, apuntó. (Gestión, 2017).

Así, según un estudio de 451 research, el objetivo de la transformación digital es optimizar la eficiencia operacional de las empresas, mejorar las ventas y la experiencia de los usuarios. “Se trata de hacer con que las empresas puedan llegar a sus clientes más rápido, con productos customizados y adaptados a sus gustos,

siendo capaces de predecir qué es lo que el cliente quiere", añadió el ejecutivo de Everis. (Gestión, 2017).

En el rubro de Supermercados, las empresas continuaron con sus planes de expansión, a pesar de mostrar tasas menores de crecimiento. Del mismo modo, las cadenas de farmacias vienen implementando agresivos planes de expansión a nivel nacional, enfocándose principalmente en provincias. Durante el 2016, se abrieron netas 183 farmacias de las cuales 186 pertenecen a nuestras farmacias. Asimismo, el mercado se consolidó aún más luego que el tercer competidor fue comprado por el segundo competidor del mercado. "El año 2016 se caracterizó por la desaceleración en el consumo que se prevé se extenderá hasta el primer semestre del 2017. Sin embargo, Supermercados Peruanos e Inkafarma se mostraron resilientes ante un consumo más lento y mostraron ventas mismas tiendas positivas y por encima de la competencia". (Inretail Perú Corp., 2016)

Realidad Empresarial

Tiendas Mass – Supermercados Peruanos S.A.

El 11 de diciembre del 2003, el grupo financiero Interbank adquirió la totalidad de las acciones de Supermercados Santa Isabel, brindando a la empresa el respaldo financiero y el prestigio necesarios para que una cadena ahora 100% peruana pudiese continuar con el proceso de expansión iniciado por Ahold. En marzo de 2004, la Junta General de Accionistas aprobó cambiar la denominación social de Supermercados Santa Isabel S.A. por Supermercados Peruanos S.A.

Desde el 2006, Supermercados Peruanos está teniendo un crecimiento constante, resultado de su plan de expansión, a través de la construcción de nuevas tiendas tanto en Lima como en Provincias se busca atender nuevos segmentos y en algunos casos remodelando tiendas ya existentes a fin de satisfacer mejor las necesidades de sus clientes.

El Formato de "Tiendas de Descuento" comenzó en abril del año 2001 con el local de Chosica, para luego expandirse a los distritos de San Juan de Miraflores (Mass Varga Machuca) y Chorrillos (Mass Guardia Civil). En la actualidad este formato se caracteriza por estar enfocado hacia compras puntuales, de bajo precio y rápidas de un número reducido de ítems, que compiten con bodegas y mercados de barrio a nivel Lima Metropolitana. Se tiene un estimado de 140 tiendas en producción

desde el año 2015, y seguirá su proceso de expansión en los siguientes años, consolidando un mínimo de 500 tiendas Mass.

Figura 1. Ubicación de Supermercados Peruanos S.A. Recuperado de "Ubicación de la empresa Supermercados Peruanos S.A." por Google Maps, 2017.

1.1.2. Definición del Problema

Las tiendas Mass está teniendo este último año una demanda de expansión acelerada mayor a los años anteriores, llegando a abrir un promedio de 7 tiendas por mes, actualmente cuenta con 129 Tiendas en funcionamiento.

Por ello el área de Redes y Telecomunicaciones cumple un rol importante, ya que es la encargada de interconectar los Servicios de Comunicación de toda la Corporación, entre oficinas y Tiendas remotas, a esto se le suma el monitoreo y soporte de la Red 24x7. Los enlaces de datos arrendados en las tiendas Mass están bajo los servicios de 3 proveedores ISP en el Perú, estos son: Telefónica del Perú, América Móvil Perú - Claro y Americatel Perú. En estos últimos meses se viene presentando inconvenientes con el Servicio de Comunicación en algunas tiendas que poseen enlaces 3G provisionadas por el proveedor Telefónica.

Primer Sub-problema: Las incidencias reportadas a Mesa de Ayuda por temas de lentitud e intermitencias en el Servicio de Comunicación 3G incrementaron, siendo un promedio de 5 a 6 incidentes a la semana y 19 incidencias al mes, ello hace deducir que existe una falencia operativa con el Servicio del proveedor Telefónica, teniendo en el tiempo problemas que afectarán directamente a la venta de la Tienda.

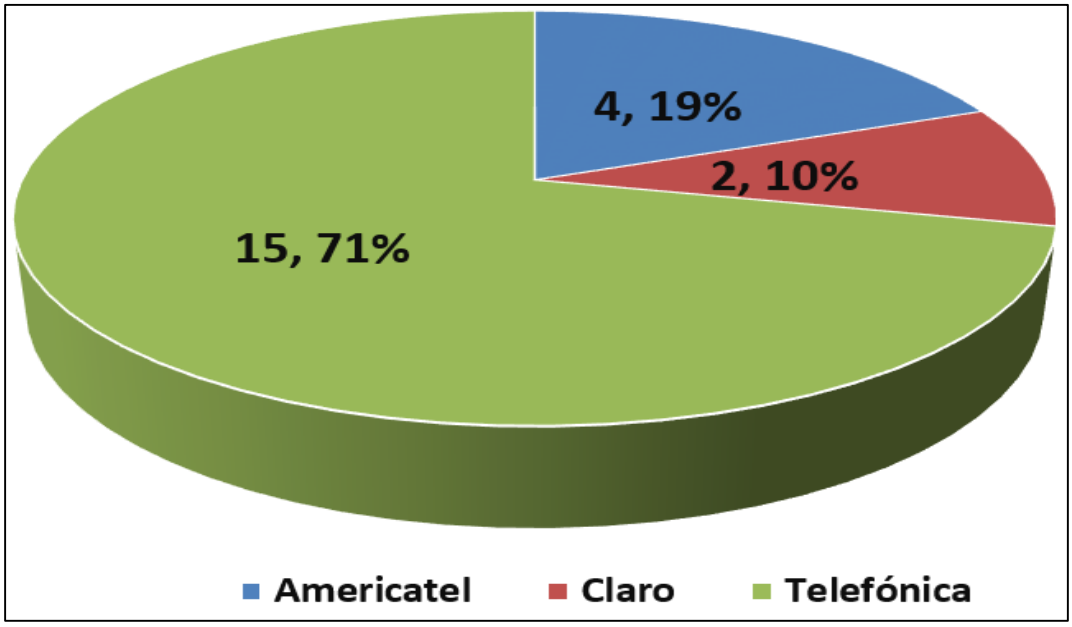

Figura 2. Cantidad de Incidencias por el Servicio de Comunicación en las tiendas Mass.

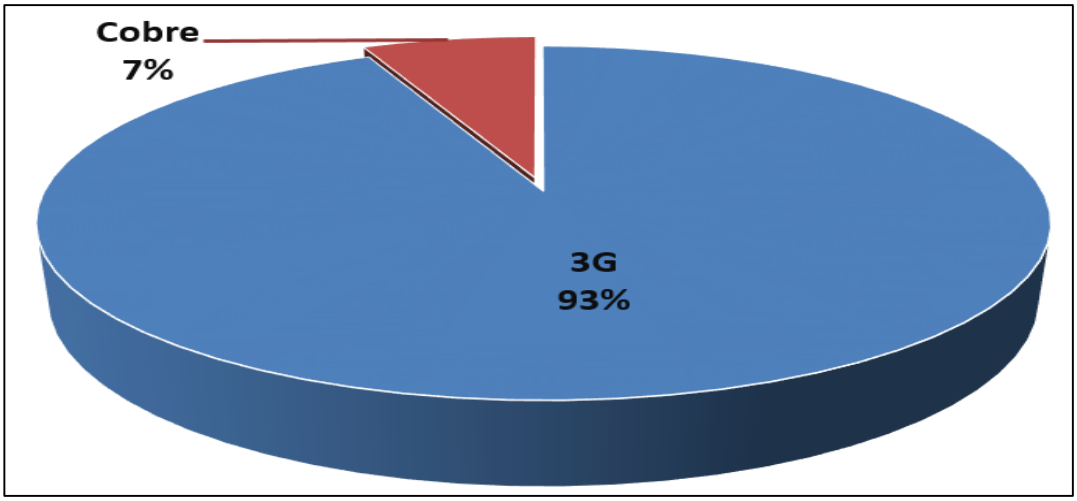

Figura 3. Cantidad Incidencias por lentitud o intermitencia producidas por el Tipo de enlace de datos en Telefónica del Perú.

Segundo Sub-problema: Las tiendas que poseen el Servicio de Comunicación con Tecnología 3G provisionadas por Telefónica son conexiones que usa un módem router y en su interior un chip 3G, lo cual hace posible la transmisión de datos inalámbricamente, pero el tiempo de latencia de la tecnología 3G viene degradándose sistemáticamente, ya sea por la poca cobertura móvil en la zona, o mala ubicación del equipo en el gabinete, llegando desde los 900 milisegundos hasta los 1500 milisegundos, ello se traduce en tiempos de espera muy altos en las transacciones de ventas en Línea generando colas de espera y disgusto por parte del consumidor, impactando la continuidad del negocio.

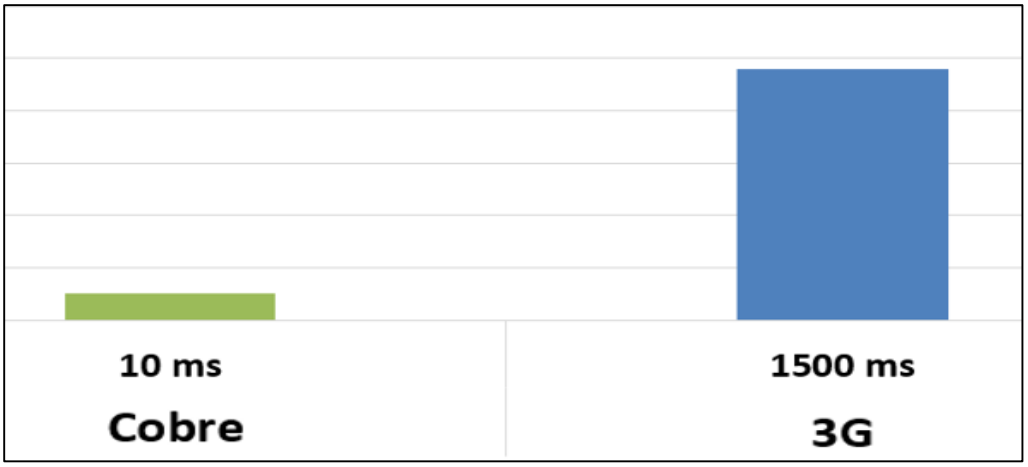

Figura 4. Tiempos de Latencia promedio por el tipo de enlace provisionado por Telefónica del Perú.

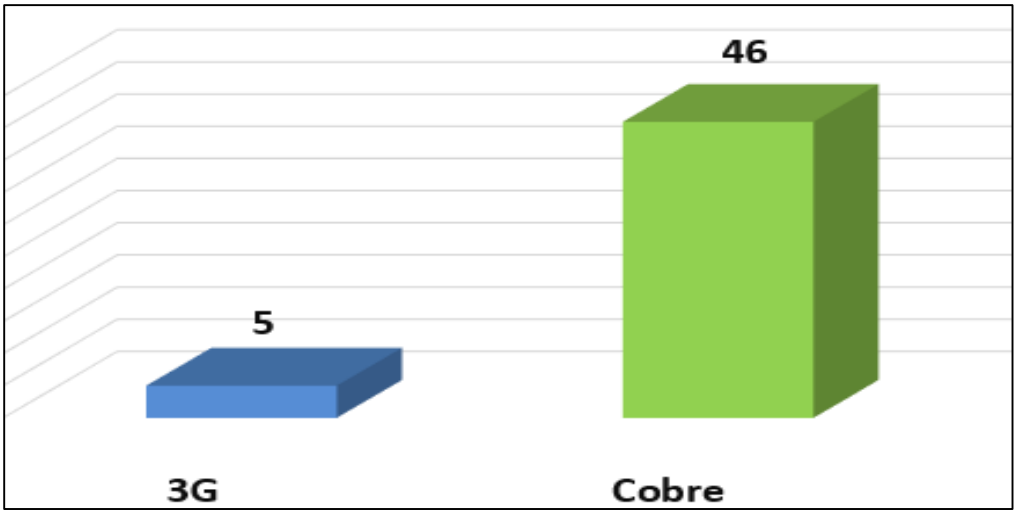

Figura 5. Cantidad de Tiendas por el tipo enlaces de datos brindado por Telefónica del Perú.

Tercer Sub-Problema: El equipo Módem 3G, cuenta con 4 puertos LAN, sólo para 4 dispositivos en Red, si la Tienda crece en un futuro y se requiere agregar dispositivos a la red LAN se verá limitada por el Hardware del equipo en ese momento. Para estos casos se debería considerar un equipo switch.

Cuarto Sub-problema: Los tiempos de carga para ingresar o realizar algún proceso desde la PC del administrador de la tienda es de 4 minutos a 7 minutos, esto conlleva a los siguientes inconvenientes:

Demora para recibir o enviar alguna información mediante Correo, lentitud en la carga de sus inventarios al sistema, lentitud al ingresar al sistema del llenado de horas del personal, lentitud para el ingreso a las carpetas compartidas, lentitud en la actualización de precios diariamente, entre otras actividades que realiza el personal de tienda, en el tiempo afectará la continuidad y productividad de la tienda.

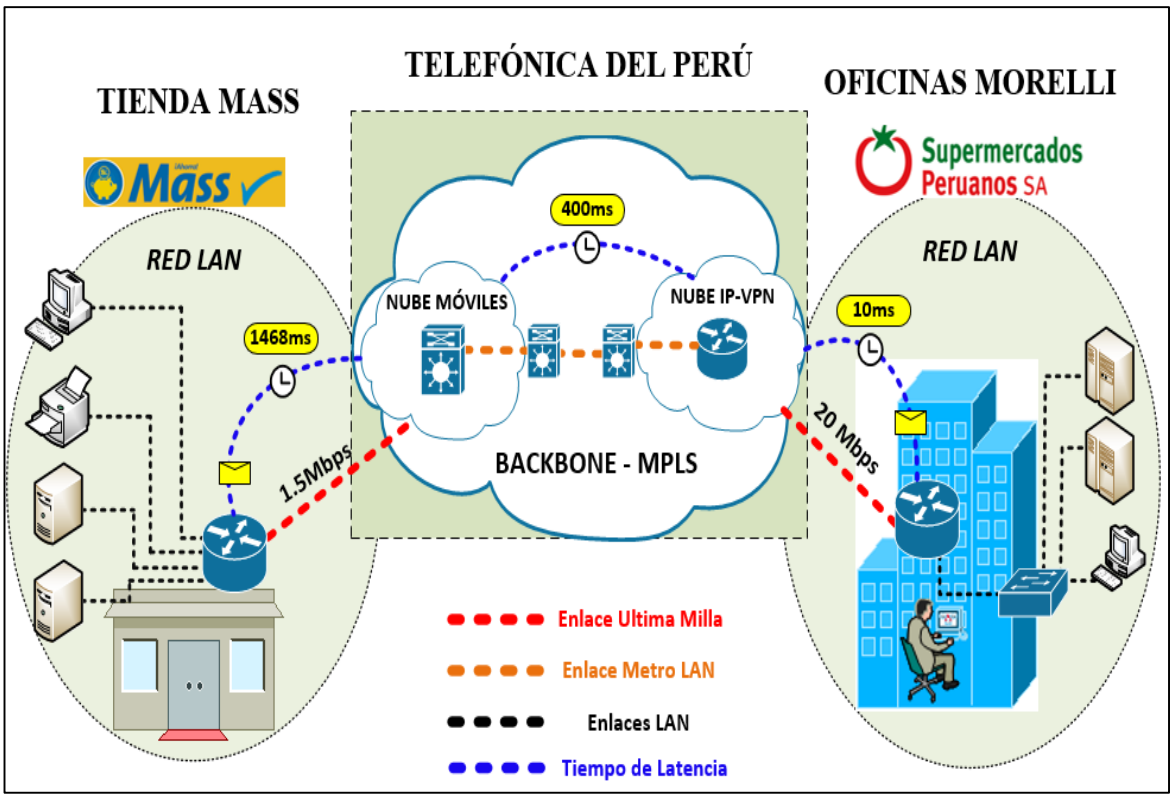

Figura 6. Diagrama del Servicio de Comunicación 3G Provisionado por Telefónica del Perú. (AS-IS).

Sexto Sub-problema: El número de saltos que recorre el paquete de datos en la Red MPLS para llegar a su destino es de un promedio de 8 saltos consecutivos, a más números de saltos más lento el proceso de la Comunicación, ocasionando todos los Sub-problemas antes descritos.

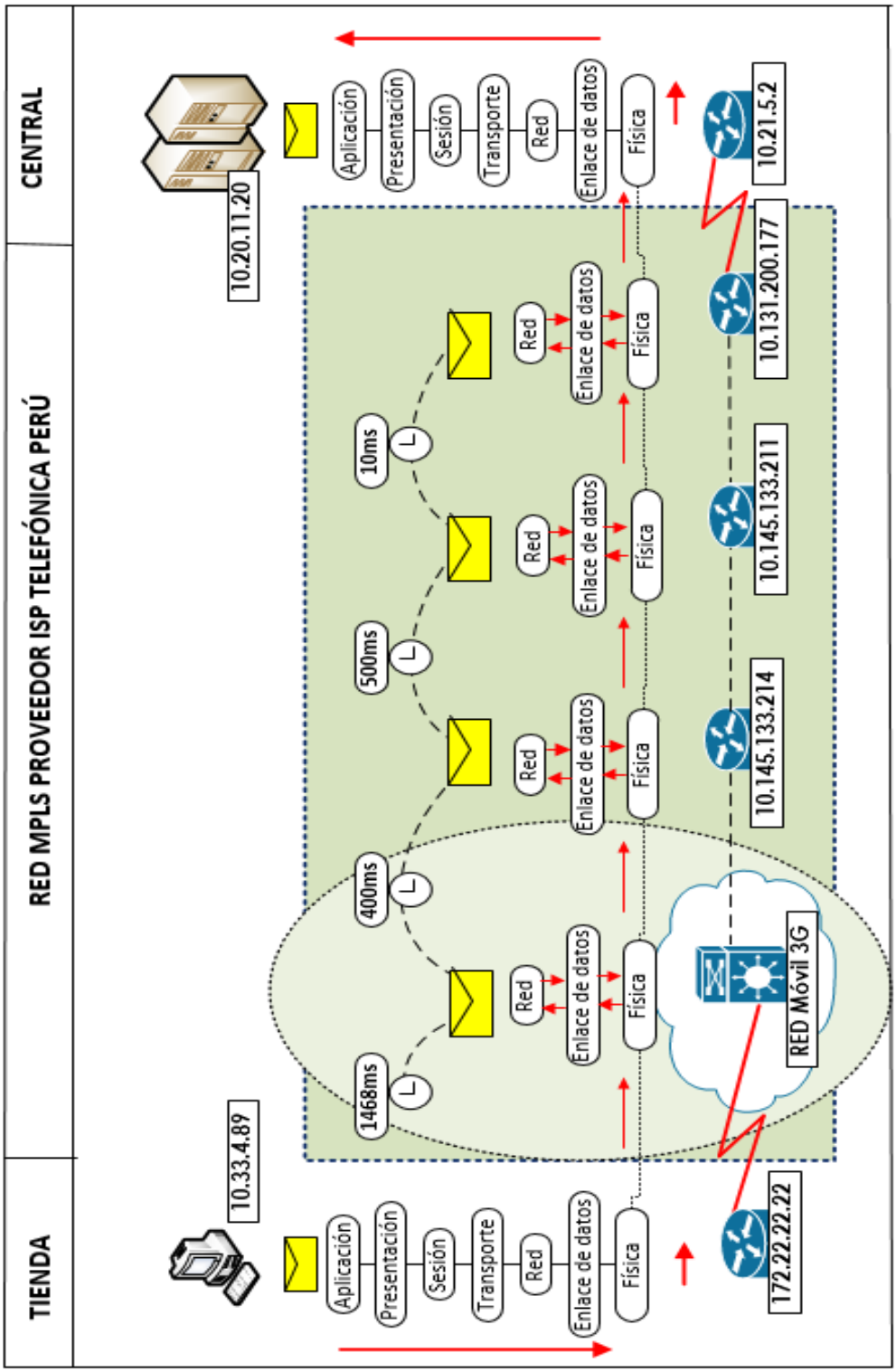

Figura 7. Recorrido del paquete de datos con el Servicio de Comunicación 3G Telefónica del Perú. (AS-IS).

El Servicio de Comunicación muestra problemas en:

- Tiempo de latencia del Servicio de Comunicación.
- Número de saltos que realiza el paquete de datos para llegar a su destino.
- Incidencias semanales por el Servicio de Comunicación a Mesa de Ayuda.
- Tiempo de carga al ingresar a los Sistemas informáticos en Red.

Tabla 1

Datos actuales de los indicadores.

INDICADOR	DATOS PRE-PRUEBA (PROMEDIO)
Tiempo de latencia del Servicio de Comunicación.	1200 milisegundos
Número de saltos que recorre el paquete de datos.	8 saltos.
Cantidad de incidencias registradas semanales.	3 veces
Tiempo de carga al ingresar a los Sistemas informáticos.	4 minutos.

Nota: Resultados correspondientes a los datos de la Pre-prueba en tiempo real.

Tabla 2

Cuadro comparativo entre la situación actual (AS - IS) y situación propuesta (TO – BE).

SITUACIÓN ACTUAL (AS-IS)	SITUACIÓN PROPUESTA (TO-BE)
El Tiempo de latencia Servicio de Comunicación 3G es muy elevado con intermitencias significativas.	Mejorar los tiempos de latencia del Servicio de Comunicación.
El número de saltos que realiza el paquete de datos en la Red es excesivo.	Reducir el número de saltos que realiza el paquete de datos en la Red.

El tiempo que demora en cargar o realizar alguna transacción en los Sistemas informáticos es muy elevado.	Reducir los tiempos de carga al momento de ingresar o realizar alguna transacción en los sistemas informáticos.
Los incidentes por lentitud o intermitencia en los Servicios de Comunicación 3G se presentan semanalmente.	Reducir la cantidad de incidencias por problemas de lentitud o intermitencia en el Servicio de Comunicación.

Nota: Se toma los datos actuales y propuestos como punto de discernimiento.

Servicio de Comunicación en la Red Actual

El servicio de comunicación en las tiendas Mass se ve afectada por la lentitud e intermitencias que presenta los enlaces de datos 3G distribuidos por el proveedor Telefónica del Perú. Primero, el Servicio de Comunicación 3G, presenta lentitud en intermitencias en la transmisión de datos, generando que los Sistemas Informáticos se demoren más de lo normal en cargar, realizar alguna operación o proceso en la Tienda, esto afecta a las actividades diarias del personal y operatividad de la Tienda, generando pérdidas de dinero significativas. Segundo, la solución del Servicio de Comunicación en las tiendas con enlaces 3G no es escalable, si se desea crecer en el tiempo y agregar más dispositivos en Red no se podrá por las limitaciones de Hardware que posee el equipo.

Servicio de Comunicación de la Red Propuesto

Observando la problemática del Servicio de Comunicación en las Tiendas Mass, se realiza la siguiente propuesta.

Se propone la realización de un diseño de una Red Privada Virtual, en la cual permita confiabilidad, integridad y escalabilidad al Servicio de Comunicación en la Tienda, dando un valor agregado a la calidad de servicio, utilizando equipos con una mejor performance, esto va de la mano con el ahorro significativo en costos de enlace dedicado, ya que no utilizarán una infraestructura tan compleja ni muchos recursos que impliquen presupuestos elevados con el proveedor. Tan solo se necesitará un enlace de Internet empresarial con un ancho de banda de 2 Mpbs y así montar toda la solución.

Por lo tanto, se propone los siguientes diagramas de solución:

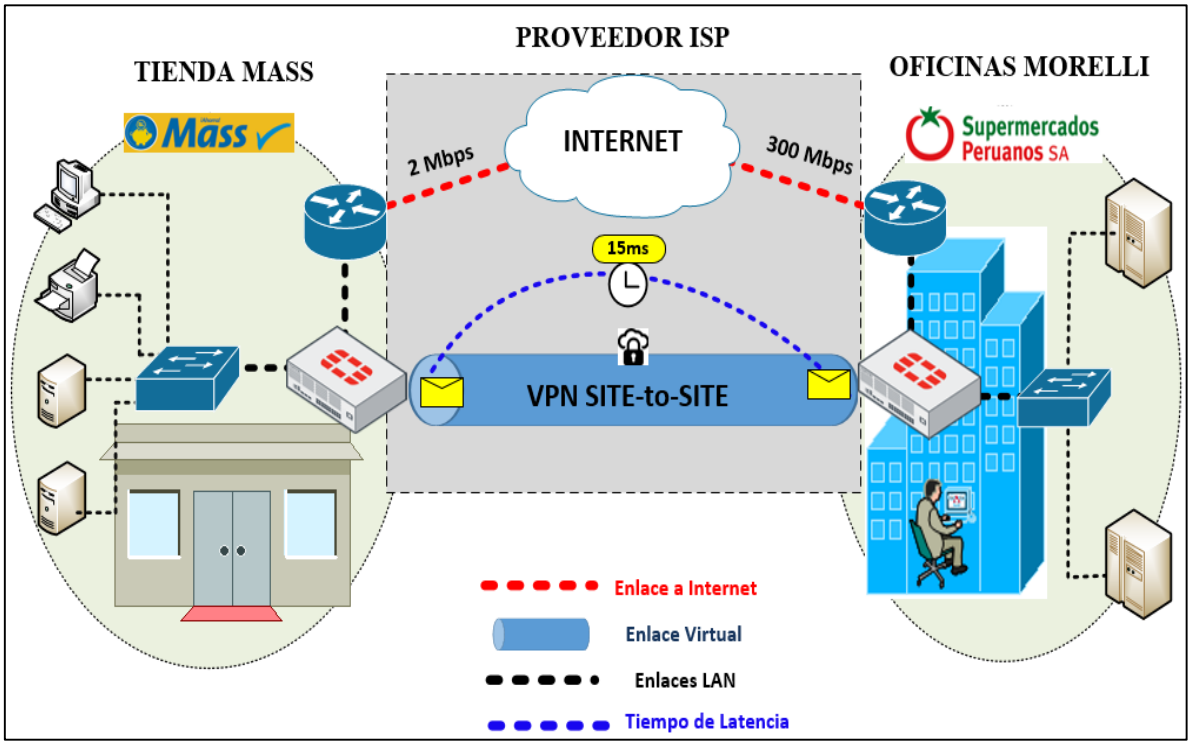

Figura 8. Servicio de Comunicación con una Red Privada Virtual sobre Internet (TO-BE).

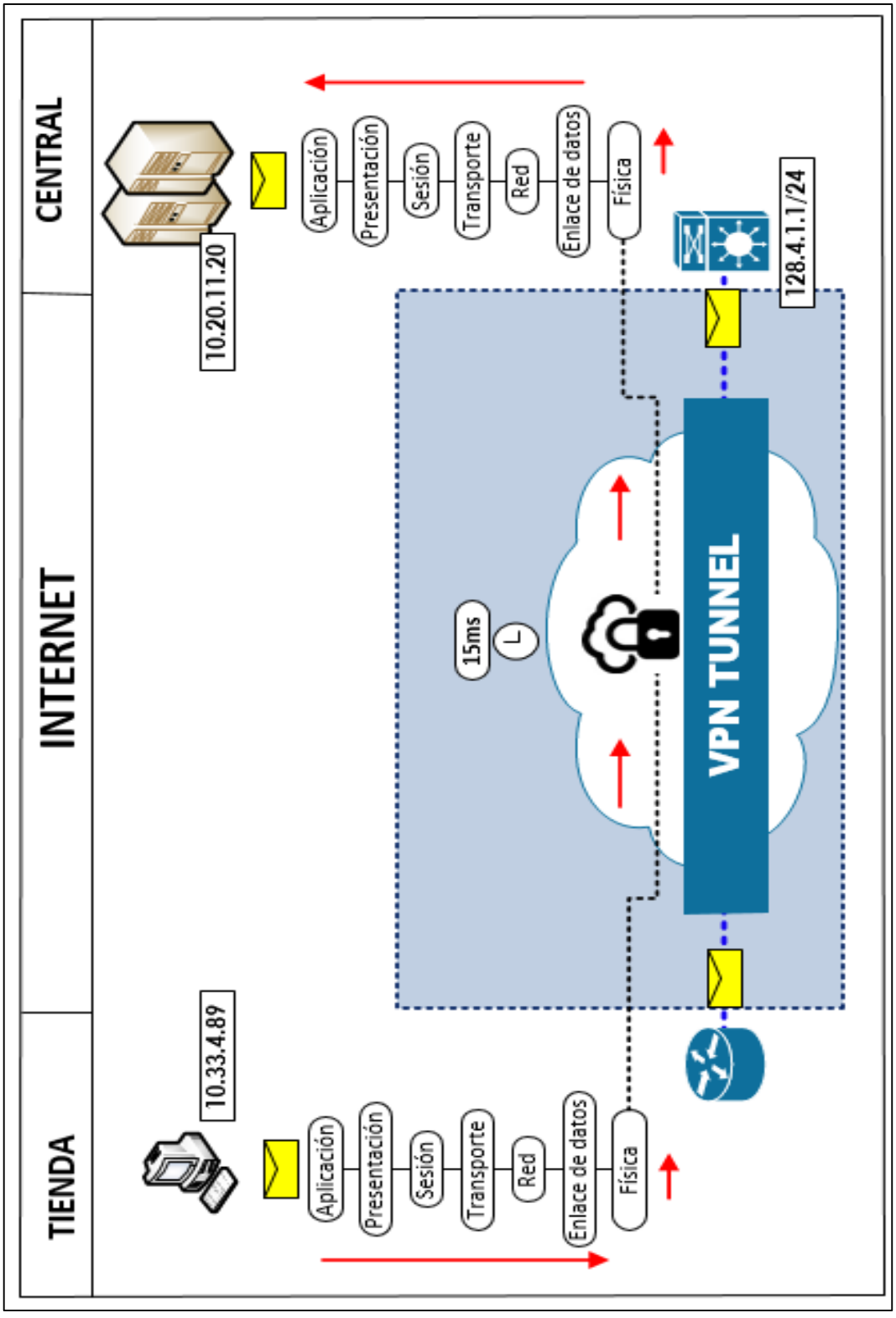

*Figura 9***.** Recorrido del paquete de datos en una Red Privada Virtual sobre Internet (TO-BE).

1.1.3. Enunciado del Problema

¿En qué medida el uso de una Red Privada Virtual, mejorará el Servicio de Comunicación en las Tiendas Mass para la Empresa Supermercados Peruanos S.A.?

1.2. TIPO Y NIVEL DE INVESTIGACIÓN

1.2.1. Tipo de investigación:

Aplicada: Se utilizará la aplicación de conocimientos en la metodología de Cisco Systems PPDIOO para el desarrollo de la investigación, también conocimientos en Diseño Redes TCP/IP, MPLS y VPNs, para el desarrollo de la solución como propuesta de una Red Privada Virtual para mejorar el Servicio de Comunicación en las tiendas Mass.

1.2.2. Nivel de investigación

Explicativa: El presente trabajo busca especificar la importancia y beneficios de usar Redes Virtuales en enlaces empresariales, para una mejor gestión de la Red, reducir costos de recursos y tener una mejor administración de la misma, utilizando técnicas de encuestas, entrevistas, documentos, etc.

1.3. JUSTIFICACIÓN DE LA INVESTIGACIÓN

Los proveedores de servicios de telecomunicaciones buscan constantemente ampliar los alcances de sus redes MPLS. La arquitectura Multi Protocol Label Switching (MPLS) proporciona alta escalabilidad y rapidez en el reenvío de paquetes, siendo su aplicación más empleada las VPNs. Sin embargo, esta arquitectura implica que los clientes de servicios VPN estén conectados a un solo proveedor. Por otro lado, las grandes empresas cuentan generalmente con sedes en diferentes ciudades o regiones, y hacen uso de los servicios VPN para poder interconectar sus sedes. A medida que las empresas crecen, los requerimientos de sus VPNs aumentan. Se hace necesario abarcar diferentes áreas geográficas, muchas veces cruzando más de un país. Inclusive, algunas VPNs necesitan extenderse a través de múltiples proveedores de servicios VPN.

Menéndez (2012) afirma:

> Independientemente de la complejidad que implique este tipo de necesidad, las conexiones que se hagan deben ser totalmente transparentes de cara al cliente. Por ello, es necesario contar con una solución que permita brindar de forma eficiente servicios VPN altamente escalables. (p. 13).

1.3.1. Justificación Práctica

El presente trabajo de investigación se basa en emplear la tecnología de red “Virtual Private Network” (VPN), “con la finalidad de mejorar la confidencialidad del intercambio de información” (Mar, 2016, p.22). Ello mejorará el Servicio de Comunicación de las tiendas Mass.

1.3.2. Justificación Tecnológica

“Las redes VPN utilizan altos estándares de seguridad para la transmisión de datos comparables con una red punto a punto. Protocolos como 3DES (Triple data encryption Standard) el cual cumple la función de encriptar la información a transferir y el protocolo IPSec (IP Security) para manejo de los túneles mediante software brindan un alto nivel de seguridad al sistema”. También se emplean varios niveles de autenticación para el acceso a la red privada mediante llaves de acceso, para validar la identidad del usuario. (Limari, 2012, p.3).

1.3.3. Justificación Metodológica

El trabajo desarrollado en la presente Tesis da solución a estos problemas de rendimiento de los servicios de red mediante el rediseño de la infraestructura de LAN switching de capas 2, 3 y 4 utilizando la metodología PPDIOO, Preparar, Planear, Diseñar e Implementar de Cisco Systems, obteniendo resultados positivos medidos a través de la mejora de las métricas de rendimiento de la red tales como la pérdida de paquetes, tiempo de respuesta y disponibilidad. (Osores, 2015, p.5).

1.4. OBJETIVOS

1.4.1. Objetivo General

Determinar en qué medida una Red Privada Virtual mejora el Servicio de Comunicación en las tiendas Mass para la Empresa Supermercados Peruanos S.A**.**

1.4.2. Objetivos Específicos

- ✓ Disminuir el número de incidencias semanales reportadas a Mesa de Ayuda.
- ✓ Disminuir el tiempo de Carga a los Sistemas Informáticos.
- ✓ Mejorar los tiempos de latencia del Servicio de Comunicación.
- ✓ Disminuir el número de Saltos que recorre el paquete en la Red.

1.5. HIPÓTESIS

El uso de una Red Privada Virtual mejorará el servicio de comunicación en las tiendas Mass para la empresa Supermercados Peruanos S.A.

1.6. VARIABLES E INDICADORES

1.6.1. Variable Independiente

Red Privada Virtual.

1.6.2. Variable Dependiente

Servicio de comunicación en las tiendas Mass para la empresa Supermercados Peruanos S.A.

INDICADORES

I. Conceptualización

a. Variable Independiente: Red Privada Virtual.

Tabla 3

Conceptos de la Variable Independiente.

INDICADOR	DESCRIPCIÓN
Ausencia	Cuando no se ha implementado la Red Privada Virtual para mejorar el servicio de comunicación en tiendas Mass para la empresa Supermercados Peruanos y aún se encuentra en la situación actual del problema.
Presencia	Cuando se ha implementado la Red Privada Virtual para mejorar el servicio de comunicación en las tiendas Mass para la empresa Supermercados Peruanos S.A.

Nota: Los indicadores de ausencia y presencia se encuentran ligados explícitamente a la variable independiente que es la solución a la problemática de dicha investigación.

b. Variable Dependiente: Servicio de comunicación en las tiendas Mass para la empresa Supermercados Peruanos S.A.

Tabla 4

Conceptos de la Variable Dependiente.

INDICADOR	DESCRIPCIÓN
Tiempo de Latencia del Servicio de Comunicación.	El tiempo en milisegundos que le toma al paquete de datos viajando en la Red para llegar a su destino y viceversa.
Número de saltos que recorre el paquete de datos para llegar a su destino.	El número de Host que recorre el Paquete de datos para entregar la información al receptor.
Número de incidencias reportadas semanal a Mesa de Ayuda.	Es el número de incidencias reportadas a Mesa de Ayuda por intermitencia o lentitud.
Tiempo de carga al ejecutar consultas o transacciones en los Sistemas Informáticos.	El tiempo que demora en cargar o realizar alguna transacción a los Sistemas informático en la Red corporativa.

Nota: Las variables independientes tendrán como objetivo identificar los puntos críticos en base a la problemática planteada en el inicio de la investigación.

II. Operacionalización

a. Variable Independiente: Red Privada Virtual.

Tabla 5

Indicador de Variable Independiente.

INDICADOR	ÍNDICE
Presencia – Ausencia	No, Sí

Nota: Cuando se afirme (Sí) es porque se tiene implementada la solución, pero sucederá lo contrario cuando se niegue dicha afirmación (No).

b. Variable Dependiente: Servicio de comunicación en las tiendas Mass para la empresa Supermercados Peruanos S.A.

Tabla 6

Indicador de Variable Dependiente.

INDICADOR	ÍNDICE	UNIDAD DE MEDIDA	UNIDAD DE OBSERVACIÓN
Tiempo de latencia del Servicio de Comunicación.	[900 - 1500]	Milisegundos/Reply ICMP	Red de Datos.
Número de saltos que recorre el paquete de datos.	[6 -11]	# Saltos /Host	Red de Datos.
Cantidad de incidencias registradas semanales.	[5 - 6]	Registro/Semana	Red de Datos.
Tiempo de carga al ingresar a los Sistemas informáticos.	[4 - 7]	Minutos/Transacción	Red de Datos

Nota: La unidad de observación será la Red de datos de una tienda Mass elegida por el coordinador regional, se tomarán muestras para el estudio correspondiente.

1.7. LIMITACIONES DE LA INVESTIGACIÓN:

De ámbito

Esta Red Privada Virtual abarca en su totalidad la mejora del Servicio de Comunicación en las tiendas Mass. Incluye el enlace virtual punto a punto además la seguridad y encriptación de la información logrando una comunicación segura y fiable a través del Internet.

De Tiempo

Esta propuesta de Red Privada Virtual se realizará y modificará durante el periodo comprendido entre el mes de septiembre y diciembre del 2017.

De Recursos

Los recursos humanos y de infraestructura tecnológica serán patrocinados por la empresa Supermercados Peruanos S.A.

1.8. DISEÑO DE INVESTIGACIÓN:

Pre Experimental

Porque demostrará la hipótesis a través de métodos experimentales. No tiene un Grupo Control para comparación de resultados.

Ge O_1 X O_2

Dónde:

- **Ge =** Grupo Experimental: Es el grupo al que se le aplicará el estímulo (Red Privada Virtual).
- **O_1 =** Datos de la Pre-Prueba para los indicadores de la Variable Dependiente. Mediciones pre-prueba del grupo experimental.
- **X =** Red Privada Virtual: Estímulo o condición experimental.
- **O_2 =** Datos Post Prueba: Para los indicadores de la variable independiente una vez implementada la Red Privada Virtual (VPN).

DESCRIPCIÓN

Se trata de la confrontación de forma intencional de un grupo Ge conformado por el servicio de comunicación en tiendas Mass, a quienes se le aplica una medición previa de los indicadores a ser estudiados (O1), después se implementará la Red Privada Virtual (X), para mejorar el servicio de comunicación y finalmente se aplicará una nueva medición de los indicadores (O2). Se espera que los valores O2 sean mejores que los valores O1. Las dos variables están constituidas de forma intencional pero representativa estadísticamente. Tanto en ausencia como la presencia de la Red Privada Virtual propuesto.

1.9. TÉCNICAS E INSTRUMENTOS PARA RECOLECCIÓN DE INFORMACIÓN

Tabla 7

Técnicas e Instrumentos para la recolección de datos.

TÉ**CNICAS**	**INSTRUMENTOS**	**ANEXO**
Seguimiento al número de saltos que realiza el paquete de datos al ejecutar el comando Tracert –d.	Ficha de Observación.	Anexo II: Número de saltos que recorre el paquete de datos para llegar a su destino.
Seguimiento al tiempo de latencia del Servicio de Comunicación ejecutar el comando ping -t.	Ficha de Observación.	Anexo I: Tiempo de latencia del Servicio de Comunicación.
Seguimiento al tiempo de carga para ingresar o realizar alguna transacción a los Sistemas Informáticos.	Ficha de Observación.	Anexo III: Tiempo de carga para realizar alguna transacción en línea.
Seguimiento a la cantidad de incidencias reportadas semanalmente.	Ficha de Observación.	Anexo IV: Incidencias reportadas por lentitud o intermitencia de la Red.

Nota: Las técnicas para las capturas de datos son propuestas por el especialista en el campo de las redes, ello se reflejará en las fichas de observación.

Tabla 8

Técnicas e instrumentos de la Investigación de Documental

TÉCNICAS	INSTRUMENTOS
Revisión de:	
	Computadoras
Libros	USB
Documentación Estadística	Fotocopias
Revistas	Diapositivas
Tesis	Impresiones
Internet	Fichas
	CD-ROM.

CAPÍTULO II

MARCO REFERENCIAL

2.1. ANTECEDENTES DE LA INVESTIGACIÓN:

A. Autor: Jenny Mar Segundo.

Título: Propuesta de implementación de una intranet vía VPN para mejorar la confidencialidad del intercambio de información entre las sedes Lima – Cusco del INEI. CASO: Servidor de Correos, 2016.

Tipo: Tesis Pre grado

Correlación:

El presente trabajo de investigación se basa en emplear la tecnología de red "Virtual Private Network" (VPN), con la finalidad de mejorar la confidencialidad del intercambio de información entre las sedes Lima - Cusco del Instituto Nacional de Estadística e Informática (INEI), ya que en la actualidad los encargados de las oficinas técnicas de informática señalaron que un porcentaje del personal administrativo en común de las sedes Lima – Cusco del INEI presenta inconvenientes con sus cuentas de correo (cuentas hackeadas), debido a los bajos niveles de seguridad. Asimismo, actualmente el personal administrativo quienes vienen laborando en ambas sedes se comunican a través de servicios de correos gratuitos (Hotmail), es decir utilizan correos no institucionales con sus cuentas personales. En vista de los problemas mencionados, se ha visto por conveniente proponer la implementación de una intranet vía VPN para mejorar la confidencialidad del intercambio de información tomando como caso un servidor de correos entre las sedes Lima y Cusco del INEI, el cual permitirá que dicha institución no solo maneje un solo dominio de correo "inei.com" para el envío y recepción de mensajes de texto relacionados únicamente a temas laborales entre el personal administrativo de ambas sedes, sino que a su vez ayudará a mejorar la confidencialidad en el intercambio de dicha información. Para llevar a cabo las pruebas de seguridad para verificar que tan eficiente es la VPN para el resguardo de la confidencialidad de la información, se realizaron los ataques man in the middle con una conexión a la intranet vía VPN y otra prueba sin conexión a la misma. La presente tesis, hace referencia a la creación de una intranet sobre una VPN utilizando el Internet como medio de acceso para enlazar los recursos informativos que poseen en la institución con otra sucursal, es una muy buena propuesta de proyecto a bajo costo utilizando nuevas tecnologías. (Mar, 2016).

B. Autor: Ricardo Armando Menéndez Ávila.

Título: Estudio del desempeño e implementación de una solución MPLS-VPN sobre múltiples sistemas autónomos, 2012.

Tipo: Tesis Pre grado

Correlación:

La presente tesis consiste en proporcionar una propuesta técnica para la implementación de una red MPLS-VPN sobre Múltiples Sistemas Autónomos (Multi Autonomous System VPN), a través de un estudio del desempeño de cuatro diferentes modelos de implementación para brindar dicha solución.

Durante el desarrollo de la tesis se presenta el marco teórico que permite conocer y entender tanto las redes VPN como las arquitecturas involucradas en su funcionamiento, principalmente la tecnología MPLS. Posteriormente se explica el porqué es necesario contemplar una solución soportada en más de un sistema autónomo.

A continuación, se presentan los distintos modelos de red para la implementación de las VPN Multi-AS y se realiza un estudio del desempeño de cada uno de ellos. Posteriormente se hace un análisis de los resultados obtenidos durante el estudio de cada opción con el fin de conocer las ventajas, desventajas, problemas y las posibles soluciones que ofrecen. Finalmente se elabora una propuesta técnica para la implementación de la red, utilizando el Modelo de Implementación “Multi Protocol eBGP Multisalto entre Route Reflectors”, con los procedimientos detallados necesarios, los aspectos económicos y resultados esperados al final del proceso.

En esta tesis referenciada, estudia el desempeño de las Redes virtuales sobre las plataformas MPLS, utilizando sistemas autónomos de enrutamiento eBGP (Eternal Border Gateway Protocol), también hace referencias a las distintas maneras de implementar una VPN, a manera de conocimiento (Menéndez, 2012).

C. Autores: Rafael Pinilla Vico.

Victor Óscar Sanchez Sanchez.

Título: Implementación de una red privada virtual para el control remoto de equipos de laboratorio, 2009.

Tipo: Tesis Pre grado.

Correlación:

Las redes privadas virtuales (VPN en sus siglas en inglés) consisten en redes en las que algunos o todos los equipos de los que forman parte están unidos por conexiones o circuitos virtuales, en lugar de estarlo físicamente. Esto, aparte de comportar una reducción de costes, permite aumentar la seguridad de las comunicaciones y facilitar la conexión entre máquinas de distintos rangos con IP's fijas o dinámicas. El objetivo de este trabajo es la puesta en marcha de una VPN del grupo de investigación de Materiales Meta-estables y Nano-estructurados del Departamento de Física Aplicada de la UPC.

- Analizar la seguridad actual de la red frente a ataques externos. Se estudiará los puntos débiles, y la forma de mejorarlos.
- Instalación de la VPN en una red multiplataforma, en la que se tendrán que analizar los pros y contras de las distintas opciones disponibles. Se deberá decidir el programa a usar (libre o comercial) y sobre la conveniencia de tener un servidor propio o uno externo.
- Establecer un protocolo detallado sobre el alta de nuevos ordenadores en la red, así como el de la baja de algún equipo obsoleto.
- Implementar un sistema que permita el control remoto a través de la VPN de los equipos de laboratorio conectados a la VPN.
- Potenciar y optimizar los recursos de cada ordenador con la VPN. Al finalizar el trabajo, se deberá establecer una red privada virtual segura que permita maximizar los recursos de cada ordenador. (p.2).

En la presente tesis referenciada, hace énfasis en la seguridad perimetral de la red, de qué manera impactará al optimizar los recursos de los ordenadores y como se gestionarán los equipos remotamente, implementando la VPN.

(Pinilla y Sánchez., 2009).

D. Autores: Manuel Auner Díaz Llatance.
Gino Luis Alberto Vieyra Dioses.

Título: Diseño de una red privada virtual para interconectar las sucursales de la empresa Terracargo S. A. C., 2015.

Tipo: Tesis Pre grado.

Correlación:

Ésta tesis está centrada en el mejoramiento de la interconexión entre las sucursales de la empresa Terracargo SAC, la cual cuenta con sucursales en distintas ciudades del Perú. Este mejoramiento se hará a través de la implementación de una VPN, permitiendo la intercomunicación en tiempo real entré las sucursales, de manera eficiente y segura. La investigación fue realizada en 3 etapas.

Como primera etapa se realiza un diagnóstico de la actualidad de la empresa, obteniendo datos importantes como la arquitectura actual en cada una de las sucursales, la disponibilidad de hardware, sus usuarios y la forma de interconexión con la que trabajan, toda esta información y algunos requerimientos importantes que solicitamos nos permiten seleccionar y diseñar el modelo de VPN adecuado.

En la segunda etapa se diseña un modelo de red VPN adecuado a los requerimientos de la empresa, esto refiere a la elección del tipo de VPN que debemos utilizar, los equipos adecuados, la arquitectura y protocolos que se deben emplear, teniendo en cuenta todos los datos obtenidos anteriormente y poder brindar la mejor solución sin generar un gasto económico excesivo.

También se propone soluciones a posibles problemas como cortes del servicio de internet y servicio eléctrico para evitar caídas en el servidor VPN ubicado en la sede central.

En esta tesis referenciada, hace mucho énfasis en enlazar las sedes remotas con la sucursal mediante una Red privada virtual, en vista de las numerosas sucursales geográficamente dispersas en la Región se ven obligados a utilizar esta tecnología asequible, de fácil gestión y mantenimiento, también evalúa costos en base al presupuesto, esto como tal es un proyecto tecnológico que en cierta medida tendrá un costo beneficio. (Díaz y Vieyra, 2015).

E. Autor: Edison Rafael Trujillo Machado

Título: Diseño Implementación de una VPN en una empresa comercializadora utilizando IPSEC, 2006.

Tipo: Tesis Pre grado.

Correlación:

El presente trabajo comprende el diseño e implementación de un VPN en una empresa comercializadora utilizando IPSec. Ha sido estructurado en 5 capítulos, a continuación, se muestra una visión de los contenidos de cada sección:

Capítulo 1. Presenta una reseña de la evolución del Internet, los diferentes tipos de conexión, los proveedores de este servicio en el Ecuador, y las tecnologías de conexión WAN que se han utilizado hasta la actualidad.

Capítulo 2. Comprende todo lo relacionado con las Redes Privadas Virtuales como son los tipos, arquitectura, tecnologías de tunneling. También se analiza las funcionalidades y aplicaciones del protocolo dentro de las VPN.

Capítulo 3. Se hace un estudio de la situación organizacional y tecnológica de la empresa comercializadora tomada como caso de estudio para este trabajo y sus posibles implementaciones VPN.

Capítulo 4. Se documenta la implementación de un protocolo VPN dentro de la empresa comercializadora, se hace un análisis de costos, ventajas, desventajas con respecto a las líneas dedicadas.

Capítulo 5. Consta de las conclusiones y recomendaciones.

Finalmente, las referencias bibliográficas y los anexos.

De esta tesis referenciada, se coge como modelo la estructura de desarrollo ya que se enfoca en el desarrollo de la VPN con un protocolo en particular, el IPsec lo cual es seguro, flexible y fiable, al momento de levantar el túnel sobre Internet, y sobre todo la implementación en la empresa le da un valor agregado al trabajo realizado. (Trujillo, 2006).

2.2. MARCO TEÓRICO:

2.2.1. Multi Protocolo Layer Switching (Mpls):

MPLS es un estándar IP de conmutación de paquetes del IETF (Internet Engineering Task Force), que trata de proporcionar algunas de las características de las redes orientadas a conexión a las redes no orientadas a conexión.

En el encaminamiento IP sin conexión tradicional, la dirección de destino junto a otros parámetros de la cabecera, es examinada cada vez que el paquete atraviesa un router. La ruta del paquete se adapta en función del estado de las tablas de encaminamiento de cada nodo, pero, como la ruta no puede predecirse, es difícil reservar recursos que garanticen la QoS; además, las búsquedas en tablas de encaminamiento hacen que cada nodo pierda cierto tiempo, que se incrementa en función de la longitud de la tabla.

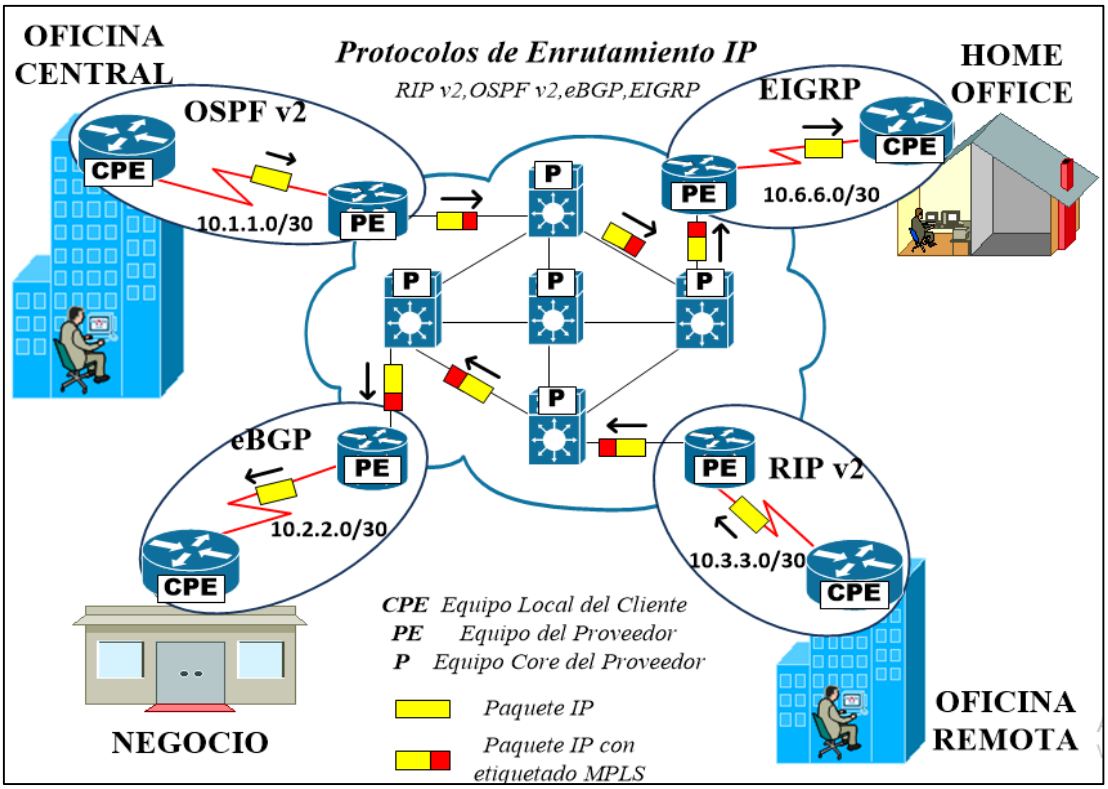

Figura 10. Diagrama de Red MultiProtocol Layer Switching (MPLS).

Sin embargo, MPLS permite a cada nodo, ya sea un switch o un router, asignar una etiqueta a cada uno de los elementos de la tabla y comunicarla a sus nodos vecinos. Esta etiqueta es un valor corto y de tamaño fijo transportado en la cabecera del paquete para identificar un FEC (*Forward Equivalence Class*), que es un conjunto

de paquetes que son reenviados sobre el mismo camino a través de la red, incluso si sus destinos finales son diferentes. La etiqueta es un identificador de conexión que sólo tiene significado local y que establece una correspondencia entre el tráfico y un FEC específico. Dicha etiqueta se asigna al paquete basándose en su dirección de destino, los parámetros de tipo de servicio, la pertenencia a una VPN, o siguiendo otro criterio. Cuando MPLS está implementado como una solución IP pura o de nivel 3, que es la más habitual, la etiqueta es un segmento de información añadido al comienzo del paquete. Los campos de la cabecera MPLS de 4 bytes, son los siguientes:

- Label (20 bits). Es el valor actual, con sentido únicamente local, de la etiqueta MPLS. Esta etiqueta es la que determinará el próximo salto del paquete.
- CoS (3 bits). Este campo afecta a los algoritmos de descarte de paquetes y de mantenimiento de colas en los nodos intermedios, es decir, indica la QoS del paquete. Mediante este campo es posible diferenciar distintos tipos de tráficos y mejorar el rendimiento de un tipo de tráfico respecto a otros.
- Stack (1 bit). Mediante este bit se soporta una pila de etiquetas jerárquicas, es decir, indica si existen más etiquetas MPLS. Las cabeceras MPLS se comportan como si estuvieran apiladas una sobre otra, de modo que el nodo MPLS tratará siempre la que esté más alto en la pila. La posibilidad de encapsular una cabecera MPLS en otras, tiene sentido, por ejemplo, cuando se tiene una red MPLS que tiene que atravesar otra red MPLS perteneciente a un ISP u organismo administrativo externo distinto; de modo que, al terminar de atravesar esa red, se continúe trabajando con MPLS como si no existiera dicha red externa.

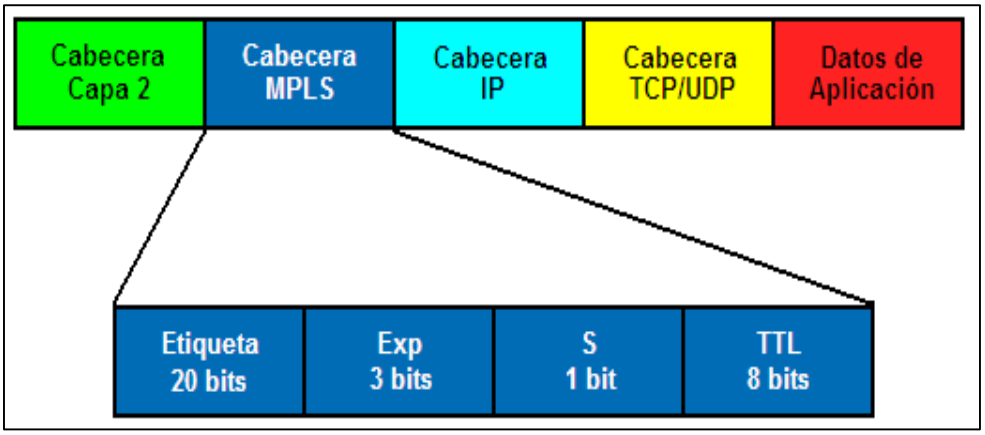

Figura 11. Estructura de un Paquete MPLS. Adaptado de "Cabecera MPLS" por García, 2009, p.42.

Principales ventajas de MPLS.

Entre las ventajas de la tecnología MPLS se pueden resaltar:

- ✓ Conmutación rápida de paquetes basado en etiquetas y no direcciones IP destino.
- ✓ Redes de clientes totalmente independientes (MPLS-VPN).
- ✓ Es multi-protocolo tanto hacia arriba (L3) como hacia abajo (PWE3).
- ✓ Trabaja con QoS (Calidad de Servicio) basado en marcación de paquetes.
- ✓ La creación de una nueva VPN sólo implica la creación del circuito de acceso y del enrutamiento.
- ✓ Permite aplicar Ingeniería de Tráfico (TE).
- ✓ Uso eficiente del ancho de banda en accesos (full-mesh virtual).

Términos Principales Utilizados en MPLS.

García (2009) afirma:

- ✓ LSR (Label Swtiching Router): Nodo interno de la red MPLS capaz de conmutar y enrutar paquetes analizando la etiqueta adicionada a cada uno de estos
- ✓ Edge LSR (Edge Label Switch Router) o LER (Label Edge Router): Nodo de borde que maneja tráfico entrante y saliente de la red MPLS. El Edge LSR de entrada adiciona la etiqueta a MPLS a cada paquete y el de salida la extrae y en ruta según la capa de Red (p.42).

Lavado (2015) afirma:

- ✓ LDP (Label Distribution Protocol): Protocolo que establece sesiones TCP entre LSR/LERs para intercambiar las etiquetas que estos utilizarán para la conmutación de paquetes

- ✓ TDP (Tag Distribution Protocol): Protocolo similar a LDP, propietario de Cisco.
- ✓ LIB (Label Information Base): Base de datos formada en un LSR/LER que contiene información de etiquetas e interfaces asociadas a las redes destino.
- ✓ FEC (Forwarding Equivalence Class): Es una clase que agrupa un conjunto de paquetes que se enviarán en base a una característica común (dirección destino, clase QoS, etc). Los paquetes que pertenezcan al mismo FEC, usarán el mismo camino a lo largo de toda la red MPLS y la misma etiqueta de salida.
- ✓ LSP (Label Switched Path): Camino unidireccional definido con QoS y formado por una secuencia de LSRs sobre el cual se envían los paquetes que pertenecen al mismo FEC. (p.1).

✓ "Traffic Engineering (TE): Proceso de control de flujo de tráfico a través de la red, que optimiza el uso de recursos con el objetivo de mejorar su rendimiento" (García, 2009).

Morales (2006) afirma:

> Primero, se establece un LSP entre los routers que van a transmitir el tráfico FEC. Los LSPs hacen las veces de túneles de transporte e incluyen los parámetros QoS específicos del flujo, que sirven para determinar la cantidad de recursos a reservar para el LSP y las políticas de desechado y la cola de procesos en cada LSR.
>
> Para intercambiar información los routers MPLS usan los protocolos LDP o TDP. Cada flujo de tráfico FEC es asignado a una etiqueta particular. La asignación de nombres y rutas se puede realizar manualmente o bien a través del protocolo empleado. (p.106).

Cuando un paquete ingresa al dominio MPLS, el Edge LSR determina los servicios de red que requiere. Luego, asigna el paquete a una FEC y a un LSP particular, lo etiqueta y lo envía. Si no existe ningún LSP, el router de borde trabaja en conjunto con los demás LSRs para definirlo. Una vez dentro del dominio MPLS, en cada LSR que recibe el paquete se llevan a cabo los siguientes procesos:

- ✓ Se retira la etiqueta de entrada y se le añade la nueva etiqueta de salida al paquete.
- ✓ Se envía el paquete al siguiente LSR dentro del LSP.

Finalmente, El LSR de salida "abre" la etiqueta y lee el encabezado IP para enviarlo a su destino final

Arquitectura MPLS

Componentes lógicos:

- ✓ Plano de Control (control plane): Hace el intercambio de etiquetas y rutas en capa 3.
- ✓ Plano de Datos (data plane): Reenvía los paquetes basado en las etiquetas.

Componentes Físicos:

Guichard et. al. (2002) define lo siguiente:

> Un término muy importante en MPLS es el Label Switch Router (LSR). Cualquier router o switch que implemente procedimientos de distribución de etiquetas y pueda enviar paquetes basándose en etiquetas se encuentra en esta categoría. Los diferentes tipos de LSR pueden ser descritos dependiendo de la arquitectura donde se encuentren como Edge-LSRs (LSRs de borde), ATM-LSRs, y ATM Edge-LSRs
>
> Un Edge-LSR es un router que realiza ya sea *label imposition* (o push action) o *label disposition* (o pop action) en el borde de la red MPLS. *Label imposition* es el acto de anteponer etiquetas a un paquete en el punto donde ingresa al dominio MPLS. *Label disposition*, por otro lado, es el acto de remover la última etiqueta de un paquete en el punto de salida para luego enviarlo a un vecino fuera del dominio MPLS.
>
> Cualquier LSR que tenga vecinos que no tienen implementado MPLS es considerado un Edge-LSR. Sin embargo, si ese LSR tiene interfaces que se conectan a un ATM-LSR a través de MPLS, también se considera un ATM Edge-LSR. Los Edge-LSRs usan una tabla de reenvío IP tradicional con la información adicional de etiquetado, para poder etiquetar y desetiquetar los paquetes.
>
> Un ATM-LSR es un switch ATM que puede actuar como un LSR. El ATM-LSR realiza enrutamiento IP y asignación de etiquetas en el plano de control y reenvía los paquetes utilizando mecanismos de conmutación ATM tradicional (ATM cell switching) en el plano de datos. En otras palabras, la matriz de conmutación de un switch ATM es utilizada como una tabla de reenvío de un nodo MPLS. Lo switches ATM tradicionales, pueden ser reasignados como ATM-LSRs a través de una actualización del software de su componente de control. (p.5).

Tabla 9

Funciones de un LSR dentro de una Red IP MPLS.

TIPO DE LSR	ACCIONES QUE REALIZA
LSR	Reenvía paquetes etiquetados.
EDGE-LSR	Recibe un paquete IP, realiza el análisis de capa 3 e inserta la etiqueta antes de reenviar el paquete. Recibe un paquete etiquetado, remueve la etiqueta, realiza el análisis de capa 3, y reenvía el paquete IP.
ATM-LSR	Ejecuta protocolos MPLS en el plano de control para implementar circuitos ATM virtuales. Reenvía paquetes etiquetados como ATM cells. Recibe un paquete etiquetado o no etiquetado, lo segmenta en ATM cells y los reenvia.

ATM EDGE-LSR	Recibe los ATM cells desde un ATM-LSR adyacente, los rearma en el paquete original y lo reenvia como un paquete etiquetado o no etiquetado.

Nota: Adaptado de “Actions Performed by Various LSR Types”, de Guichard et. al., 2002.

Tipos de Encapsulamiento MPLS

- **Modo Trama (frame-mode)**: Los LSR son routers conectados por cualquier enlace de capa 2 (Ethernet, FR, ATM, PPP, etc).

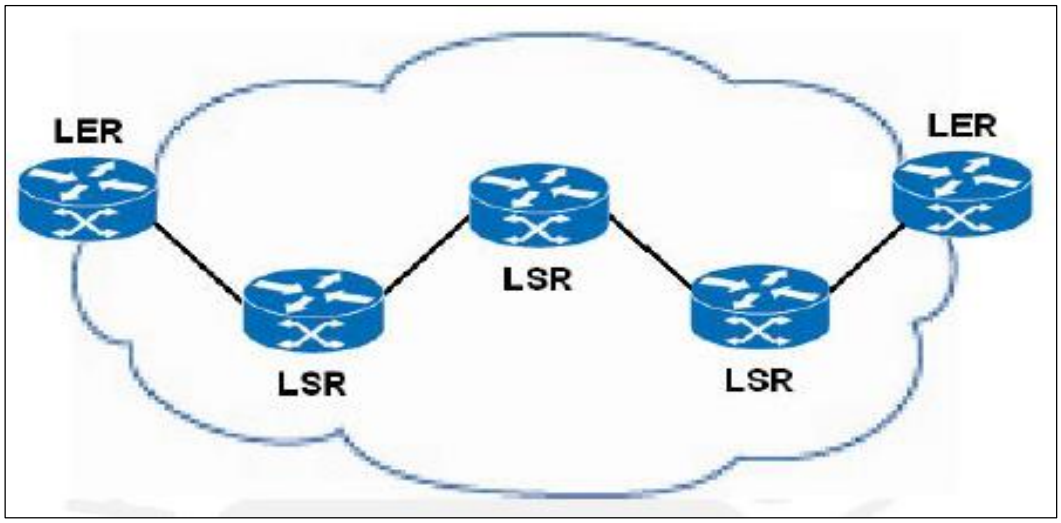

Figura 12. Esquema Frame Mode. Adaptado de“Frame Mode” por Lavado, 2010.

Se inserta un campo de 32 bits denominado ‘Shim Header’ que contiene la etiqueta, 3 bits experimentales (QoS), 1 bit ‘S’ que permite agregar más de una etiqueta en una trama y 8 bits para tiempo de vida del paquete o TTL (Time-to-live - similar a IP)

- **Modo Celda (cell-mode):** Los LSR son Switches ATM, que conectan los routers de cliente (Lavado, 2010)

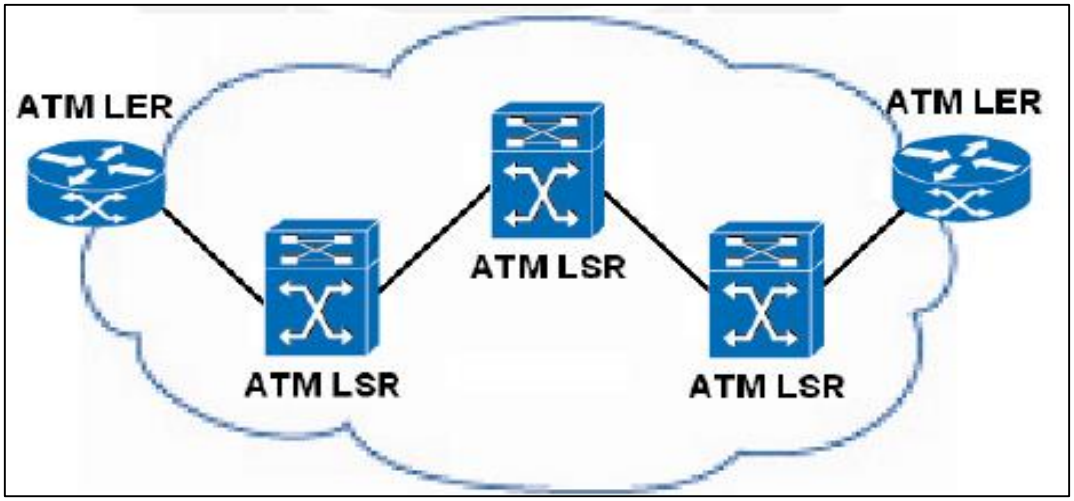

Figura 13. Esquema modo celda. Adaptado de ”Cell Mode” por Lavado, 2010.

Etiquetado en el Borde de la Red MPLS

El encapsulamiento previamente descrito es una función de borde, que implica que los paquetes sean etiquetados antes de ser reenviados a través del dominio MPLS. Para realizar esta función, un Edge-LSR necesita entender hacia dónde va el paquete y qué etiqueta, o pila de etiquetas, debe asignar al paquete. En el reenvío convencional de paquetes IP, en cada salto dentro de la red se busca en la tabla de reenvío la dirección IP destino que se encuentra en la cabecera de Capa 3 del paquete. Se selecciona una dirección IP como siguiente salto en cada iteración de la búsqueda y finalmente envía el paquete por una interface a su destino final. El proceso de escoger el siguiente salto para el paquete IP consiste en dos funciones. La primera partición a todo el conjunto de paquetes posibles en un conjunto de prefijos destino. La segunda mapea cada prefijo IP destino con una dirección IP de siguiente salto. Esto significa que cada destino en la red es alcanzable por una ruta en lo que respecta a flujo de tráfico desde un dispositivo de ingreso hacia un dispositivo de destino (Múltiples caminos pueden estar disponibles si el balanceo de carga es realizado usando rutas de igual costo o de diferente costo, como ocurre con los protocolos IGP). Los resultados de la primera función vienen a ser las FECs. Una FEC puede corresponder a una subred IP destino, pero también puede corresponder a cualquier clase de tráfico que el Edge-LSR considere significativo. Por ejemplo, todo el tráfico interactivo hacia cierto destino o todo el tráfico con un cierto valor de prioridad IP pueden conformar una FEC. Puede ser inclusive un subconjunto de la tabla BGP, incluyendo todos los prefijos de destino alcanzables

a través del mismo punto de salida.En el reenvío IP convencional, el procesamiento de paquetes se realiza en cada salto dentro de la red.

Guichard et. al. (2002) afirma:

> En cambio, en MPLS un paquete individual es asignado a una FEC particular solo una vez en el dispositivo de borde cuando el paquete entra a la red. Luego se codifica la FEC en un identificador corto de longitud fija, que viene a ser la etiqueta. Cuando el paquete es reenviado hacia su siguiente salto, se antepone la etiqueta al paquete IP para que el siguiente dispositivo en la ruta pueda reenviarlo basándose en la etiqueta codificada en lugar de analizar la información de la cabecera de capa 3.(p.1)

En la Figura 14 se ilustra mejor el proceso.

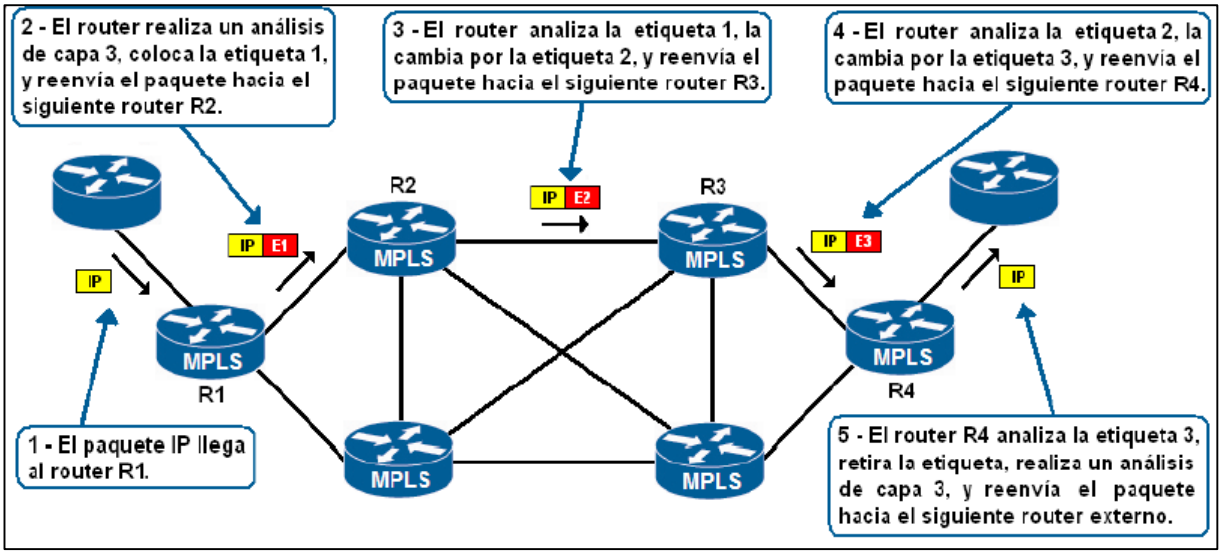

Figura 14. Etiquetado y Reenvío MPLS. Adaptado de "MPLS Label Imposition and Forwarding" por Guichard et.al., 2002.

Reenvío de Paquetes MPLS y LSPs (Label Switched Paths).

Se definió previamente un Label Switched Path (LSP) como el conjunto de LSRs que un paquete etiquetado debe atravesar para alcanzar el LSR de salida para una FEC particular. Al ser unidireccional, se utiliza un FEC diferente para el tráfico de retorno. La creación del LSP es un esquema orientado a conexión porque la ruta está priorizada antes que cualquier flujo de tráfico.

Esto quiere decir que la ruta es creada independientemente de si hay requerimiento de tráfico para ser enviado por ella hacia un conjunto particular de FECs. Mientras el paquete atraviesa la red MPLS, cada LSR cambia la etiqueta entrante por una saliente, de forma similar al mecanismo usado en ATM donde el VPI/VCI es cambiado a un par VPI/VCI diferente al salir del switch ATM. Esto continúa hasta que el último LSR, conocido como el LSR de egreso, es alcanzado. Cada LSR tiene

dos tablas, que guardan información relevante para el reenvío. La primera, conocida en Cisco IOS como Tag Information Base (TIB) y en términos estándar como Label Information Base (LIB), contiene todas las etiquetas asignadas por el LSR y las asignaciones de éstas etiquetas a etiquetas recibidas de cualquier vecino. Guichard et.al. (2002) afirma:

Estas asignaciones de etiquetas son distribuidas a través de LDP o TDP La segunda tabla, conocida en Cisco IOS como Tag Forwarding Information Base (TFIB) y en términos estándar como Label Forwarding Information Base (LFIB), es usada 32 durante el enrutamiento de paquetes y mantiene sólo las etiquetas que están siendo utilizadas por el componente de reenvío MPLS. La LFIB vendría a ser el equivalente MPLS de la matriz de conmutación de un switch ATM. (p.2).

Aplicaciones de MPLS.

Ya se mencionó que MPLS permite la integración de routers tradicionales y switches ATM en un backbone IP (arquitectura IP+ATM). Sin embargo, su verdadero potencial se encuentra en otras aplicaciones que van desde ingeniería de tráfico hasta Redes Privadas Virtuales punto a punto (peer-to-peer Virtual Private Networks). Todas ellas usan una funcionalidad del plano de control similar al plano de control del enrutamiento IP.

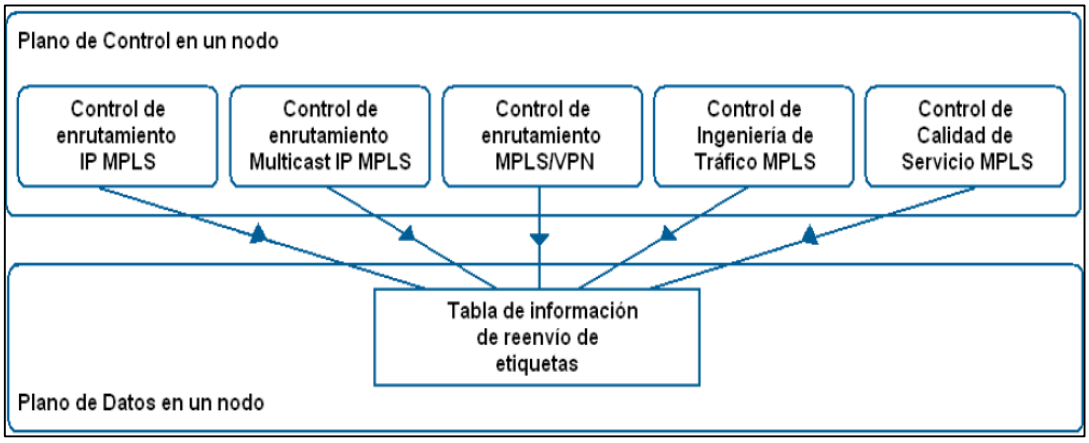

Figura 15. Aplicaciones MPLS. Adaptado de “Various MPLS Applications and Their Interactions” por Guichard et.al. 2002.

La Figura 15 muestra la “interacción entre estas aplicaciones y la matriz de conmutación de etiquetas”. (Guichard et. al. 2002, p2).

Según Guichard et. Al. (2002) define:

Cada aplicación MPLS tiene el mismo conjunto de componentes que una aplicación con enrutamiento.

• Una base de datos que define la tabla FEC para la aplicación (En IP, la tabla de enrutamiento IP).

• Protocolos de control que intercambian el contenido de la tabla FEC entre los LSRs (Protocolos de enrutamiento IP o enrutamiento estático en IP).

• Un proceso de control que realiza el enlazado de etiquetas con las FECs y un protocolo para intercambiar los enlazados de etiquetas entre LSRs (TDP o UDP en una aplicación con enrutamiento IP).

• Opcionalmente, una base de datos interna del trazado FECs-etiquetas (Base de datos con información de etiquetas para el caso de IP).

Cada aplicación usa su propio conjunto de protocolos para intercambiar tablas FEC o trazados FEC-etiquetas entre los nodos. La tabla 2-3 resume dichos protocolos y las estructuras de datos empleados. (p.3).

Tabla 10

Protocolos de Aplicación – MPLS.

APLICACIÓN	TABLA FEC	PROTOCOLO EMPLEADO PARA CONSTRUIR LA TABLA FEC	PROTOCOLO EMPLEADO PARA INTERCAMBIAR EL TRAZADO FEC-ETIQUETA
Enrutamiento IP	Tabla de enrutamiento	Cualquier protocolo de enrutamiento IP	Tag Distribution Protocol (TDP) ó Label Distribution Protocol (LDP)
Enrutamiento IP Multicast	Tabla de enrutamiento Multicast	PIM	Extensiones PIM version 2
Enrutamiento VPN	Tabla de enrutamiento Multicast	Protocolos de enrutamiento IP entre proveedores y clientes. Multi Protocol BGP dentro de la red del proveedor de servicio.	Multi Protocol BGP
Ingeniería de Tráfico	Tabla de enrutamiento Multicast	Definición manual de interfaces, extensiones a IS-IS u OSPF	RSVP ó CR-LDP
Ingeniería de Tráfico	Tabla de enrutamiento Multicast	Protocolos de enrutamiento IP	Extensiones a TDP LDP

2.2.2. Red Privada Virtual (Vpn):

Una VPN es una estructura de red que emula una red privada sobre infraestructura pública existente. Brinda comunicación a nivel de las capas 2 ó 3 del modelo OSI. La VPN pertenece generalmente a una compañía y le permite tener diferentes locales interconectados a través de la infraestructura de un proveedor de servicios. Esto es posible ya que la tecnología permite crear un túnel de encriptación a través de la Internet u otra red pública de tal forma que permita a los usuarios que se encuentran en los extremos del túnel disfrutar de la seguridad, privacidad y funciones que antes estaban disponibles sólo en redes privadas.

Ventajas de una VPN.

Implantar una VPN tiene varios puntos beneficiosos:

- ✓ Integridad, confidencialidad y encriptación de datos. La integridad de los datos hace referencia a que un mensaje enviado no pueda ser alterado.
- ✓ La confidencialidad se refiere a que sólo los usuarios permitidos tienen acceso a la información de la VPN. La encriptación de datos está basada en cifrar estos para que no puedan ser leídos por personas a las que no van dirigidos.
- ✓ Reducen los costes y son sencillas de usar.
- ✓ Facilita la comunicación entre dos usuarios/sedes situados en lugares distantes.

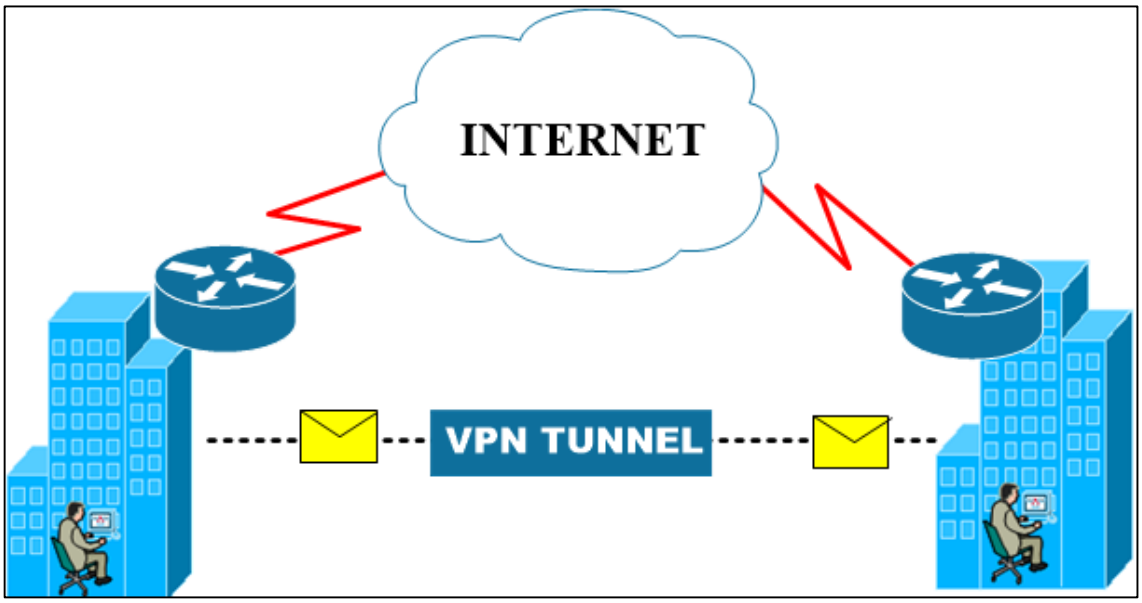

Figura 16. Diagrama de una Red Privada Virtual sobre Internet.

Razones para Implementar una VPN.

Reducción de Costos:

Para una implementación de red que abarque empresas alejadas geográficamente ya no será indispensable en términos de seguridad realizar enlaces mediante líneas dedicadas (punto a punto). En su lugar, se puede emplear un acceso ADSL. Es de bajo costo, brinda un ancho de banda alto y está disponible en la mayoría de zonas urbanas. Los usuarios remotos móviles podrán ahorrar costos de llamadas telefónicas de larga distancia, realizándolas a través de un acceso local a Internet. (Limari V., 2004).

Alta Seguridad:

Las redes VPN utilizan altos estándares de seguridad para la transmisión de datos, comparables con una red punto a punto. Protocolos como 3DES (Triple data encryption standard) el cual cumple la función de encriptar la información a transferir y el protocolo IPSec (IP Security) para manejo de los túneles mediante software brindan un alto nivel de seguridad al sistema. “También se emplean varios niveles de autenticación para el acceso a la red privada mediante llaves de acceso, para validar la identidad del usuario”. (Limari, 2004, p.22).

Escalabilidad:

No es necesario realizar inversiones adicionales para agregar usuarios a la red. El servicio se provee con dispositivos y equipos configurables y manejables. “La desarrollada infraestructura de los proveedores de Internet hace innecesario realizar un enlace físico que puede significar una gran inversión de dinero y de tiempo”. (Limari, 2004, p.22).

Compatibilidad con Tecnologías de Banda Ancha:

Una VPN puede aprovechar infraestructura existente de banda ancha inalámbrica, TV cable o conexiones de alta velocidad del tipo ADSL o ISDN. Con ello brinda un alto grado de flexibilidad al momento de configurar la red.

“Se pueden emplear tecnologías como Voz sobre IP (VoIP), que permiten ahorrar en telefonía de larga distancia”. (Limari, 2004, p.22).

Mayor Productividad:

“Una VPN da un nivel de acceso durante mayor tiempo, que significa una mayor productividad de los usuarios de la RED. Además, con la consecutiva reducción en las necesidades de espacio físico, se fomenta el teletrabajo”. (Limari, 2004, p.23).

Tipos de VPNs:

VPN Interna

Una aplicación realmente desconocida pero muy útil y potente consiste en establecer redes privadas virtuales dentro de una misma red local.

El objetivo último es aislar partes de la red y sus servicios entre sí, aumentando la seguridad. Una aplicación muy típica de este modelo se utiliza para aumentar la seguridad en redes de acceso inalámbrico, separándolas así de la red física para evitar posibles fugas de información o accesos no autorizados. (Pinto de Olivera, 2014).

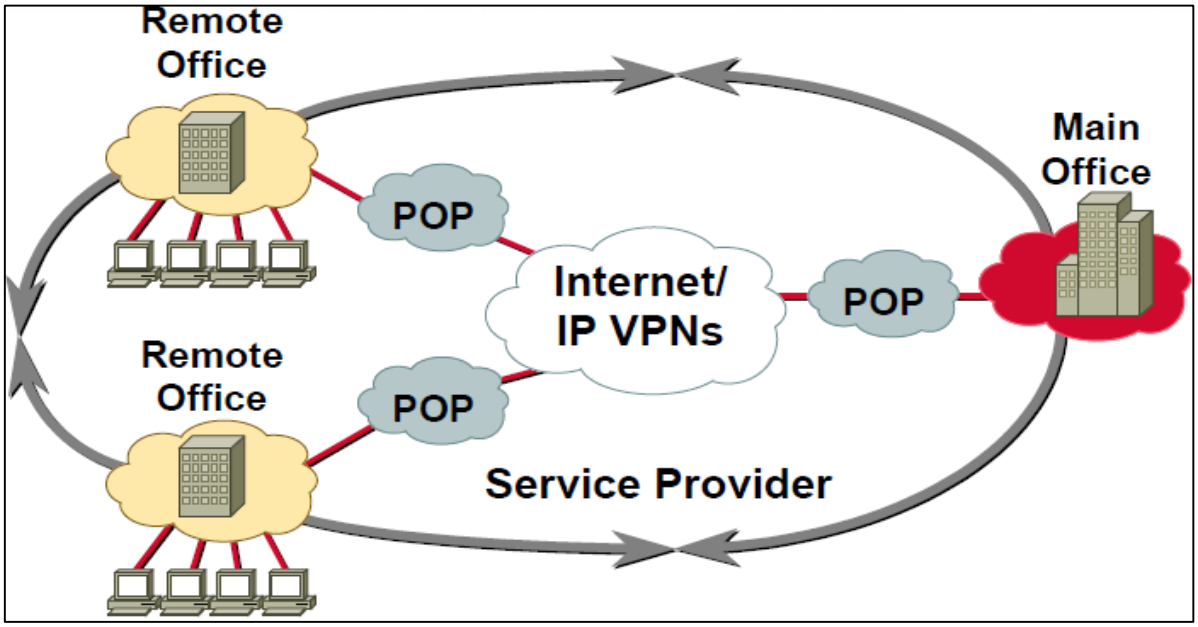

Figura 17. Esquema Intranet. Adaptado de “Introduction to VPNs” por Cisco Systems, 2017.

VPN de Acceso Remoto.

Muchas empresas han reemplazado con esta tecnología VPN su infraestructura "dial-up", donde el cliente utilizaba un modem para llamar a través de la Red Telefónica Conmutada a un nodo del Proveedor de Servicios de Internet y este con un servidor PPP establecía un enlace módem-a-módem, que permite entonces que se enrute a Internet. Esta implementación se trata de comunicaciones donde los usuarios se conectan con la empresa desde sitios remotos (oficinas comerciales, casas, hoteles, etc.) utilizando Internet como medio de acceso. “Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa”. (Pinto de Olivera, 2014).

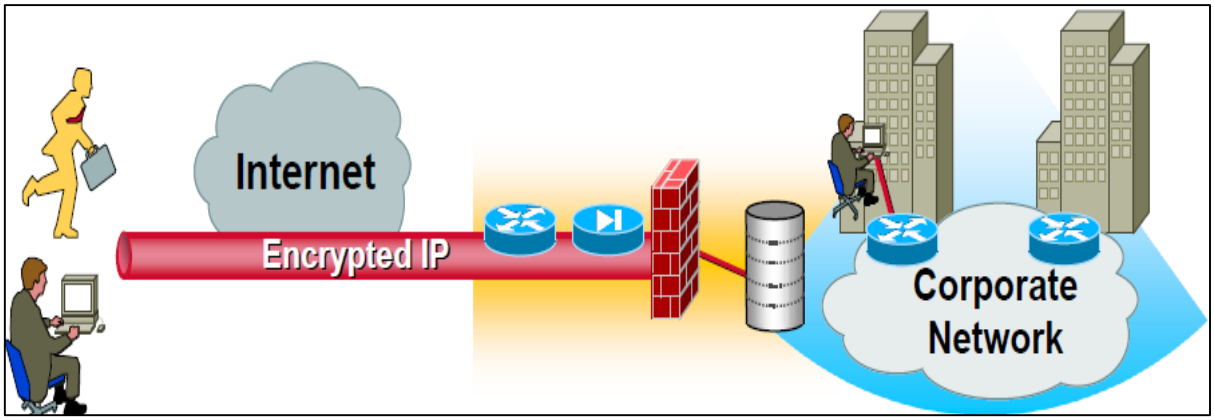

Figura 18. Esquema Remote Access. Adaptado de “Introduction to VPNs” por Cisco Systems, 2017.

VPN Sitio-a-Sitio

Este esquema se utiliza para conectar oficinas remotas con la sede central de organización. El equipo central vpn, que posee un vínculo a Internet permanente, acepta las conexiones vía Internet provenientes de los sitios y establece el "túnel" vpn. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. “Esto permite eliminar los costosos vínculos punto a punto tradicional, sobre todo en las comunicaciones internacionales”. (Pinto de Olivera, 2014).

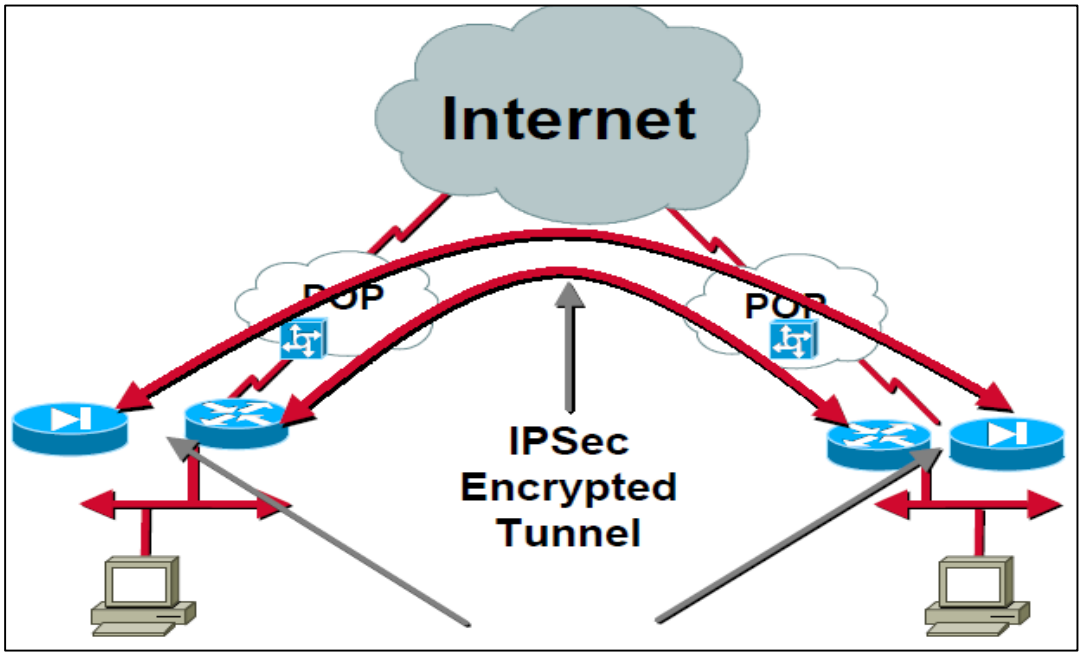

Figura 19. Esquema Site-to-Site. Adaptado de “Introduction to VPNs” por Cisco Systems, 2017.

Protocolos de Tunneling VPNs.

Point-to-Point Tunneling Protocol (PPTP):

Fue desarrollado por ingenieros de Ascend Communications, U.S. Robotics, 3Com Corporation, Microsoft, y ECI Telematics para proveer entre usuarios de acceso remoto y servidores de red una red privada virtual. PPTP fue diseñado para permitir a los usuarios conectarse a un servidor RAS desde cualquier punto en Internet para tener la misma autenticación, encriptación y los mismos accesos de LAN como si discaran directamente al servidor.

Internet Protocol Security (IPsec):

IPSec trata de remediar algunas falencias de IP, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme.

IPSec provee confidencialidad, integridad, autenticidad y protección a repeticiones mediante dos protocolos, que son Authentication Protocol (AH) y Encapsulated Security Payload (ESP).

Layer-2 Tunneling Protocol (L2TP):

facilita el encapsulamiento de paquetes PPP a través de una red de manera tal que sea lo más transparente posible a los usuarios de ambos extremos del túnel y para las aplicaciones que éstos corran. L2TP utiliza dos tipos de mensajes: de control y de datos. Los mensajes de control son usados para el establecimiento, el mantenimiento y el borrado de los túneles y las llamadas. Utilizan un canal de control confiable dentro de L2TP para garantizar el envío. Los mensajes de datos encapsulan los marcos PPP y son enviados a través del túnel.

2.2.3. Metodologías:

PPDIOO (Preparar, Planificar, Diseñar, Implementar, Operar, Optimizar)

El enfoque principal de esta metodología es definir las actividades mínimas requeridas, por tecnología y complejidad de red, que permitan asesorar de la mejor forma posible a nuestros clientes, instalando y operando exitosamente las tecnologías Cisco.

Así mismo logramos optimizar el desempeño a través del ciclo de vida de su red.

- ✓ Es secuencial, por que separa las etapas.
- ✓ Es iterativa, porque se alimenta continuamente.

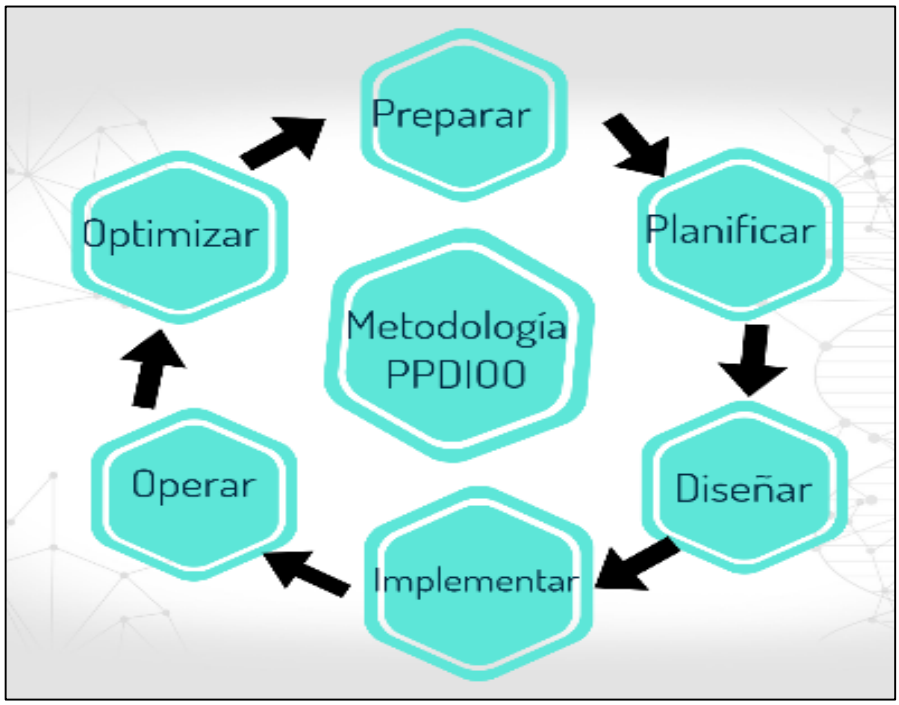

Figura 20. Metodología PPDIOO. Adaptado de "Metodología Cisco Systems" por Cisco Systems, 2017.

Fases de la Metodología:

1) Fase de Preparación:

En la fase de preparación, una empresa determina un caso de negocio y justificación financiera para apoyar la adopción de nuevas tecnologías. Al anticipar cuidadosamente las necesidades futuras y desarrollar tanto una estrategia de tecnología y arquitectura de alto nivel para satisfacer las necesidades de un negocio está en mejores condiciones de contener los costos durante el despliegue y las operaciones.

"En esta fase se anticipa la visión general, los requisitos y las tecnologías necesarias para construir y mantener una ventaja competitiva". (Arteaga y Huamán, 2014, p.20).

2) Fase de Planeación:

Una implementación satisfactoria de la tecnología depende de una evaluación precisa de la de una empresa de la red actual, la seguridad del estado, y la disposición general para apoyar la solución propuesta. En esta fase de plan, una empresa determina si se cuenta con recursos suficientes para gestionar un proyecto de implementación de la tecnología para su finalización. Para evaluar y mejorar la seguridad de la red, la empresa pone a prueba su red de la vulnerabilidad

a los intrusos y redes externas. “Entonces, la empresa desarrolla un plan de proyecto detallado para identificar recursos, las dificultades potenciales, las responsabilidades individuales y las tareas críticas necesarias para entregar el proyecto final a tiempo y dentro del presupuesto”. (Arteaga y Huamán, 2014, p.25).

3) Fase de Diseño:

El diseño de la red es desarrollado basado y alineado a los objetivos del negocio, requisitos técnicos de la red pueden mejorar el rendimiento y soporte de alta disponibilidad, fiabilidad, seguridad y estabilidad, todo es obtenido desde las fases anteriores, esta fase incluye diagramas de red física y lógica complementada con la lista de equipos. El plan del proyecto es actualizado con información más granular para la implementación. “Después de esta fase aprobada empieza la implementación. La fase de diseño también puede orientar y acelerar la implementación con éxito con un plan para montar, configurar, probar y validad las operaciones de red”. (Arteaga y Huamán, 2014, p.20).

4) Fase de Implementación:

En la fase implementación una empresa trabaja para integrar los dispositivos y las nuevas capacidades de acuerdo con el diseño, sin comprometer la disponibilidad o rendimiento de la red.

Después de identificar y resolver problemas potenciales, la empresa intenta acelerar retorno de la inversión con una migración eficiente y exitosa implementación, incluyendo la instalación, configuración, integración, prueba y puesta en marcha todos los sistemas. “Después de validar el funcionamiento en red, una organización o empresa puede comenzar a ampliar y mejorar las habilidades del personal de TI para aumentar aún más la productividad y reducir el tiempo de inactividad del sistema”. (Arteaga y Huamán, 2014, p.15).

5) Fase de Operación:

En la fase de operación, una empresa proactiva vigila los signos vitales y de salud de la red para mejorar la calidad del servicio, reducir las interrupciones, y mantener una alta disponibilidad, fiabilidad y seguridad. Al proporcionar un marco eficiente y herramientas operativas para responder a los problemas, una empresa puede evitar el costoso tiempo de inactividad y pérdida de beneficios. Operaciones de Expertos también permiten a una organización para dar cabida a las actualizaciones, movimientos, adiciones y cambios, y la reducción efectiva de costos de operación. En esta fase incluye la administración y monitoreo de los componentes de la red,

mantenimiento de ruteo, administración de actualizaciones, Esta fase es la prueba final del diseño. (Arteaga y Huamán, 2014).

6) Fase de Optimización:

En la fase optimización, una empresa está continuamente buscando maneras de lograr la excelencia operativa a través de un mejor desempeño, servicios ampliados y reevaluaciones periódicas del valor de la red. Es una administración pro-activa, identificando y resolviendo cuestiones antes que afecten a la red. Esta fase puede crear una modificación al diseño y demasiados problemas aparecen, para mejorar cuestiones de desempeño o resolver cuestiones de aplicaciones. (Arteaga y Huamán, 2014, p.25).

INEI (Instituto Nacional de Estadística e Informática)

Para llevar adelante los Proyectos, el INEI ha adoptado un marco Metodológico único, esto nos permitirá el desarrollo del Diseño de una Red Informática. El Marco Metodológico para un Proyecto constará de cuatro etapas siendo estas las siguientes:

Etapas:

- ✓ Organización.
- ✓ Análisis.
- ✓ Desarrollo.
- ✓ Implementación.

Etapas de la Metodología:

1) Etapa de Organización:

La Etapa de Organización es la primera Etapa del Marco Metodológico, en ésta se llevará adelante las siguientes actividades:

Modelamiento del Requerimiento:

Se sugiere la creación de una RED LAN.

Redes de área Local (LAN): El término LAN (Local Área Network) alude a una red, a veces llamada subred instalada en una misma sala, oficina o edificio. Los nodos o puntos finales de una LAN se conectan a una topología de red compartida utilizando un protocolo determinado. Con la autorización adecuada, se puede acceder a los dispositivos de la LAN, esto es, estaciones de trabajo, impresoras,

etc. desde cualquier otro dispositivo de la misma. Las aplicaciones software desarrolladas para las LAN (mensajería electrónica, procesamiento de texto, hojas electrónicas, etc.) también permiten ser compartidas por los usuarios.

Redes de área Ancha (WAN): Una red de área ancha o WAN (Wide Área Network) es una colección de LAN interconectadas. Las WAN pueden extenderse a ciudades, estados, países o continentes. Las redes que comprenden una WAN utilizan enrutadores (routers) para dirigir sus paquetes al destino apropiado. Los enrutadores son dispositivos hardware que enlazan diferentes redes para proporcionar el camino más eficiente para la transmisión de datos. Estos enrutadores están conectados por líneas de datos de alta velocidad, generalmente, líneas telefónicas de larga distancia, de manera que los datos se envían junto a las transmisiones telefónicas regulares.

Se propone las Redes LAN/WAN ya que para la LAN abarca un Radio local y se sugiere la WAN ya las sucursales de las otras ciudades.

2) Etapa de Análisis:

En esta etapa se analizará los recursos de la red y su estructura; Descripción de las estrategias para la integrar todas las áreas a la red. También se debe considerar la topología que se empleará.

Criterio de selección:

- ✓ Son más seguras, pero más costosa área.
- ✓ Cada computadora estará conectada a un Switch ubicada centralmente.
- ✓ Recomendable cuando se tiene más de 5 estaciones de trabajo.
- ✓ Debido a la fundamental del nodo central es importante que se encuentre duplicado, en caso de fallas. Pero cuando falla el nodo central, falla toda la red.
- ✓ Sencillas de instalar.
- ✓ Permite incrementar o disminuir estaciones con sencillez y que las modificaciones son sencillez.
- ✓ Protección contra roturas de cables. Si se corta un cable para una estaciona de trabajo solo cae el segmento mas no la red entera.
- ✓ Nos permite cursar grandes flujos de tráfico por congestionarse el nodo central.

3) Etapa de Desarrollo:

En esta etapa se tiene en cuenta los siguientes pasos.

- ✓ Diseño
- ✓ Diseño lógico

4) Etapa de Implementación:

Comprende toda la instalación en la empresa.

- ✓ Cableado

Conclusiones:

La implementación del rediseño de red planteado, permitirá estar a la vanguardia tecnológica, optimizando recursos y costos. Vendría a solucionar, en gran medida, muchos de los problemas de las empresas en la actualidad presenta en lo que al manejo de la información respecta, permitiéndole a quienes allí laboran poder acceder a ésta de manera más rápida, eficiente y confiable. La implementación de una red LAN con categoría 6, permitirá estar a la vanguardia tecnológica, optimizando recursos y costos. Elegimos esta marca porque tiene una muy buena integración con todos los sistemas de instalación. Además, nos brinda mejor soporte. La solución de cableado estructurado es capaz de soportar tanto la red de datos, como los servicios de telefonía IP, al igual que cámaras de vigilancia presentes en el edificio y los servicios de videoconferencia, y asegura disponibilidad, escalabilidad y seguridad para la red". Una red inalámbrica permitirá reducir tiempo y problemas en la correcta actualización de la información y el cambio automático de uno a otro, para que sea más fácil el acceso inalámbrico al desplazarse entre distintos puntos de acceso.
Se realizó la factibilidad económica: costo de materiales, costo de accesorios, costo de herramientas, costo de implantación, costo de mantenimiento y Costo de Hardware

Recomendaciones:

Verificar la calidad de los materiales empleados para la instalación de la red.
Optar por una marca de equipos y medios de transmisión reconocida a escala mundial que aseguren el éxito del diseño. Una vez implementada la interconexión, realizar el mantenimiento preventivo una vez al año para que la antena esté alineada correctamente y no cause problemas en la transmisión. No exceder la distancia de los cables recomendada por el fabricante. Para el manejo de los distintos equipos de comunicación es necesario la capacitación y adiestramiento al personal que va a estar a cargo de estos. Sustituir las máquinas obsoletas que se

encuentran en el edificio por otras que se adapten a los requerimientos propios de la red propuesta.

La capacitación al personal debe realizarse en forma constante para que el manejo de la red sea de forma eficiente. Tenerse informado acerca de los avances de la tecnología en lo que respecta a componentes de red, puesto que sería novedoso estar a la vanguardia, y optar por tener un mayor prestigio. Tener un software de monitoreo de red, para ubicar posibles fallas en los determinados host, o puntos. Dar mantenimiento a la Red cada cierto tiempo.

Evaluación comparativa entre las Metodologías

Tabla 11

Cuadro de valores para los indicadores.

INDICADOR	VALOR	DESCRIPCIÓN	PESO
Orientado a las necesidades de la Organización	Sí	La entrega de un producto en base a los alcances y planificación.	1
	No	No posee.	0
Iteratividad	Sí	Repite el proceso con la intención de mejorar y alcanzar una meta deseada, objetivo o resultado.	1
	No	No repite los procesos, deja seguir el flujo.	0
Optimización de recursos	Sí	Es una administración pro-activa, identificando y resolviendo cuestiones antes que afecten a la operatividad.	1
	No	No posee.	0
Posibilidad de éxito	Sí	Indica el éxito que ha tenido la Metodología en otros proyectos.	1
	No	No indica.	0
Prueba	Alto	Se evalúa el rendimiento del prototipo construido, identificando errores, no se generó errores al utilizar la metodología con respecto al caso.	1
	Bajo	Se evalúa el rendimiento del prototipo construido, identificando errores se generó errores al utilizar la metodología con respecto al caso.	0

Nota: Cada indicador según su composición tendrá un peso la cual se irá sumará al final para elegir la metodología idónea en el desarrollo de la investigación.

En esta investigación compararemos las metodologías PPDIOO y del INEI, debido a sus beneficios e indicadores:

Tabla 12

Cuadro comparativo entre Metodologías.

INDICADOR	PPDIOO	INEI
Orientado a las necesidades de la Organización	Sí	Sí
Iteratividad	Sí	No
Optimización de recursos	Sí	No
Posibilidad de éxito	Sí	Sí
Prueba	Alto	Alto
Resultados	5	3

Nota: Resultados obtenidos en base a los indicadores se denota que la metodología PPDIOO de Cisco es más completa en todos los aspectos.

Según los criterios en la Tabla 11 se denota en la Tabla 12 que ambas son metodologías orientadas a la entrega de un producto final, basándose en la planificación y diseño, pero la Metodología PPDIOO de Cisco Systems posee Iteratividad en sus Fases esto le da un valor agregado al proyecto como tal, ya que va orientado a donde queremos llegar, mejorar el Servicio de Comunicación en las Tiendas Mass.

El INEI en cambio propone seguir con las fases del proyecto hasta su finalización, sin revisión de algún percance en sus fases.

También en cuanto a optimización de recursos el PPDIOO de Cisco Systems propone una mejora continua y pro-activa identificando las amenazas para mitigarlas en el acto. El INEI no posee ello, esto podría causar problemas después de la implementación.

CAPÍTULO III

DESARROLLO DE LA PROPUESTA DE UNA RED PRIVADA VIRTUAL

3.1. ESTUDIO DE FACTIBILIDAD

3.1.1. Factibilidad Técnica

Esta propuesta de una Red Privada Virtual es factible técnicamente, ya que tiene la disponibilidad y accesibilidad a la información para el desarrollo y la implementación. Cabe resaltar que el Servicio de Comunicación en las tiendas Mass que se desea mejorar cuenta con el respaldo de la tecnología necesaria para brindar dicha solución, la inversión de los gastos será auspiciada por la empresa Supermercados Peruanos S.A.

En el sentido de tecnología de Hardware que se utilizó:

- ✓ FortiGate 30 E.
- ✓ Switch Cisco SG 200-08P.
- ✓ Enlace de Internet de 2 Mbps.
- ✓ Gabinete de Pared de 6RUs.
- ✓ Patch-cords Cat6 – Panduit.
- ✓ Bandeja de 1RU.
- ✓ Laptop HP I3.

En el sentido de tecnología de Software que se utilizó:

- ✓ FortiClient 5.6 for Windows.
- ✓ Software de conexión Remota Putty.
- ✓ Office 2013.

Costos:

El costo será asumido por la empresa Supermercados Peruanos S.A.

Escalabilidad

Se espera que la solución de una Red Privada Virtual en las tiendas Mass sea una solución soportada para más de 100 Servicios de Comunicación.

3.1.2. Facilidad de Uso

Al poseer un correcto diseño de la solución de Red, se podrá realizar la gestión de estos equipos, minimizando así las incidencias que estas puedan presentar, optimizando los tiempos de carga y transacciones en los Sistemas Informáticos, generando mayores ingresos de utilidades a la Tienda. Con el valor agregado de la seguridad e integridad de la información, proporcionando calidad al Servicio.

3.1.3. Factibilidad Operativa

Se cuenta con la disponibilidad y compromiso de la organización implementar la mejora del Servicio de Comunicación en la tienda Mass, para ello se posee un

personal capacitado y con conocimientos sólidos en Redes Privadas y enlaces de datos IP.

3.1.4. Factibilidad Económica

La propuesta de una Red Privada Virtual es viable económicamente, ya que la empresa cuenta con los recursos económicos necesarios para la implementación.

Tabla 13

Presupuesto del Proyecto.

RESERVA DE CONTIGENCIA		20%
PRESUPUESTO	**RESERVA**	**TOTAL**
S/. 7.860,00	S/.1.572,00	S/. 9.432,00

CATEGORÍA	RECURSO	TIPO DE UNIDADES	PRESUPUESTO
Personal	Renato Espinoza Chipane	Horas/mensual	S/. 3.500,00
Hardware	Laptop HP ProBook 4440s I3.	1 Und.	S/. 2.500,00
	FortiGate 30 E-Soporte 1 año.	1 Und.	S/. 400,00
	Switch SG-200-08-Soporte 1 año.	1 Und.	S/. 200,00
	Servicio de Internet 2Mbps.	1 Und.	S/. 150,00
	Gabinete de Pared 6RUs.	1 Und.	S/. 120,00
	Bandeja 1RU.	1 Und.	S/. 10,00
	Patch-cord Cat6 Panduit.	2 Und.	S/. 30,00
Software	FortiClient 5.6 for Windows.	----------	S/. 00,00
	Office 2013.	----------	S/. 00,00
	Putty.	----------	S/. 00,00
Movilización	Viajes en taxis.	Ruta/ Semanal	S/. 00,00 S/. 500,00
Materiales	Impresiones	Und.	S/. 400,00
	Útiles de Oficina	Und.	S/. 50,00

3.2. MODELAMIENTO DEL NEGOCIO

Desde el 2006, Supermercados Peruanos está teniendo un crecimiento constante, resultado de su plan de expansión, a través de la construcción de nuevas tiendas tanto en Lima como en Provincias se busca atender nuevos segmentos y en

algunos casos remodelando tiendas ya existentes a fin de satisfacer mejor las necesidades de sus clientes.

El formato de “Tiendas de Descuento” comenzó en abril del año 2001 con el local de Chosica, para luego expandirse a los distritos de San Juan de Miraflores (Mass Varga Machuca) y Chorrillos (Mass Guardia Civil).

En la actualidad este formato se caracteriza por estar enfocado hacia compras puntuales, de bajo precio y rápidas de un número reducido de ítems, que compiten con bodegas y mercados de barrio a nivel Lima Metropolitana. Se tiene un estimado de 140 tiendas en producción desde el año 2015, y seguirá su proceso de expansión en los siguientes años, consolidando un mínimo de 500 tiendas Mass.

Razón Social	:	Supermercados Peruanos S.A.
Gerente General	:	Juan Carlos Vallejo.
Estado	:	Activo.
Actividad	:	Vta. Min. En Almacenes No Especializada.
Fecha de Inscripción	:	01 de julio de 1979.
Tipo de Organización	:	Privada.
Ubicación	:	Lima – San Borja.
Dirección	:	Calle Morelli #181 – San Borja.
Teléfono	:	618-8000

Se resalta también que Supermercados Peruanos cuenta con otras marcas reconocidas en Mercado Retail tales como Plaza vea y Vivanda.

Organización Interna

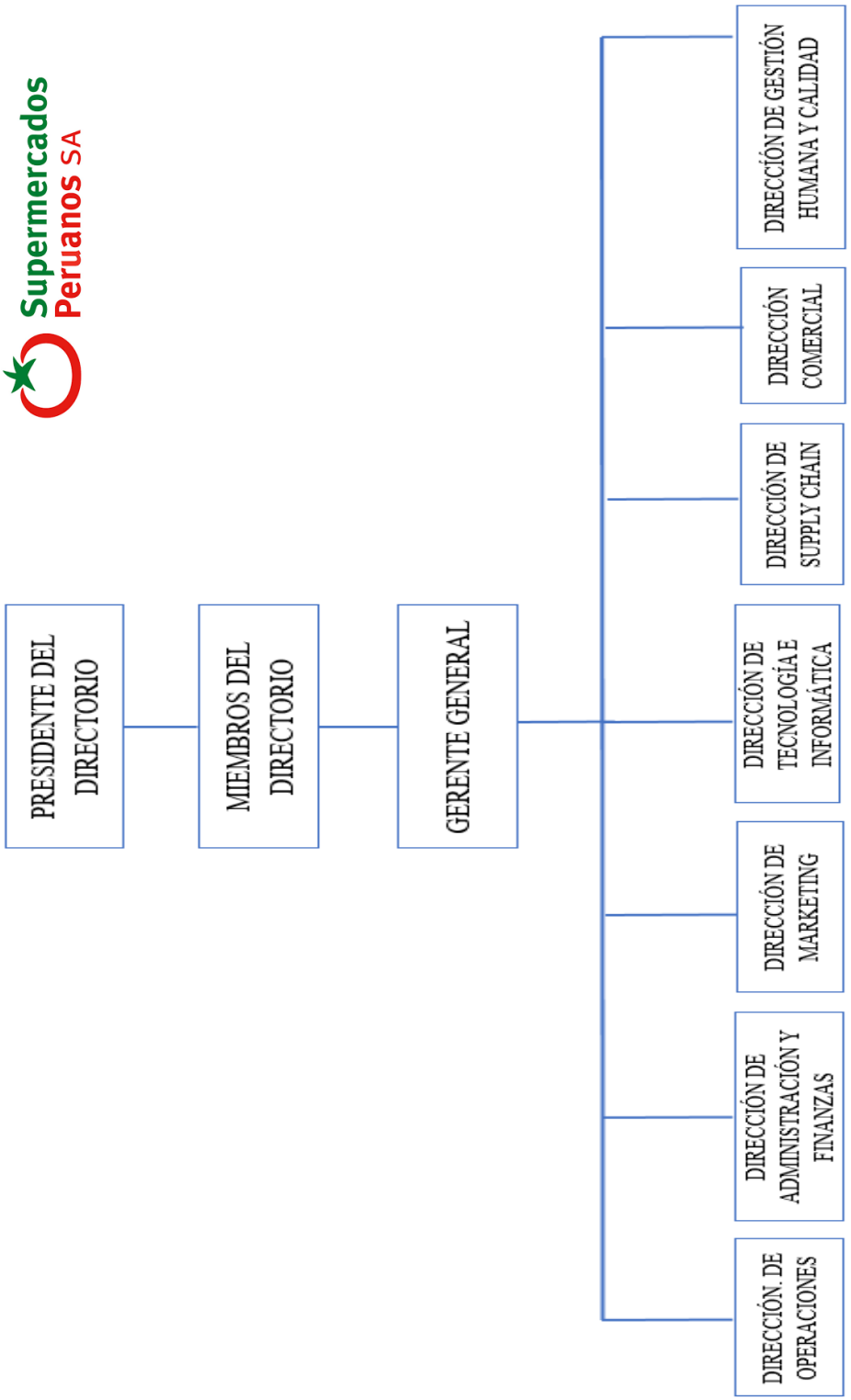

Figura 21. Organigrama de Supermercados Peruanos S.A.

3.3. METODOLOGÍA PPDIOO

3.3.1 Fase de Preparación

3.3.1.1. Direccionamiento IP

La cantidad de Dispositivos conectados en Tienda son de 5 Host:

- ✓ Desktop.
- ✓ Módulo de Caja 1.
- ✓ Módulo de Caja 2.
- ✓ Impresora.
- ✓ Print Server.

El esquema del direccionamiento IP se basa en tomar una Red Privada (Clase A, B, C) para realizar el VLSM (variable length subnet mask) en pequeñas porciones de Red

Tabla 14

Sub-Red y Máscara de red Privada de Clase A.

CLASE A	CLASE C
10.33.X.X	255.255.255.240

Nota: Se toma como referencia la gran Red de Clase A = 10.x.x.x 255.x.x.x para luego realizar el proceso de subneteo y dividirlas en 16 Host por Sub-red obteniendo 4096 Sub-redes equivalentes a 4096 tiendas Mass, ello por la escalabilidad que se tendrá en el crecimiento de las tiendas Mass en los próximos años.

Para mantener un estándar a nivel de gestión y servicio de las comunicaciones se realizó el proceso de Subneting a una máscara de Red clase C, obteniendo 4096 Subredes de la Red principal. Algunas Sub-Redes se encuentran ya en uso por la demanda de Tiendas.

Tabla 15

Sub-Red y Máscara de red que se encuentran en uso.

CLASE A	CLASE C	ESTADO
10.33.1.x	255.255.255.240	USADO
10.33.2.x	255.255.255.240	USADO
10.33.3.x	255.255.255.240	USADO
10.33.5.x	255.255.255.240	USADO
10.33.6.x	255.255.255.240	USADO
10.33.7.x	255.255.255.240	USADO

Nota: Actualmente se tienen ya utilizadas las Sub-redes en la gran Red MPLS de Supermercados Peruanos.

Se trabajará con el segmento de la Sub-Red 10.33.4.X esto implica que por cada segmento incluye 16 direcciones IPs (solo 14 Utilizables), el despliegue será el siguiente:

Tabla 16

Planificación por Segmento de Sub-Red para las Tiendas.

RED	GATEWAY	IPS UTILIZABLES	MÁSCARA
10.33.4.0	10.33.4.2	10.33.4.5 -10.33.4.14	255.255.255.240
10.33.4.16	10.33.4.18	10.33.4.19 -10.33.4.30	255.255.255.240
10.33.4.32	10.33.4.34	10.33.4.37 -10.33.4.46	255.255.255.240
10.33.4.48	10.33.4.50	10.33.4.53 - 10.33.4.64	255.255.255.240
10.33.4.64	10.33.4.66	10.33.4.69 - 10.33.4.70	255.255.255.240
10.33.4.80	10.33.4.82	10.33.4.85 - 10.33.4.94	255.255.255.240
10.33.4.96	10.33.4.98	10.33.4.101 - 10.33.4.110	255.255.255.240
10.33.4.112	10.33.4.114	10.33.4.117 - 10.33.4.126	255.255.255.240
10.33.4.128	10.33.4.130	10.33.4.133 - 10.33.4.142	255.255.255.240
10.33.4.144	10.33.4.146	10.33.4.149 - 10.33.4.158	255.255.255.240
10.33.4.160	10.33.4.162	10.33.4.165 - 10.33.4.174	255.255.255.240
10.33.4.176	10.33.4.178	10.33.4.181 - 10.33.4.190	255.255.255.240
10.33.4.192	**10.33.4.194**	**10.33.4.197 - 10.33.4.206**	**255.255.255.240**
10.33.4.208	10.33.4.210	10.33.4.213 - 10.33.4.222	255.255.255.240
10.33.4.224	10.33.4.226	10.33.4.229 - 10.33.4.238	255.255.255.240
10.33.4.240	10.33.4.242	10.33.4.245 - 10.33.4.254	255.255.255.240

Nota: Del rango del segmento 10.33.4.x 255.255.255.240 se obtienen 16 Sub-redes con 16 host por cada una, se toma la Sub-red 10.33.4.192 por encontrase libre y sin uso.

3.3.1.2. Topología Lógica

La topología de Red LAN que posee es en Estrella, ya que los dispositivos están conectadas directamente a un punto central, en este caso vendría hacer el Módem Router 3G de la marca TELDAT, todas las comunicaciones se hacen necesariamente a través de él. Los dispositivos no están directamente conectados entre sí.

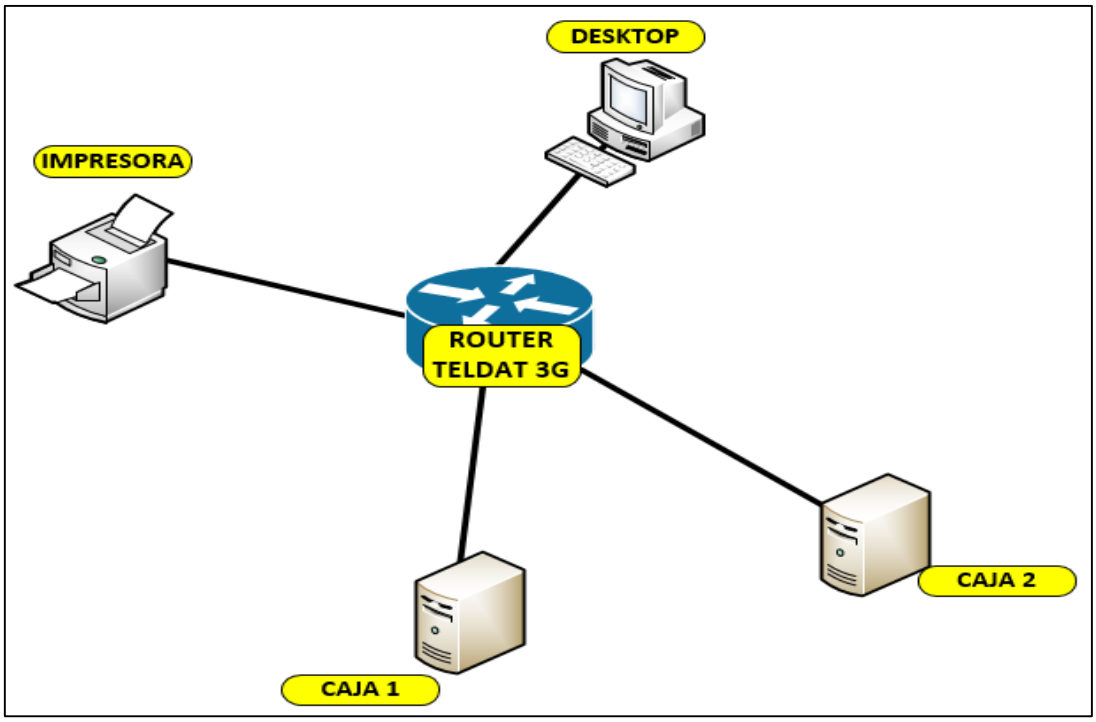

Figura 22. Topología de Red en Estrella en relación a la manera que se encuentran conectadas las terminales.

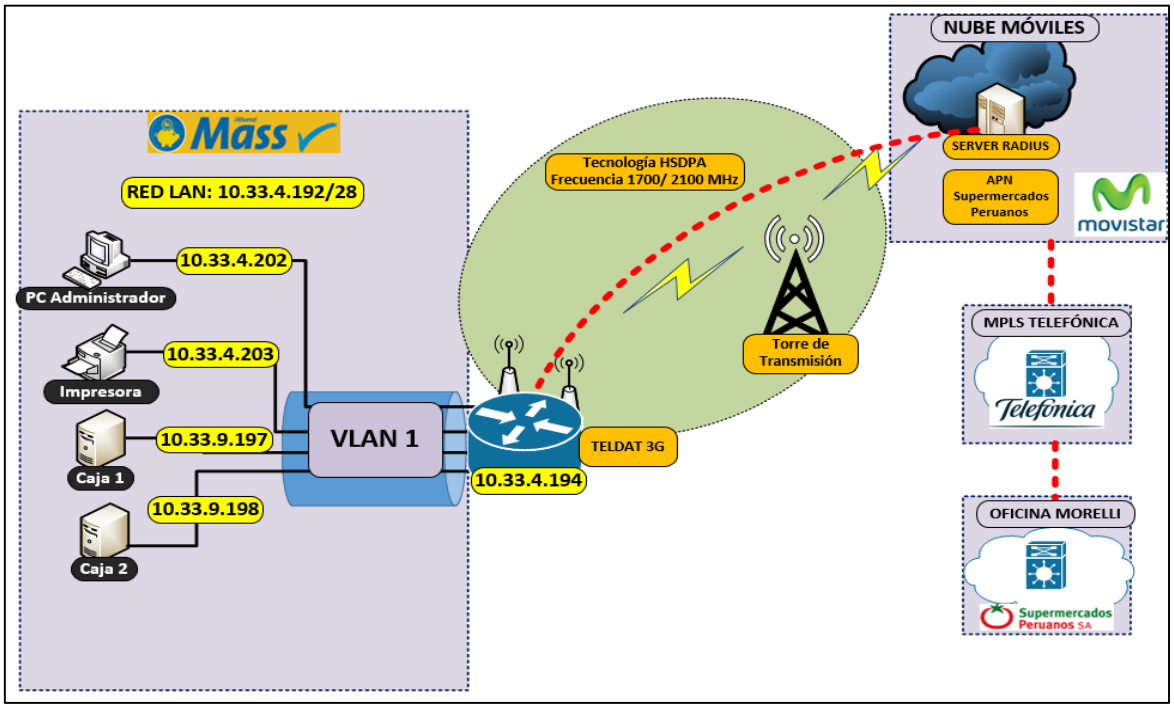

Figura 23. Topología Lógica del Servicio de Comunicación 3G para la comunicación con la central y demás sedes de Supermercados Peruanos.

3.3.1.3. Topología Física

Equipos Intermediarios

Módem Router Teldar 3G: Ofrece conectividad 3G/4G. Este equipo lleva embebido 4 puertos LAN Giga-Ethernet es a donde los dispositivos se conectan para la transmisión y recepción de Datos.

Figura 24. Módem Router. Recuperado de “Teldat-V” por teldat.com, 2017.

Cableado Estructurado:

Es un cable estándar para Gigabit-Ethernet y otros protocolos de red que es compatible con la Cat.5/5e y Cat.3. La Categoría 6 cuenta con especificaciones más estrictas para crosstalk y ruido del sistema. El estándar de cable proporciona un rendimiento de hasta 250 MHz y es adecuado para 10BASE -T / 100BASE -TX y 1000BASE -T / 1000BASE -TX (Gigabit Ethernet).

Tabla 17

Clasificación del Cableado estructurado en las Tiendas Mass.

ITEM	DESCRIPCIÓN
Estándar utilizado	100Base-Tx
Tipo de Cableado	Norma TIA/EIA 568-B
Marca y Categoría del Cableado	Panduit - Cat.6A.
Tecnología del Cableado	Cobre- UTP - 0 halógeno

Nota: Se mantiene el estándar de cableado estructurado según norma de la TIA/EIA en Cat6A para la comunicación a 100Mbps por puerto de Red según lo requiera.

Conexión Física de los dispositivos:

En la Figura 25 se observa la conectorización de los puntos de datos al equipo Módem Router Teldat y en la Tabla 18 se detalla la ubicación, estado y etiquetado de los puntos de Red.

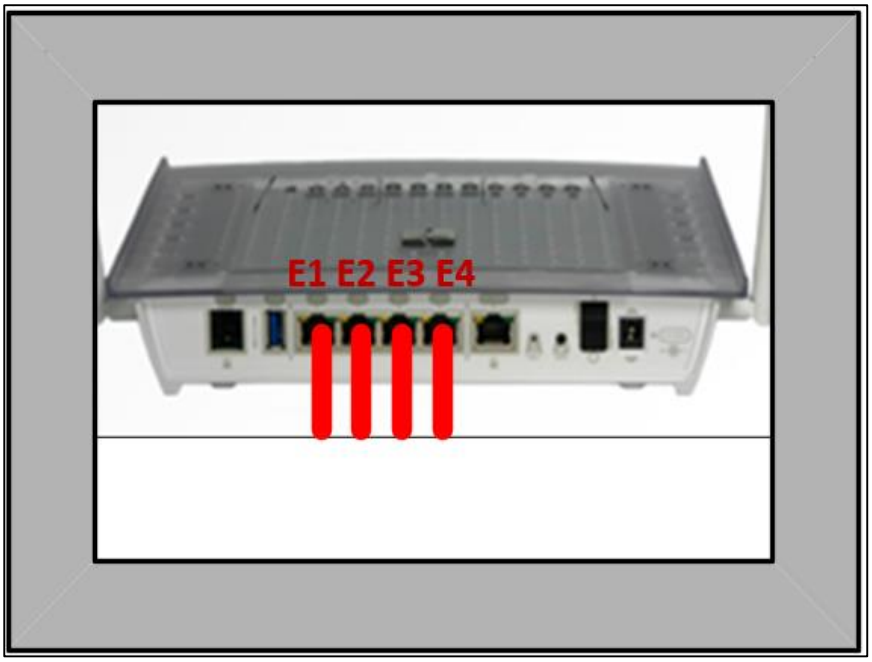

Figura 25. Conexión Física de los puntos de Red al Módem actualmente.

Tabla 18

Descripción de puntos de Red conectados al Módem Router Teldat 3G.

ETIQUETA LADO USUARIO	CONECTADO A:	ESTADO	VLAN	PUERTO	DESCRIPCIÓN
D-1	Router Teldat 3G	Activo	1	E-1	Caja 2
D-2	Router Teldat 3G	Activo	1	E-2	Caja 1
D-3	Router Teldat 3G	Activo	1	E-3	Pc Admin.
D-4	Router Teldat 3G	Activo	1	E-4	Impresora
-	-	-	-	DSL	-
-	-	-	-	E-WAN	-

Nota: Layout de la distribución de puntos de Red en la Tienda Mass, es un estándar que cumple para todos los locales en Lima Metropolitana.

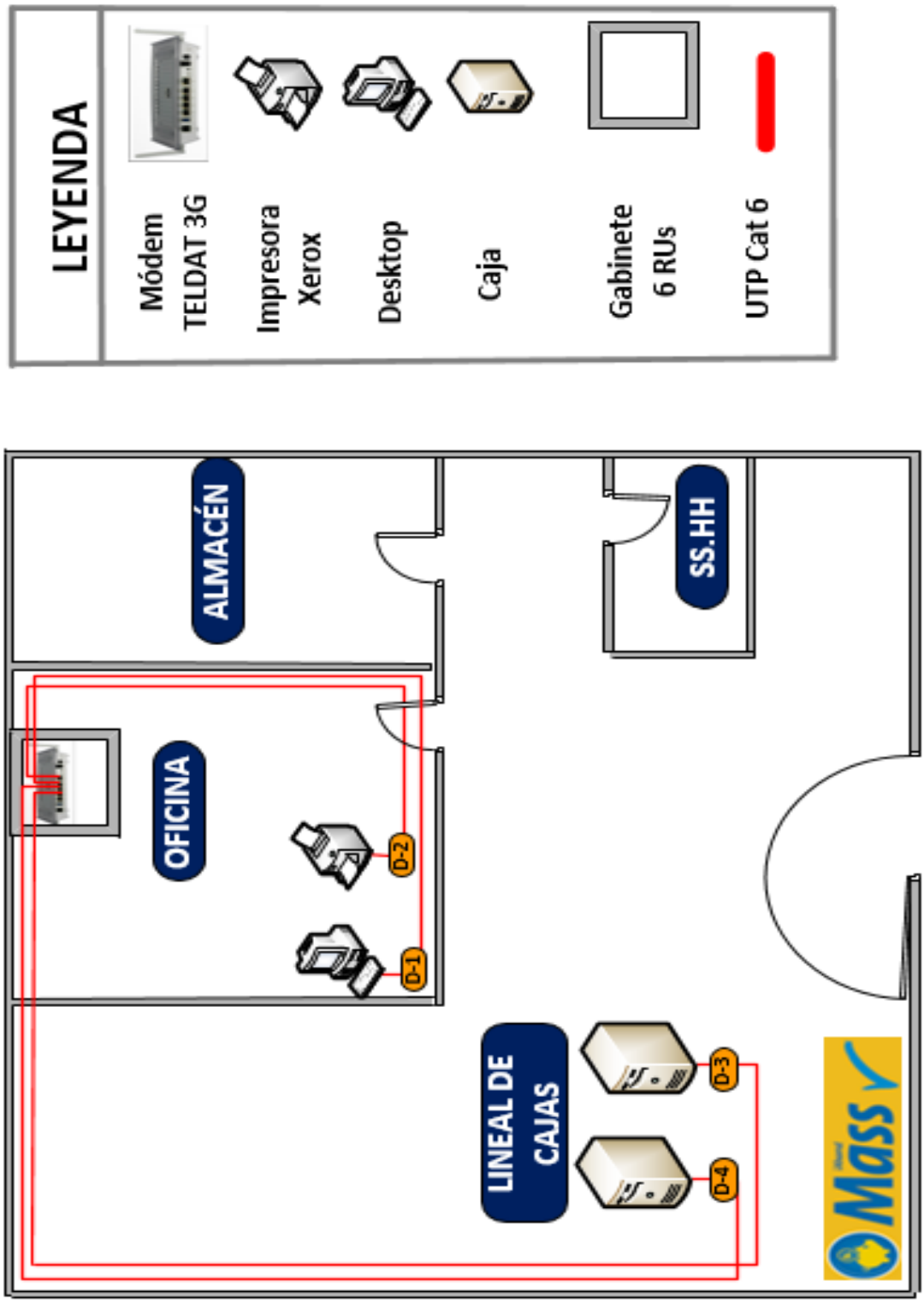

Figura 26. Ubicación Física de los Dispositivos intermediarios y finales actual.

3.3.2. Fase de Planificación

3.3.2.1. Análisis de Requerimientos del Servicio de Comunicación:

Después del levantamiento de Información que se realizó en la Fase de Preparación se requiere una serie de consideraciones para el rediseño a nivel de capa 2, 3 y 4 para responder a una serie de falencias y situaciones desfavorables que ocasionan deficiencias en el rendimiento del Servicio de Comunicación, ello involucra los siguientes requerimientos:

Requerimiento de Usuario final:

Haciendo mención a la Tabla 19, especifica los requerimientos a nivel de usuarios, ello se resume mediante el método menos formal de obtener información, entrevistas con los principales grupos de usuarios, y encuestas formales para obtener una lectura válida de la percepción de usuario con respecto a un nivel determinados servicios de red. En la misma los usuarios establecen disponibilidad, escalabilidad y estabilidad de tiempos de respuesta.

Tabla 19

Requerimientos de Usuario final.

REQUERIMIENTO	OBJETIVO
Conexiones permanentes.	Minimizar los errores sobre enlaces y nodos, optimizar el tiempo de recuperación para reducir al mínimo el tiempo de inactividad de los servicios de Comunicación.
Accesibilidad de usuarios.	Expandir la red para admitir a nuevos usuarios y aplicaciones sin afectar el rendimiento de los servicios a los usuarios.
Rapidez de acceso a los Sistemas informáticos	Mejorar los tiempos de respuesta al cargar los Sistemas Informáticos en Tienda.

Nota: Requerimientos sujetos al estudio de campo mediante los instrumentos de investigación antes descrito en el capítulo anterior.

Requerimientos de Aplicación:

En la Tabla 20, muestra los requerimientos a nivel de aplicaciones de rendimiento intensivo que generalmente implican las actividades de envío de emails, transferencia y acceso a los diferentes Sistemas Informáticos. La comunicación con estos servicios es vital porque existe replicación bidireccional de datos o acuses de recibo. Como resultado, pérdida de paquetes aceptables, priorización de tráfico, alta disponibilidad de la red junto con la seguridad, son los requisitos más importantes para estos servicios.

Tabla 20

Requerimientos de Aplicación

REQUERIMIENTO	OBJETIVO
Perdida de paquetes aceptables	Hacer fiable los datos de unidifusión IP que se generan y envían a los usuarios finales.
Priorización de tráfico.	Enfrentar los requerimientos de servicios sensibles a pérdidas, retrasos y variaciones de retraso permitiendo la preferencia de flujos de aplicación críticas en el ancho de banda disponible.
Seguridad.	Control de acceso a la red de datos, con la finalidad de proteger la información que es el recurso más valioso.

Nota: Requerimientos sujetos al estudio de campo mediante los instrumentos de investigación antes descrito en el capítulo anterior.

Requerimientos de Infraestructura:

Se requiere que el Servicio de Comunicación tenga una infraestructura escalable con tolerancia a soportar más de 10 dispositivos transmitiendo a la vez, para ello se requiere equipos aptos para dicha solución. Que sea manejable y a la vez redundante ante posibles fallas lógicas. En la Tabla 21 se detalla:

Tabla 21

Requerimientos de Infraestructura

REQUERIMIENTO	OBJETIVO
Manejable	Resumir un conjunto complejo de datos, protocolos, configuraciones y tecnologías en una estructura ordenada y comprensible.
Convergencia	Transportar datos y voz sobre un mismo medio, considerando escalas de tráfico, calidad de servicio y operación de estos servicios.
Redundancia	Garantizar el funcionando continuado de la red a través de hardware adicional y rutas alternativas.

Nota: Requerimientos sujetos al estudio de campo mediante los instrumentos de investigación antes descrito en el capítulo anterior.

Tabla 22

Lista de equipos y accesorios para la implementación.

N°	NOMBRE	DESCRIPCIÓN
1	Fortigate 30-E Fortinet	Velocidad de Transferencia LAN 10/100/1000 Mbps. 950 Mbps salida a través del Firewall. 75Mbps rendimiento VPN. 900.000 sesiones concurrentes. 15.000 nuevas sesiones/Segundos Corre en FortiOS 5.
2	Switch SG-200-08 Small Business	Velocidad de Transferencia LAN 10/100/1000 Mbps. Estándares IEEE 802.3, 802.1Q trunk, vlans. Capacidad de conmutación 13,66 Gbps. Capacidad de 8 puertos LAN GigaEthernet. Priorización de tráfico de VoIP.
4	Accesorios de Red	1 Gabinete de Pared 9RUs. Regleta Power (Embebido al Gabinete). 2 Patch-cord Cat.6. 1 Bandeja de 1RU.
5	Módem Router Empresarial	Accesos a la Red Pública Internet. Medio de acceso tecnología ADSL o Híbrido (Fibra Óptica/Coaxial). Ancho de Banda 2Mbps. Velocidad de transferencia mínima 1Mbps.

Nota: Los equipos y accesorios son resultado a un estudio especializado previo para la solución final.

3.3.2.2. Recurso Humano designado para la Implementación

Para el desarrollo de cada una de las fases de la Metodología será asignado el siguiente Especialista:

Tabla 23

Personal designado a la Implementación.

N°	NOMBRE	DESCRIPCIÓN
1	Renato Espinoza Chipane.	Especialista en Redes y Telecomunicaciones

Nota: Se nombra al especialista encargado del proyecto de la implementación para la solución.

3.3.2.3. Presupuesto del Proyecto

Tabla 24

Descripción del presupuesto detallado.

RESERVA DE CONTIGENCIA		20%
PRESUPUESTO	**RESERVA**	**TOTAL**
S/. 7.860,00	S/.1.572,00	S/. 9.432,00

CATEGORÍA	RECURSO	TIPO DE UNIDADES	PRESUPUESTO
Personal	Renato Espinoza Chipane	Horas/mensual	S/. 3.500,00
	Laptop HP ProBook 4440s I3.	1 Und.	S/. 2.500,00
	FortiGate 30 E-Soporte 1 año.	1 Und.	S/. 400,00
Hardware	Switch SG-200-08-Soporte 1 año.	1 Und.	S/. 200,00
	Servicio de Internet 2Mbps.	1 Und.	S/. 150,00
	Gabinete de Pared 6RUs.	1 Und.	S/. 120,00
	Bandeja 1RU.	1 Und.	S/. 10,00
	Patch-cord Cat6 Panduit.	2 Und.	S/. 30,00
	FortiClient 5.6 for Windows.	----------	S/. 00,00
Software	Office 2013.	----------	S/. 00,00
	Putty.	----------	S/. 00,00
Movilización	Viajes en taxis.	Ruta/ Semanal	S/. 00,00 S/. 500,00
Materiales	Impresiones	Und.	S/. 400,00
	Útiles de Oficina	Und.	S/. 50,00

3.3.2.4. Cronograma de Actividades

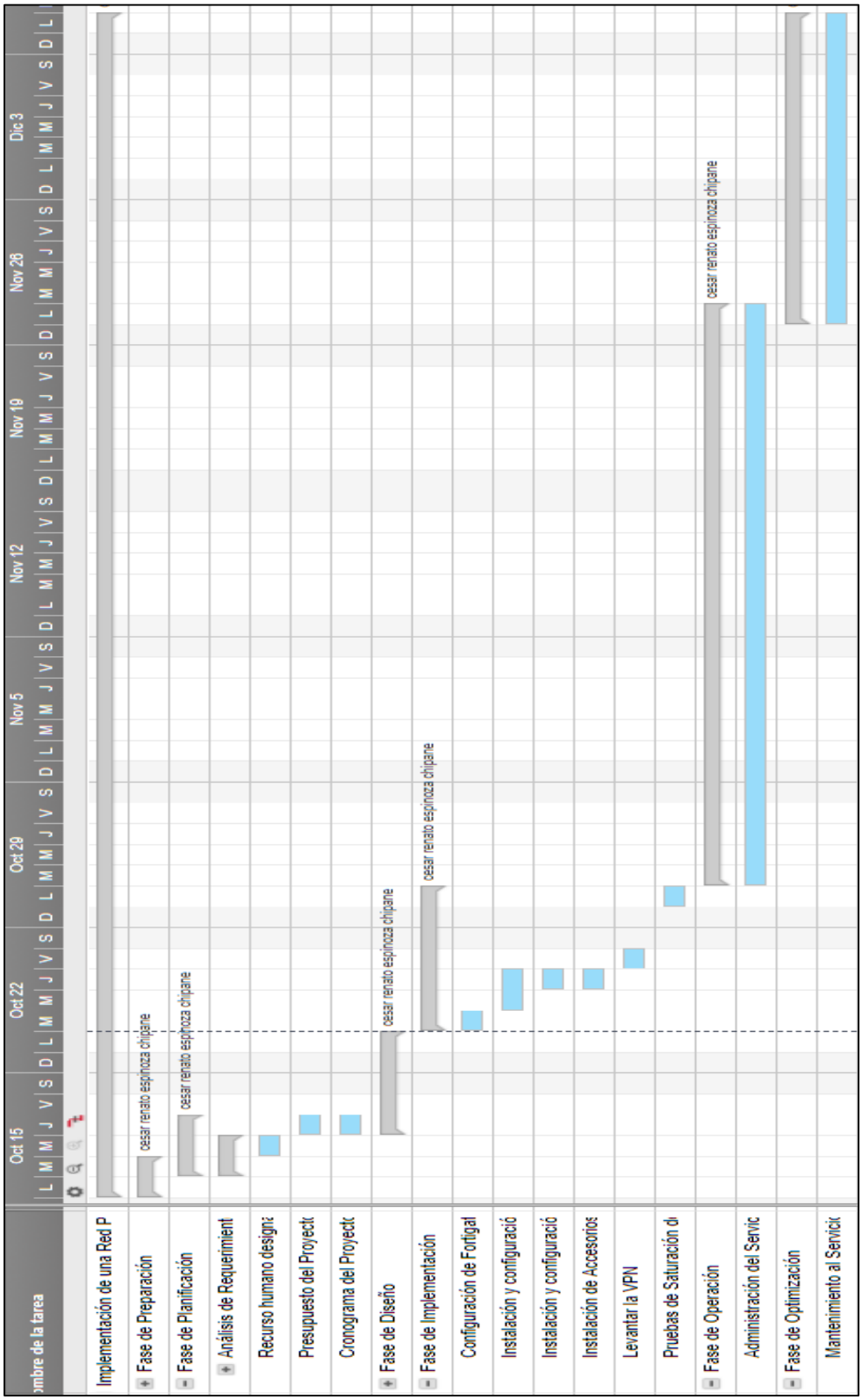

Figura 27. Cronograma en Gantt de las Actividades del Proyecto.

3.3.3. Fase de Diseño

3.3.3.1. Planeamiento IP

Para la asignación del direccionamiento IP en la Tienda se tomó la siguiente dirección de Sub-Red.

Tabla 25

Sub-Red asignado a la Tienda.

RED	MÁSCARA	GATEWAY	IPS UTILIZABLES
10.33.4.192	255.255.255.240	10.33.9.130	10.33.4.197 - 10.33.9.206

Nota: Selección de la Sub-red para la implementación de la solución en la tienda Mass México.

Tabla 26

Direccionamiento IP asignado a los dispositivos LAN.

VLAN	IP	DISPOSITIVO	GATEWAY	MÁSCARA
1	10.33.4.194	FortiGate 30-E	-	255.255.255.240
1	10.33.4.195	Swich SG-200-08	10.33.4.194	255.255.255.240
1	10.33.4.197	Caja 1	10.33.4.194	255.255.255.240
1	10.33.4.198	Caja 2	10.33.4.194	255.255.255.240
1	10.33.4.202	Pc Administrador	10.33.4.194	255.255.255.240
1	10.33.4.203	Impresora Epson	10.33.4.194	255.255.255.240

Nota: Distribución del direccionamiento IP actualmente en tienda.

3.3.3.2. Diseño Lógico Propuesto

Para la propuesta del Diseño Lógico será en Árbol, se contemplará una serie de protocolos y estándares que hacen posible la comunicación entre los dispositivos intermediarios (Switch, Router, etc) y los dispositivos finales (Pc, Impresora, Cajas, Servidores, etc). Esto conlleva al diseño final detallado de la solución propuesta. Se utilizó el modelo de Referencia OSI para la identificación de protocolos y estándares que hace posible la comunicación a nivel de Red, adicional a ello también se identificarán en que capa del modelo OSI operan los dispositivos intermediarios y finales.

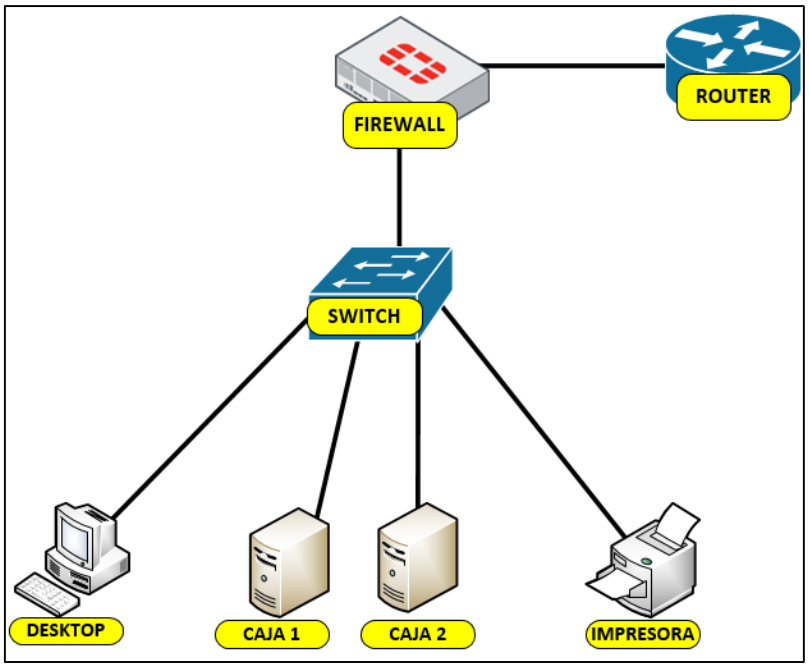

Figura 28. Topología en Árbol Propuesta de Red.

Tabla 27

Protocolos y estándares a nivel de Hardware físico y lógico – Modelo OSI.

N°	CAPA	PROTOCOLO / ESTANDAR	DISPOSITIVO
1	Acceso al Medio	✓ Ethernet 100/1000 BASE-TX ✓ FastEthernet ✓ GigaEthernet	Switch SG-200-08
2	Enlace de Datos	✓ IEEE 802.1Q ✓ IEEE 202.3	Switch SG-200-08
3	Red	✓ IP ✓ IPSec Tunnel	Módem Router Fortinet 30-E
4	Transporte	✓ TCP / UDP	Fortinet 30-E

Nota: Los protocolos nombrados van en relación al modelo de referencia OSI (Open System Interconnection) Para la identificación a nivel de capas de Red, cabe resaltar que dicho modelo de referencia posee 7 capas.

Tabla 28

Protocolos y estándares a nivel de Software - Modelo OSI.

N°	CAPA	PROTOCOLO / ESTANDAR	DISPOSITIVO
5	Sesión	✓ TELNET ✓ SSH	----------
6	Presentación	✓ HTTP ✓ HTTPS ✓ SMTP	----------
7	Aplicación	✓ SNMP	----------

Nota: Los protocolos nombrados van en relación al modelo de referencia OSI (Open System Interconnection) Para la identificación a nivel de capas de Red, cabe resaltar que dicho modelo de referencia posee 7 capas.

En la Tabla 28 se nombran a los dispositivos que trabajan en cada una de las capas del modelo de referencia OSI, no se hace referencia de la PC y demás dispositivos finales, ya que ellos operan en todas las capas de dicho modelo.

3.3.3.3. Seguridad en la Red Privada Virtual propuesto

El FortiGate 30-E es un equipo compacto que posee grandes características, ofrece una seguridad de red de extremo a extremo en una sola plataforma, un sistema operativo de seguridad y gestión unificada desde un único panel. Con este producto Fortinet se tendrá la mejor protección de la industria contra las amenazas de seguridad más avanzadas y los ataques dirigidos. Con fines de salvaguardar la integridad de la información se diseñará una Red segura, contra intrusos y demás ataques informáticos, se utilizará la tecnología de VPN Site to Site, el tipo de protocolo será IpSec en la cual se entablará un password de autenticación antes de enlazar el túnel virtual entre los dos equipos FortiGate.

Se detalla las direcciones IP destino el cual la VPN permitirá tráfico hacia la dirección de Red origen y viceversa.

Tabla 29

Direcciones IPs aceptados en el Tunel VPN Ipsec.

DIRECCIÓN ORÍGEN	IP/RED DESTINO	DESCRIPCIÓN	TRAFICO IN/OUT	ACCIÓN
10.33.4.192/28	10.20.17.101	SAP PMM	Sí	Aceptar
10.33.4.192/28	10.20.17.105	PROXY	Sí	Aceptar
10.33.4.192/28	128.4.1.0/24	OPERACIONES	Sí	Aceptar
10.33.4.192/28	10.1.9.1	FULL CARGA	Sí	Aceptar
10.33.4.192/28	10.20.12.30	PAPERLESS	Sí	Aceptar
10.33.4.192/28	10.20.12.32	SERVER MQ	Sí	Aceptar
10.33.4.192/28	10.20.16.64	VIÑETAS	Sí	Aceptar
10.33.4.192/28	10.20.1.30	DNS2	Sí	Aceptar
10.33.4.192/28	10.20.16.10	DNS3	Sí	Aceptar
10.33.4.192/28	10.20.12.100	DPC4/SDPOS	Sí	Aceptar
10.33.4.192/28	10.81.1.28	PMM 1	Sí	Aceptar
10.33.4.192/28	10.81.1.29	PMM 2	Sí	Aceptar
10.33.4.192/28	10.20.11.20	PMM 3	Sí	Aceptar
10.33.4.192/28	10.20.11.31	PMM Carpeta	Sí	Aceptar
10.33.4.192/28	172.29.1.91	Impresión PMM	Sí	Aceptar
10.33.4.192/28	10.20.17.9	Server PRTG 1	Sí	Aceptar
10.33.4.192/28	10.20.17.23	Server PRTG 2	Sí	Aceptar
10.33.4.192/28	172.31.23.0/24	Monitoreo Morelli	Sí	Aceptar
10.33.4.192/28	130.30.14.110	CORREO	Sí	Aceptar
10.33.4.192/28	10.20.16.10	DNS1	Sí	Aceptar
10.33.4.192/28	172.31.32.0/24	Soporte Cajas	Sí	Aceptar
10.33.4.192/28	10.20.11.13	BCT	Sí	Aceptar
10.33.4.192/28	10.20.11.14	CEM	Sí	Aceptar
10.33.4.192/28	10.20.11.11	Jsatelli	Sí	Aceptar
10.33.4.192/28	10.33.0.0/16	Red_Mass	Sí	Aceptar
10.33.4.192/28	172.16.1.0/24	Red DMZ	Sí	Aceptar
10.33.4.192/28	172.31.35.0/24	Soporte Morelli	Sí	Aceptar
10.33.4.192/28	10.20.16.8	DNS3	Sí	Aceptar
10.33.4.192/28	10.20.16.45	Cubo Excel	Sí	Aceptar

Nota: Se mapearon las direcciones IPs que tendrá comunicación con la tienda, cabe resaltar que redes ajenas a esta lista no establecerá comunicación y será rechazada del túnel VPN.

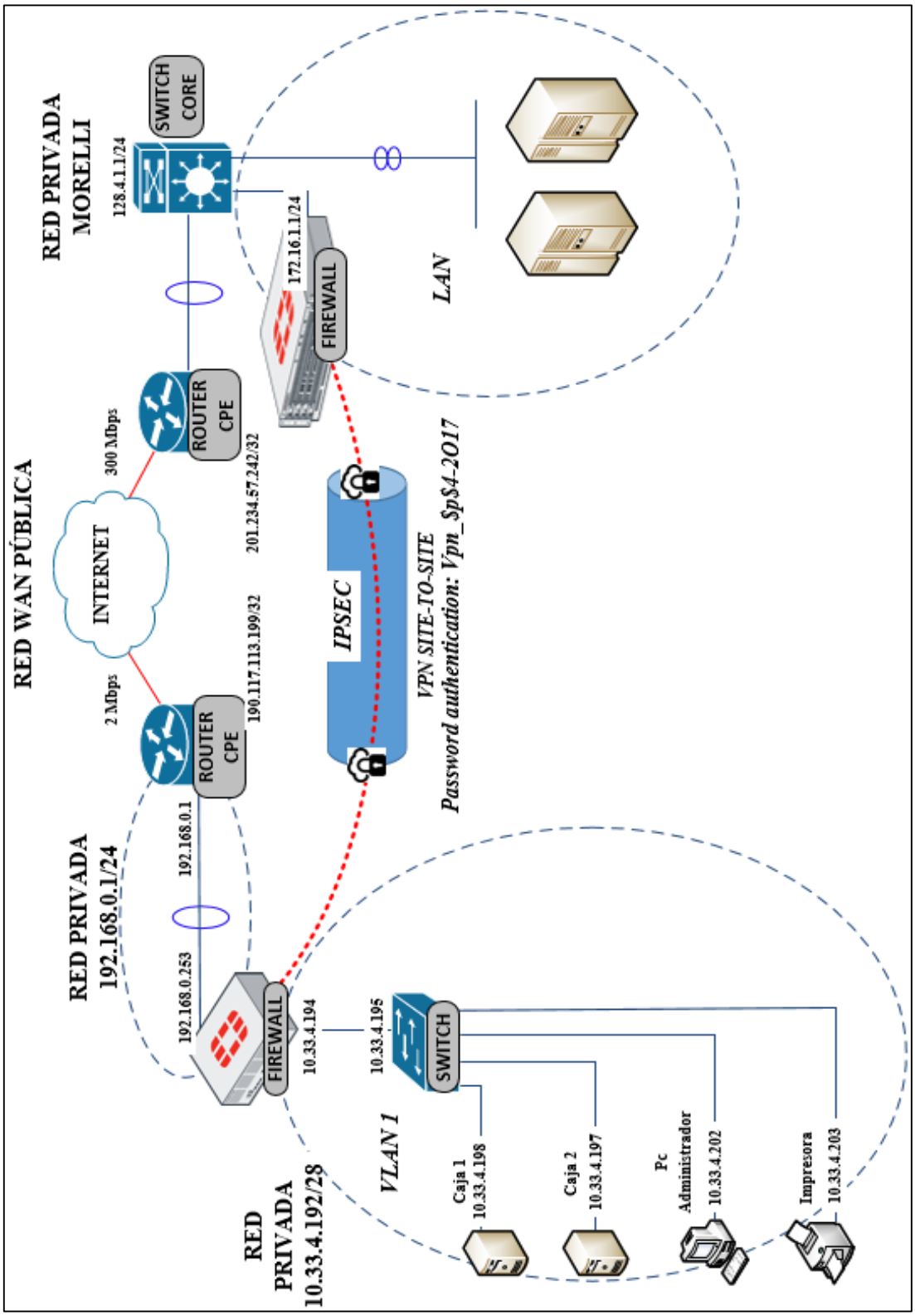

Figura 29. Topología Lógica del Servicio de Comunicación propuesto.

3.3.3.4. Diseño Físico Propuesto

Equipos Intermediarios:

Firewall FortiGate 30-E

Es un equipo de capa 3(Red) fundamental para la realización de la Red Privada Virtual a través del protocolo IPSec, consta de 4 puertos LAN y 1 puerto WAN, ello irá directamente conectado al Módem Router que el proveedor ISP proporcionará para el acceso a Internet.

Figura 30. Equipo Firewall 30-E. Recuperado de"FortiGate 30-E" por Globalgate, 2017.

Switch Cisco SG 200-08:

Es un equipo de capa 2(Enlace de Datos) el cual hará posible la conexión entre dispositivos a nivel LAN y conmutación de tráfico en la Red de la Tienda. Consta de 8 puertos LAN y uno de dichos puertos estará directamente conectado al Firewall FortiGate 30-E.

Figura 31. Equipo Switch SG 200-08. Recuperado de"Cisco SG200-08" por Globalgate, 2017.

Conexión Física de los dispositivos:

En la Figura 32 se observa la conexión de los puntos de datos al Switch SG 200-08 para luego enlazar al equipo Firewall FG 30-E y en la Tabla 31 se detalla la ubicación, estado y etiquetado de los puntos de Red.

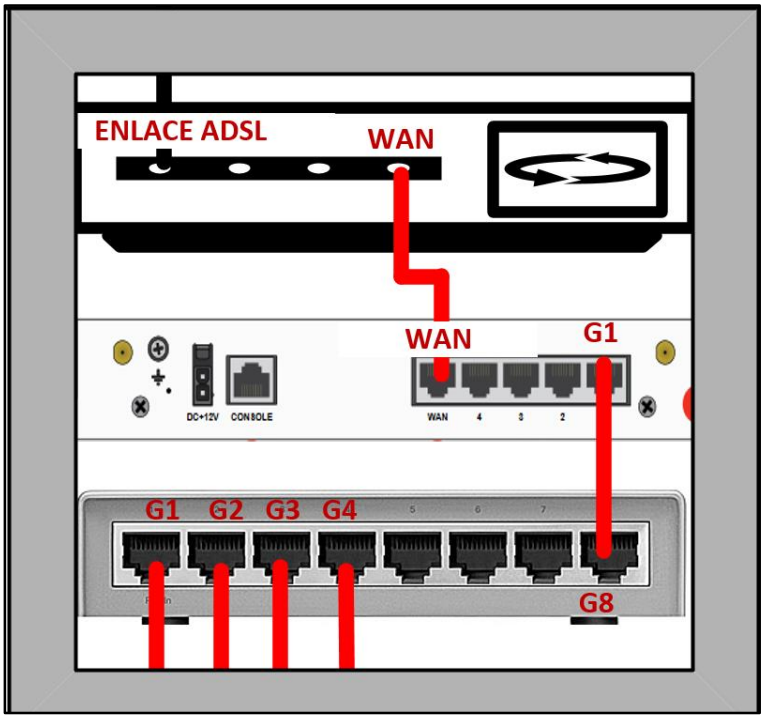

Figura 32. Conexión Física del cableado de Red Propuesto.

Tabla 30

Conectorización de enlaces al FortiGate 30-E.

CONECTADO A	ESTADO	VLAN	PUERTO	DESCRIPCIÓN
Switch SG200-08	Libre	1	G1	Enlace LAN-to-LAN
-	Down	1	G2	Puerto Libre
-	Down	1	G3	Puerto Libre
-	Down	1	G4	Puerto Libre
Módem Router	Activo	-	WAN	Enlace WAN-to-Internet

Nota: Distribución de enlaces para los equipos de comunicación entre switch, Firewall y módem Router

Tabla 31

Conexión de puntos de Red al Switch Cisco SG200-08.

ETIQUETA LADO USUARIO	CONECTADO A:	ESTADO	VLAN	PUERTO	DESCRIPCIÓN
D-1	Switch SG200-08	Up	1	G1	Caja 1
D-2	Switch SG200-08	Up	1	G2	Caja 2
D-3	Switch SG200-08	Up	1	G3	Pc Administrador
D-4	Switch SG200-08	Up	1	G4	Impresora
-	-	Down	-	G5	Puerto Libre
-	-	Down	-	G6	Puerto Libre
-	-	Down	-	G7	Puerto Libre
-	FortiGate 30-E	Activo	1	G8	Enlace LAN-to LAN

Nota: Nueva planificación para la distribución de puntos en el nuevo switch para los host finales.

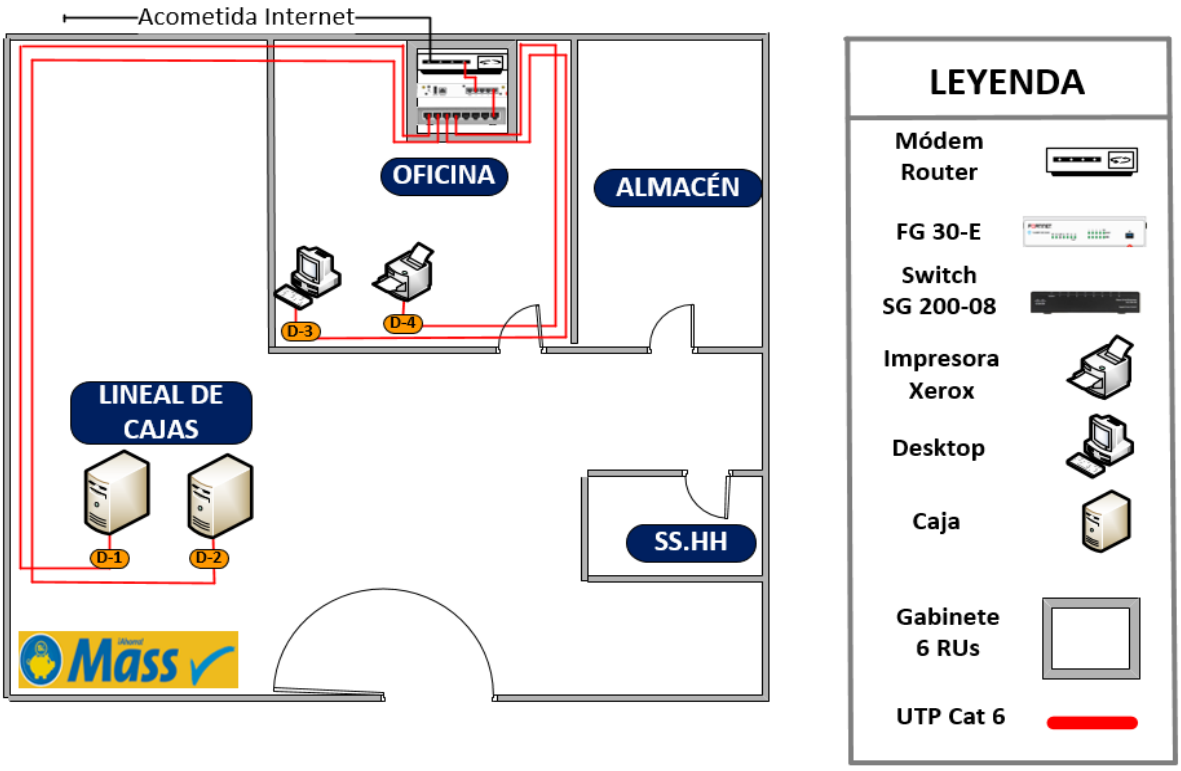

Figura 33. Ubicación Física de los Dispositivos intermediarios y finales propuesta.

3.3.4. Fase de Implementación

3.3.4.1. Configuración de la VPN IPsec Site-to-Site

A) Oficinas de Morelli - Firewall 1500-D

En el menú seleccionar **VPN / Ipsec / Tunnel:**

Crear el Nombre del Tunel VPN **TIENDA_MASS_VPN**, luego configurar la IP Pública del Gateway Remoto **190.117.113.199/32,** luego seleccionar la interfaz de Internet proporcionada Level 3.

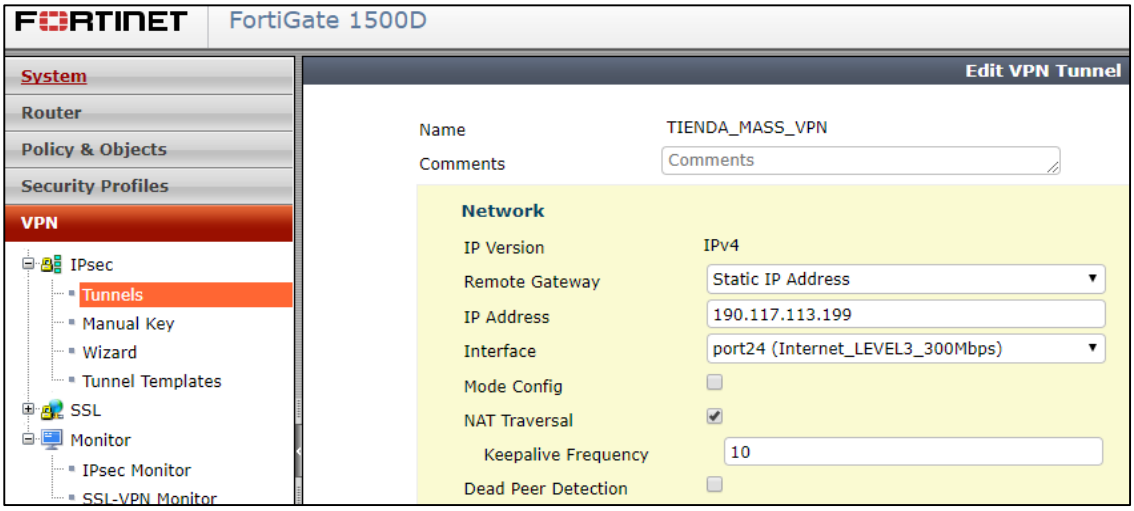

Figura 34. Creación de la VPN IPsec en el Firewall Master.

Seguir en la Sección **VPN / Ipsec / Tunnel:**

Configurar la Autenticación, Pre-Shared Key: **Vpn_p4-2O17** y dejar valores predeterminados.

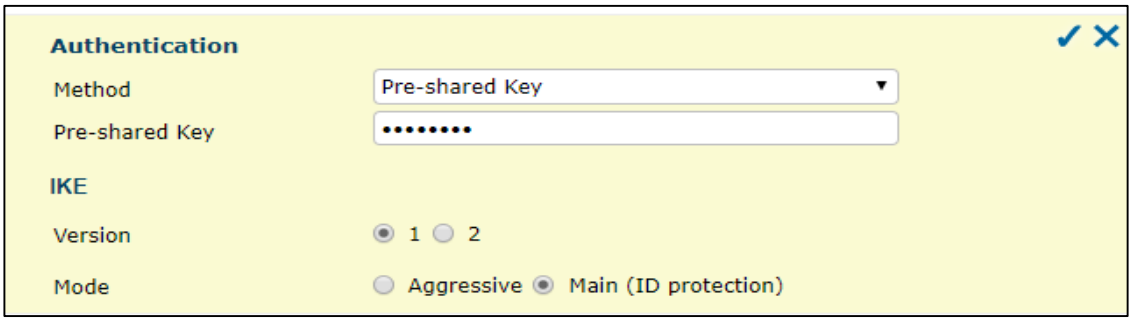

Figura 35. Creación del key de autenticación para la comunicación VPN Site_to_Site.

Seguir en la Sección **VPN / Ipsec / Tunnel:**

En la primera Fase del Tunel IPsec seleccionar únicamente el tipo de encriptación **AES256** con autenticación **SHA1**, los demás valores dejarlos por defecto.

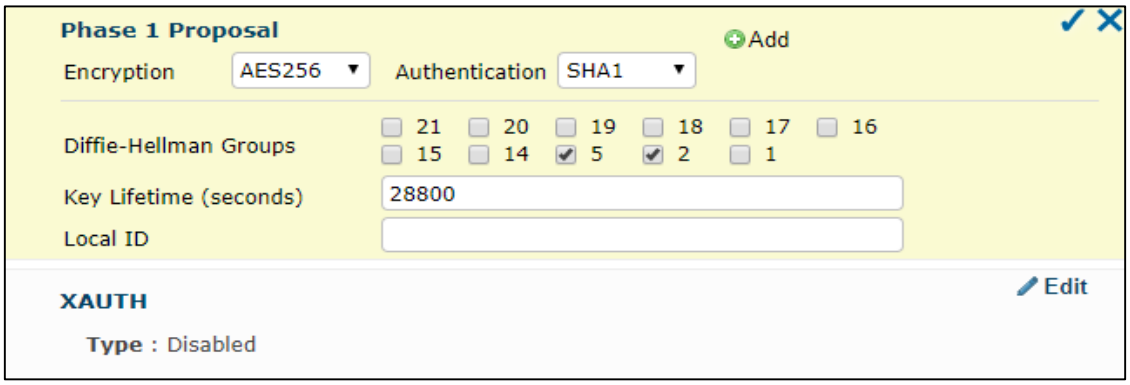

Figura 36. Phase 1 modo de encriptación de seguridad de la VPN IPsec.

Seguir en la Sección **VPN / Ipsec / Tunnel:**

En la segunda Fase del Tunel IPsec empezar a agregar las Direcciones de Red o Ips específicas locales, esta acción permitirá el tráfico hacia la Sub-Red destino en este caso es la **10.33.4.192/28**.

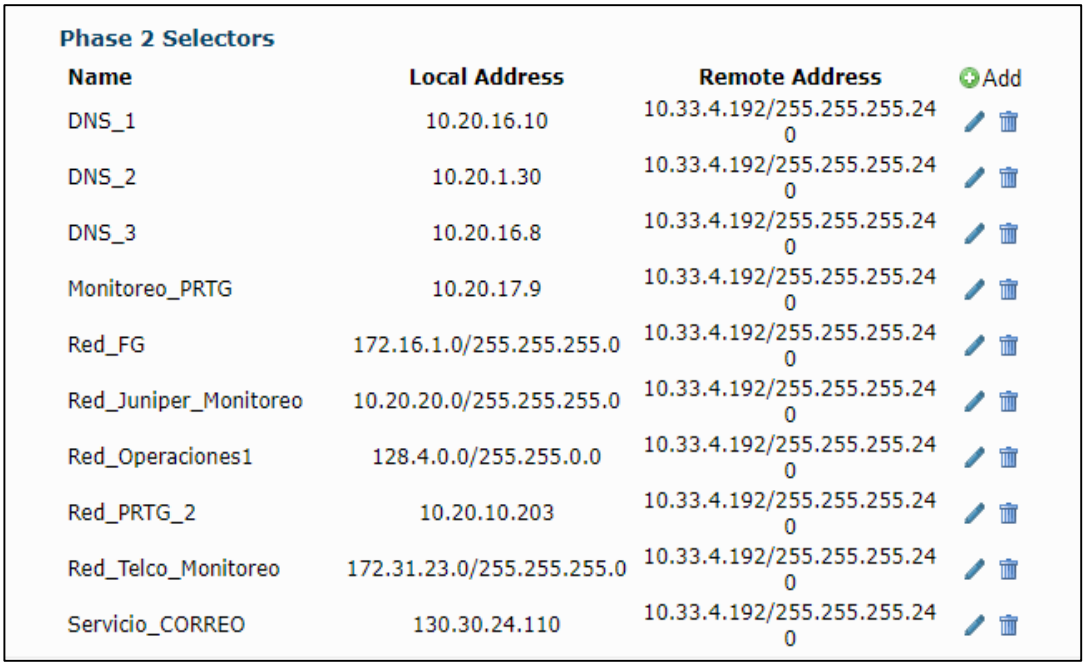

Figura 37. Phase 2 declaración de las Redes que pasarán en la VPN Ipsec.

Culminada la configuración del IPsec, proceder a crear el objeto de nombre **TIENDA_MASS_VPN_remote_subnet_1**, que hará mención a la Sub-Red de destino, en este caso la **10.33.4.192/28.**

En el menú seleccionar **Policy & Objects / Addresses / Create New/ Addresses.**

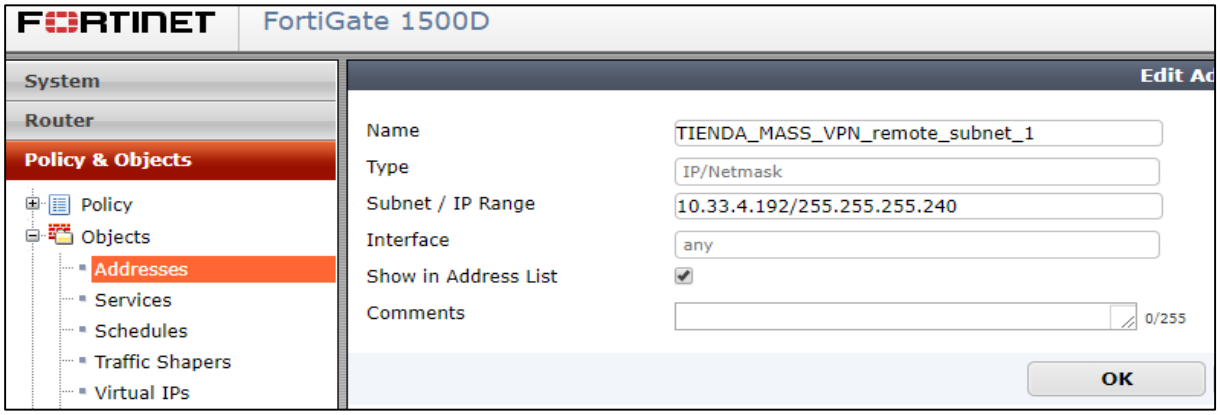

Figura 38. Creación en el Firewall Master la Sub-Red remota como objeto.

Seguir en la sección **Policy & Objects / Addresses.**

Ahora crearemos un grupo con nombre **TIENDA_MASS_VPN_remote** para el alojamiento del objeto **TIENDA_MASS_VPN_remote_subnet_1**, esto para mantener un orden y seguimiento a los futuros objetos que se creen para ser anunciados en la política**.**

Seleccionar **Create New/ Addresses Group.**

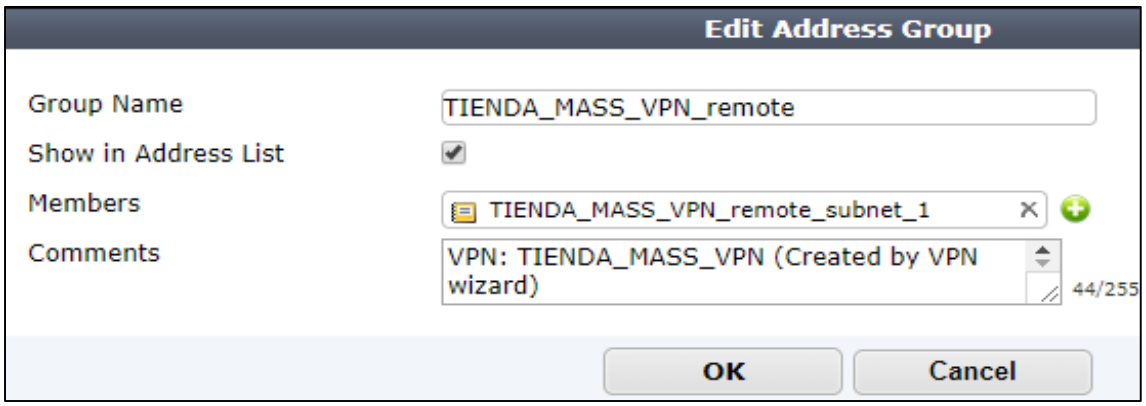

Figura 39. Creación del Grupo asociando el Objeto de la Sub-Red Remota.

Creación de la política para permitir el tráfico de la LAN Morelli hacia la Sub-Red remota por la VPN IPsec.

En la sección **Policy & Objects / IPv4 / Create New/ Policy:**

Seleccionar el **puerto 17** como tráfico de salida, el **Source** será **all**, en **Outgoing Interface** seleccionar **TIENDA_MASS_VPN**, ello hace mención a la VPN IPsec creada para la Tienda Mass, en **Action** seleccionar **ACCEPT.**

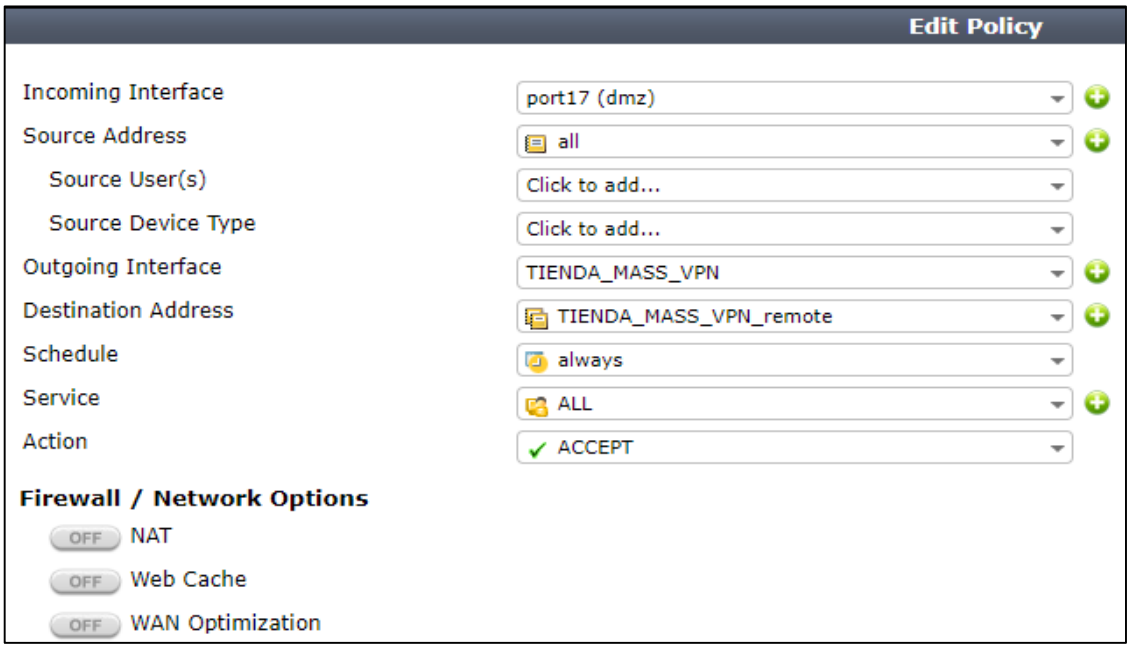

Figura 40. Creación de la Política para tráfico de entrada a las Redes Morelli.

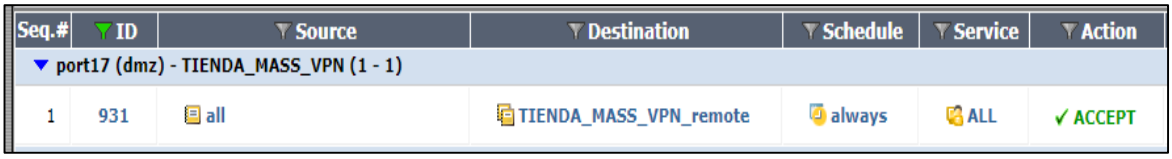

Figura 41. Apreciación de la Política N°1 asociada al Puerto 17 de la DMZ para el tráfico in.

Creación de la política para permitir el tráfico desde la Sub-Red hacia la LAN Morelli por la VPN IPsec.

Seguir **Policy & Objects / IPv4 / Create New/ Policy:**

En **Incoming Interface** seleccionar **TIENDA_MASS_VPNS** como tráfico de salida, el **Source** será **TIENDA_MASS_VPN_remote (Sub-Red Tienda Mass)**, en **Outgoing Interface** seleccionar el Puerto 17, luego en **Action** seleccionar **ACCEPT.**

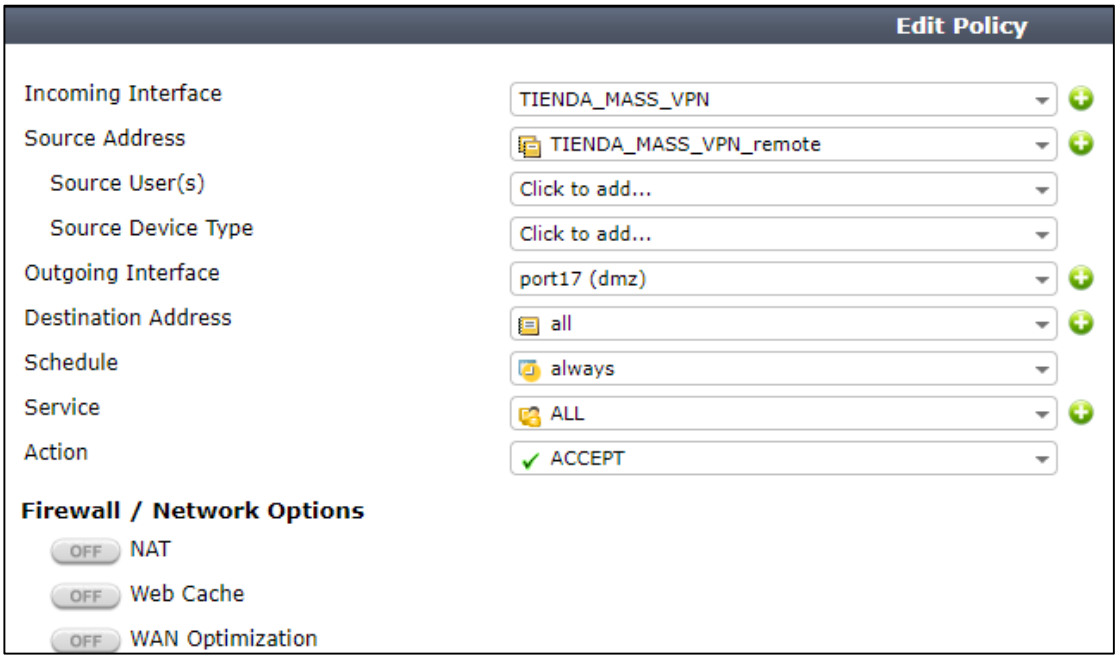

Figura 42. Creación de la Política para tráfico de salida a Sub-Red remota.

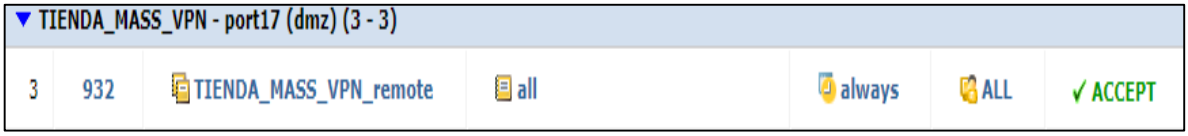

Figura 43. Apreciación de la Política N° 2 asociada al Puerto 17 de la DMZ de tráfico out.

Creación de la política para permitir el tráfico de la LAN Morelli hacia la Sub-Red remota por la VPN IPsec.

En la sección **Policy & Objects / IPv4 / Create New/ Policy:**

Seleccionar el **puerto 22** como tráfico de salida, el **Source** será **all**, en **Outgoing Interface** seleccionar **TIENDA_MASS_VPN**, ello hace mención a la VPN IPsec creada para la Tienda Mass, en **Action** seleccionar **ACCEPT.**

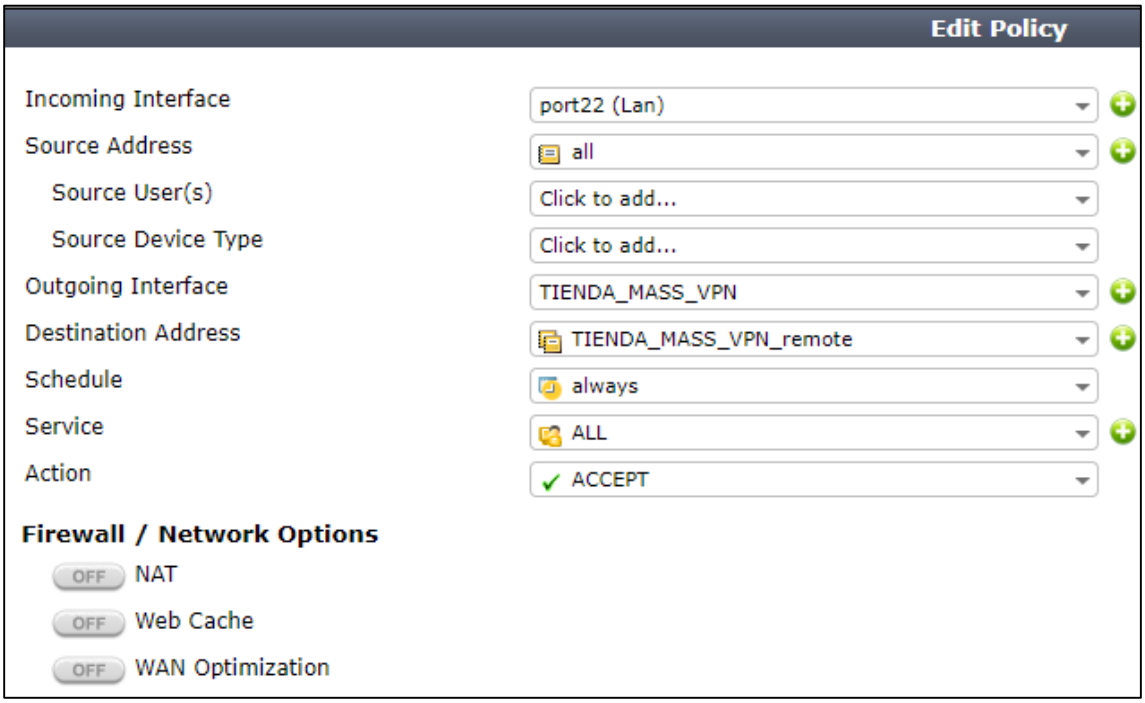

Figura 44. Creación de la Política para tráfico de entrada a las Redes Morelli.

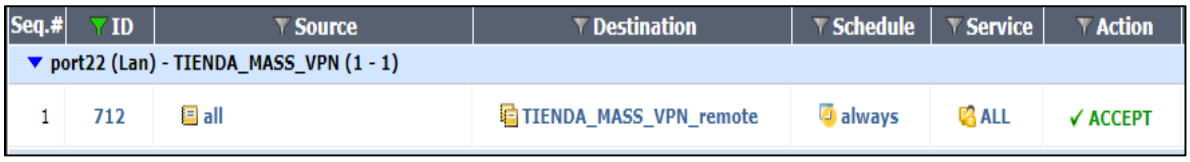

Figura 45. Apreciación de la Política N°1 asociada al Puerto 22 de la LAN Morelli para el tráfico in

Creación de la política para permitir el tráfico desde la Sub-Red hacia la LAN Morelli por la VPN IPsec.

Seguir **Policy & Objects / IPv4 / Create New/ Policy:**

En **Incoming Interface** seleccionar **TIENDA_MASS_VPNS** como tráfico de salida, el **Source** será **TIENDA_MASS_VPN_remote (Sub-Red Tienda Mass)**, en

Outgoing Interface seleccionar el Puerto 22, luego en **Action** seleccionar **ACCEPT.**

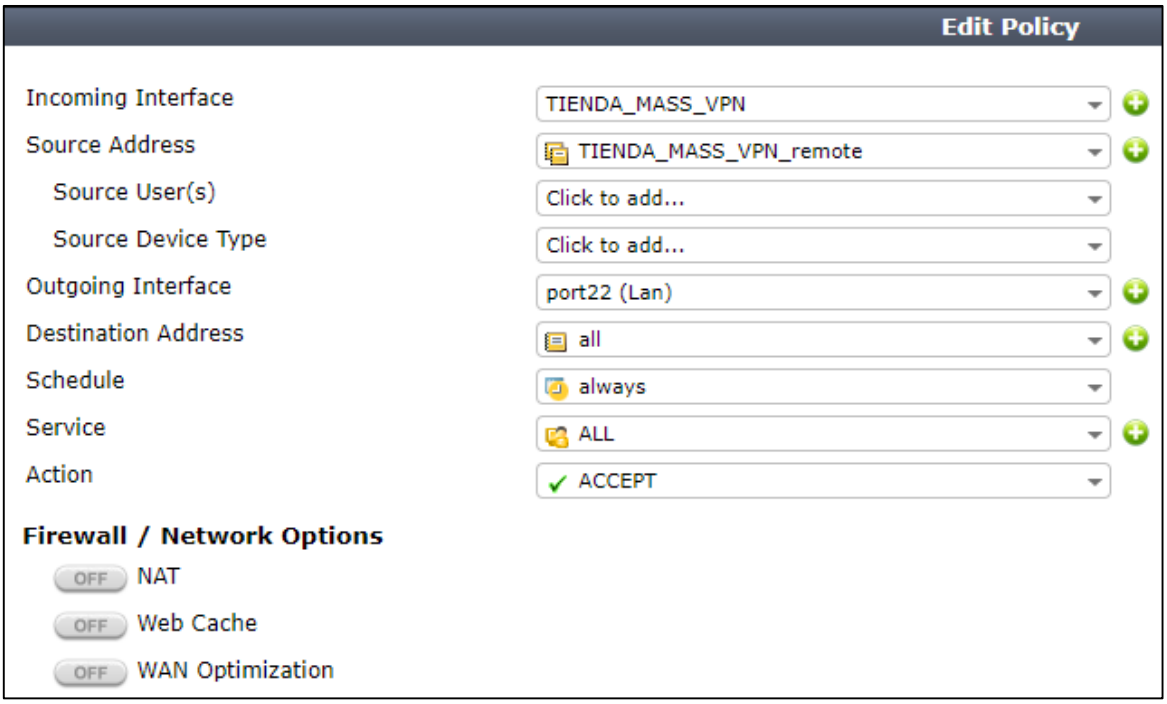

Figura 46. Creación de la Política para tráfico de salida a la Sub-Red remota.

Figura 47. Apreciación de la Política N°2 asociada al Puerto 22 de la VPN Mass para el tráfico out.

En el menú seleccionar **Router / Static Routes / Create New.**

Se creará una ruta estática para redirigir el tráfico indicando el destino **10.33.4.192/28** conociéndolo por la VPN Ipsec creada **TIENDA_MASS_VPN.**

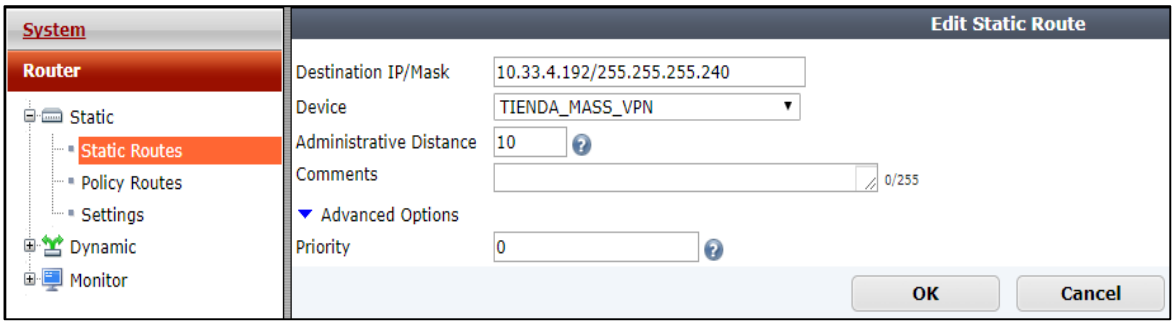

Figura 48. Creación de la Ruta estática para el tráfico de datos generado por la VPN IPsec.

B) Tienda Mass – Firewall 30-E

En el menú seleccionar **VPN / Ipsec Tunnels/ Createm New.**

Crear el Nombre del Tunel VPNV **MASS_MORELLI**, luego configurar la IP Pública del Gateway Remoto **201.234.57.242/32,** luego seleccionar la interfaz el cual se tiene salida a Internet WAN.

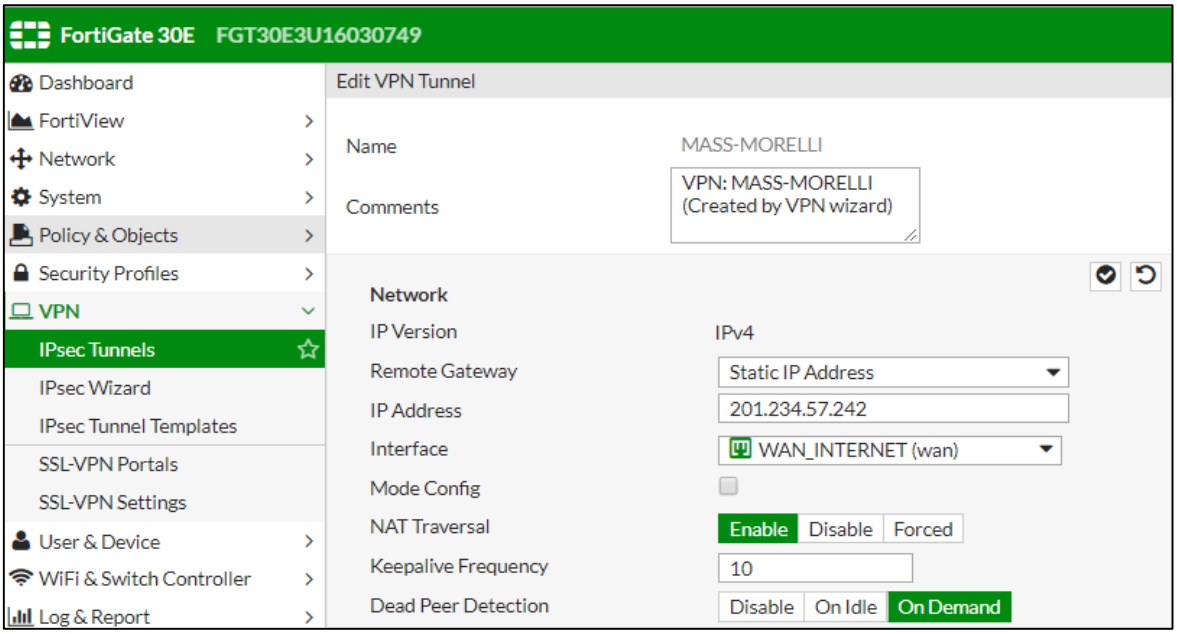

Figura 49. Creación de la VPN Ipsec en Firewall 30-E remoto.

Seguir en la sección **VPN / Ipsec Tunnels:**

Configurar la Autenticación, Pre-Shared Key: **Vpn_p4-2O17** y dejar valores predeterminados.

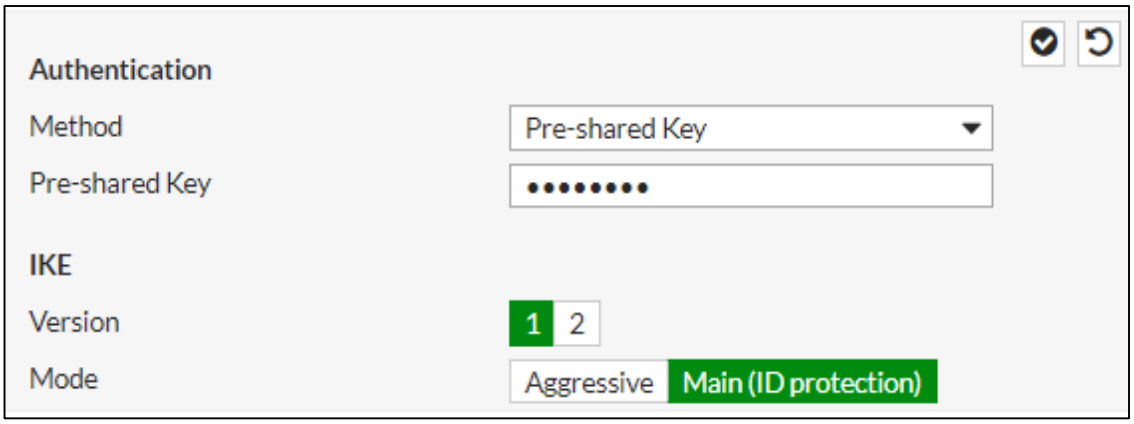

Figura 50. Autenticación para establecer la comunicación Site_to_Site entre los Firewalls.

Seguir en la Sección **VPN / Ipsec Tunnels:**

En la primera Fase del Tunel IPsec seleccionar únicamente el tipo de encriptación **AES256** con autenticación **SHA1**, los demás valores dejarlos por defecto.

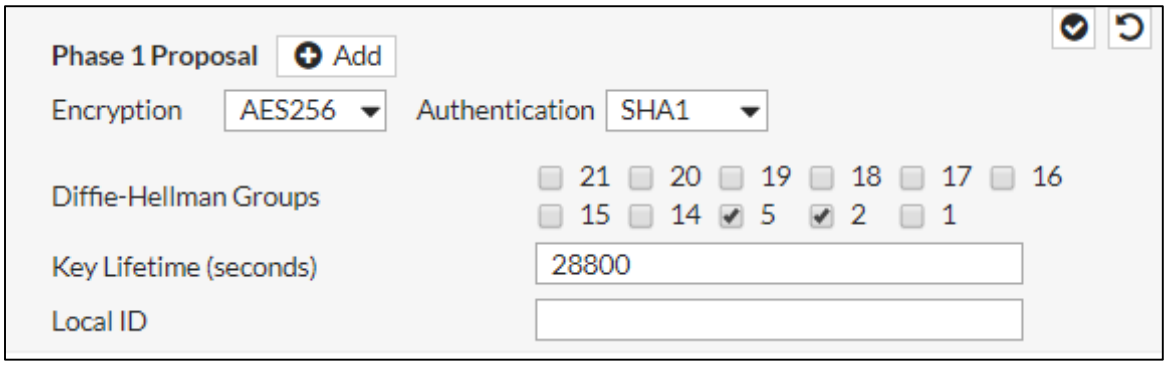

Figura 51. Phase 1 modo de encriptación seguridad en la VPN IPsec.

Seguir en la Sección **VPN / Ipsec Tunnels:**

En la segunda Fase del Tunel IPsec empezar a agregar las Direcciones de Red o Ips específicas remotas, esta acción permitirá el tráfico por LAN Morelli.

Phase 2 Selectors

Name	Local Address	Remote Address	Add
DNS_1	10.33.4.192/255.255.255.240	10.20.16.10	
DNS_2	10.33.4.192/255.255.255.240	10.20.1.30	
DNS_3	10.33.4.192/255.255.255.240	10.20.16.8	
MASS-MORELLI	10.33.4.192/255.255.255.240	172.31.23.0/255.255.255.0	
Monitoreo_PRTG_1	10.33.4.192/255.255.255.240	10.20.17.9	
Monitoreo_PRTG_2	10.33.4.192/255.255.255.240	10.20.10.203	
Red_DMZ	10.33.4.192/255.255.255.240	172.16.1.0/255.255.255.0	
Red_Juniper_VPN	10.33.4.192/255.255.255.240	10.20.20.0/255.255.255.0	
Red_Operaciones	10.33.4.192/255.255.255.240	128.4.0.0/255.255.0.0	
Servicio_CORREO	10.33.4.192/255.255.255.240	130.30.24.110	

Figura 52. Phase 2 declaración de la Sub-Red y Redes que admitirá la VPN Ipsec.

Culminada la configuración del IPsec, proceder a crear los objetos con los nombres que llevarán las IPs o Redes remotas.

En el menú seleccionar **Policy & Objects / Addresses / Create New/ Addresses.**

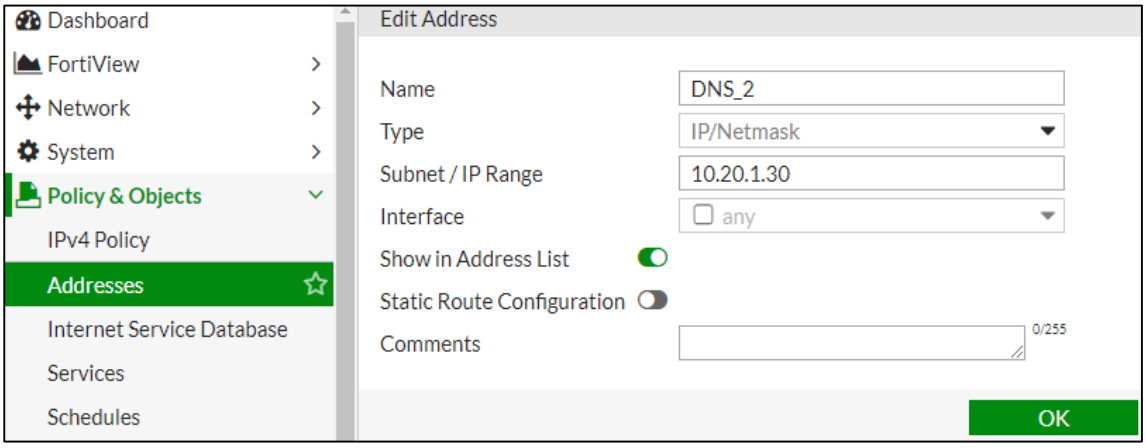

Figura 53. Creación de los Objetos Redes de Morelli.

Se denotará el siguiente listado:

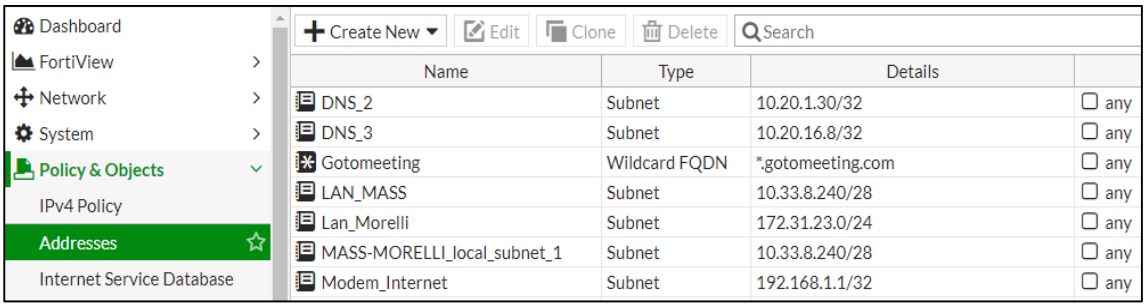

Figura 54. Listado de Objetos creados en el Firewall remoto.

Esto aumentará a medida que se vallan agregando Ips el cual desee comunicar desde la Sub-Red de la Tienda Mass.

Seleccionar en el menú **Policy & Policy / IPv4 Policy / Create New.**

Ahora crearemos directamente la política de tráfico de salida con nombre **TIENDA_MASS_to_MORELLI** hacia las Redes o Ips remotas que se desea llegar, el **Incoming Interface** será la **lan,** el **Outgoing Interface** será por la **VPN IPsec creada MASS-MORELLI,** en la acción seleccionar **ACCEPT.**

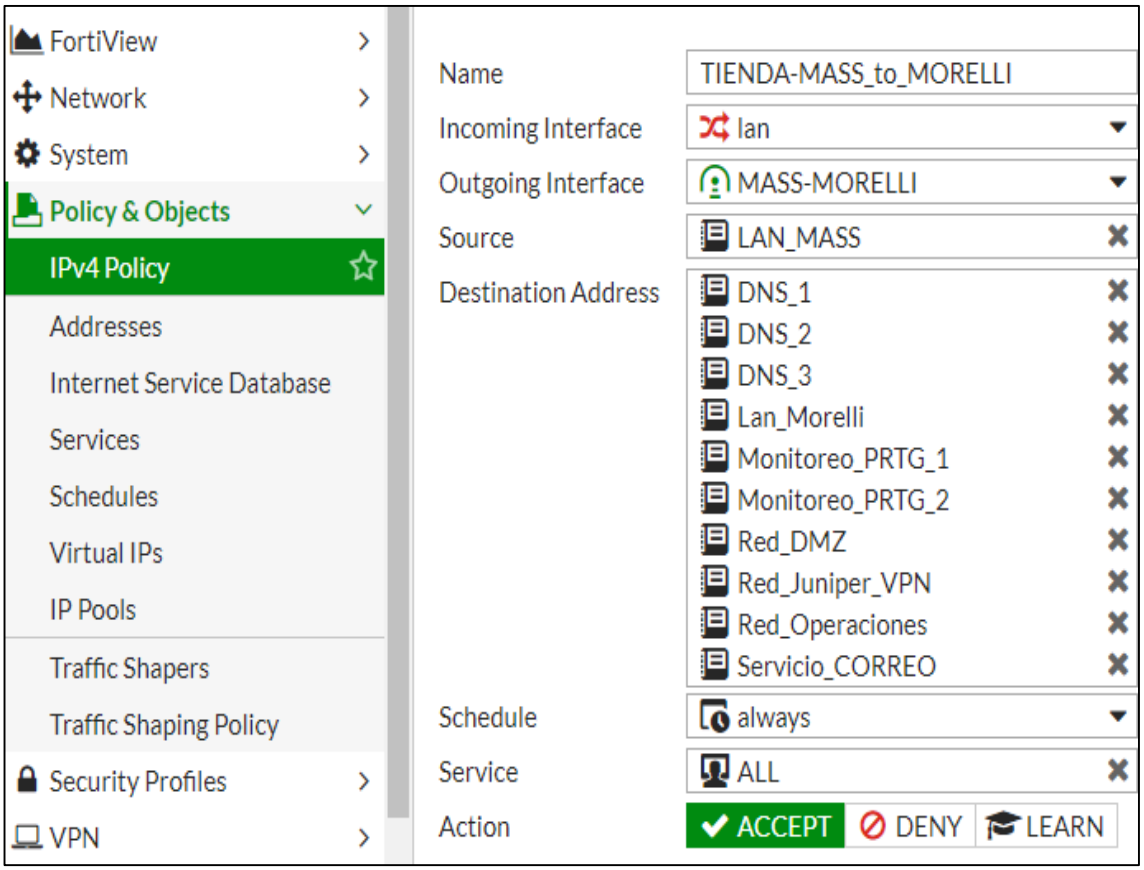

Figura 55. Creación de la Política para permitir tráfico de salida desde la Sub-Red Tienda Mass.

En **Destination Address** se es válido agregar directamente los objetos o un grupo que aloje dichos objetos, las dos opciones son válidas. Seguir la sección **Policy & Policy / IPv4 Policy / Create New.**

Ahora crearemos directamente la política de tráfico de entada con nombre **MORELLI_to_TIENDA-MASS** hacia la Sub-Red de la Tienda, en este caso la 10.33.4.192/28, el **Incoming Interface** será la VPN **MASS-MORELLI,** el **Outgoing Interface** será por la **LAN,** en la acción seleccionar **ACCEPT,** según Figura 56.

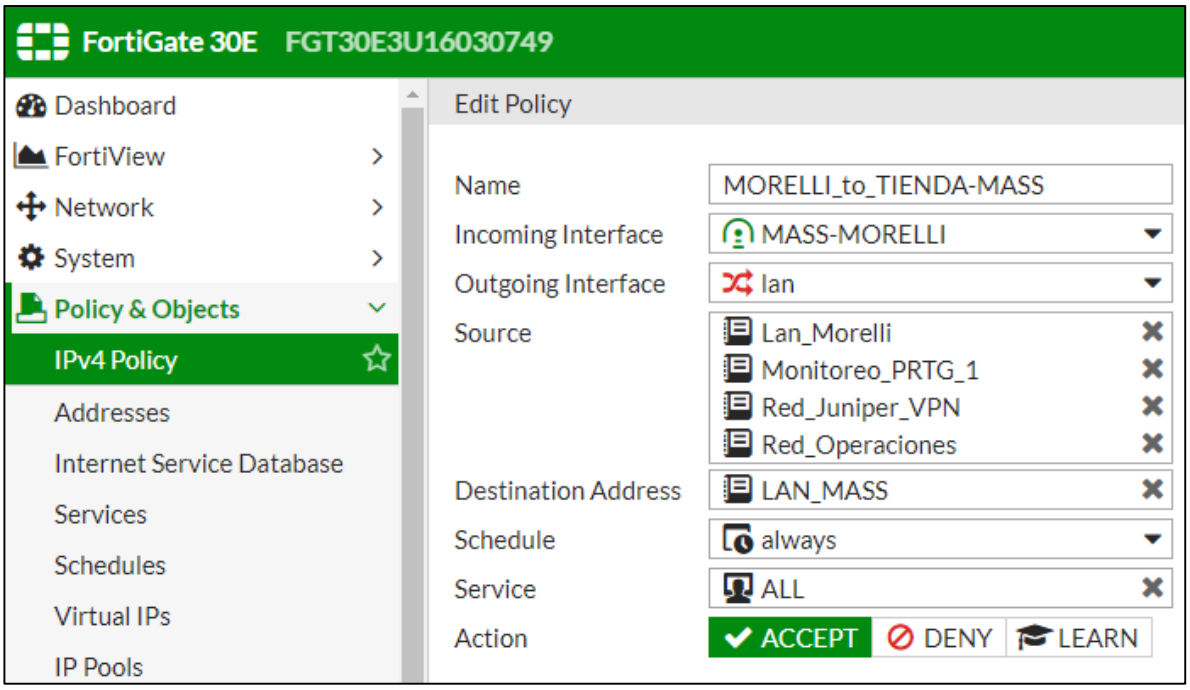

Figura 56. Creación de la Política para permitir tráfico entrada desde las Redes Morelli.

En **Destination Address** se es válido agregar directamente los objetos o un grupo que aloje dichos objetos, las dos opciones son válidas.

Para hace posible la conectividad hacia internet desde el Firewall 30-E en la Tienda Mass se debe cumplir ciertos parámetros:

Ingresar al menú **Network / Interfaces / Lan / Create New.**

Seleccionar la Ip/Máscara de Red asignada para la LAN en Tienda.

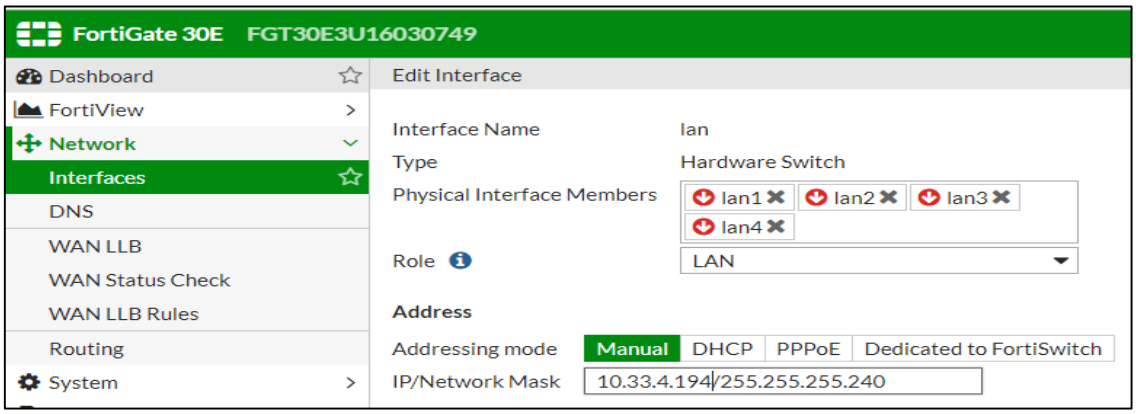

Figura 57. Configuración de la Red LAN para la tienda Mass.

Seguir en la sección **Network / Interfaces / Lan.**

Podemos asignar ciertas restricciones por puertos en este caso el firewall admitirá los protocolos HTTPS, PING, FMG-Access, CAPWAP, SSH y SNMP.

En DHCP Server se puede habilitar si es el caso.

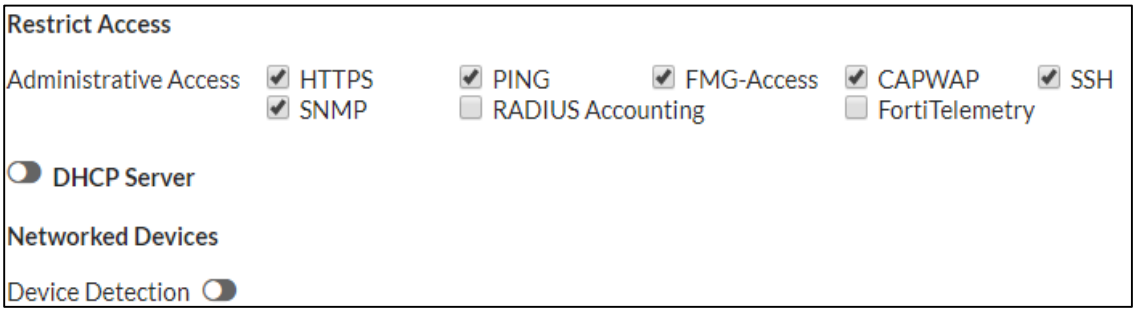

Figura 58. Habilitación de protocolos para administración remota.

Seguir en la sección **Network / Interfaces / WAN / Create New**

Procedemos a la configuración a nivel WAN, es la interfaz que se utilizará para la salida hacia Internet, con nombre: WAN_INTERNET.

Le asignamos la IP/ Máscara de Red del rango que se encuentra actualmente configurado en Módem Router del Proveedor ISP.

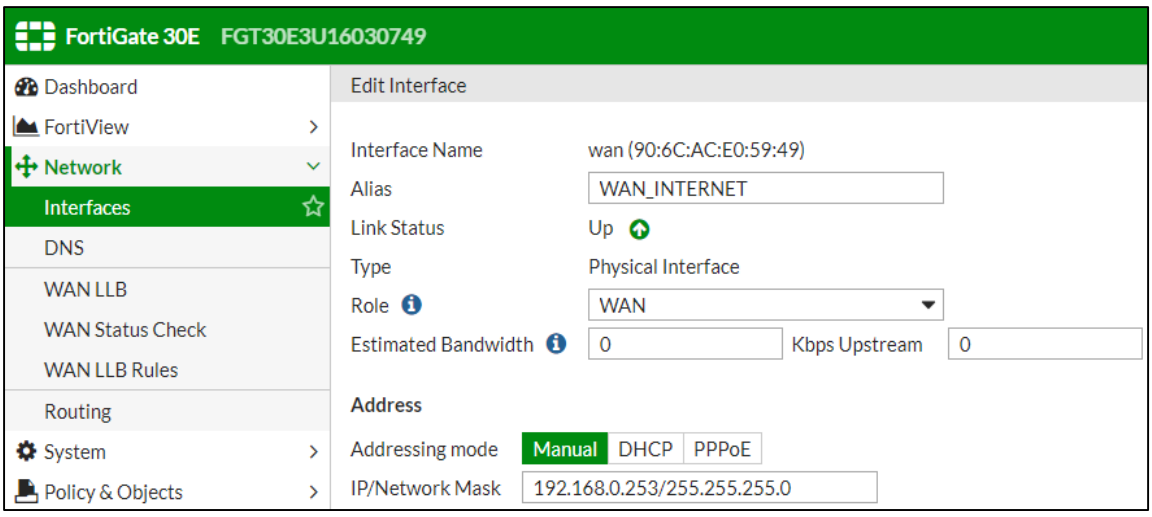

Figura 59. Configuración de la Red WAN acceso a Internet.

Seguir en la sección **Network / Interfaces / Wan.**

Podemos darle ciertas restricciones por puertos en este caso el firewall admitirá los protocolos HTTPS, PING, FMG-Access, SSH y SNMP.

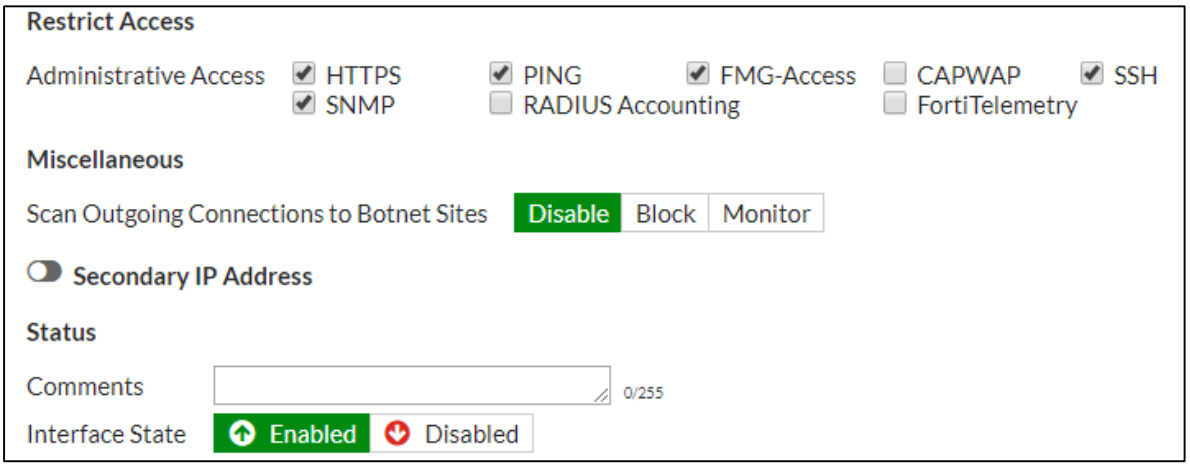

Figura 60. Habilitación de protocolos para administración remota.

Seguir en la sección **Network / Interfaces.**

Asignar DNS estáticos al Firewall 30-E, según configuración.

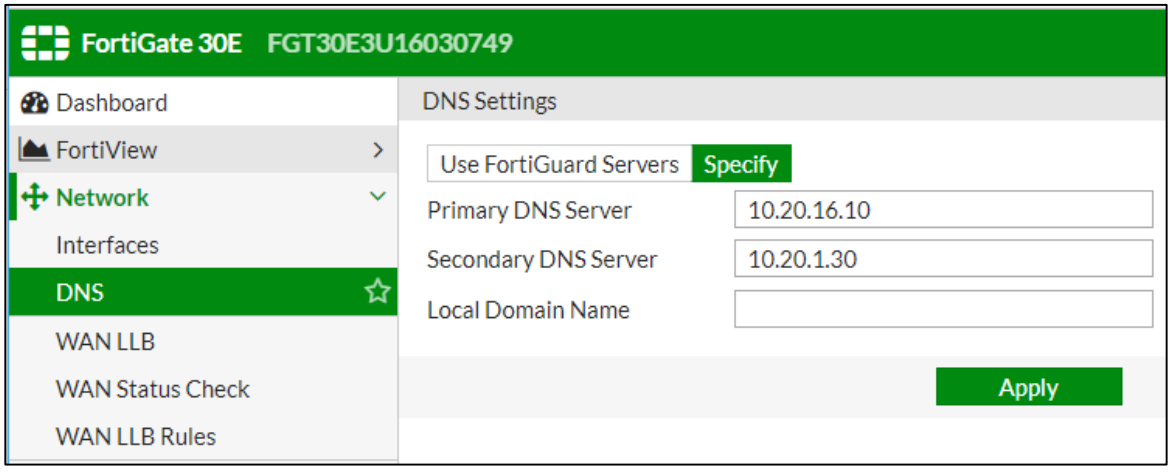

Figura 61. Configuración de los DNS predeterminados.

Para tener conexión al Módem Router desde el Firewall 30-E, realizar la siguiente ruta estática, ello también servirá para la salida hacia Internet.

En el menú seleccionar **Network / Routing / Create New.**

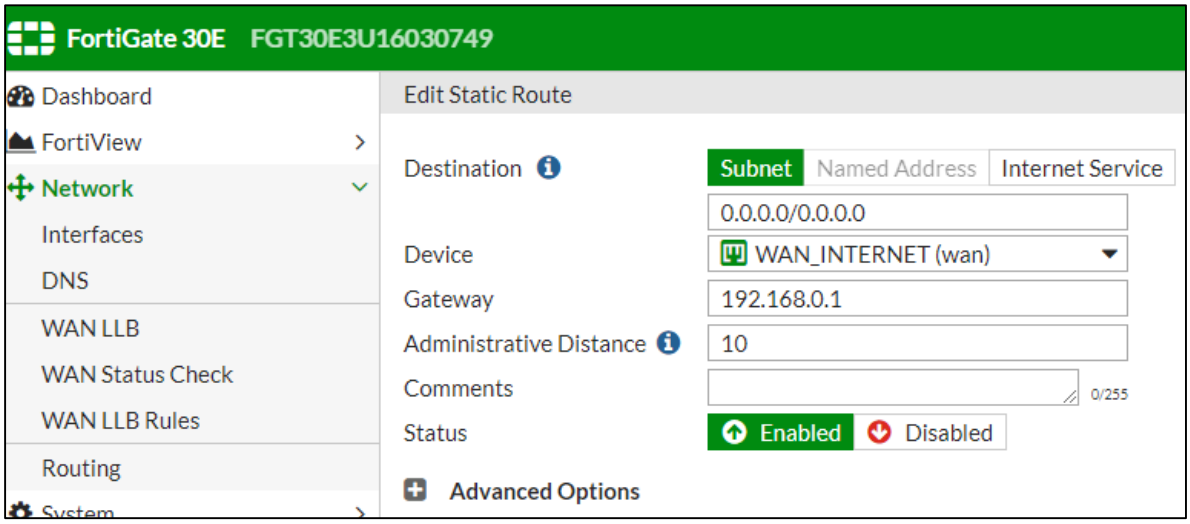

Figura 62. Creación de la Ruta estática hacia Internet.

Seguir en la sección **Network / Routing / Create New.**

Se creará las rutas estáticas para re direccionar el tráfico IP.

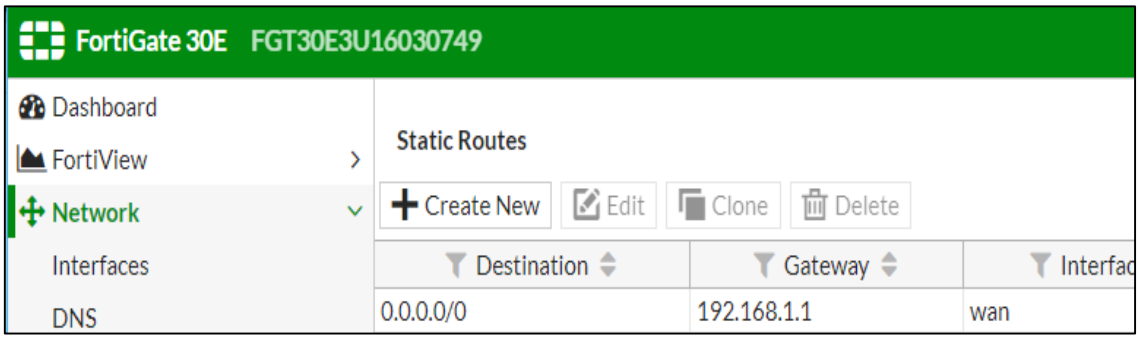

Figura 63. Tabla de Ruta hacia Internet en el Firewall.

Procedemos a la configuración a nivel de VPN, es la interfaz que se utilizará para la comunicación entre IPs públicas con (Tienda Mass – Oficinas Morelli). Le asignamos la IP pública del Módem Router **190.117.113.199/32** para luego colocar la **Remote IP** en este caso la IP pública de Morelli **201.234.57.242/32,** como muestra la Figura 64.

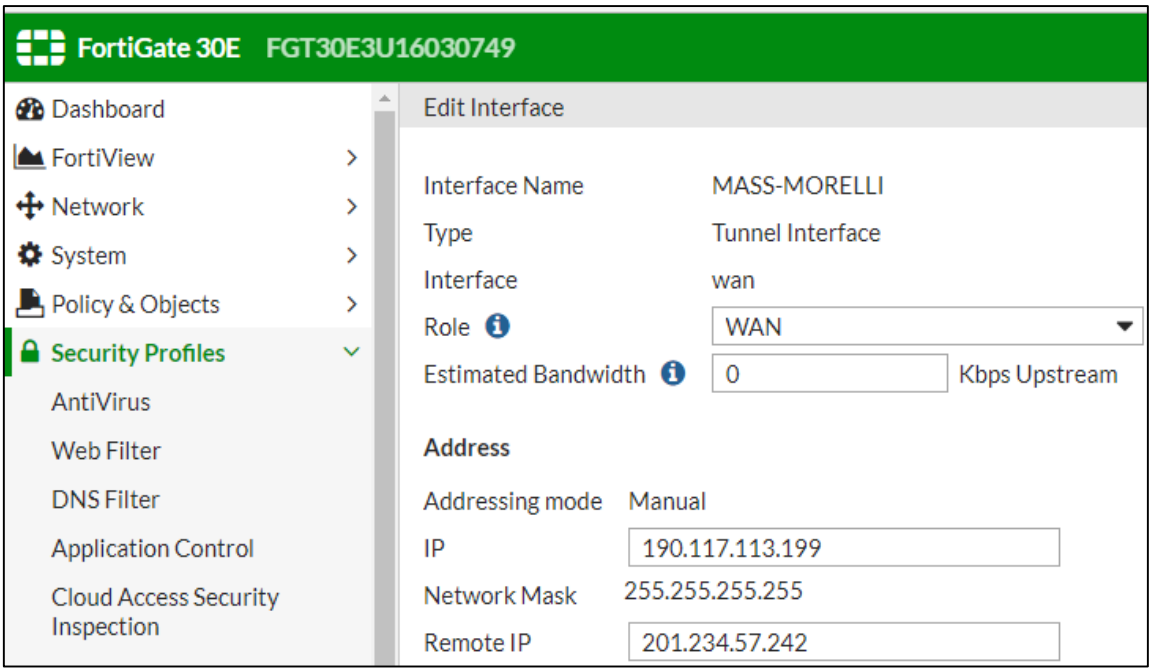

Figura 64. Configuración de las IPs públicas Origen-Destino.

El **destination** será la Sub-Red o IPs remota en este caso la **172.31.23.0/24** aprendiendo la ruta por la VPN **MASS-MORELLI.**

Esto aplicará para todas las Ips o Sub-Redes remotas el cual se desea mantener una comunicación.

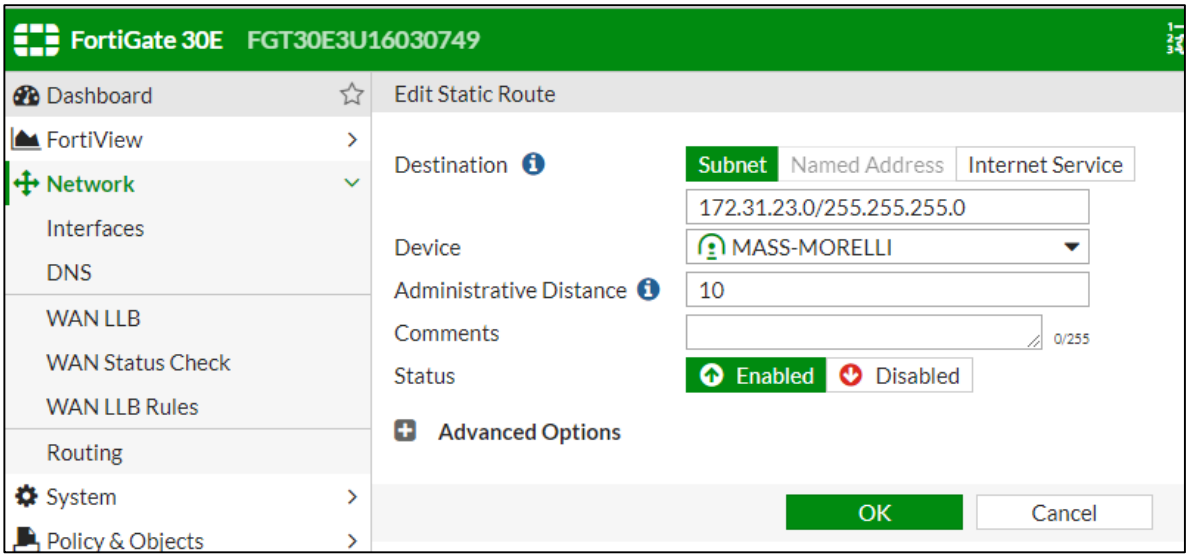

Figura 65. Creación de las Rutas estáticas para las Redes Morelli.

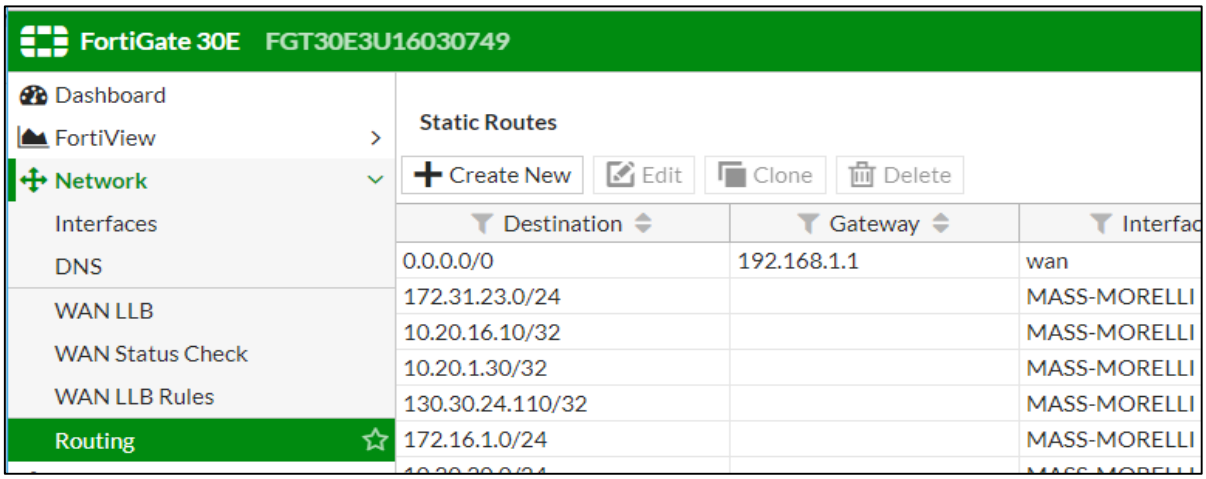

Figura 66. Tabla de Rutas hacías las Redes Morelli.

En el menú seleccionar **Monitor / IPsec Monitor / Refresh**.

Se denota los objetos creados cada una de ellas haciendo mención a un Red o IP determinada.

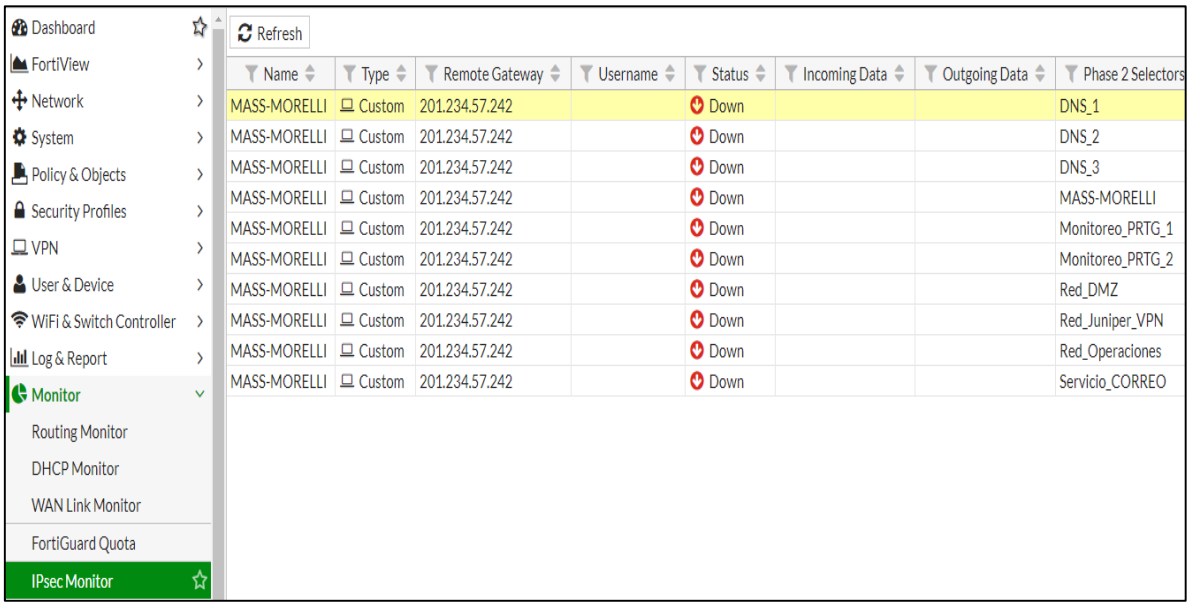

Figura 67. Tabla de las Redes Morelli por el Túnel VPN IPsec.

Proceder haciendo click derecho a cada una de las interfaces en DOWN, para luego seleccionar BRING UP, ello hará posible la comunicación VPN Site-To-Site con las Oficinas de Morelli.

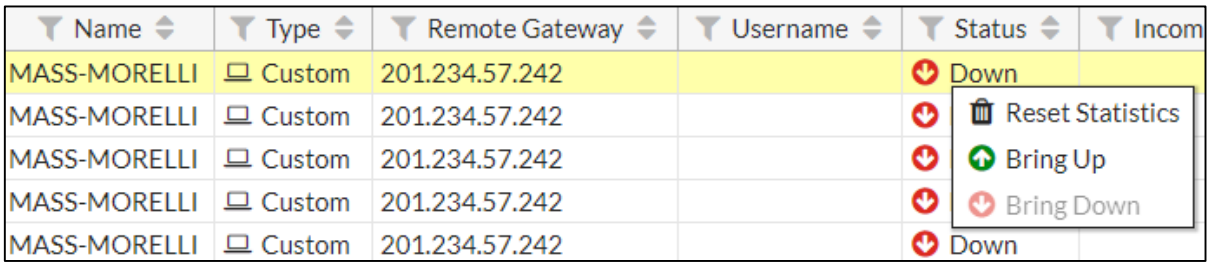

Figura 68. Redes Operando sobre el Túnel VPN IPsec.

3.3.4.2. Configuración de la Red LAN en la Tienda Mass

Ingresamos al menú del Switch Cisco SG 200-08:

Administration / Management Interface / IPv4 Interface.

Asignarle la Red correspondiente, Ip, Máscara y Gateway de administración, esto servirá para poder realizar troubleshooting y a la vez monitoreo del equipo.

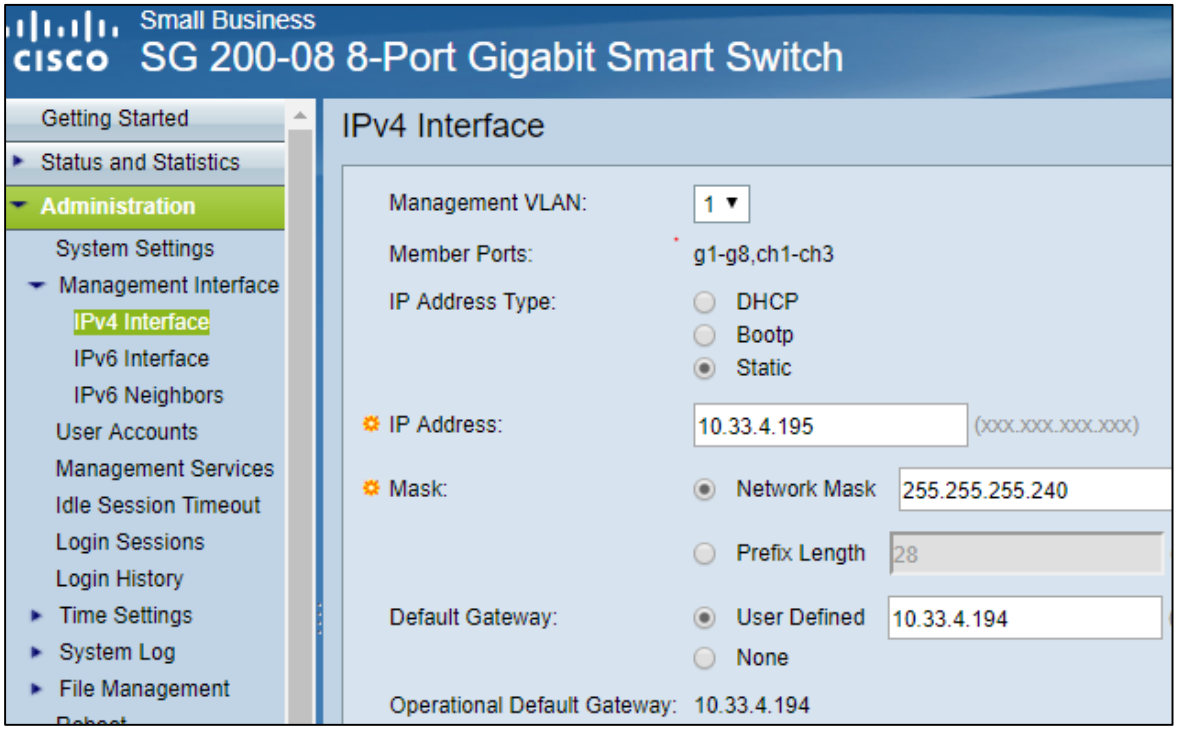

Figura 69. Configuración de la IP/Máscara de Red en el Switch SG 200-08.

En el menú dirigirse a **Port Management / Interface Settings.**

Dejar todos el **PVID (Port Vlan ID)** 1 por defecto.

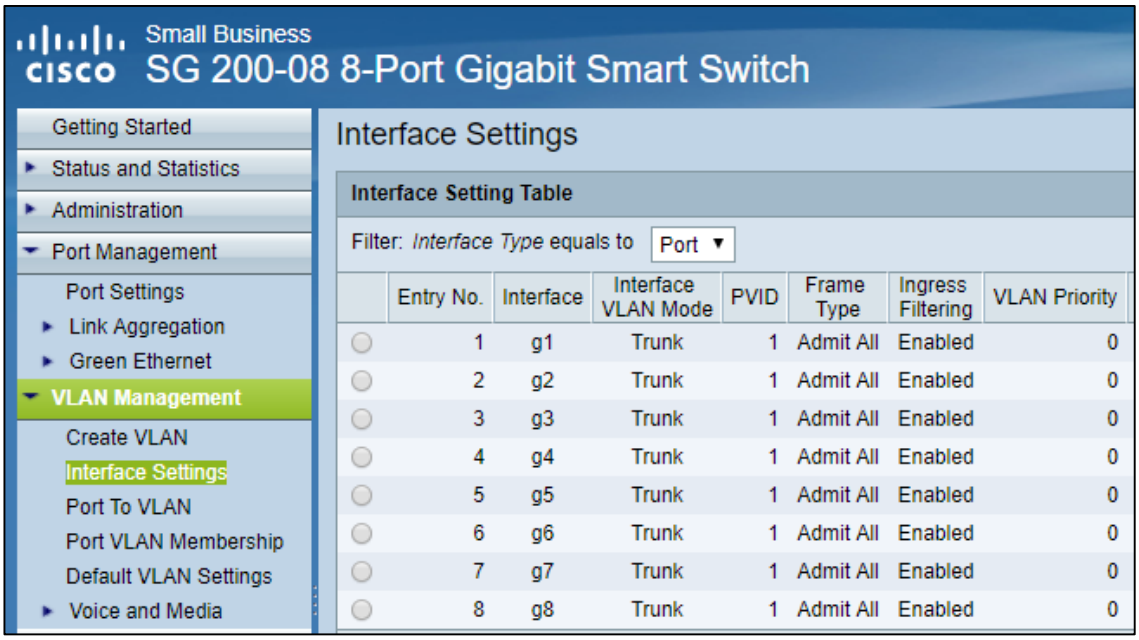

Figura 70. Tabla de Puertos Giga-Ethernet asociados a la VLAN 1.

Conectar los dispositivos a la Red en el orden según nombrado en la etapa de planificación.

Verificar estado de los puertos en el menú **Status and Statistics / Systems Summary.**

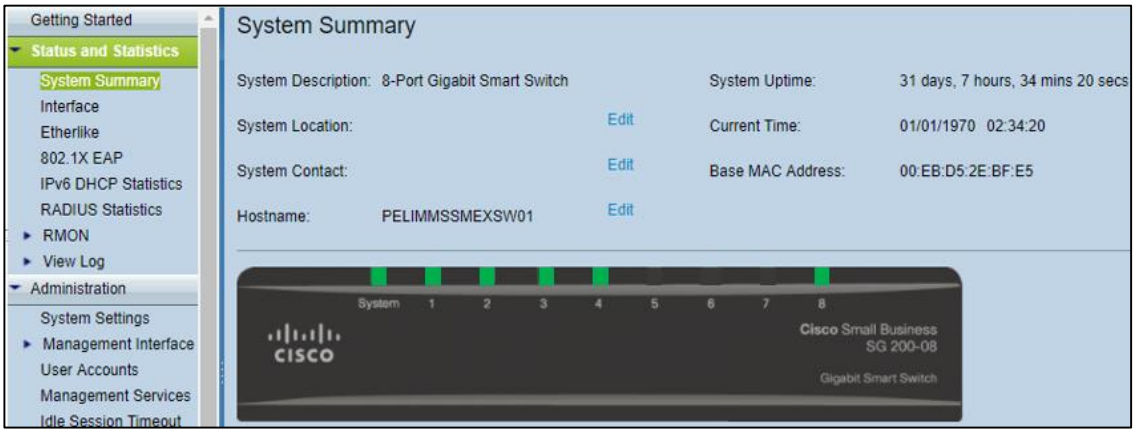

Figura 71. Estatus de puertos en Link Up.

3.3.4.3. Instalación física de los equipos

Se presenta el Gabinete de 6Rus dentro de ella se colocará la bandeja de 1Ru como soporte para el Switch y Firewall.

La conexión de Red se realizará en base a la Tabla N° 31 descrito en la fase de planificación.

Figura 72. Gabinete de 6RUs y Bandeja de 1RU.

La conexión a la energía para los equipos se realizará mediante un supresor de picos conectada a la toma eléctrica situada en la parte superior del gabinete.

Figura 73. Conexión a la energía eléctrica.

Una vez realizado los pasos anteriores dejar cerrada con llave la puerta para prever posibles daños, o manipulación de estos equipos.

Figura 74. Equipos instalados y debidamente conectados.

3.3.5. Fase de Operación

Anuncio de Ruta estática para salida a Internet en la VPN.

Como parte del Monitoreo y Gestión del Servicio de Comunicación implementado se realiza la siguiente configuración en el equipo Switch Core de Morelli esto con fines de mantener la conexión de la comunicación por una Ruta estática permanente.

Ingresamos con el Software SecureCRT y establecemos conexión con el Switch Core mediante la dirección Ip de administración 128.4.1.1 y por el Puerto 22 – SSH.

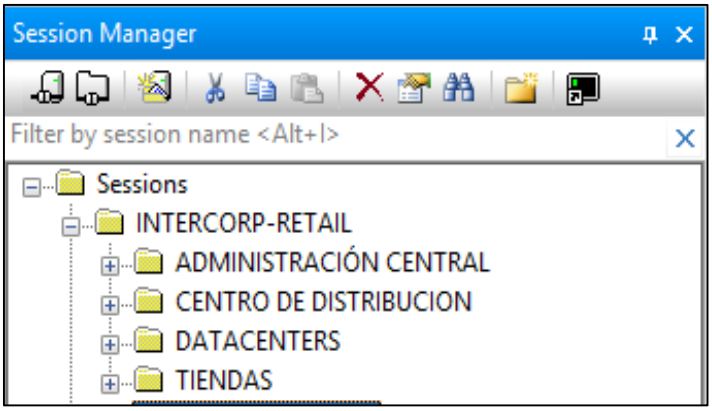

Figura 75. Software de conexiones remotas. Adaptado de “Secure CRT” por Vandyke.com, 2017.

Una vez establecida la conexión ingresar las credenciales para ingresar al equipo, luego habilitar el modo de configuración global en el Switch Core.

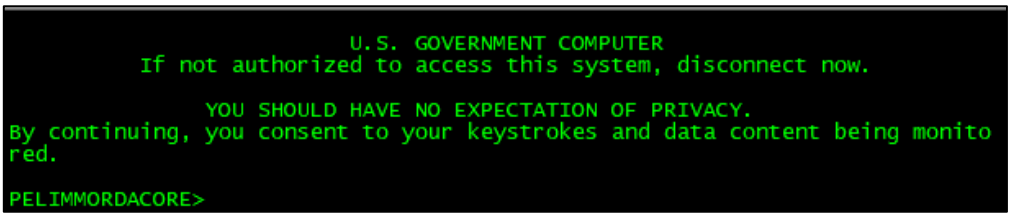

Figura 76. Promt de logeo al Switch Core de Morelli.

Aplicar la siguiente ruta estática en el Switch Core de Morelli

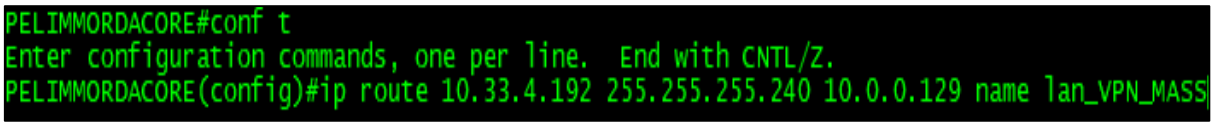

Figura 77. Ruta estática de salida para conocer a la Sub-Red por el Firewall 1500-D.

Descripción lógica de la ruta estática en el Switch Core de Morelli.

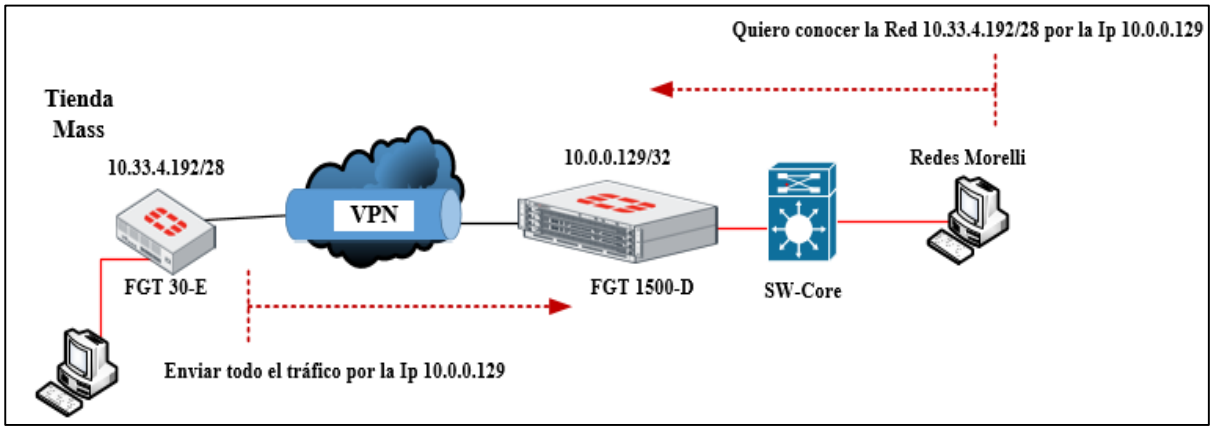

Figura 78. Diagrama Lógico de la ruta estática en el Switch Core.

Monitoreo del Servicio de Comunicación.

Para una resolución de problemas (troubleshooting) se debe mantener una administración y monitoreo constante de la Red de datos, se propone monitorear los equipos con el software de Red PRTG, lo cual brindará alertas de algún desperfecto de la red en tiempo real.

Figura 79. Software de monitoreo de Red. Recuperado de "software PRTG" por Google.com.pe, 2017.

Ingresamos al software de monitoreo PRTG de Supermercados Peruanos.

Figura 80. Monitoreo de la red Supermercados Peruanos.

Una vez dentro nos ubicamos en el grupo **PUNTO DE VENTA,** se verá un árbol de dependencia **SPSA** subdivido en dos grupos **LIMA y PROVINCIA,** ello a su vez en subgrupos tales como: **MASS, PLAZA VEA HÍPER, SUPER, etc.** Según formato de Tienda.

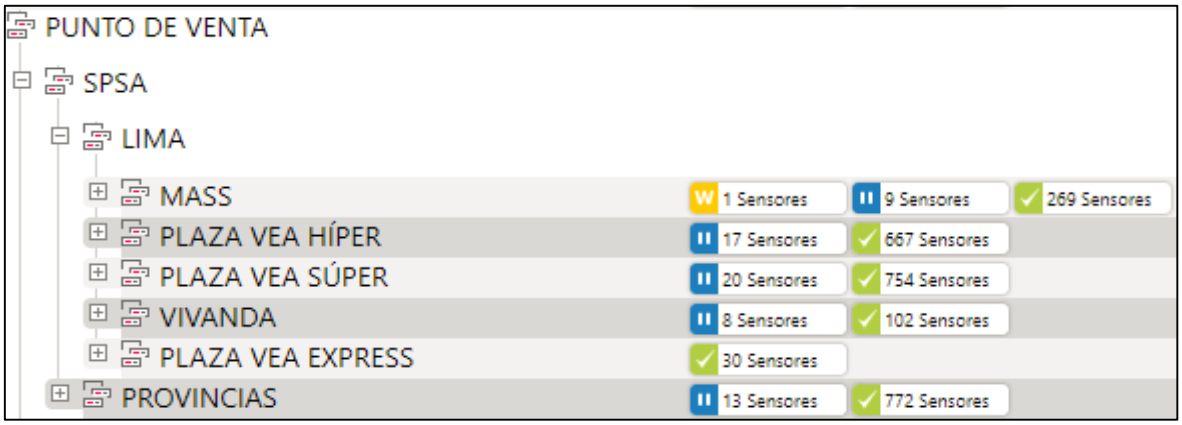

Figura 81. Árbol de dependencias formatos de tiendas.

Nos ubicamos en el subgrupo **MASS**, luego seguiremos desglosando por **DISTRITOS y CONOS** para luego llegar a crear dentro de él el grupo de la tienda al cual se monitoreará el servicio de comunicación.

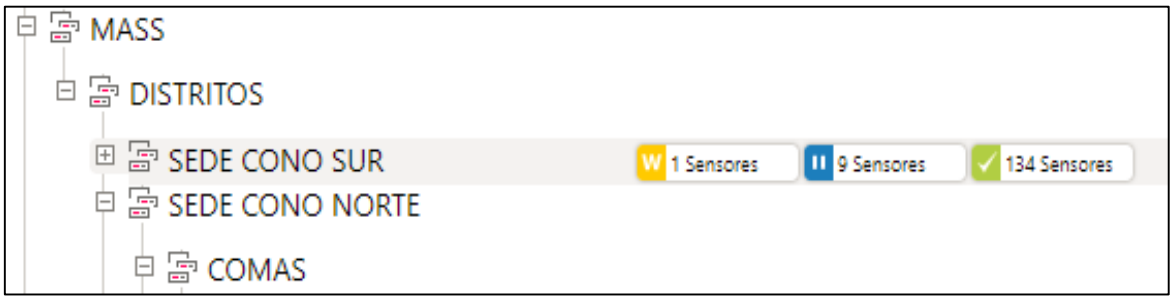

Figura 82. Subgrupos creados para las tiendas Mass según ubicación geográfica.

Creamos la dependencia con nombre del subgrupo **MASS MÉXICO** haciendo referencia al servicio de comunicación implementado, agregamos la dirección IP del dispositivo a Monitorear en este caso el Firewall Fortigate 30-E y el switch Cisco SG200-08.

Figura 83. Monitoreo de red en tiempo real para la tienda Mass México.

3.3.6. Fase de Optimización

Activación de Dectec Viruses

Como se tiene conocimiento es un enlace virtual VPN Ipsec para la transmisión de datos fiable, confiable y seguro, pero no por ello deja de ser vulnerable ante los ataques de virus y demás ataques informáticos, ya que este servicio de comunicación trabaja sobre Internet (Red pública), por ello se requiere habilitar ciertos parámetros que ayuden a bloquear dicho traficó que pueda intersectar en la comunicación del Tunel VPN.

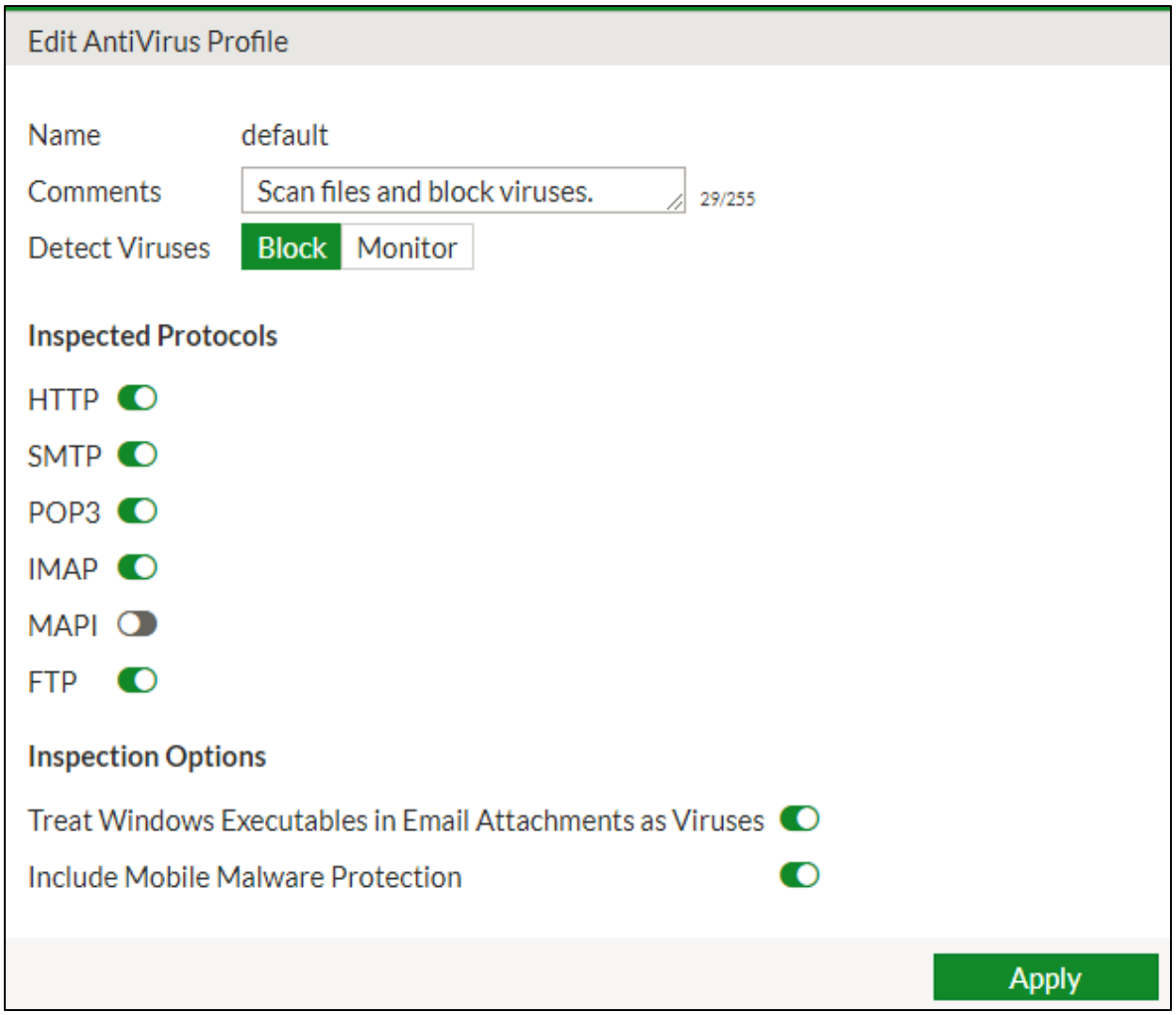

Figura 84. Activación de Detección de virus para los protocolos de comunicación.

Certificado SSL

La inspección de Secure Sockets Layer (SSL) es muy utilizada por FortiGate ello para analizar el tráfico o las sesiones de comunicación que usan SSL para el cifrado, incluido el protocolo HTTPS (443).

Realizar la descarga del Certificado, luego instalar en la PC.

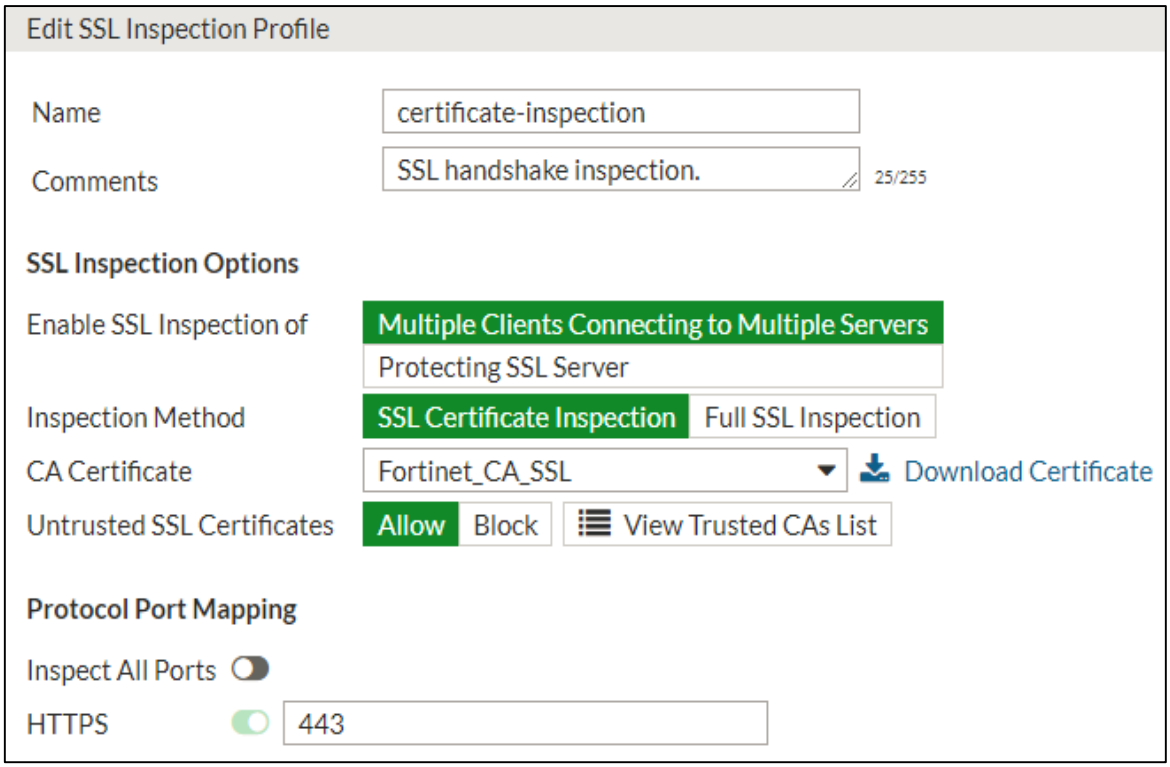

Figura 85. Activación del certificado de inspección SSL para las conexiones seguras.

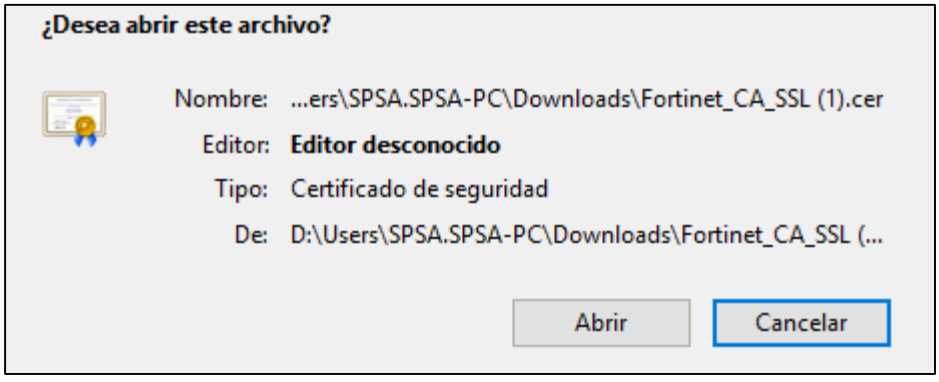

Figura 86. Descarga e instalación del certificado SSL.

CAPÍTULO IV
ANÁLISIS DE RESULTADOS Y CONTRASTACIÓN DE HIPÓTESIS

4.1. POBLACIÓN Y MUESTRA:

4.1.1. Población:

Todos los Servicios de Comunicación en las Tiendas Mass, indeterminado.

4.1.2. Muestra:

En esta investigación se tomó los niveles del Servicio de la Comunicación

N = 30 testeos al Servicio de Comunicación de una Tienda.

4.1.3. NIVEL DE CONFIANZA Y GRADO DE SIGNIFICANCIA:

Para la prueba de hipótesis y los datos que se recolectó para su evaluación, se utilizó los siguientes parámetros:

- ✓ El nivel de confianza será del 95%
- ✓ El nivel de significancia será del 5%

4.2. ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS:

4.2.1. Resultados Genéricos:

I. Modelo de Negocio

I.A. Descripción del negocio.

I.B. Estructura Organizacional.

II. Requerimientos

II.A. Descripción del negocio.

II.B. Identificar y clasificar requerimientos.

III. Fase de Preparación

III.A. Levantamiento de información de la infraestructura de Red.

IV. Fase de Planificación

IV.A. Alcances de la Implementación

IV.B. Requerimientos del Servicio de Comunicación.

V. Fase de Diseño

IV.A. Diseño de Red propuesto.

IV.B. Planeamiento IP.

IV.C. Seguridad de la Red.

VI. Fase de Implementación

V.A. Configuración de la VPN IPsec Site-to-Site en los Firewalls.

V.B. Configuración a nivel LAN del Switch SG 200-08.

V.C. Instalación de la Solución.

VII. Fase de Operación

VII.A. Gestión y Mantenimiento del Servicio del Comunicación.

VIII. Fase de Optimización

VIII.A. Monitoreo del Servicio.

4.2.2. Resultados Específicos:

Se presenta las medidas de los KPIs para la Pre-Prueba y Post-Prueba.

Tabla 32

Resultados de pre-prueba y post-prueba para los, $KPI_1, KPI_2, KPI_3, KPI_4$.

	KPI_1 Tiempo de Latencia del Servicio de Comunicación		KPI_2 Número de Saltos que recorre el paquete de datos		KPI_3 Cantidad de Incidencias registradas semanales		KPI_4 Tiempo de carga al ingresar a los Sistemas Informáticos	
N°	Pre-Prueba	Post-Prueba	Pre-Prueba	Post-Prueba	Pre-Prueba	Post-Prueba	Pre-Prueba	Post-Prueba
1	910	9	6	3	6	2	4	0.07
2	1200	9	6	3	6	1	4	0.07
3	1000	9	6	3	7	1	4	0.09
4	960	12	11	8	5	2	4	0.06
5	980	10	9	6	4	1	4	0.06
6	1150	10	9	6	4	3	4	0.06
7	1400	9	9	6	7	1	5	0.09
8	1430	10	9	6	7	1	5	0.09
9	1500	11	6	3	4	1	4	0.05
10	1380	9	6	3	6	2	6	0.06
11	1510	9	11	8	6	1	4	0.06
12	1400	8	6	3	5	1	5	0.06
13	1110	12	6	3	5	3	6	0.05
14	1100	9	11	8	5	1	4	0.05
15	990	9	9	6	4	2	7	0.06
16	900	9	6	3	4	2	4	0.06
17	1320	10	6	3	6	3	4	0.06
18	1500	8	9	6	4	1	4	0.06
19	1450	10	9	6	7	1	4	0.09
20	1430	10	9	6	4	2	4	0.09
21	1200	8	6	3	4	1	5	0.09
22	1300	8	11	8	4	3	4	0.09
23	1330	12	9	6	7	2	4	0.09
24	1200	9	9	6	6	1	4	0.08
25	1495	10	11	8	6	2	6	0.08
26	1510	10	9	6	5	1	6	0.08
27	1200	8	6	3	4	2	4	0.08
28	1190	9	6	3	4	1	5	0.05
29	920	12	11	8	7	1	7	0.05
30	1500	8	6	3	7	3	7	0.05

Nota: Los datos de la Post-prueba son tomados en base al testeo de la red en la tienda Mass México.

4.2.3. Análisis de Resultados Genéricos:

Tabla 33

Interpretación de resultados de los datos Pre y Post Prueba.

INDICADOR	PRE-PRUEBA (Media: X 1)	POST-PRUEBA (Media X 2)
$\mathbf{KPI_1}$: Tiempo de Latencia del Servicio de Comunicación.	1248.8 milisegundos	9.53 milisegundos
$\mathbf{KPI_2}$: Número de Saltos que recorre el paquete de datos en Red.	8.1 saltos	5.1 saltos
$\mathbf{KPI_3}$: Cantidad de Incidencias registradas semanales.	6.23 incidencias	1.23 incidencias
$\mathbf{KPI_4}$: Tiempo de carga al ingresar a los Sistemas Informáticos.	4.73 minutos	0.07 minutos

Nota: Claro mejoramiento en los tiempos para procesar la información con los sistemas de la empresa.

A. Indicador 1: Tiempo de Latencia del Servicio de Comunicación.

Tabla 34

Resultados obtenidos de la Pre –Prueba y Post- Prueba para el KPI_1.

Pre-Prueba	Post-Prueba		
910	9	9	9
1200	9	9	9
1000	9	9	9
960	12	12	12
980	10	10	10
1150	10	10	10
1400	9	9	9
1430	10	10	10
1500	11	11	11
1380	9	9	9
1510	9	9	9
1400	8	8	8
1110	12	12	12
1100	9	9	9
990	9	9	9
900	9	9	9
1320	10	10	10
1500	8	8	8
1450	10	10	10
1430	10	10	10
1200	8	8	8
1300	8	8	8
1330	12	12	12
1200	9	9	9
1495	10	10	10
1510	10	10	10
1200	8	8	8
1190	9	9	9
920	12	12	12
1500	8	8	8
Promedio	1248,83	9,53	
Meta Planteada		12	
N° Menor a la Meta	17	26	30
% Menor al Promedio	56.67	86.67	100

- ✓ El 56.67 % referente al Tiempo de Latencia por el Servicio de Comunicación en la Post-prueba ha sido menor al Tiempo de Latencia promedio logrado.
- ✓ El 86.67 % del Tiempo de Latencia en el Servicio de Comunicación fueron menores a la meta planteada.
- ✓ El 100 % de los datos obtenidos por el Tiempo de Latencia del Servicio de Comunicación en la Post-prueba fueron notoriamente menores al tiempo promedio en la Pre-prueba.

Tabla 35

Aplicando Estadística Descriptiva Pre-Prueba KPI_1.

Variable	N	Porcentaje	Media	Error estándar de la media	Desv. Est.	Varianza	CoefVar
Pre-prueba KPI_1	30	100	1248.8	38.1	208.7	43551.2	16.71

Variable	Mínimo	Q1	Mediana	Q3	Máximo	Rango	N para moda
Pre-prueba KPI_1	900.0	1075.0	1250.0	1435.0	1510.0	610.0	4

Variable	Asimetría	Curtosis
Pre-prueba KPI_1	-0.29	-1.30

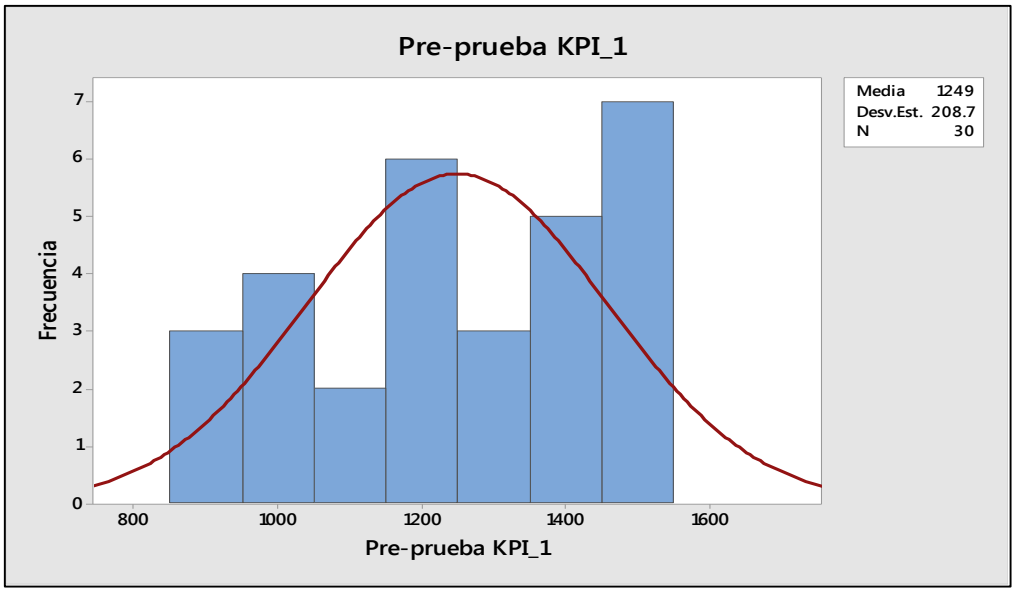

Figura 87. Resumen del tiempo de latencia para el KPI 1 de Pre-prueba.

Tabla 36

Aplicando Estadística Descriptiva Post-Prueba KPI_1:

Variable	N	Porcentaje	Media	Error estándar de la media	Desv .Est.	Varianza	Coef. Var.
Post-prueba KPI_1	30	100	9.533	0.229	1.252	1.568	13.13

Variable	Mínimo	Q1	Mediana	Q3	Máximo	Rango	N para moda
Post-prueba KPI_1	8.000	9.000	9.000	10.000	12.000	4.000	11

Variable	Asimetría	Curtosis
Post-prueba KPI_1	0.77	-0.11

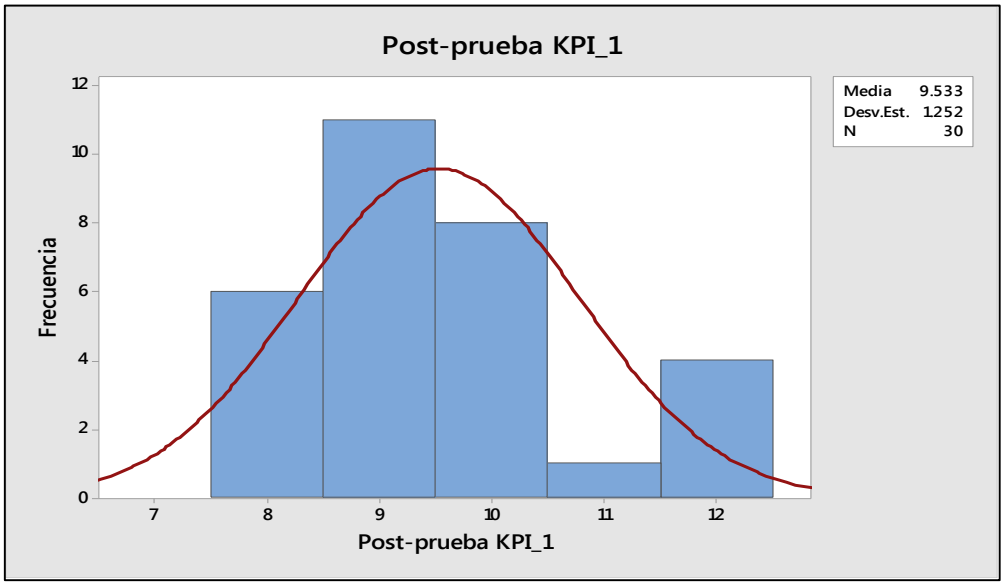

Figura 88. Resumen del tiempo de latencia para el KPI 1 de Post-prueba.

Interpretación

- Se obtuvo como media los milisegundos promedio de latencia del servicio de comunicación 3G con el proveedor Telefónica del Perú, en la Pre-prueba

muestra el valor de 1249 milisegundos, mientras en la Post-prueba el valor fue de 9.533 milisegundos; esto indica una gran diferencia antes y después de la implementación de la Red Privada Virtual.

- Monitoreando la varianza la dispersión de los datos con respecto al Tiempo de Latencia del Servicio de Comunicación, en la Pre-prueba (43551.2) frente a la Post-prueba (1.252) esto demuestra la precisión y el nivel de confianza implementada la Red Privada Virtual, tuvo un impacto favorable ya que disminuyó el número de defectos que esta pueda ocasionar en los nuevos tiempos de latencia del servicio de comunicación en la tienda Mass.
- Con respecto a los cuartiles Q1 y Q3 para la Pre-prueba:
  El 25% de datos es menor que o igual a los 1075.0 milisegundos.
  El 75% de los datos es menor que o igual a los 1435.0 milisegundos.
- Con respecto a los cuartiles Q1 y Q3 para la Post-prueba:
  El 25% de datos es menor que o igual a los 9.000 milisegundos.
  El 75% de los datos es menor que o igual a los 10.000 milisegundos.
- La asimetría en la Pre-prueba fue de -0.29 esto nos indica que existen tiempos de respuesta con latencia muy elevados, lo que es adverso a la asimetría de la Post-prueba con 0.77 ello nos acerca a los tiempos de respuesta con latencia mucho más bajos y aceptables para el servicio de comunicación en la tienda Mass.

B. Indicador: Número de Saltos que recorre el paquete de datos en Red.

Tabla 37.

Resultados obtenidos de la Pre –Prueba y Post- Prueba para el KPI_2.

Pre-Prueba	Post-Prueba		
6	3	3	3
6	3	3	3
6	3	3	3
11	8	8	8
9	6	6	6
9	6	6	6
9	6	6	6
9	6	6	6
6	3	3	3
6	3	3	3
11	8	8	8
6	3	3	3
6	3	3	3
11	8	8	8
9	6	6	6
6	3	3	3
6	3	3	3
9	6	6	6
9	6	6	6
9	6	6	6
6	3	3	3
11	8	8	8
9	6	6	6
9	6	6	6
11	8	8	8
9	6	6	6
6	3	3	3
6	3	3	3
11	8	8	8
6	3	3	3
Promedio	8,10	5,10	
Meta Planteada			12
N° Menor a la Meta		17	26 30
% Menor al Promedio		56.67	86.67 100

- ✓ El 43.33 % referente al Número de Saltos que recorre el paquete de datos en Red en la Post-prueba ha sido menor al promedio logrado.
- ✓ El 80 % del Número de Saltos que recorre el paquete en Red fueron menores a la meta planteada.
- ✓ El 100 % de los datos obtenidos por el Número de Saltos que recorre el paquete de datos en Red en la Post-prueba fueron menores a los saltos promedio en la Pre-prueba.

Tabla 38

Aplicando Estadística Descriptiva Pre-Prueba KPI_2.

Variable	N	Porcentaje	Media	Error estándar de la media	Desv. Est.	Varianza	Coe fVar
Pre-prueba KPI_2	30	100	8.100	0.366	2.006	4.024	24.7

Variable	Mínimo	Q1	Mediana	Q3	Máximo	Rango	N para moda
Pre-prueba KPI_2	6.000	6.000	9.000	9.000	11.000	5.000	13

Variable	Asimetría	Curtosis
Pre-prueba KPI_2	0.16	-1.54

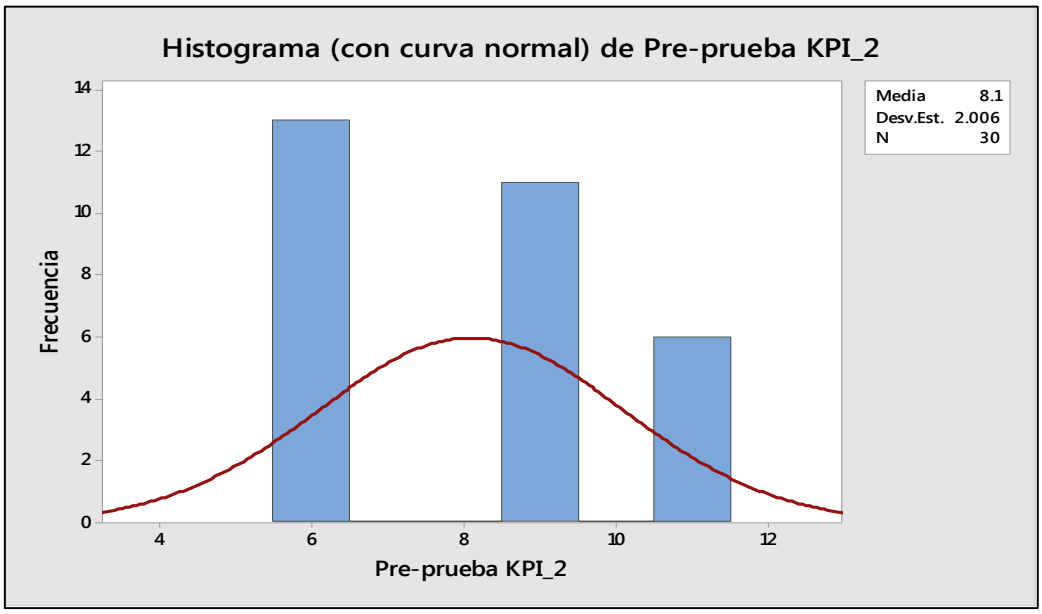

Figura 89. Resumen de número de saltos que recorre el paquete KPI 2 de Pre-prueba.

Tabla 39

Aplicando Estadística Descriptiva Post-Prueba KPI_2.

Variable	N	Porcentaje	Media	Error estándar de la media	Desv .Est.	Varianza	CoefVar
Post-prueba KPI_2	30	100	5.100	0.366	2.006	4.024	39.33

Variable	Mínimo	Q1	Mediana	Q3	Máximo	Rango	N para moda
Post-prueba KPI_2	3.000	3.000	6.000	6.000	8.000	5.000	13

Variable	Asimetría	Curtosis
Post-prueba KPI_2	0.16	-1.54

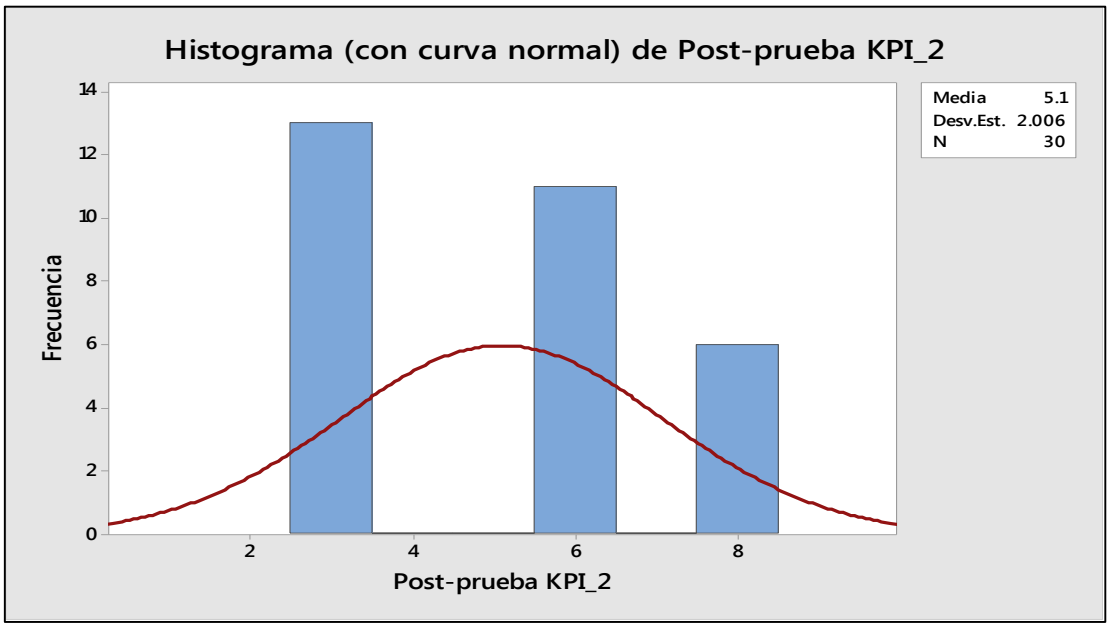

Figura 90. Resumen de número de saltos que recorre el paquete KPI 2 de Post-prueba.

Interpretación

- Se obtuvo como media los promedios que realiza el paquete de datos en la Red del servicio de comunicación 3G con el proveedor Telefónica del Perú, en la

Pre-prueba muestra el valor de 8.1 saltos, mientras en la Post-prueba el valor fue de 5.1 saltos; ello hace referencia a una diferencia antes y después de la implementación de la Red Privada Virtual.

- Monitoreando los datos para la Mediana en la Pre-prueba (9.000) se interpreta que existen valores impares y asimétricos que hacen la volatilidad en lo que concierne al números de saltos del paquete de datos en la Red, por otro en la Post-prueba (6.000) se observa datos simétricos y estables para la cantidad de saltos en Red, haciendo viable la conectividad en la Red Privada Virtual.
- Con respecto a los cuartiles Q1 y Q3 para la Pre-prueba:
  El 25% de datos es menor que o igual a los 6.000 saltos.
  El 75% de los datos es menor que o igual a los 9.000 saltos.
- Con respecto a los cuartiles Q1 y Q3 para la Post-prueba:
  El 25% de datos es menor que o igual a los 3.000 saltos.
  El 75% de los datos es menor que o igual a los 6.000 saltos.
- Se interpreta que hubo una optimización para el número de saltos que recorre el paquete en Red.

C. Indicador: Cantidad de Incidencias registradas semanales.

Tabla 40

Resultados obtenidos de la Pre –Prueba y Post- Prueba para el KPI 3.

Pre-Prueba		Post-Prueba	
6	**2**	**2**	**2**
6	1	1	1
7	1	1	1
5	2	2	2
5	1	1	1
7	3	3	3
7	1	1	1
7	1	1	1
7	1	1	1
6	2	2	2
6	1	1	1
5	1	1	1
5	3	3	3
5	1	1	1
7	2	2	2
7	2	2	2
6	3	3	3
5	1	1	1
7	1	1	1
6	2	2	2
6	1	1	1
7	3	3	3
7	2	2	2
6	1	1	1
6	2	2	2
5	1	1	1
7	2	2	2
7	1	1	1
7	1	1	1
7	3	3	3
Promedio	6,23	1,63	
Meta Planteada		12	
N° Menor a la Meta		16	25	30
% Menor al Promedio		53.33	83.33	100

- ✓ El 53.33 % referente a la cantidad de incidencias registradas semanales en la Post-prueba ha sido menor al promedio logrado.
- ✓ El 83.33 % de la cantidad de incidencias registradas semanales fueron menores a la meta planteada.
- ✓ El 100 % de los datos obtenidos por la cantidad de incidencias registradas semanales en la Post-prueba fueron menores a las incidencias promedio en la Pre-prueba.

Tabla 41

Aplicando Estadística Descriptiva Pre-Prueba KPI_3.

Variable	N	Porcentaje	Media	Error estándar de la media	Desv.Est.	Varianza	Coef Var
Pre-prueba KPI_3	30	100	6.233	0.149	0.817	0.668	13.11

Variable	Mínimo	Q1	Mediana	Q3	Máximo	Rango	N para moda
Pre-prueba KPI_3	5.000	5.75	6.000	7.000	7.000	2.000	14

Variable	Asimetría	Curtosis
Pre-prueba KPI_3	-0.47	-1.33

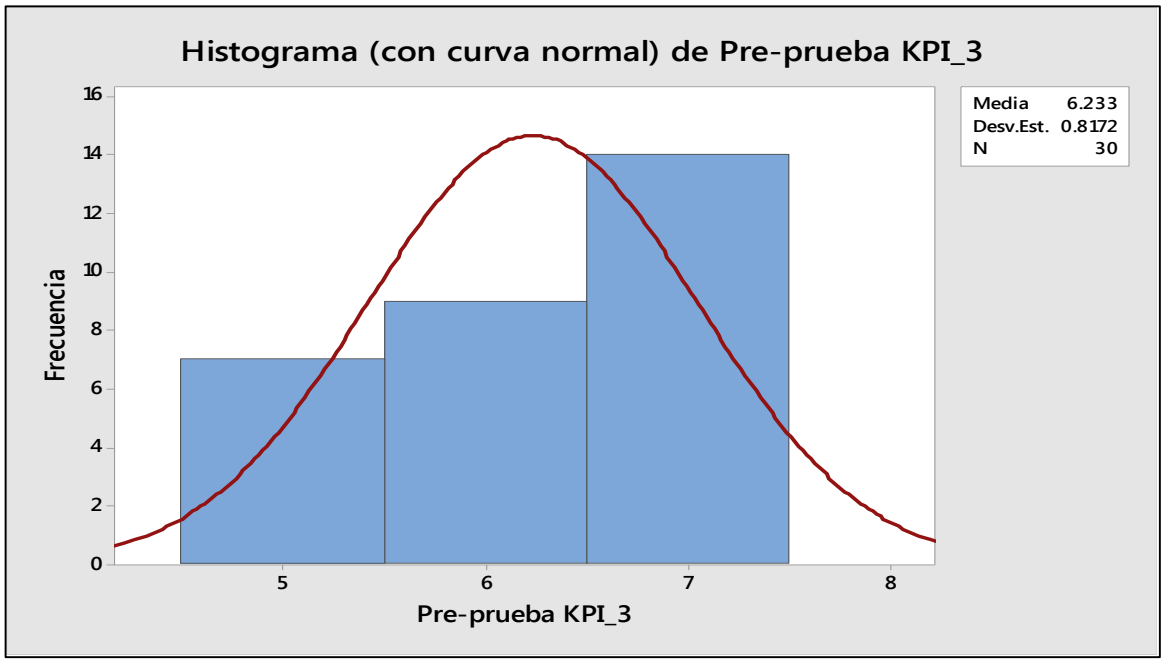

Figura 91. Cantidad de incidencias registradas semanales KPI 3 de Pre-prueba.

Tabla 42

Aplicando Estadística Descriptiva Post-Prueba KPI_3.

Variable	N	Porcentaje	Media	Error estándar de la media	Desv.Est.	Varianza	CoefVar
Post-prueba KPI_3	30	100	1.633	0.140	0.765	0.585	46.83

Variable	Mínimo	Q1	Mediana	Q3	Máximo	Rango	N para moda
Post-prueba KPI_3	1.000	1.000	1.000	2.000	3.000	2.000	16

Variable	Asimetría	Curtosis
Post-prueba KPI_3	0.75	-0.84

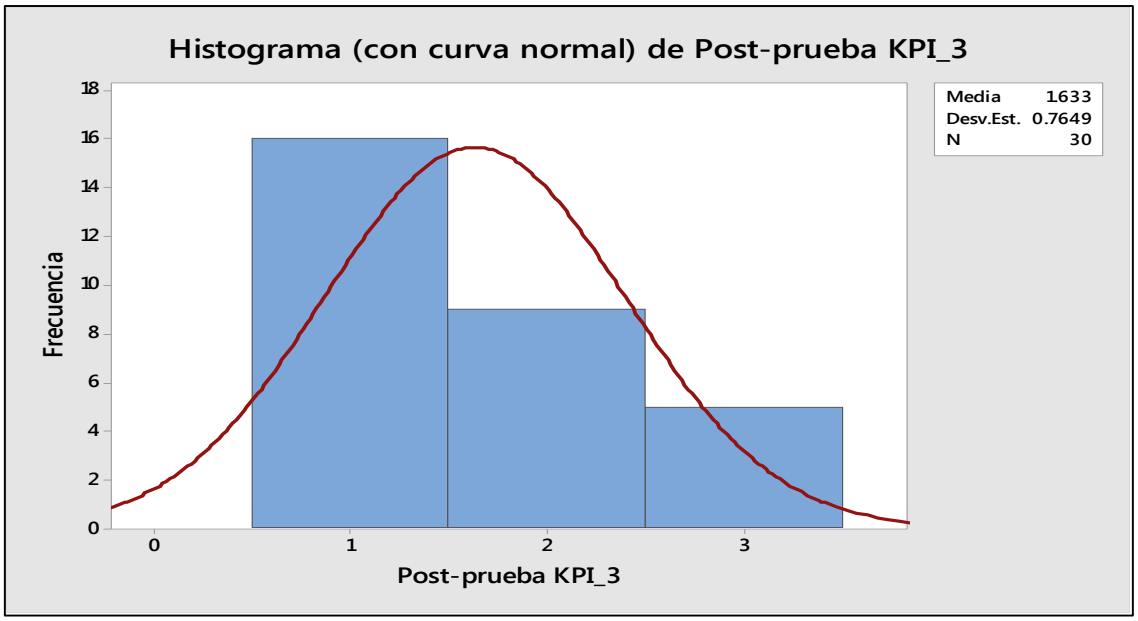

Figura 92. Cantidad de incidencias registradas semanales KPI 3 de Post-prueba.

Interpretación

- Se obtuvo como media la cantidad de incidencias registradas semanalmente a Mesa de ayuda por el servicio de comunicación 3G con el proveedor Telefónica del Perú, en la Pre-prueba muestra el valor de 6.233 incidencias registradas, mientras en la Post-prueba el valor fue de 1.633 incidencias; ello se interpreta que hubo una mejora en el servicio de comunicación antes y después de la implementación de la Red Privada Virtual.
- Monitoreando la varianza la dispersión de los datos con respecto a las incidencias registradas a Mesa de ayuda semanalmente, en la Pre-prueba (0.668) frente a la Post-prueba (0.585) ello demuestra la estabilidad y confiabilidad de la Red Privada Virtual implementada un antes y después, disminuyendo los índices de incidencias semanales para la Tienda el cual se Implementó la solución.
- Con respecto a los cuartiles Q1 y Q3 para la Pre-prueba:
  El 25% de datos es menor que o igual a las 5.750 incidencias registradas.
  El 75% de los datos es menor que o igual a las 7.000 incidencias registradas.
- Con respecto a los cuartiles Q1 y Q3 para la Post-prueba:
  El 25% de datos es menor que o igual a las 1.000 incidencias registradas.
  El 75% de los datos es menor que o igual a las 2.000 incidencias registradas.
- La asimetría en la Pre-prueba fue de -0.47 esto nos indica que existen registros de incidencias consecutivos y de carácter mayor, lo que es adverso a la asimetría de la Post-prueba con 0.75 ello se interpreta que se muestra registros de incidencias muy bajas semanalmente para el servicio de comunicación en la tienda Mass.

D. Indicador: Tiempo de carga al ingresar a los Sistemas Informáticos.

Tabla 43

Resultados obtenidos de la Pre –Prueba y Post- Prueba para el KPI 4

Pre-Prueba	Post-Prueba		
4	0.07	0.07	0.07
4	0.07	0.07	0.07
4	0.09	0.09	0.09
4	0.06	0.06	0.06
4	0.06	0.06	0.06
4	0.06	0.06	0.06
5	0.09	0.09	0.09
5	0.09	0.09	0.09
4	0.05	0.05	0.05
6	0.06	0.06	0.06
4	0.06	0.06	0.06
5	0.06	0.06	0.06
6	0.05	0.05	0.05
4	0.05	0.05	0.05
7	0.06	0.06	0.06
4	0.06	0.06	0.06
4	0.06	0.06	0.06
4	0.06	0.06	0.06
4	0.09	0.09	0.09
4	0.09	0.09	0.09
5	0.09	0.09	0.09
4	0.09	0.09	0.09
4	0.09	0.09	0.09
4	0.08	0.08	0.08
6	0.08	0.08	0.08
6	0.08	0.08	0.08
4	0.08	0.08	0.08
5	0.05	0.05	0.05
7	0.05	0.05	0.05
7	0.05	0.05	0.05
Promedio	4,73	0.07	
Meta Planteada		0.09	
N° Menor a la Meta		16	22	30
% Menor al Promedio		53.33	73.33	100

- ✓ El 53.33 % referente al Tiempo de carga al ingresar a los Sistemas Informáticos en la Post-prueba ha sido menor al promedio logrado.
- ✓ El 73.33 % del Tiempo de carga al ingresar a los Sistemas Informáticos fueron menores a la meta planteada.
- ✓ El 100 % del Tiempo de carga al ingresar a los Sistemas Informáticos en la Post-prueba fueron menores al Tiempo promedio en la Pre-prueba.

Tabla 44

Aplicando Estadística Descriptiva Pre-Prueba KPI_4.

Variable	N	Porcentaje	Media	Error estándar de la media	Desv. Est.	Varianza	Coef Var
Pre-prueba KPI_4	30	100	4.733	0.191	1.048	1.099	22.15

Variable	Mínimo	Q1	Mediana	Q3	Máximo	Rango	N para moda
Pre-prueba KPI_4	4.000	4.000	4.000	5.250	7.000	3.000	18

Variable	Asimetría	Curtosis
Pre-prueba KPI_4	1.16	-0.01

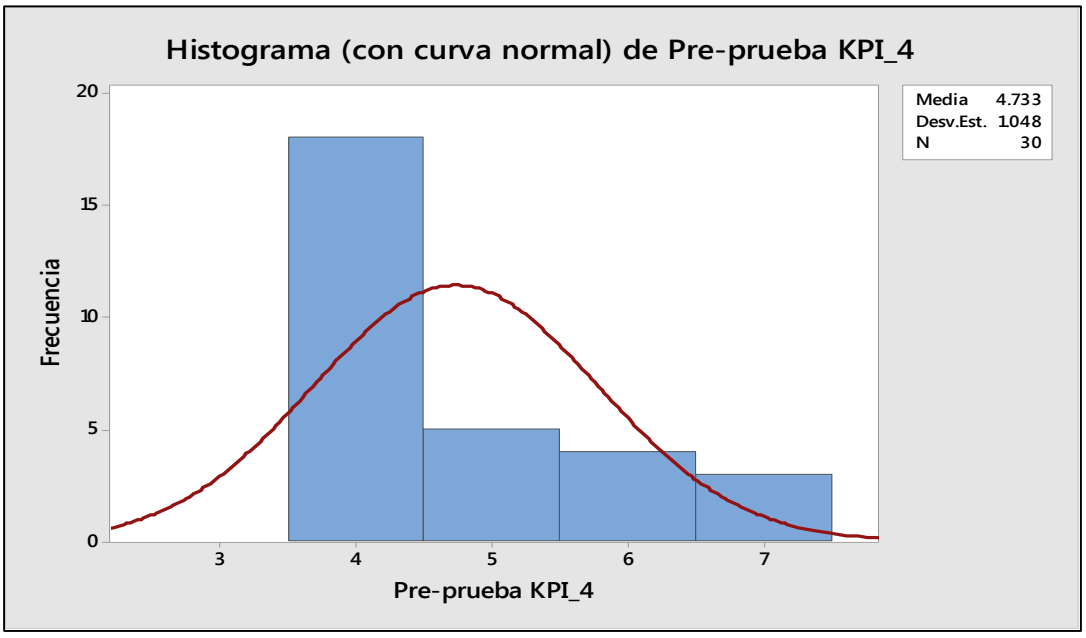

Figura 93. Tiempo de carga para ingresar a los sistemas KPI 4 de Pre-prueba.

Tabla 45

Aplicando Estadística Descriptiva Post-Prueba KPI_4.

Variable	N	Porcentaje	Media	Error estándar de la media	Desv .Est.	Varianza	Coef Var
Post-prueba KPI_4	30	100	0.0693	0.00283	0.01552	0.00024	22.39

Variable	Mínimo	Q1	Mediana	Q3	Máximo	Rango	N para moda
Post-prueba KPI_4	0.05000	0.06000	0.06000	0.09000	0.09000	0.04000	10

Variable	Asimetría	Curtosis
Post-prueba KPI_4	0.24	-1.56

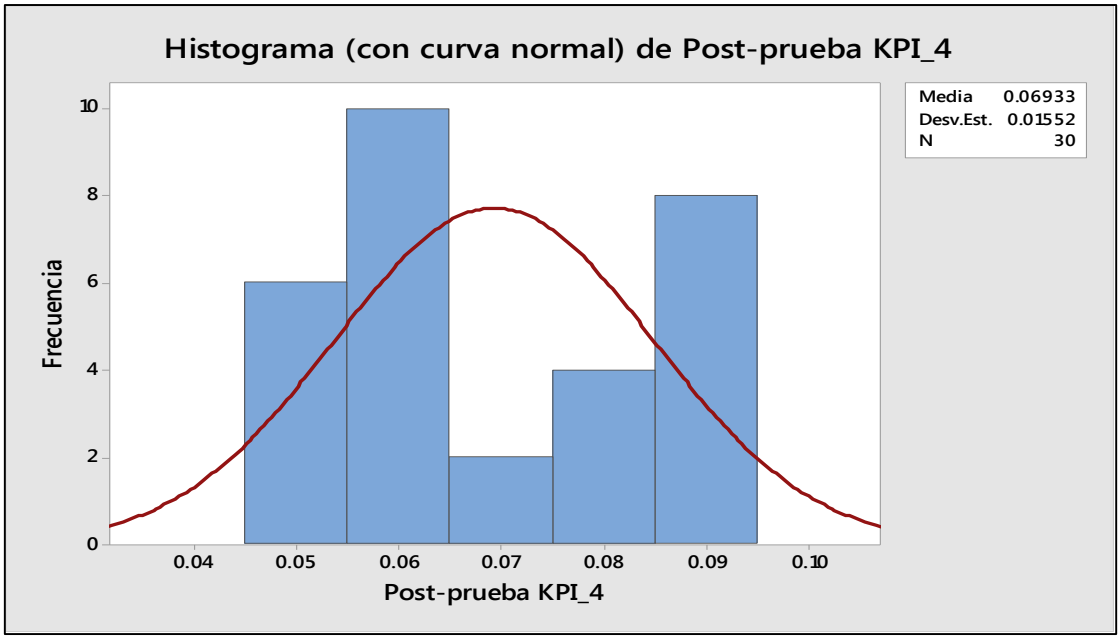

Figura 94. Tiempo de carga para ingresar a los sistemas KPI 4 de Post-prueba.

Interpretación

- Se obtuvo como media el tiempo promedio de carga al ingresar o realizar alguna transacción en los sistemas informáticos para el servicio de comunicación 3G con el proveedor Telefónica del Perú, en la Pre-prueba muestra el valor de 4.733 minutos, mientras en la Post-prueba el valor fue de 0.0693 minutos que, haciendo la conversión se obtiene 6 segundos; ello se interpreta que hubo una mejora en el servicio de comunicación antes y después de la implementación de la Red Privada Virtual.
- Monitoreando la varianza la dispersión de los datos con a los tiempos de carga a los sistemas informáticos, en la Pre-prueba se obtuvo el 1.099 frente a la Post-prueba de 0.00024 ello demuestra ampliamente la variación en los tiempos de carga y transacción haciendo de la Red Privada Virtual un servicio de comunicación eficaz y óptimo para los usuarios quien lo utilizan en la Tienda Mass.
- Con respecto a los cuartiles Q1 y Q3 para la Pre-prueba:
  El 25% de datos es menor que o igual a las 5.000 incidencias registradas.
  El 75% de los datos es menor que o igual a las 2.250 incidencias registradas.
- Con respecto a los cuartiles Q1 y Q3 para la Post-prueba:
  El 25% de datos es menor que o igual a las 0.06000 minutos.
  El 75% de los datos es menor que o igual a las 0.09000 minutos.
- La curtosis en la Pre-prueba fue de -0.01 esto nos indica que existen tiempos de carga para los sistemas informáticos elevado afectando a las ventas directas de la Tienda, lo que es adverso a la curtosis de la Post-prueba con -1.56 ello se interpreta que se muestra tiempos de carga mucho menores haciendo eficaz la operatividad del negocio en la tienda Mass.

4.2.4. CONTRASTACIÓN DE HIPÓTESIS

En este punto de la investigación presentaremos la contrastación de las muestras Pre-Prueba y la Post-Prueba de los KPI's para "La Propuesta de una Red Privada Virtual, mejorará el Servicio de comunicación en las Tiendas Mass para la empresa Supermercados Peruanos S.A."

A. Contrastación para el indicador Tiempo de Latencia del Servicio de Comunicación KPI_1

Se debe validar el impacto que tiene el uso de una Red Privada Virtual en el tiempo de latencia del Servicio de Comunicación, llevado a cabo en la muestra. Se realiza una medición antes de la implementación de la Red Privada Virtual (Pre-Prueba) y otra después de la implementación de la Red Privada Virtual (Post-Prueba). La tabla contiene los Tiempos latencia del servicio para las dos muestras:

Tabla 46

Datos Pre-prueba KPI 1.

Pre-prueba									
910	1200	1000	960	980	1150	1400	1430	1500	1380
1400	1110	1100	990	900	1320	1500	1450	1430	1200
1510	1510	1190	1500	1200	1200	920	1300	1330	1495

Nota: Testeo a la red referente a la latencia en milisegundos antes de la implementación de la VPN.

Tabla 47

Datos Post-prueba KPI 1.

Post-prueba									
9	12	9	9	12	9	10	8	10	9
9	10	10	9	9	10	10	12	10	12
9	10	11	8	9	8	8	9	8	8

Nota: Testeo a la red referente a la latencia en milisegundos después de la implementación de la VPN.

Hi: El uso de una Red Privada Virtual disminuye el tiempo de latencia del Servicio de Comunicación (Post-Prueba) con respecto a la muestra a la que no se aplicó (Pre-Prueba).

Solución

Planteamiento de la Hipótesis

μ1= Media del Tiempo de latencia del Servicio de Comunicación Pre-Prueba.

μ2= Media del Tiempo de latencia del Servicio de Comunicación Post-Prueba.

$$H0: \mu 1 = \mu 2 \qquad Ha: \mu 1 > \mu 2$$

Criterios de decisión

Para las pruebas se utilizó la técnica de Mann-Whitney por ser de dos datos independientes no paramétricos.

Tabla 48

Estadísticas descriptivas KPI 1.

Muestra	N	Mediana
Pre-prueba KPI_1	30	1250
Post-prueba KPI_1	30	9

Tabla 49

Estimación de la diferencia KPI 1.

Diferencia	IC para la diferencia	Confianza lograda
1240	(1181, 1390)	95.16%

Tabla 50

Prueba de la hipótesis KPI 1.

Método	Valor W	Valor p
No ajustado para empates	1365.00	0.000
Ajustado para empates	1365.00	0.000

Decisión Estadística

Puesto que el valor p =0.000 < α =0.05, los resultados proporcionan suficiente evidencia para rechazar la hipótesis nula ($H0$), y la hipótesis alterna (Ha) es cierta. La prueba resulto ser estadísticamente significativa.

B. Contrastación para el indicador Número de Saltos que recorre el paquete de datos en Red KPI_2

Se debe validar el impacto que tiene el uso de una Red Privada Virtual en el Número de Saltos que recorre el paquete de datos en Red, llevado a cabo en la muestra. Se realiza una medición antes de la implementación de la Red Privada Virtual (Pre-Prueba) y otra después de la implementación de la Red Privada Virtual (Post-Prueba). La tabla contiene los números de saltos que recorre el paquete de datos en red para las dos muestras:

Tabla 51

Datos Pre-prueba KPI 2.

Pre-prueba									
6	11	9	6	6	6	9	11	11	6
6	9	9	11	11	6	9	9	9	11
6	9	6	6	9	9	6	9	6	6

Nota: Testeo a la red referente al número de saltos que realiza el paquete para llegar a su destino antes de la implementación de la VPN.

Tabla 52

Datos Post-prueba KPI 2.

Post-prueba									
3	8	6	3	3	3	6	8	8	3
3	6	6	8	8	3	6	6	6	8
3	6	3	3	6	6	3	6	3	3

Nota: Testeo a la red referente al número de saltos que realiza el paquete para llegar a su destino después de la implementación de la VPN.

Hi: El uso de una Red Privada Virtual disminuye los números de saltos que recorre el paquete de datos (Post-Prueba) con respecto a la muestra a la que no se aplicó (Pre-Prueba).

Solución

Planteamiento de la Hipótesis

μ1= Media del Número de Saltos que recorre el paquete de datos en Red Pre-Prueba.

μ2= Media del Número de Saltos que recorre el paquete de datos en Red Post-Prueba.

$$H0: \mu 1 = \mu 2 \qquad Ha: \mu 1 > \mu 2$$

Criterios de decisión

Para las pruebas se utilizó la técnica de Mann-Whitney por ser de dos datos independientes no paramétricos.

Tabla 53

Estadísticas descriptivas KPI 2.

Muestra	N	Mediana
Pre-prueba KPI_2	30	9
Post-prueba KPI_2	30	6

Tabla 54

Estimación de la diferencia KPI 2.

Diferencia	IC para la diferencia	Confianza lograda
3	(3, 3)	95.16%

Tabla 55

Prueba de la hipótesis KPI 2.

Método	Valor W	Valor p
No ajustado para empates	1215.50	0.000
Ajustado para empates	1215.50	0.000

Decisión Estadística:

Puesto que el valor p =0.000 < α =0.05, los resultados proporcionan suficiente evidencia para rechazar la hipótesis nula ($H0$), y la hipótesis alterna (Ha) es cierta. La prueba resulto ser estadísticamente significativa.

C. Contrastación para el indicador Cantidad de Incidencias registradas semanales KPI_3:

Se debe validar el impacto que tiene el uso de una Red Privada Virtual en la cantidad de incidencias registradas semanales, llevado a cabo en la muestra. Se realiza una medición antes de la implementación de la Red Privada Virtual (Pre-Prueba) y otra después de la implementación de la Red Privada Virtual (Post-Prueba). La tabla contiene la cantidad de incidencias registradas semanales para las dos muestras:

Tabla 56

Datos Pre-prueba KPI 3.

Pre-prueba									
6	5	7	6	5	7	7	7	6	7
6	5	7	6	5	6	6	7	5	7
7	7	7	5	7	5	6	6	7	7

Nota: Testeo a la red referente a la cantidad de incidencias antes de la implementación de la VPN.

Tabla 57

Datos Post-prueba KPI 3.

Post-prueba									
2	2	1	2	3	2	1	3	2	1
1	1	1	1	1	3	2	2	1	1
1	3	1	1	2	1	1	1	2	3

Nota: Testeo a la red referente a la cantidad de incidencias después de la implementación de la VPN.

Hi: El uso de una Red Privada Virtual disminuye la cantidad de incidencias registradas semanales (Post-Prueba) con respecto a la muestra a la que no se aplicó (Pre-Prueba).

Solución

Planteamiento de la Hipótesis

μ1= Media del Número de Saltos que recorre el paquete de datos en Red Pre-Prueba.

μ2= Media del Número de Saltos que recorre el paquete de datos en Red Post-Prueba.

$$H0: \mu 1 = \mu 2 \qquad Ha: \mu 1 > \mu$$

Criterios de decisión

Para las pruebas se utilizó la técnica de Mann-Whitney por ser de dos datos independientes no paramétricos.

Tabla 58

Estadísticas descriptivas KPI 3.

Muestra	N	Mediana
Pre-prueba KPI_3	30	6
Post-prueba KPI_3	30	1

Tabla 59

Estimación de la diferencia KPI 3.

Diferencia	IC para la diferencia	Confianza lograda
5	(4, 5)	95.16%

Tabla 60

Prueba de la hipótesis KPI 3.

Método	Valor W	Valor p
No ajustado para empates	1365.00	0.000
Ajustado para empates	1365.00	0.000

Decisión Estadística:

Puesto que el valor p =0.000 < α =0.05, los resultados proporcionan suficiente evidencia para rechazar la hipótesis nula ($H0$), y la hipótesis alterna (Ha) es cierta. La prueba resulto ser estadísticamente significativa.

D. Contrastación para el indicador Tiempo de carga al ingresar a los Sistemas Informáticos KPI_4:

Se debe validar el impacto que tiene el uso de una Red Privada Virtual en tiempo de carga al ingresar a los sistemas informáticos, llevado a cabo en la muestra. Se realiza una medición antes de la implementación de la Red Privada Virtual (Pre-Prueba) y otra después de la implementación de la Red Privada Virtual (Post-Prueba). La tabla contiene los tiempos de carga al ingresar a los sistemas informáticos para las dos muestras:

Tabla 61

Datos Pre--prueba KPI 4.

Pre-prueba									
4	4	5	6	6	4	4	4	6	5
4	4	5	4	4	4	4	4	6	7
4	4	4	5	7	4	5	4	4	7

Nota: Testeo a la red referente al tiempo de carga en minutos de los sistemas informáticos antes de la implementación de la VPN.

Tabla 62

Datos Post--prueba KPI 4.

Post-prueba									
0.07	0.06	0.09	0.06	0.05	0.06	0.09	0.09	0.08	0.05
0.07	0.06	0.09	0.06	0.05	0.06	0.09	0.09	0.08	0.05
0.09	0.06	0.05	0.06	0.06	0.06	0.09	0.08	0.08	0.05

Nota: Testeo a la red referente al tiempo de carga en minutos de los sistemas informáticos después de la implementación de la VPN.

Hi: El uso de una Red Privada Virtual disminuye el tiempo de carga al ingresar a los sistemas informáticos (Post-Prueba) con respecto a la muestra a la que no se aplicó (Pre-Prueba).

Solución:

Planteamiento de la Hipótesis

μ1= Media del Tiempo de carga al ingresar a los Sistemas Informáticos Pre-Prueba.

μ2= Media del Tiempo de carga al ingresar a los Sistemas Informáticos Post-Prueba.

$$H0: \mu 1 = \mu 2 \qquad Ha: \mu 1 > \mu 2$$

Criterios de decisión

Tabla 63

Estadísticas descriptivas KPI 4.

Muestra	N	Mediana
Pre-prueba KPI_4	30	4.00
Post-prueba KPI_4	30	0.06

Tabla 64

Estimación de la diferencia KPI 4.

Diferencia	IC para la diferencia	Confianza lograda
3.95	(3.94, 4.92)	95.16%

Tabla 65

Prueba de la hipótesis KPI 4.

Método	Valor W	Valor p
No ajustado para empates	1365.00	0.000
Ajustado para empates	1365.00	0.000

Decisión Estadística

Puesto que el valor p =0.000 < α =0.05, los resultados proporcionan suficiente evidencia para rechazar la hipótesis nula ($H0$), y la hipótesis alterna (Ha) es cierta. La prueba resulto ser estadísticamente significativa.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

a) La utilización de las fases de la Metodología PPDIOO logró llevar a cabo el diseño la implementación y puesta en marcha del nuevo Servicio de Comunicación, obteniendo como resultado nuestros objetivos específicos.
b) La implementación de una Red Privada Virtual redujo los tiempos de Latencia que anteriormente se tenía con el enlace 3G, pasando en un Intervalo de < 900ms -1500ms > a un intervalo de <10ms - 20ms>, gracias al enlace Virtual diseñado sobre Internet.
c) Se observa que se logró reducir el número de saltos que realiza un Paquete de Datos para llegar a su desino en la Red, anteriormente era un intervalo de < 4 Host - 11 Host > en enlaces de 3G ahora se redujo a 5. Esto mejorará la performance de la integridad del Paquete de Datos, ya que llegará más rápido a su destino.
d) Se denota que ahora con esta nueva propuesta de innovación tecnológica los usuarios pueden ingresar a los sistemas informáticos mucho más rápida, la carga es inmediata, pasó de estar en un intervalo de <4 min – 7min> a menos de 7seg promedio esto ayudará en las actividades y productividad del usuario en Tienda.
e) Con la propuesta de una Red Privada Virtual se demuestra que los Usuarios ya no están reportando a Mesa de Ayuda incidencias por Lentitud o cortes en Sistema, esto es favorable ya que no están ocupándose en solucionar un problema que debería ser automático y visto por el área de Sistemas.
f) Se Logró reducir los costos por el servicio de comunicación exponencialmente apoyando a las ventas diarias y mensuales en Tienda.

5.2. RECOMENDACIONES

a) Se lograría reducir aún más el tiempo de latencia si se adquiriera un enlace de Internet dedicado uno a uno.
b) Se podría explotar aún más las funcionalidades de los equipos FortiGate si se tiene el respaldo de un proveedor que desee brindar servicios en Redes Privadas Virtuales.
c) Para mejorar los niveles del Servicio de Comunicación se requiere un monitoreo y mantenimiento preventivo cada 6 meses del equipo Firewall 30-E esto para prevenir posibles fallas físicas.
d) Se recomienda mantener el Gabinete de comunicaciones ordenada sin acumular cosas u objetos que puedan perjudicar a la funcionalidad de los equipos de telecomunicaciones.
e) Mantener la operatividad de los Servicios de Comunicación Virtuales 24x7.

REFERENCIAS BIBLIOGRÁFICAS

Libros

Guichard et. al. (2002). *MPLS and VPN Architectures*. Recuperado de https://www.safaribooksonline.com/library/view/mpls-and-vpn/1587050811/

Tesis

Arteaga, F. y Huamán, J. (2014). *Sistema de Consultoría On-line aplicando la Metodología PPDIOO para el proceso de Comercialización en la empresa Sabha Perú.* (Tesis para optar el título profesional de Ingeniero de Sistemas). Recuperado de http://repositorio.autonoma.edu.pe/handle/AUTONOMA/128.

Díaz, M. y Vieyra, G. (2015). *Diseño de un modelo de red privada virtual para optimizar la interconexión entre las sucursales de la empresa TERRACARGO S.A.C*. (Tesis para optar el título profesional de Ingeniero Electrónico). Recuperado de http://repositorio.unprg.edu.pe/handle/UNPRG/462.

García, G. (2009). *Propuesta de Migración de la Red NGN de una Operadora Implementada en IP hacia MPLS.* (Tesis para optar el título de Ingeniero de las Telecomunicaciones). Recuperado de http://tesis.pucp.edu.pe/repositorio/handle/123456789/1063

Limari, V. (2004). *Protocolos de Seguridad para Redes Privadas Virtuales (VPN).* (Tesis para optar el título de Ingeniero Electrónico). Recuperado de http://cybertesis.uach.cl/tesis/uach/2004/bmfcil732p/sources/bmfcil732p.pdf

Mar, J. (2016). *Propuesta de implementación de una intranet vía VPN para mejorar la confidencialidad del intercambio de información entre las sedes Lima – Cusco del INEI.* (Tesis para optar al título profesional de Ingeniero de Sistemas). Repositorio de Universidad Andina del Cusco. Recuperado de http://repositorio.uandina.edu.pe/handle/UAC/398

Menéndez, R. (2012). *Estudio del desempeño e implementación de una solución MPLS-VPN sobre múltiples sistemas autónomos.* (Tesis para optar el título de licenciado en Ingeniería de Telecomunicaciones). Recuperado de http://tesis.pucp.edu.pe/repositorio/handle/123456789/1500

Osores, J. (2015). *Rediseño de la infraestructura de Lan Switching de capas 2, 3 y 4 para mejorar el rendimiento de los servicios de red de la Empresa Minero Metalúrgica Doe Run Perú S.R.L Unidad La Oroya*. (Tesis para optar el grado de Ingeniero de Telecomunicaciones). Recuperado de http://repositorio.uncp.edu.pe/handle/UNCP/1134

Morales, L. (2012). *Investigación de Redes VPN con Tecnología MPLS.* (Tesis para optar la Licenciatura en Ingeniería en Sistemas Computacionales). Recuperado de http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/morales_d_l/

Trujillo, E. (2006). *Diseño e Implementación de una VPN en una Empresa Comercializadora utilizando IPSEC.* (Proyecto previo a la obtención del título de Ingeniero en Informática). Repositorio de Escuela Politécnica Nacional, Recuperado de http://bibdigital.epn.edu.ec/handle/15000/214

Pinilla, R. y Sánchez O. (2009). *Implementación de una red privada virtual para el control remoto de equipos de laboratorio*. (Titulación en Ingeniería técnica de Telecomunicaciones, especialidad en telemática). Recuperado de https://upcommons.upc.edu/bitstream/handle/2099.1/8268/memoria.pdf

Pinto de Oliveira, R. (2014). *Infraestructura de Defensa.* (Para el título de profesional de Ingeniero de Sistemas e Informática). Recuperado de http://repositorio.unapiquitos.edu.pe/bitstream/handle/UNAP/4489/Russell_Tesis_Titulo_2014.pdf?sequence=1&isAllowed=y

Sitios web

Cisco Systems. (junio, 2017). *Como las Redes privadas virtuales funcionan*. [Mensaje en un blog]. Recuperado de

https://www.cisco.com/c/es_mx/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html

Gestión. (noviembre, 2017). *La importancia de la transformación digital en las empresas*. [Mensaje en un blog]. Recuperado de https://gestion.pe/panelg/importancia-transformacion-digital-empresas-2205495

Globalgate, (noviembre, 2017). *Soluciones y Productos*. [Mensaje en un blog]. Recuperado de http://fortinet.globalgate.com.ar/index.php/modo/home.

InRetail Perú Corp. (mayo, 2017). *¿Qué aspectos influyen en el crecimiento del sector retail en el Perú?.* [Mensaje en un blog]. Recuperado de https://www.peru-retail.com/aspectos-influyen-crecimiento-sector-retail-peru/

Lavado, G. (2015). *MPLS – Multiprotocol Label Switching –Introducción al protocolo Características*. Slideshare. [Mensaje en un blog]. Recuperado de https://es.slideshare.net/GianpietroLavado/mpls-multiprotocol-label-switching-v13

Vandyke Software (noviembre, 2017*). We listen. Then we make software better*. [Mensaje en un blog]. Recuperado de https://www.vandyke.com/

APÉNDICES

APENDICE I: MATRIZ DE CONSISTENCIA

PROPUESTA DE UNA RED PRIVADA VIRTUAL PARA MEJORAR EL SERVICIO DE COMUNICACIÓN EN LAS TIENDAS MASS PARA LA EMPRESA SUPERMERCADOS PERUANOS S.A.

PROBLEMA PRINCIPAL	OBJETIVO GENERAL	HIPÓTESIS GENERAL	VARIABLES	INDICADORES	ÍNDICES	UNIDAD DE OBSERVACIÓN	
¿En qué Medida la propuesta de Implementación de una Red Privada Virtual, mejorará el Servicio de Comunicación en las tiendas Mass para la Empresa Supermercados Peruanos S.A?	Implementar una Red Privada Virtual para mejorar el Servicio de Comunicación en las tiendas Mass para la Empresa Supermercados Peruanos S.A	El uso de una Red Privada Virtual mejora el Servicio de Comunicación en las tiendas Mass para la Empresa Supermercados Peruanos S.A.	Variable Independiente Red Privada Virtual	Presencia - Ausencia	No, Sí	-	**TIPO DE INVESTIGACIÓN** Aplicada. **NIVEL DE INVESTIGACIÓN** Explicativa. **METÓDOS DE INVESTIGACIÓN** Campo Experimental Documental **POBLACIÓN** Todos los Servicios de Comunicación en las Tiendas Mass. **MUESTRA** 30 testeos al Servicio de Comunicación de una Tienda. **TIPO DE MUESTREO** Intencional (No Aleatorio)
			Variable Dependiente Servicio de Comunicación en las tiendas Mass	Tiempo de latencia del Servicio de Comunicación.	[900 - 1500]	Red de Datos.	
				Número de saltos que recorre el paquete de datos.	[6 - 11]	Red de Datos.	
				Cantidad de incidencias registradas semanales.	[4- 7]	Red de Datos.	
				Tiempo de carga al ingresar a los Sistemas informáticos.	[4- 7]	Red de Datos.	

APENDICE II: MATRIZ DE LA SOLUCIÓN DEL PROBLEMA

DATOS GENERALES	ESTADO DEL ARTE	TECNOLOGÍAS	ARQUITECTURA DE LA SOLUCIÓN
1. Área de Investigación: Propuesta de una Red. **2. Línea de Investigación:** Red Privada Virtual. **3. Título de la tesis:** Propuesta de una Red Privada Virtual para mejorar el Servicio de Comunicación en las tiendas Mass para la Empresa Supermercados Peruanos S.A. **4. Variable Independiente:** Red Privada Virtual. **5. Variable Dependiente:** Servicio de Comunicación en las tiendas Mass.	**1. Modelo de referencia:** **1.1. Justificación:** El Servicio de Comunicación 3G brindados por el proveedor Telefónica del Perú, está afectando de manera que los servicios de la Tienda se ven limitadas por la lentitud e intermitencia que esta presenta, generando retardos en la operatividad, ello se ve reflejada en las bajas utilidades que perciben. **2. Metodologías:** **2.1. Metodología de Desarrollo del Proyecto:** - Fase de Preparación. - Fase de Planificación. - Fase de Diseño. - Fase de Implementación. - Fase de Operación. - Fase de Optimización. **3. Método Seleccionado** No hay método seleccionado. **4. Técnica Seleccionada** No hay método seleccionado. **5. Algoritmo Seleccionado** No hay Algoritmo Seleccionado.	**Plataformas:** **Firewall:** FortiGate 1500-D. **Firewall:** FortiGate 30-E. **Sistema Operativo:** FortiOS. **Versión Propuesta:** 5.4 **Switch:** Cisco SG 200-08P. **Versión Propuesta:** 1.0.6.2 **Enlace de Internet:** Empresarial. **Proveedor:** Indistinto. **Capacidad Requerida:** 2Mbps. **Software:** FortiClient for VPN. **Versión Propuesta:** 5.6 **Laptop:** I3-2330M 2.2GHZ (x64). **Sistema Operativo:** Windows 7. **Versión propuesta:** Windows 7.	La Red Privada Virtual será diseñada en base a la tecnología de Fortinet. En una de las tiendas Mass se instalará el equipo FortiGate 30-E, utilizando los protocolos y estándares de las Redes TCP/IP se hará posible una Comunicación de Red Privada Virtual Punto a Punto con la Sede Central, que cuenta con un equipo Master FortiGate 1500D. Cuando se logre enlazar la tienda mediante Internet el servicio de Comunicación mejorará, por consiguiente se logrará los objetivos específicos.

ANEXOS

ANEXO I:

FICHA DE OBSERVACIÓN: Tiempo de latencia del Servicio de Comunicación.

Fecha	Hora	Tipo Servicio	Tiempo de Latencia del enlace Ida y Vuelta en Milisegundos	Paquetes Enviados	Paquetes Recibidos	Paquetes Perdidos	Paquetes perdidos %
06/10/2017	10:00 AM	Móvil 3G	910	32	20	12	38%
06/10/2017	11:00 AM	Móvil 3G	900	32	15	17	53%
06/10/2017	12:00 PM	Móvil 3G	850	32	18	14	44%
09/10/2017	6:00 PM	Móvil 3G	560	32	10	22	69%
09/10/2017	2:00 PM	Móvil 3G	1000	32	20	12	38%
09/10/2017	3:00 PM	Móvil 3G	1050	32	15	17	53%
14/10/2017	4:00 PM	Móvil 3G	1100	32	18	14	44%
14/10/2017	11:00 AM	Móvil 3G	1300	32	10	22	69%
14/10/2017	12:00 PM	Móvil 3G	1400	32	20	12	38%
17/10/2017	6:00 PM	Móvil 3G	990	32	12	20	63%
17/10/2017	2:00 PM	Móvil 3G	1100	32	15	17	53%
21/10/2017	3:00 PM	Móvil 3G	1400	32	15	17	53%
21/10/2017	10:00 PM	Móvil 3G	1800	32	18	14	44%
23/10/2017	11:00 PM	Móvil 3G	1950	32	20	12	38%
23/10/2017	12:00 AM	Móvil 3G	1950	32	17	15	47%
23/10/2017	6:00 PM	Móvil 3G	1800	32	10	22	69%
28/10/2017	12:00 PM	Móvil 3G	1890	32	20	12	38%
28/10/2017	4:00 PM	Móvil 3G	1400	32	12	20	63%
28/10/2017	11:00 AM	Móvil 3G	900	32	15	17	53%
01/11/2017	12:00 PM	Móvil 3G	900	32	15	17	53%
01/11/2017	6:00 PM	Móvil 3G	890	32	18	14	44%
01/11/2017	2:00 PM	Móvil 3G	700	32	10	22	69%
06/11/2017	4:00 PM	Móvil 3G	1900	32	10	22	69%
06/11/2017	11:00 AM	Móvil 3G	1850	32	20	12	38%
06/11/2017	12:00 PM	Móvil 3G	1350	32	12	20	63%
11/11/2017	1:00 PM	Móvil 3G	1350	32	15	17	53%
11/11/2017	2:00 PM	Móvil 3G	1450	32	15	17	53%
11/11/2017	3:00 PM	Móvil 3G	1500	32	18	14	44%
14/11/2017	2:00 PM	Móvil 3G	1550	32	20	12	38%
14/11/2017	3:00 PM	Móvil 3G	990	32	17	15	47%

ANEXO II.

FICHA DE OBSERVACIÓN: Número de Saltos que recorre el Paquete de Datos para llegar a su destino.

Fecha	Hora	Tipo Servicio de Comunicación	Traza sobre caminos de 30 Saltos como máximo	Servicio al cual se establece la comunicación
06/10/2017	10:00 AM	Móvil 3G	11	Servidor Outlook
07/10/2017	11:00 AM	Móvil 3G	6	Servidores DC Morelli
08/10/2017	12:00 PM	Móvil 3G	9	Servidores DC Holguín
09/10/2017	6:00 PM	Móvil 3G	11	Servidor Outlook
10/10/2017	2:00 PM	Móvil 3G	6	Servidores DC Morelli
13/10/2017	3:00 PM	Móvil 3G	6	Servidores DC Holguín
14/10/2017	4:00 PM	Móvil 3G	11	Servidor Outlook
15/10/2017	11:00 AM	Móvil 3G	6	Servidores DC Morelli
16/10/2017	12:00 PM	Móvil 3G	9	Servidores DC Holguín
17/10/2017	6:00 PM	Móvil 3G	11	Servidor Outlook
20/10/2017	2:00 PM	Móvil 3G	9	Servidores DC Holguín
21/10/2017	3:00 PM	Móvil 3G	6	Servidores DC IBM
22/10/2017	10:00 PM	Móvil 3G	6	Servidores DC Morelli
23/10/2017	11:00 PM	Móvil 3G	11	Servidor Outlook
24/10/2017	12:00 AM	Móvil 3G	6	Servidores DC IBM
27/10/2017	6:00 PM	Móvil 3G	6	Servidor Outlook
28/10/2017	12:00 PM	Móvil 3G	9	Servidores DC IBM
29/10/2017	4:00 PM	Móvil 3G	9	Servidores DC Morelli
30/10/2017	11:00 AM	Móvil 3G	9	Servidores DC Holguín
01/11/2017	12:00 PM	Móvil 3G	9	Servidores DC IBM
04/11/2017	6:00 PM	Móvil 3G	6	Servidor Outlook
05/11/2017	2:00 PM	Móvil 3G	6	Servidores DC IBM
06/11/2017	4:00 PM	Móvil 3G	9	Servidores DC Morelli
07/11/2017	11:00 AM	Móvil 3G	8	Servidores DC Holguín
08/11/2017	12:00 PM	Móvil 3G	11	Servidores DC Holguín
11/11/2017	1:00 PM	Móvil 3G	6	Servidor Outlook
12/11/2017	2:00 PM	Móvil 3G	6	Servidores DC IBM
13/11/2017	3:00 PM	Móvil 3G	9	Servidores DC Morelli
14/11/2017	2:00 PM	Móvil 3G	9	Servidores DC Holguín
15/11/2017	3:00 PM	Móvil 3G	11	Servidor Outlook

ANEXO III.

FICHA DE OBSERVACIÓN: Tiempo de Carga para ingresar o realizar alguna transacción en los Sistemas Informáticos.

Fecha	Hora	Tipo Servicio	Tiempo en Minutos al Realizar la carga de los Sistemas Informáticos		Tiempo en Minutos al Realizar una consulta o transacción en los Sistemas Informáticos	
			Sistemas de Escritorio	Sistemas Web	Sistemas de Escritorio	Sistemas Web
06/10/2017	10:00 AM	Móvil 3G	4	3	6	7
07/10/2017	11:00 AM	Móvil 3G	5	4	5	5
08/10/2017	12:00 PM	Móvil 3G	3	3	3	3
09/10/2017	6:00 PM	Móvil 3G	5	4	5	4
10/10/2017	2:00 PM	Móvil 3G	3	4	3	4
13/10/2017	3:00 PM	Móvil 3G	5	5	7	5
14/10/2017	4:00 PM	Móvil 3G	5	4	5	4
15/10/2017	11:00 AM	Móvil 3G	5	4	5	4
16/10/2017	12:00 PM	Móvil 3G	3	3	3	7
17/10/2017	6:00 PM	Móvil 3G	5	4	5	4
20/10/2017	2:00 PM	Móvil 3G	3	4	3	3
21/10/2017	3:00 PM	Móvil 3G	5	5	5	4
22/10/2017	10:00 PM	Móvil 3G	5	4	3	4
23/10/2017	11:00 PM	Móvil 3G	5	4	7	5
24/10/2017	12:00 AM	Móvil 3G	3	3	5	4
27/10/2017	6:00 PM	Móvil 3G	5	4	5	4
28/10/2017	12:00 PM	Móvil 3G	3	4	3	7
29/10/2017	4:00 PM	Móvil 3G	5	5	5	4
30/10/2017	11:00 AM	Móvil 3G	5	4	3	3
01/11/2017	12:00 PM	Móvil 3G	5	4	5	4
04/11/2017	6:00 PM	Móvil 3G	3	3	3	4
05/11/2017	2:00 PM	Móvil 3G	5	4	7	5
06/11/2017	4:00 PM	Móvil 3G	3	4	3	3
07/11/2017	11:00 AM	Móvil 3G	5	5	5	4
08/11/2017	12:00 PM	Móvil 3G	5	4	3	4
11/11/2017	1:00 PM	Móvil 3G	3	3	7	5
12/11/2017	2:00 PM	Móvil 3G	5	4	5	4
13/11/2017	3:00 PM	Móvil 3G	3	4	5	4
14/11/2017	2:00 PM	Móvil 3G	5	5	3	7
15/11/2017	3:00 PM	Móvil 3G	5	4	5	4

ANEXO IV.

FICHA DE OBSERVACIÓN: Incidencias reportadas a Mesa de Ayuda por Lentitud o Intermitencia en el Servicio de Comunicación.

Fecha	Hora	Tipo Servicio	Tipo de Incidencia			Impacto
			Intermitencia	Lentitud	Caída Parcial	
06/10/2017	10:00 AM	Móvil 3G	X	X		Medio
07/10/2017	11:00 AM	Móvil 3G	X		X	Alto
08/10/2017	12:00 PM	Móvil 3G	X		X	Alto
09/10/2017	6:00 PM	Móvil 3G	X	X		Medio
10/10/2017	2:00 PM	Móvil 3G	X	X		Medio
13/10/2017	3:00 PM	Móvil 3G	X	X		Medio
14/10/2017	4:00 PM	Móvil 3G	X	X		Medio
15/10/2017	11:00 AM	Móvil 3G	X	X		Medio
16/10/2017	12:00 PM	Móvil 3G	X		X	Alto
17/10/2017	6:00 PM	Móvil 3G	X		X	Alto
20/10/2017	2:00 PM	Móvil 3G		X		Medio
21/10/2017	3:00 PM	Móvil 3G		X		Medio
22/10/2017	10:00 PM	Móvil 3G		X		Medio
23/10/2017	11:00 PM	Móvil 3G		X		Medio
24/10/2017	12:00 AM	Móvil 3G	X	X		Medio
27/10/2017	6:00 PM	Móvil 3G		X		Medio
28/10/2017	12:00 PM	Móvil 3G		X		Medio
29/10/2017	4:00 PM	Móvil 3G	X	X		Medio
30/10/2017	11:00 AM	Móvil 3G	X		X	Alto
01/11/2017	12:00 PM	Móvil 3G	X		X	Alto
04/11/2017	6:00 PM	Móvil 3G	X		X	Alto
05/11/2017	2:00 PM	Móvil 3G	X	X		Medio
06/11/2017	4:00 PM	Móvil 3G		X		Medio
07/11/2017	11:00 AM	Móvil 3G		X		Medio
08/11/2017	12:00 PM	Móvil 3G	X	X		Medio
11/11/2017	1:00 PM	Móvil 3G	X		X	Alto
12/11/2017	2:00 PM	Móvil 3G	X	X		Medio
13/11/2017	3:00 PM	Móvil 3G	X		X	Alto
14/11/2017	2:00 PM	Móvil 3G	X		X	Alto
15/11/2017	3:00 PM	Móvil 3G	X	X		Medio

ANEXO V. Acta de conformidad del Servicio de Comunicación Implementado**.**

Supermercados Peruanos SA

ACTA DE CONFORMIDAD DEL SERVICIO

EJECUTOR	:	Renato Espinoza Chipane.
ÁREA	:	Redes y Telecomunicaciones.
GERENCIA	:	Tecnología.
DESCRIPCION DEL SERVICIO	:	Habilitación del Servicio de Comunicación VPN.

Mediante el presente documento, se deja constancia que se ha recibido a satisfacción el trabajo del Sr. César Renato Espinoza Chipane - Especialista de Redes y Telecomunicaciones el Servicio de Comunicación por VPN para la tienda Mass México.

Comas, 06 de Enero del 2018

SUPERMERCADOS PERUANOS S.A.
JOSE L. AMPUERO HUAMAN
ADMINISTRADOR DE TIENDA

SUPERMERCADOS PERUANOS S.A.
MASS MEXICO

JOSE LUIS AMPUERO HUAMÁN.
Administrador Mass México

GLOSARIO DE TÉRMINOS

A

Americatel Corp.: Es la empresa proveedora de servicios de telecomunicaciones de habla hispana más grande de los Estados Unidos.

América Móvil S.A.: Es una empresa Mexicana de Telecomunicaciones con presencia en 18 países de América, Con Más De 260 Millones de usuarios, y actualmente la cuarta compañía de Telecomunicaciones más grande e importante del Mundo.

B

BGP: En telecomunicaciones, el protocolo de puerta de enlace de frontera o BGP es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos.

C

Caja: Una caja registradora es un aparato mecánico o electrónico que permite calcular y registrar transacciones comerciales, e incluye un cajón para guardar dinero.

CPE: Customer Premises Equipment (Equipo Local el Cliente) un término de telecomunicaciones usado tanto en interiores como en exteriores para originar, encaminar o terminar una comunicación.

D

Desktop: Computadora de escritorio u ordenador de sobremesa es un tipo de computadora personal, diseñada y fabricada para ser instalada en una ubicación fija, como un escritorio o mesa

E

Estándar: es el proceso de elaborar, aplicar y mejorar las normas que se aplican a distintas actividades científicas, industriales o económicas, con el fin de ordenarlas y mejorarlas.

Ethernet: Es un estándar de redes de área local para computadores con acceso al medio por detección de la onda portadora y con detección de colisiones. Su nombre viene del concepto físico de ethernet.

F

FastEthernet: Ethernet de alta velocidad es el nombre de una serie de estándares de IEEE de redes Ethernet de 100 Mbps.

Firewall: Comúnmente llamado cortafuegos, es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

G

GigaEthernet: Gigabit Ethernet, también conocida como GigaE, es una ampliación del estándar Ethernet que consigue una capacidad de transmisión de 1 gigabit por segundo, correspondientes a unos 1000 Mbps.

I

Internet: Es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, lo cual garantiza que las redes físicas heterogéneas que la componen formen una red lógica única de alcance mundial.

Iteratividad: Acto de repetir un proceso con la intención de alcanzar una meta deseada, objetivo o resultado.

L

LAN: Es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.

Latencia: En redes informáticas de datos la latencia es la suma de retardos temporales dentro de una red. Un retardo es producido por la demora en la propagación y transmisión de paquetes dentro de la red.

M

Mbps: Un megabit por segundo es una unidad que se usa para cuantificar un caudal de datos equivalente a 1000 kb/s.

Módem: Dispositivo que convierte señales digitales en analógicas, o viceversa, para poder ser transmitidas a través de líneas de teléfono, cables coaxiales, fibras ópticas y microondas; conectado a una computadora, permite la comunicación con otra computadora por vía telefónica.

MPLS: La conmutación de etiquetas multiprotocolo o MPLS es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI

O

OSI: El modelo de interconexión de sistemas abiertos, más conocido como “modelo OSI”, es un modelo de referencia para los protocolos de la red de arquitectura en capas, creado en el año 1980 por la Organización Internacional de Normalización.

P

Paquete de datos: Es cada uno de los bloques en que se divide la información para enviar, en el nivel de red.

Protocolo: En informática y telecomunicación, un protocolo de comunicaciones es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir.

PE: Provider Edge (Enrutador de Borde) es un enrutador entre el área de un proveedor de servicios de red y las áreas administradas por otros proveedores de red. Un proveedor de red suele ser también un proveedor de servicios de Internet (o solo eso).

Q

QoS: Calidad de Servicio es el rendimiento promedio de una red de telefonía o de computadoras, particularmente el rendimiento visto por los usuarios de la red.

R

Routing: El encaminamiento, enrutamiento o ruteo es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad.

S

Sub-Red: es un rango de direcciones lógicas. Cuando una red de computadoras se vuelve muy grande, conviene dividirla en subredes, por los siguientes motivos: Reducir el tamaño de los dominios de broadcast.

Swiching: Conmutador es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI.

T

Telefonía Móvil 3G Es la abreviación de tercera generación de transmisión d
y datos a través de telefonía móvil mediante UMTS. Los servicios asociados con la tercera generación proporcionan la posibilidad de transferir voz y datos no-voz.

Telefónica S.A.: Es una empresa multinacional española de telecomunicaciones, con sede central en Madrid, España, situada como la compañía de telecomunicaciones más importante de Europa y la quinta del mundo

Topología: La topología de red se define como el mapa físico o lógico de una red para intercambiar datos. En otras palabras, es la forma en que está diseñada la red, sea en el plano físico o lógico.

Tracert: Traceroute es una consola de diagnóstico que permite seguir la pista de los paquetes que vienen desde un host.

V

VoIP: Voz sobre protocolo de internet o Voz por protocolo de internet, también llamado voz sobre IP, voz IP, vozIP o VoIP, es un conjunto de recursos que hacen posible que la señal de voz viaje a través de Internet empleando el protocolo IP.

VLAN: Acrónimo de virtual LAN, es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física.

VPN: Una red privada virtual, en inglés: Virtual Private Network es una tecnología de red de computadoras que permite una extensión segura de la red de área local sobre una red pública o no controlada como Internet.

W

WAN: Una red de área amplia, es una red de computadoras que une varias redes locales, aunque sus miembros no estén todos en una misma ubicación física.