UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

FACULTAD DE INGENIERIA

**PROGRAMA ACADÉMICO DE INGENIERÍA DE REDES Y
COMUNICACIONES**

Diseño de una red de comunicación VPN sobre internet para un Distribuidor

Autorizado de Claro basado en el RFC 2764

TESIS

Para optar el título profesional de Ingeniero de Redes y Comunicaciones

AUTOR

Martel Velasquez, Victor Ronald (0000-0001-9042-789X)

ASESOR

Seminario García, Hernán (0000-0001-6971-355X)

Lima, 3 de abril de 2019

DEDICATORIA

Dedico esta tesis primeramente a Dios, que fue quien me permitió culminarla con éxito, en donde pude entender y valorar cada una de las bendiciones con las cuales Él me rodea.

Gracias a Dios por mi hijo Joaquin, que más que el motor de mi vida fue parte muy importante de lo que hoy puedo presentar como tesis, gracias a él por cada palabra de apoyo, gracias por cada momento en familia sacrificado para ser invertido en el desarrollo de esta, gracias por entender que el éxito demanda algunos sacrificios y que el compartir tiempo con ellos, hacia parte de estos.

A mi hijo dedico esta tesis, a él dedico todas las bendiciones que de parte de Dios vendrán a nuestras vidas como recompensa de tanta dedicación, trabajo y esfuerzo por salir adelante.

RESUMEN

El presente proyecto sobre redes de comunicación VPN sobre internet nos muestra una guía de configuraciones necesarias por requisitos en base al RFC 2764 incluyendo las funcionalidades de la red que permitirá ejecutar las acciones requeridas para agilizar los procesos de negocio mediante un eficiente uso de los recursos TI para la disponibilidad de la información.

Actualmente las empresas desean tener presencia en nuevos mercados, por lo que se expanden a nuevas sucursales en distintos distritos y hasta en el interior del país lo que origina la necesidad de mantenerse conectados en todo momento de manera segura, confiable, y sobre todo a un costo aceptable entre todos sus locales con el fin de compartir información que les permita tomar decisiones en tiempo real.

La solución consiste en el diseño de una red de comunicación mediante redes privadas virtuales entre sus locales con el fin de optimizar recursos y agilizar las transacciones diarias propias del giro del negocio, para lo cual el eje principal de la solución es la interconexión de la sede principal y sus sucursales, es así que se consideraron diversas soluciones de comunicación entre locales, las cuales se explicaran y analizaran. En dicho análisis se buscara que la solución responda a criterios como: escalabilidad, seguridad de datos, disponibilidad de información, y sobre todo economía.

Palabras clave: Redes de comunicación; Red privada virtual; Escalabilidad; Disponibilidad; Seguridad de datos.

Design of a communication network VPN through internet for an Authorized Claro
Distributor based on RFC 2764

ABSTRACT

The present project on VPN communication networks over the Internet shows us a guide of necessary configurations by requirements based on RFC 2764 including the functionalities of the network that will allow executing the actions required to streamline business processes through an efficient use of IT resources for the availability of information.

Currently companies want to have a presence in new markets, so they expand to new branches in different districts and even in the interior of the country which causes the need to stay connected at all times in a safe, reliable, and especially at a Acceptable cost among all its premises in order to share information that allows them to make decisions in real time.

The solution consists of the design of a communication network through virtual private networks between its premises in order to optimize resources and streamline the daily transactions of the business, for which the main focus of the solution is the interconnection of the headquarters principal and its branches, so that various communication solutions between the premises were considered, which will be explained and analyzed. In this analysis we will look for the solution to respond to criteria such as: scalability, data security, availability of information, and above all economy.

Keywords: Communication networks; Virtual private network; Scalability; Availability; Data security.

TABLA DE CONTENIDOS

1	ASPECTOS INTRODUCTORIOS CAPÍTULO.....	1
1.1	INTRODUCCIÓN MOTIVACIÓN DEL TEMA.....	1
1.2	ORGANIZACIÓN OBJETIVO.....	4
1.3	CAMPO DE ACCIÓN DE LA ORGANIZACIÓN OBJETIVO	5
1.4	SITUACIÓN PROBLEMÁTICA.....	5
1.5	IDENTIFICACIÓN DEL PROBLEMA	6
1.6	OBJETIVOS DEL PROYECTO GENERAL Y ESPECÍFICOS.....	7
1.6.1	Objetivo General.....	7
1.6.2	Objetivos Específicos	7
1.6.3	Indicadores o Mecanismos del Logro de los Objetivos.....	8
1.6.4	Justificación del Proyecto.....	8
1.6.5	Estado del Arte	10
1.6.5.1	Canales Arrendados	11
1.6.5.2	VPN Sobre MPLS	11
1.6.5.3	Enlaces Satelitales	12
1.6.5.4	Enlaces Microondas.....	12
1.6.5.5	VPN sobre Internet de Banda Ancha.....	13
2	MARCO TEORICO.....	14
2.1	QUE ES UNA RED PRIVADA VIRTUAL (VPN)	14
2.2	CARACTERÍSTICAS DE UNA VPN	15
2.3	TIPOS DE VPN	16
2.3.1	VPN Sitio a Sitio	16
2.3.2	VPN Acceso Remoto.....	17
2.4	PROTOCOLOS DE TUNNELING VPN.....	18
2.4.1	Protocolo PPTP	20
2.4.2	Protocolo L2TP	21
2.4.3	Diferencias entre PPTP y L2TP	22
2.4.4	Protocolo IPsec	23
2.4.5	Combinación L2TP/IPsec.....	25
2.5	REQUEST FOR COMMENTS (RFC).....	26

2.5.1	RFC 1878: Variable Length Subnet Table for IPv4	27
2.5.2	RFC 2764: Framework for IP based Virtual Private Networks.....	28
2.5.3	RFC 3193: Securing L2TP Using IPsec	32
2.6	ORGANISMOS REGULADORES	33
2.6.1	Internet Engineering Task Force (IETF)	33
2.6.2	Virtual Private Network Consortium (VPNC)	33
2.7	COMPARACIÓN ENTRE ALTERNATIVAS DE SOLUCIÓN.....	34
2.7.1	VPN Basadas en Cortafuegos o Firewalls.....	37
2.7.2	VPN Basadas en Enrutador y/o Proporcionadas por un ISP	37
2.7.3	VPN Basadas en Software	37
2.8	SELECCIÓN DE ALTERNATIVA DE SOLUCIÓN	38
3	DEFINICION DEL PROBLEMA	39
3.1	EL PROBLEMA	39
3.2	DESCRIPCIÓN DEL ENTORNO DE LA ORGANIZACIÓN	41
3.3	IDENTIFICACIÓN DE LOS INTERESADOS	44
3.4	REQUERIMIENTOS DEL CLIENTE	44
3.4.1	Segmentación de Red de Datos Escalable	45
3.4.2	Configuración de Red VPN que brinde Seguridad.....	46
3.4.3	Topología de Red con Distribución Centralizada.....	47
3.5	EDT DEL PROYECTO	48
4	DISEÑO DE LA SOLUCION	51
4.1	DESCRIPCIÓN DEL DISEÑO DE LA SOLUCIÓN.....	51
4.2	JUSTIFICACIÓN DEL RECURSO HUMANO PARA LA SOLUCIÓN.....	52
4.3	RECURSOS DISPONIBLES EN LA ORGANIZACIÓN OBJETIVO	53
4.3.1	Recurso Humano Disponible.....	53
4.3.2	Recurso Material Disponible	54
4.4	ESPECIFICACIONES DEL DISEÑO DE LA SOLUCIÓN	55
4.4.1	Segmentación de Red de Datos Escalable	59
4.4.2	Configuración de Red VPN que brinde Seguridad.....	61
4.4.3	Topología de red con Distribución Centralizada	64
4.5	COSTO DE LA SOLUCIÓN	66
5	PRUEBAS, RESULTADOS Y VALIDACION	68

5.1	PLAN DE PRUEBAS	68
5.1.1	Plan de Pruebas por Objetivo Específico	70
5.2	EJECUCIÓN DE PRUEBAS OBJETIVO ESPECIFICO 1	71
5.2.1	Resultados y Validación Objetivo Especifico 1	75
5.3	EJECUCIÓN DE PRUEBAS OBJETIVO ESPECIFICO 2	77
5.3.1	Resultados y Validación Objetivo Especifico 2	82
5.4	EJECUCIÓN DE PRUEBAS OBJETIVO ESPECIFICO 3	87
5.4.1	Resultados y Validación Objetivo Especifico 3	91
6	CONCLUSIONES	93
7	RECOMENDACIONES	95
8	REFERENCIAS	97
9	GLOSARIO.....	100
10	SIGLARIO	101
11	ANEXOS	102
11.1	INSTALACIÓN DE MICROSOFT FOREFRONT TMG 2010.....	103
11.2	CONFIGURACIÓN VPN SITIO A SITIO SERVIDORES SRV-TMG1 Y SRV-TMG2. 116	
11.3	CONFIGURACIÓN VPN SITIO A SITIO ENTRE SRV-TMG1 Y SRV-VPN1	147
11.4	CONFIGURACIÓN DE CONTROLADOR DE DOMINIO ADICIONAL.....	166
11.5	MANUAL DE INSTALACIÓN DE SQL SERVER	176
11.6	CONFIGURACIÓN DE REPLICACIÓN DE BASE DE DATOS.....	188
11.7	CONFIGURACIÓN FOREFRONT TMG: REGLA VPN ACCESO REMOTO.....	220
11.8	CONFIGURACIÓN FOREFRONT TMG: REGLA ACCESO INTERNET.....	225
11.9	CONFIGURACIÓN FOREFRONT TMG: REGLA INTERNET RESTRINGIDO	231
11.10	MANUAL DE CONFIGURACIÓN PROXY EN PC	238

ÍNDICE DE TABLAS

Tabla 1 Protocolos que componen IPSec	25
Tabla 2 Numero de Sub Redes de Red Clase B	28
Tabla 3 Comparación de Características de Soluciones de Conectividad.....	35
Tabla 4 Ventajas y Desventajas de Arquitecturas VPN	38
Tabla 5 Equipos y Usuarios en Oficina Principal.....	41
Tabla 6 Lista de Aplicaciones	42
Tabla 7 Dispositivos de Red.....	42
Tabla 8 Internet y Ancho de Banda	43
Tabla 9 Servidores de la Organización.....	43
Tabla 10 Identificación de los Interesados	44
Tabla 11 Tabla Resumen de Objetivos Específicos y Requerimientos	49
Tabla 12 Recurso Humano Disponible y por Adquirir.....	53
Tabla 13 Servidores Organización DAC	54
Tabla 14 Características de Servidor HP Proliant	55
Tabla 15 Requisitos y Componentes VPN	58
Tabla 16 Numero de Sub Redes de Red Clase B	59
Tabla 17 Asignación de direcciones IP para Servidores	60
Tabla 18 Direccionamiento IP para Sucursales	60
Tabla 19 Costo de Hardware y Software	66
Tabla 20 Costo de Instalación y Configuración	67
Tabla 21 Inversión Total.....	67
Tabla 22 Direcciones IP Disponibles	75
Tabla 23 Sub Redes de Red Clase B	76
Tabla 24 Vulnerabilidades Amenazas e Impacto	82
Tabla 25 Medición de Impacto y Probabilidad	83
Tabla 26 Valoración de Probabilidad de Ocurrencia.....	84
Tabla 27 Valoración del Impacto	84
Tabla 28 Matriz de Riesgo 1.....	85
Tabla 29 Valoración de Riesgos de Seguridad.....	86
Tabla 30 Matriz de Riesgo 2.....	87
Tabla 31 Métricas América Móvil.....	92

ÍNDICE DE FIGURAS

Figura 1. Esquema de una Red VPN	14
Figura 2. VPN Sitio a Sitio.....	17
Figura 3. VPN Acceso Remoto	18
Figura 4. Funcionamiento del Túnel.....	19
Figura 5. Protocolos VPN en el modelo OSI según el modo de trabajo	19
Figura 6. Diagrama del Protocolo PPTP	20
Figura 7. Diagrama del Protocolo L2TP	22
Figura 8. Diagrama del Protocolo IPSec	23
Figura 9. Combinación de Protocolos L2TP / IPSEC	26
Figura 10. EDT del Proyecto.....	48
Figura 11. Estructura del Recurso Humano.....	52
Figura 12. Segmentación de Red por Sucursal.....	61
Figura 13. Valores de Configuración TMG1.....	62
Figura 14. Valores de Configuración TMG21.....	63
Figura 15. Distribución Centralizada.....	65
Figura 16. Diagrama Red SRV-DC	71
Figura 17. Ping exitoso de servidor SRV-DC	72
Figura 18. Ping exitoso de servidor SRV-DC2	72
Figura 19. Diagrama Red SRV-BD	73
Figura 20. Ping exitoso del servidor SRV-BD	74
Figura 21. Ping exitoso del servidor SRV-DB2	74
Figura 22. Diagrama Red Routers	77
Figura 23. Ping exitoso de servidor R1	78
Figura 24. Ping exitoso de servidor R2	78
Figura 25. Diagrama Red SRV-TMG.....	79
Figura 26. Ping exitoso de servidor SRV-TMG1	80
Figura 27. Ping exitoso de servidor SRV-TMG2	80
Figura 28. Diagrama Red Routers R1 y R2.....	81
Figura 29. Protocolos IPsec	81
Figura 30. Usuario user01 en servidor SRV-DC.....	88
Figura 31. Usuario user01 en servidor SRV-DC2.....	89

1 ASPECTOS INTRODUCTORIOS CAPÍTULO

1.1 Introducción Motivación del Tema

En la actualidad los recientes y continuos avances tecnológicos crecen rápidamente, significando importantes cambios en la forma en que los individuos y distintos segmentos de la sociedad trabajan, se comunican e interactúan. Es así que las tecnologías de la información y comunicación (TIC), como Internet a través de las redes de datos, cobran un papel muy importante convirtiéndose en un medio global de comunicación de uso cotidiano en nuestras vidas, llegando a ser su uso una necesidad básica comparada al uso de la electricidad.

Por lo expresado anteriormente, existe una relación directa entre el acceso a las comunicaciones mediante las redes de datos y el desarrollo socioeconómico de las personas, comunidades, empresas y organizaciones que se ven en la necesidad de comunicarse de manera constante continua e ininterrumpida. Queda claro que hoy en día las comunicaciones son de vital importancia para el desarrollo de cualquier persona u organización y que por la competitividad y desarrollo económico es inaceptable permanecer aislado o incomunicado con otras organizaciones y menos aún con nuestras propias sucursales u oficinas.

En diversos estudios internacionales como es el caso del Banco Interamericano de Desarrollo (BID) se ha concluido que la infraestructura de transporte como son las carreteras son un importante impulsor del crecimiento y desarrollo de un país. Es así que al contar con una adecuada y operativa infraestructura como son las carreteras esta posibilitará la reducción de los costos de las mercancías que por ahí se transportan, además del desarrollo de las comunidades o poblados que comunican, entre otros importantes beneficios¹. Esta definición fue importante y necesaria para poder entender cuan significativa es contar con una adecuada infraestructura de comunicaciones, sin embargo, tan importante como contar con ella es hacer uso de las mismas para lograr desarrollo y beneficios a quienes gozan de este importante recurso.

Actualmente, las empresas desean tener presencia en nuevos mercados, por esta razón se expanden a nuevos locales en distintos distritos y hasta en el interior del país lo que origina la necesidad de mantenerse conectados en todo momento de manera segura, confiable, y sobre todo a un costo aceptable entre todos sus locales con el fin de compartir información

¹ Cfr. BID 2013:2

propia de la empresa que les permita tomar decisiones en tiempo real. Es así que las redes de comunicación han demostrado que reducen tiempo en las gestiones y lo más importante reduce costos considerables a las empresas.

Ante esta situación se cuenta con diversas soluciones de comunicación entre locales siendo las más popular y utilizada el uso de Internet para el envío de la información, sin embargo esta red pública no brinda un nivel de seguridad requerido por las empresas. Por otro lado se cuenta con la posibilidad de arrendar con un proveedor ISP líneas dedicadas de conexión para las sucursales, sin embargo esta solución resulta ser costosa sin contar con lo que significaría la cantidad de locales y distancias entre ellos. Es así que ante la necesidad de contar con una comunicación segura y confiable a costos razonables se deberá buscar nuevas alternativas de interconexión que cumplan con estas características.

Las redes privadas virtuales (VPN) cumplen con estas características mediante la conexión de redes locales (LAN) y usuarios que se encuentran en distintas ubicaciones geográficas mediante un túnel que se construye sobre Internet o cualquier red pública, permitiéndoles trabajar desde distintas ubicaciones usando infraestructura provista por una red pública como lo es Internet. Entre sus principales características y tal como su nombre lo indica las redes privadas virtuales son: “privadas” porque establecen comunicación única y exclusivamente entre el emisor y el receptor previamente definidos, y “virtuales” pues la comunicación directa entre el emisor y receptor no es por medio de una conexión física punto a punto o de extremo a extremo como se podría realizar con un cable o cualquier otro medio físico, sino más bien la comunicación es realizada a través de Internet donde se sabe que las comunicaciones recorren diversos caminos para llegar a su destino (no necesariamente punto a punto) y es por este medio por el cual se establece una comunicación "virtual" NO física de extremo a extremo entre el emisor y receptor logrando conectar de manera segura dos o más redes LAN "físicas" mediante una conexión insegura como lo es Internet². Entonces una VPN es una estructura de red que emula o virtualiza una red privada sobre infraestructura pública como Internet pudiendo brindar comunicación a nivel de las capas 2 o 3 del modelo OSI.

Por lo expuesto las VPN nos brindan importantes razones para ser consideradas como una importante y atractiva alternativa que cubrirá nuestras necesidades tales como:

² Cfr. TRUJILLO 2006:60

Alta Seguridad, las VPN utilizan estándares de seguridad como protocolos 3DES (Triple data encryption standard) cuya función es encriptar la información a transferir y el protocolo IPSec (IP Security) para manejo de los túneles mediante software brindando un alto nivel de seguridad. Además provee autenticación para el acceso mediante llaves de seguridad que validan la identidad del usuario³.

Mayor Productividad, brindando acceso y comunicación continua, que significa una mayor productividad de los usuarios. Además, con la consecutiva reducción de la necesidad de tener que transportarse de una ubicación a otra, logrando que las distancias no sean impedimento para el trabajo que antes eran limitadas por el espacio físico, fomentando así el teletrabajo⁴.

Escalabilidad, de necesitar enlaces adicionales para una oficina o sucursal remota no será necesario realizar inversiones adicionales para agregar usuarios a la red. El servicio se provee con equipos manejables y de fácil configuración. Gracias a la avanzada infraestructura de los proveedores de Internet (ISP) no es necesario realizar un enlace físico propio o rentado que podría significar una costosa inversión⁵.

Reducción de Costos, para la interconexión de locales separados geográficamente no será necesario en términos de seguridad realizar enlaces mediante líneas dedicadas (punto a punto). En su lugar, se puede emplear un acceso público como Internet de bajo costo que nos brinda un ancho de banda alto y que está disponible en la gran mayoría de zonas urbanas⁶.

En resumen, las VPN tienen un gran potencial como solución de comunicación y seguridad de conexiones remotas siendo el ahorro de costos el gran atractivo que ofrecen ya que se construyen sobre una red pública insegura, sin descuidar la seguridad de los datos transmitidos. Es así que dada la creciente importancia de la seguridad en las redes de comunicación y de conexiones más económicas requeridas por las empresas, las VPN pueden cubrir estas necesidades con las ventajas y soluciones propias de esta tecnología.

³ Cfr. LIMARI 2004:3

⁴ Cfr. LIMARI 2004:3

⁵ Cfr. LIMARI 2004:3

⁶ Cfr. LIMARI 2004:3

1.2 Organización Objetivo

La organización que se beneficiara con el proyecto es un distribuidor autorizado de Claro (DAC) con más de 10 años de operación en el mercado nacional dedicándose a la venta de servicios de telefonía e internet móvil. Además, ofrece la venta de equipos celulares, chips y recargas virtuales. Actualmente dicha organización cuenta con 5 locales comerciales ubicados en los principales centros comerciales de Lima, con un promedio de 10 usuarios por local y una oficina administrativa con 32 usuarios desde donde se gestionan los locales comerciales. Así también se tiene proyectado seguir creciendo con nuevos locales en los nuevos centros comerciales que se vienen inaugurando tanto en Lima como en el interior del país. Motivo por el cual la organización ha decidido mejorar los controles administrativos a sus diversos locales comerciales desde su oficina principal con el fin de optimizar recursos y agilizar las transacciones diarias propias del giro del negocio, es así que se tomara toda la organización iniciando desde su sede principal hasta sus locales comerciales actuales y proyectándose a los futuros locales, con el fin de mantenerlas interconectadas todas y cada una de ellas.

Visión: Mantenerse como uno de los principales Distribuidores Autorizados de Claro, expandiendo su presencia a nivel nacional con el fin de lograr ser el principal Distribuidor Autorizado de Claro del Perú.

Misión: Brindar a nuestros clientes los mejores productos y servicios para optimizar su red de telecomunicaciones.

Estrategia de Negocio: Es importante aclarar que un distribuidor autorizado goza de las principales estrategias de negocio de la casa matriz América Móvil Perú SAC (Claro) quienes desarrollan las principales y fuertes estrategias de negocio a nivel nacional, posicionando así sus productos y servicios. Teniendo entre sus principales estrategias la constante actualización de equipos de última generación, continuas y nuevas ofertas con promociones en planes de comunicación y equipos, agresiva publicidad en todos los medios de comunicación a nivel nacional, entre otras estrategias. Sin embargo por su parte el Distribuidor Autorizado, desarrolla las siguientes estrategias:

Incremento de locales comerciales. Apertura de nuevos locales en los principales centros comerciales lo cual representaría mayor presencia en el mercado.

Calidad de servicio. La calidad de servicio juntamente con la fidelización de los clientes asegura el retorno del cliente para futuras compras.

Atención personalizada. Hoy en día se tiende a la personalización de nuestros equipos móviles por lo cual un adecuado asesoramiento ofrecería la satisfacción del cliente.

Apoyo tecnológico. Debido a los últimos avances de la tecnología es necesario contar con un adecuado asesoramiento en el uso de las características de los nuevos productos.

Aumento de la publicidad y mejora del merchandising de la empresa. Por la gran competencia entre distribuidores es importante marcar la diferencia en la atención al cliente con promociones y regalos por su compra.

1.3 Campo de acción de la Organización Objetivo

Actualmente la carga administrativa para el control de las sucursales soportada por la sede principal es crítica más aun en fechas de alto transito comercial como son fiestas patrias y navidad, esto debido a que toda la organización se encuentra incomunicada entre sus diversos locales, por lo que por encargo de la Gerencia de Operaciones se requiere un sistema de comunicación de datos entre la sede principal y sus sucursales que sea eficiente, segura, continua en tiempo real y que a su vez ayude a la alta disponibilidad de sus datos, es por eso que el campo de acción para el presente proyecto serán las áreas de Logística, Comercial, Finanzas y Sistemas, cuyas soluciones impactaran en toda la organización gracias al diseño de un sistema de comunicación efectivo que interconectara a todos los locales de la organización.

1.4 Situación Problemática

La empresa cuenta una sede principal y 5 sucursales, estas instalaciones cuentan cada una con su propio acceso a internet independiente una de otra sin comunicación de redes de datos entre ellas, cuenta con tres servidores ubicados en la oficina principal: Un servidor Active Directory, otro servidor de base de datos para los registros de controles de stock de almacenes, de ventas, de cajas (ERP Microsoft Dynamics), y un tercero que aloja el software Microsoft Forefront TMG, que actúa como proxy para el control de accesos (Ver Anexo 1). Sin embargo solo la oficina principal tiene acceso y uso de estos recursos, mientras las

sucursales se encuentran aisladas a esta infraestructura, debido a esto el registro de la información en el ERP Microsoft Dynamics proveniente de las sucursales es realizado manualmente por el personal de la oficina principal quienes la reciben por medio de cuadros Excel enviados a diario por correo electrónico. Esto genera casos de duplicidad de la información de datos, y muchas veces la información se encuentra desactualizada. Es así que el acceso a la información relevante propia del negocio como stock de los almacenes por sucursal, ventas diarias y control diario de cajas por sucursal, solo es accesible desde la sede principal, por lo que las sucursales solo son capaces de acceder a la información vía correo electrónico o comunicación telefónica.

Debido a que los servidores de Active Directory y el software Microsoft Forefront TMG se encuentran ubicados físicamente en la sede principal (LAN), es que solo esta sede puede contar con controles de seguridad y acceso, es así que al no existir comunicación de la sede principal con las sucursales(WAN), estas últimas se encuentran sin medidas de seguridad motivo por el cual los empleados tienen el acceso libre y sin restricción alguna a redes sociales, chat y páginas web, lo cual afecta directamente el desempeño laboral del empleado.

1.5 Identificación del Problema

Debido a lo expuesto anteriormente la organización presenta como problema principal la falta de comunicación en tiempo real entre la sede principal y sus sucursales, donde la red actual posee un direccionamiento IP no segmentado por sucursal lo que impide el crecimiento ordenado y la correcta administración de direcciones IP, así mismo la red actual no cuenta con medidas de seguridad que protejan el flujo de datos en sus comunicaciones, además la topología actual de red no permite la centralización de recursos TI lo que afecta la disponibilidad de la información para las sucursales, originando que las mismas no cuenten con acceso en línea a la información e infraestructura que se encuentran en la sede principal, teniendo la información de cada sucursal desactualizada en los sistemas de la oficina principal, lo cual causa errores y lentitud en la toma de decisiones importantes para la organización.

1.6 Objetivos del Proyecto General y Específicos

1.6.1 Objetivo General

Diseñar una red de comunicación VPN sobre internet que permita comunicación en tiempo real para agilizar los procesos de negocio mediante un eficiente uso de los recursos TI basado en el RFC 2764 para un DAC.

1.6.2 Objetivos Específicos

- Establecer una segmentación de red escalable para las sucursales mediante el cálculo VLSM bajo el cumplimiento del RFC 1878.
- Desarrollar una configuración VPN que brinde seguridad de datos en el flujo de sus comunicaciones mediante el uso protocolos L2TP/IPSec bajo el cumplimiento del RFC 3193.
- Presentar una topología de red lógica centralizada que permita proponer medidas de optimización de recursos TI para la disponibilidad de la información.

1.6.3 Indicadores o Mecanismos del Logro de los Objetivos

Objetivo Específico	Indicador de Logro	Métrica
Establecer una segmentación de red escalable para las sucursales mediante el cálculo VLSM bajo el cumplimiento del RFC 1878.	Informe de la segmentación en sub redes y tabla con direccionamiento IP.	Nivel de escalabilidad de la red clase B mayor al 90% del total de redes disponibles.
Desarrollar una configuración VPN que brinde seguridad de datos en el flujo de su información mediante el uso protocolos L2TP/IPSec bajo el cumplimiento del RFC 3193.	Guía de configuración de protocolos de seguridad y Matriz de evaluación de riesgos de seguridad de la información.	Nivel de riesgos bajos de la seguridad de la información al 100%.
Presentar una topología de red lógica centralizada que permita proponer medidas de optimización de recursos TI para la disponibilidad de la información.	Diseño de topología de red y distribución centralizada con disponibilidad de Infraestructura TI.	Nivel de disponibilidad de la red mayor al 90% mensual.

1.6.4 Justificación del Proyecto

Algunos puntos importantes que justifican el proyecto:

- La interconexión de las redes de cada sucursal con la oficina principal permitirá la mejoría del trabajo y del intercambio de la información entre los usuarios.
- Gracias al acceso de la base de datos desde cualquiera de las sucursales será posible que los usuarios tengan disponible la información inmediata y en tiempo real.
- Con el respaldo y replicación de datos en tiempo real se podrá estar preparado ante alguna incidencia y retomar las operaciones casi inmediatamente.
- Las políticas de seguridad, tales como prohibiciones de las páginas web comúnmente conocidas, contribuirán en la productividad laboral de los empleados.

- Se contara con mayor seguridad de la información al ser transportada por la red privada virtual (VPN) que se utiliza protocolos de seguridad tales como PPTP y L2TP.

JUSTIFICACIÓN ECONÓMICA

- En el área de Logística: Información de stock actualizada

Información en tiempo real permitirá tomar decisiones en tiempo real, como por ejemplo, abastecimiento de productos, evitando así la falta de producción. Esto contribuirá al incremento de las ventas y al respectivo beneficio económico de la empresa.

- En el área Comercial: Información de ventas actualizada

Se podrá conocer las ventas por producto y por cada punto de venta en tiempo real lo cual permitirá conocer los hábitos de consumo por local de esta forma se podrán tomar decisiones comerciales como ofertas y/o promociones que permitan vender aquellos productos de poca rotación logrando así generar liquidez para próximas compras, con el respectivo beneficio económico que esta gestión origina.

- En el área Finanzas: Información de ventas actualizada

Se tendrá acceso los montos recaudados por cada punto de venta en tiempo real lo cual permitirá tener un conocimiento del dinero actual recaudado producto de las ventas del día para así tener la información real y actual de la liquidez para la compra de más productos.

- En el área de Sistemas:

Respaldo de datos, ante algún problema de caída de energía o internet en el local del servidor de base de datos, existirá un servidor de respaldo en una ubicación física diferente (otro local) listo para ser utilizado en tiempo real, y accesible desde cualquier sucursal de la red, con lo cual se retomaran inmediatamente las actividades diarias propias de la empresa con lo que el tiempo de inactividad será imperceptible y transparente para los usuarios, garantizando así el normal funcionamiento de la empresa lo cual evitaría pérdidas económicas por tiempos de inoperatividad.

Seguridad, las políticas de seguridad permitirán tener un control sobre el acceso de los usuarios a páginas donde comúnmente se conectan, restringiendo acceso, donde los usuarios pueden perder tiempo, y permitiendo a los usuarios utilizar este tiempo en los trabajos de la empresa.

Las redes de comunicaciones de datos reducen tiempo y dinero a la empresa. Esto significa una gran ventaja para la organización, especialmente las organizaciones en proceso de expansión o con oficinas remotas. Estos ahorros de costos son el principal atractivo que ofrece las redes privadas virtuales, ya que se construyen sobre la red pública (Internet) sin olvidar la seguridad de los datos transmitidos.

1.6.5 Estado del Arte

Desde tiempos remotos el ser humano siempre ha necesitado comunicarse pero solo con determinados receptores es decir de manera privada con el fin de que el mensaje sea solo para quien va dirigido. Sucede lo mismo en las telecomunicaciones, más aun en el sector empresarial donde siempre se necesitara comunicaciones privadas que transporten información confidencial propia de cada empresa.

Actualmente los recientes avances tecnológicos crecen rápidamente, significando importantes cambios en nuestra forma de vida en la que los individuos y distintos segmentos de la sociedad trabajan, se comunican e interactúan. Es así que Internet, cobra un papel muy importante convirtiéndose en un medio global de comunicación de uso cotidiano en nuestras vidas, llegando a ser su uso una necesidad básica comparada al uso de la electricidad.

Es así que existe una estrecha relación entre el acceso a las comunicaciones mediante las redes de datos y el desarrollo socioeconómico de las personas, comunidades, empresas y organizaciones quienes se ven en la necesidad de comunicarse constantemente de manera continua e ininterrumpida. Por lo expresado anteriormente las comunicaciones son de vital importancia para el desarrollo de cualquier persona u organización ya que por la competitividad y desarrollo económico es inaceptable permanecer aislado o incomunicado con otras organizaciones y menos aún con nuestras propias sucursales u oficinas.

Una tecnología ampliamente usada son las VPN las que se han desarrollado rápidamente como un medio para interconectar redes y conectar usuarios remotos a redes privadas. Esto debido a su forma simple de operar pues proporcionar un mecanismo para establecer un canal de datos seguro a través de una red existente como Internet o una conexión punto a punto como líneas dedicadas donde se asigna al uso exclusivo de un grupo de usuarios restringidos y se pueden establecer y eliminar de forma dinámica, según sea necesario.

El mercado actual los sistemas de telecomunicaciones ofrecen diversas soluciones para la conectividad entre sedes separadas geográficamente, la diferencia entre ellas está en la tecnología a utilizar y principalmente en el costo que estas conexiones significan. Es así que las más usadas son canales arrendados, enlaces satelitales, enlaces microondas y VPN a través de Internet, las cuales se explicara a continuación:

1.6.5.1 Canales Arrendados

Los canales arrendados también llamados líneas dedicadas son líneas de comunicación entre dos puntos que provee un ISP (Internet Services Provider), donde lleva un terminal a cada punto de interés. En su mayoría los canales dedicados son conexiones de fibra óptica, en donde el proveedor brinda la conexión necesaria así como los equipos de red requeridos para tal fin.⁷ Su desventaja seria el costo mensual que significa contar con esta solución, además de que su configuración, control y seguridad dependería enteramente del proveedor ISP.

1.6.5.2 VPN Sobre MPLS

Una solución del tipo Canales Arrendados debido a que es llamada también VPN IP que es un servicio de valor agregado de los ISP con el fin de crear y administrar servicios como telefonía IP y transmisión de datos para poder ofrecerlos a sus clientes. Para entender esta solución es importante saber que MPLS es un tecnología de transmisión de paquetes multiprotocolo que opera entre la capa de enlace de datos y capa de red del modelo OSI donde su principal ventaja es que reemplaza el enrutamiento basado en direcciones IP de capa 3 por etiquetas llamadas cabeceras MPLS.⁸ EL uso de MPLS en VPN no necesita una malla completa de tráfico a través del ISP pues puede soportar la comunicación entres sitios VPN directamente, es decir para cada sitio VPN el ISP puede gestionar la comunicación como una red trocal IP privada.⁹ VPN sobre MPSL es una solución WAN de capa 3 que proporciona conectividad entre muchos sitios es decir se puede tener una topología de malla completa con capacidades a nivel de capa 3.¹⁰ Las VPN sobre MPLS ofrecen conectividad entre todos los locales del cliente y que a su vez sean separadas o diferenciadas de otras

⁷ Cfr. TRUJILLO 2006:37

⁸ Cfr. MENENDEZ 2012:24

⁹ Cfr. OROZCO 2014:10

¹⁰ Cfr. SANTAMARIA 2016:38

VPNs que viajan por el mismo medio, así mismo son capaces de brindar conectividad entre diferentes VPNs además de proveer conexión a Internet.¹¹

Al ser parte de canales arrendados su desventaja seria el costo mensual que significa contar con esta solución, además de que su configuración, control y seguridad dependería enteramente del proveedor ISP.

1.6.5.3 Enlaces Satelitales

Por muchos años una solución muy usada pues fue uno de los primeros sistemas de comunicación por su gran cobertura ya que tiene alcance a casi todos los lugares habitados en la tierra. Para esta comunicación es necesaria la puesta en órbita de un satélite artificial cuya función es servir como puente visual entre el transmisor y receptor de la comunicación.¹²

Una desventaja es la latencia de las comunicaciones pues tiene que recorrer grandes distancias para llegar de un punto a otro, y la principal desventaja seria el costo elevado que esta solución representa.

1.6.5.4 Enlaces Microondas

Uno de los medios más usados por su gran cobertura en largas distancias, es una conexión entre diferentes equipos de telecomunicaciones usando ondas electromagnéticas, en donde miles de canales son ajustados a altas frecuencias logrando la comunicación entre estaciones que se encuentran separadas geográficamente siendo necesario contar con antenas con línea de vista instaladas en torres o edificios con el fin de que no haya obstáculos físicos entre ellas.¹³

Su principal desventaja radica en el equipamiento necesario en las estaciones base como son las torres, antenas y equipos de comunicación, todo esto significa una gran inversión, además de contar con línea de vista continua entre ellas, siendo esto último algo impredecible por las recientes y continuas construcciones de altos edificios en nuestra ciudad.

¹¹ Cfr. MENENDEZ 2012:33

¹² Cfr. TRUJILLO 2006:35

¹³ Cfr. FLORES 2007:13

1.6.5.5 VPN sobre Internet de Banda Ancha

Una red privada virtual puede ser construida dentro de una infraestructura de red pública como lo es Internet donde las organizaciones pueden usar VPNs para conectar de forma segura sus oficinas y empleados remotos mediante Internet cuyo acceso es proporcionado por algún ISP en vez de costosos enlaces WAN dedicados, es así que las empresas pueden usar VPNs sobre redes públicas con el fin de reducir costos de redes WAN así mismo poder aumentar la velocidades de conexión de manera dinámica gracias a los continuos incrementos de ancho de banda ofrecidos constantemente por los ISP. Las redes privadas virtuales brindan seguridad IP gracias al protocolo IPSec y tecnologías de autenticación las que protegen la información que se transmite de accesos no autorizados. Gracias a lo sencillo que es el acceso a Internet las organizaciones pueden agregar de manera rápida nuevos sitios o sucursales así como usuarios remotos.¹⁴

Una red privada virtual y tal como su nombre lo indica es una red privada por ser una comunicación exclusiva entre el emisor y transmisor manteniendo la confidencialidad y la seguridad de la comunicación, también llamada virtual pues conecta redes físicas privadas LAN mediante un canal virtual punto a punto construido sobre una infraestructura pública como lo es Internet la misma que es provista por los ISP en vez de costosos enlaces WAN dedicados, por lo que es posible aumentar las velocidades de conexión mediante la conectividad a Internet que hoy en día ofrecen grandes anchos de banda gracias a la Red Dorsal Nacional de Fibra Óptica (RDNFO). Al igual que un canal arrendado o dedicado una VPN requiere un gasto mensual no por la tecnología en sí, sino por el medio que necesita para su ejecución que sería el acceso a Internet donde el usuario deberá pagar el costo de conexión a Internet en cada una de las sedes a interconectar.

Después de explicar las diversas soluciones para la conectividad entre sedes separadas geográficamente, se deberá evaluar cada una de ellas y seleccionar la que mejor se ajuste a las necesidades de la organización, siendo hasta el momento la solución VPN a través de Internet la que mejor se ajusta a los requerimientos de la empresa, la misma que pasaremos a explicar en el próximo capítulo.

¹⁴ Cfr. FONSECA 2014:18

2 MARCO TEORICO

2.1 Que es una Red Privada Virtual (VPN)

Una Red Privada Virtual (VPN) es una red de datos segura pues permite la transmisión de información entre sedes ubicadas en diferentes áreas geográficas utilizando Internet como medio de transmisión, siendo Internet una red pública y abierta, la transmisión es realizada por medio de túneles virtuales lo que asegura la confidencialidad e integridad de la información transmitida.¹⁵

Figura 1. Esquema de una Red VPN

Fuente: VIVANCO 2003:30

En una red privada virtual se realiza un proceso de comunicación segura gracias al cifrado o encapsulación de los datos que se transfieren entre dos puntos distantes geográficamente. Dicho de otra manera una red privada virtual es una forma de conectar dos redes, llamada virtual pues toda la información viaja en un túnel virtual a través de Internet, y privada ya que los datos son encriptados por medio de protocolos de seguridad robustos.¹⁶

A continuación algunas otras definiciones interesantes:

“Una VPN combina dos conceptos: redes virtuales y redes privadas. En una red virtual, los enlaces de la red son lógicos y no físicos. La topología de esta red es independiente de la topología física de la infraestructura utilizada para soportarla.”
(GONZALES 2006:61)

¹⁵ Cfr. VIVANCO 2003:30

¹⁶ Cfr. GUZMAN 2008:46

“Una red privada virtual - VPN (Virtual Private Network), es una tecnología de red que permite a sus usuarios, extender su red local sobre una red pública. Es un ejemplo de red WAN (red de área amplia).” (MARECOS 2010:3)

“Las VPN son una estructura donde el cifrado, la autenticación y la confidencialidad pueden coexistir y operar.” (GUZMAN 2008:46)

2.2 Características de una VPN

Una de las principales características en el uso de las VPN es la seguridad, siendo muy importante garantizar la autenticación, confidencialidad e Integridad de las comunicaciones en todo momento que se tenga una comunicación activa. A continuación se explica algunas de sus características más importantes:

Confidencialidad:

Debido a que Internet es una red pública y abierta es necesario asegurar la confidencialidad de los datos que viajan por este medio, es así que se emplean métodos de cifrado de información como Data Encryption Standard (DES), Triple DES (3DES) y Advanced Encryption Standard (AES), con el fin de que solo puedan ser leídos única y exclusivamente por aquellos destinatarios quienes van dirigidos.¹⁷

Autenticación:

Gracias a las firmas digitales o mecanismo desafío-respuesta una VPN ofrece la seguridad de que el emisor y receptor sean plenamente identificados y que no exista duda alguna sobre la identidad de los mismos lo que permitirá definir si cuenta con autorización para ingresar a la red e incluso el nivel de acceso permitido que posee dicho usuario.¹⁸

¹⁷ Cfr. GUGLIELMO 2012:21

¹⁸ Cfr. VIVANCO 2003:31

Integridad:

La integridad consiste en garantizar que los datos enviados no fueron alterado o modificados para este fin se hace uso de algoritmos de hash como Message Digest (MD2 y MD5) y el secure Hash Algorithm (SHA), con lo cual se asegura que los datos recibidos por el receptor sean exactamente los mismos que el emisor transmitió inicialmente.¹⁹

No repudio:

Consiste en tener la garantía de que el emisor del mensaje no pueda negar la emisión del mismo esto se da gracias a las firmas digitales que se incluyen en el mensaje las cuales son únicas e identifican plenamente al emisor.²⁰

2.3 Tipos de VPN

Básicamente existen dos tipos de VPN que son de sitio a sitio y de acceso remoto, ambas pueden ser provistas por un mismo firewall o servidor VPN.

2.3.1 VPN Sitio a Sitio

Este tipo de VPN es utilizado ampliamente para conectar sucursales remotas con la sede principal de la organización, en donde un servidor o firewall VPN mantiene una conexión permanente a Internet y es usando este medio que se establece un túnel virtual de comunicación con los servidores de las sucursales quienes tienen su propia conexión local a Internet. Las conexiones a Internet tanto de la sede principal como las sucursales son típicamente conexiones de banda ancha lo cual permite eliminar los costosos enlace dedicados punto a punto más aun en conexiones distantes como lo son las nacionales e internacionales.²¹

Se permite comunicar con esta topología dos redes que pueden pertenecer a la misma empresa o a diferentes empresas. Estas configuraciones son las siguientes:

¹⁹ Cfr. GUGLIELMO 2012:21

²⁰ Cfr. VIVANCO 2003:31

²¹ Cfr. TRUJILLO 2006:64

Tipo Intranet: Es tipo se da cuando la organización tiene una o más sucursales que necesitan ser conectadas a la sede principal para lo cual comparten los mismos niveles de seguridad que la sede principal.

Tipo Extranet: Es tipo se da cuando la organización tiene empresas asociadas, proveedores o clientes que necesitan conectar sus redes para un trabajo compartido teniendo en cuenta restricciones y niveles de seguridad diferenciados en el acceso de la red de la sede principal.

Figura 2. VPN Sitio a Sitio

Fuente: OROZCO 2014:25

En este tipo de VPN es posible usar servidores, ruteadores o firewalls cuya función es crear la conexión VPN en donde ambos extremos de la comunicación deberán usar los mismos algoritmos de encriptación y encapsulamiento. Una de sus características más resaltantes de este tipo de VPN es que los usuarios de ambos extremos no notan los procesos de encriptación o encapsulamiento percibiendo la comunicación como si estuvieran dentro de la misma red local.²²

2.3.2 VPN Acceso Remoto

Este tipo de VPN más usado actualmente por la gran mayoría de empresas, orientado a los usuarios móviles ya sean trabajadores o proveedores que acceden a la red de la organización desde lugares distantes. Usa como medio de comunicación el acceso a Internet de banda

²² Cfr. CEVALLOS 2006:14

ancha, donde luego de que el usuario remoto se haya autenticado podrá trabajar como si estuviera conectado localmente a la organización.²³

Figura 3. VPN Acceso Remoto

Fuente: OROZCO 2014:24

Para establecer la conexión con la organización es necesario que el usuario remoto utilice un software instalado en su terminal para la creación de un túnel virtual hacia la organización, donde es un servidor, ruteador o firewall quien provee la conexión, no sin antes validar la identidad del usuario que desea conectarse a la red.²⁴

2.4 Protocolos de Tunneling VPN

Los protocolos de VPN hacen referencia principalmente a los niveles OSI inferiores como son la capa de enlace de datos y la capa de red. Es en estas capas que se puede establecer un túnel entre el cliente y el servidor donde ambos deberán usar el mismo protocolo tunneling. Los protocolos de la capa de enlace o nivel 2 utilizan tramas como unidad de intercambio, siendo los protocolos PPTP o L2TP los que encapsulan los datos a transmitirse en una trama de protocolo de punto a punto (PPP) que es enviada a través de la red. Los protocolos de la capa de red o nivel 3 utilizan paquetes como unidad de intercambio, donde un encabezado adicional a los paquetes IP es agregado por IPSec con el fin de ser transmitidos de forma segura a través de la red.²⁵

²³ Cfr. OROZCO 2014:24

²⁴ Cfr. CEVALLOS 2006:13

²⁵ Cfr. TORRES 2002:23

Figura 4. Funcionamiento del Túnel

Fuente: TORRES 2002:17

Para que una VPN logre un funcionamiento efectivo es necesario hacer uso de una serie de protocolos orientados a garantizar la confidencialidad e integridad de la información transmitida. Es así que en el siguiente grafico se muestra los protocolos VPN según el modelo de referencia OSI.²⁶

Figura 5. Protocolos VPN en el modelo OSI según el modo de trabajo

Fuente: LIMARI 2004:13

Según el grafico anterior podemos observar que existen 3 protocolos tunneling distribuidos entre la capa 2 y 3 del modelo OSI necesario para establecer una VPN, y que a continuación se brindara mayor detalle de cada uno de ellos:

²⁶ Cfr. LIMARI 2004:13

2.4.1 Protocolo PPTP

PPTP (Point to Point Tunneling Protocol), es un protocolo de túnel punto a punto desarrollado por un grupo de fabricantes como Microsoft, U.S. Robotics, Ascend Communications, 3Com/Primary Access, ECI Telematics conocidas como PPTP Forum, con el fin de implementar redes privadas virtuales. PPTP es el resultado de una combinación de protocolos como el protocolo punto a punto (PPP) del cual se utilizan funciones como multiprotocolo, autenticación, compresión y cifrado, por otro lado también en combinación con PPP es usado el protocolo de control de transmisión / protocolo Internet (TCP/IP) el cual permite el intercambio de datos entre cliente y servidor ofreciendo la capacidad para enrutar paquetes por Internet, de esta manera con la suma de estas importantes funcionalidades brindadas por estos protocolos es posible crear una red privada virtual, sobre un red de trabajo vía TCP/IP.²⁷

PPTP encapsula las tramas PPP en datagramas IP para ser transmitidas por una red IP ya sea privada como la de una red corporativa o publica como lo es Internet, donde gracias a la funcionalidad multiprotocolo PPP es posible enviar tráfico de cualquiera de los protocolos: IP, IPX o NetBEUI.²⁸

Inicialmente PPP era ideal para un VPN ya que en su funcionalidad imitaba el comportamiento que una VPN necesitaría que es un túnel punto a punto, sin embargo no contaba con mecanismos de seguridad, es así que PPTP no solo ofreció un canal de comunicaciones seguro de host a host sino además brindo la posibilidad de trabajar en conjunto con el protocolo IPsec el cual brindaría los mecanismos de seguridad que una red privada virtual necesita.²⁹

Figura 6. Diagrama del Protocolo PPTP

Fuente: VIVANCO 2003:41

²⁷ Cfr. ORTEGA 2003:56

²⁸ Cfr. ORTEGA 2003:48

²⁹ Cfr. SCOTT 1998:36

2.4.2 Protocolo L2TP

L2TP (Layer 2 Tunneling Protocol) fue diseñado por un grupo de trabajo de IETF conformado por las mismas compañías creadoras de los protocolos PPTP y L2F, con el fin de corregir las deficiencias de estos protocolos, es así que L2TP heredo de PPTP y de L2F las mejores funciones y características. L2TP es un protocolo que crea un túnel entre un cliente y servidor (ambos L2TP) donde encapsula las tramas PPP para su envío a través de redes como IP, X.25, Frame Relay o ATM. Una vez establecido el túnel se configura un mecanismo de autenticación de usuario con el fin de establecer su identidad. A través de las redes internas IP, L2TP utiliza el Protocolo de Datagrama de Usuario (UDP) y una serie de mensajes L2TP con el fin de crear, mantener y optimizar los túneles por donde se transmiten los datos.³⁰

Al igual que PPTP, es posible usar L2TP como protocolo VPN a través de Internet debido a que puede usarse IP como protocolo de transporte. Gracias a la combinación entre L2TP sobre IPsec se puede proporcionar un vínculo de red seguro pues para la encriptación se hace uso del protocolo ESP (ESP Encapsulating Security Payload) de IPsec, ya que L2TP no dispone de su propio servicio de encriptación. Es así que para contar con los mecanismos de seguridad necesarios, el cliente como el servidor VPN deberán de disponer de L2TP y de IPsec en sus configuraciones, donde primeramente IPsec realiza una negociación de seguridad haciendo uso de certificados de autenticación entre el cliente y el servidor VPN, es entonces cuando L2TP utiliza una cuenta y contraseña de usuario para la autenticación necesaria.³¹

Así como PPTP, L2TP reduce el tamaño de los paquetes debido a que ofrece funciones de compresión, así mismo puede también añadir un nivel de encriptación en la comunicación. Debido a que L2TP pertenece a la capa de enlace de datos podrá ser usado por otros protocolos de capa de red que añadan seguridad a las comunicaciones como es el caso de IPsec.³²

³⁰ Cfr. ORTEGA 2003:61

³¹ Cfr. TORRES 2002:28

³² Cfr. CEVALLOS 2006:24

Figura 7. Diagrama del Protocolo L2TP

Fuente: VIVANCO 2003:42

2.4.3 Diferencias entre PPTP y L2TP

Ambos protocolos están basados sobre PPP siendo estos muy similares entre sí, sin embargo existen diferencias entre el PPTP y L2TP:

- PPTP por sí solo no proporciona autenticación de túnel, L2TP si lo hace, sin embargo ambos protocolos en combinación con IPSec si proporcionan autenticación de túnel a nivel de capa 3, siendo innecesaria la autenticación del túnel a nivel de capa 2.³³
- PPTP requiere autenticación solo a nivel de usuarios usando un protocolo de autenticación basado en PPP de la misma forma que lo realiza L2TP, sin embargo L2TP en combinación con IPSec adicionalmente puede contar con un nivel de autenticación de maquina usando certificados digitales.³⁴
- Con PPTP se usa el cifrado MPPE el cual está basado en RSA usando llaves de 40, 56 o 128 bits, con L2TP se usa DES y 3-DES con llaves de 56 bits y 3 llaves de 56 bits respectivamente. Además para el caso de DES los datos son cifrados en bloques de 64 bits.³⁵
- PPTP necesita que la red sea de tipo IP, L2TP solo necesita que los medios del túnel proporcionen conectividad punto a punto orientado a paquetes, además L2TP puede ejecutarse sobre IP, Frame Relay, X.25, ATM.³⁶
- PPTP puede soportar solo un único túnel entre dos puntos externos. L2TP permite crear múltiples túneles con diferentes calidades de servicio.³⁷

³³ Cfr. ORTEGA 2003:64

³⁴ Cfr. BROLLO 2010:51

³⁵ Cfr. SCOTT 1998:57

³⁶ Cfr. CEVALLOS 2006:24

³⁷ Cfr. BROLLO 2010:51

- PPTP proporciona la compresión de encabezados de 6 bytes, L2TP opera solo con 4 bytes adicionales.³⁸
- Con PPTP, el cifrado de datos inicia después de que la conexión se procese (después de la autenticación PPP), con L2TP, el cifrado inicia antes de la conexión PPP negociando una asociación de seguridad IPSec.³⁹

2.4.4 Protocolo IPsec

IPSec (Internet Protocol Security), el protocolo de seguridad reconocido para conexiones VPN. Al desarrollar IPv4 se descuidó la seguridad de los datos por lo que fue necesario contar con protocolos y procedimientos adicionales a IPv4. Es así que surge IPSec que es un conjunto de protocolos que asegura la comunicación sobre el protocolo de Internet IP autenticando y/o cifrando los paquetes IP basado en criptografía robusta tanto en IPv4 como para IPv6, teniendo este último IPSec incluido en su composición. Los principales servicios de seguridad definidos en IPSec son: autenticación, integridad, control de acceso y confidencialidad. Adicionalmente IPSec es modular en cuanto a protocolos criptográficos ya que no depende de un algoritmo de criptografía específico.⁴⁰

Figura 8. Diagrama del Protocolo IPSec

Fuente: VIVANCO 2003:43

IPSec cuenta con dos importantes protocolos que cubren la privacidad, autenticación e integridad de un mensaje: Authentication Header (AH) y Encapsulating Security Payload (ESP), donde AH brinda autenticación y por extensión también integridad, por otro lado ESP asegura la privacidad mediante el encriptado de datos. El protocolo IPSec pertenece a

³⁸ Cfr. ORTEGA 2003:64

³⁹ Cfr. BROLLO 2010:51

⁴⁰ Cfr. BROLLO 2010:52

la capa de red del modelo de referencia OSI por lo que resulta transparente para las aplicaciones, es ampliamente usado en las redes privadas virtuales sitio a sitio así como también en el acceso remoto. La utilidad de IPSec puede ser directamente entre los hosts que se comunican, llamando a esta forma de conectividad como modo transporte, o también a través de un túnel por Internet siendo esta forma de conectividad denominada modo túnel. IPSec define los mecanismos de codificación y el formato de un paquete para el tráfico IP mediante el modo de túnel IP o llamado también túnel de IPSec. Este modo de túnel utiliza un método de seguridad negociado entre el cliente y el servidor del túnel para encapsular y codificar todos los paquetes IP con la finalidad de obtener seguridad en la transferencia de datos a través de las redes IP públicas o privadas. El protocolo Internet Key Exchange (IKE) complementa la seguridad de IPSec cuya función es el intercambio secreto de claves con los que se gestiona IPSec. IKE usa claves públicas, claves precompartidas, o firmas digitales.⁴¹

El conjunto de protocolos que forman el protocolo IPSec fueron desarrollados por Engineering Task Force (IETF) quienes a su vez tienen un grupo de trabajo llamado IP Security donde se encargan de definir estándares y protocolos relativos a la seguridad de Internet, estos protocolos son usados por las redes privadas virtuales como parte de sus medidas de seguridad, es así que IETF tiene una serie de publicaciones denominadas RFC relacionadas con IPSec entre las cuales tenemos:⁴²

RFC 2401: Arquitectura de seguridad para el Protocolo de Internet.

RFC 2402: Cabecera de Autenticación IP.

RFC 2403: Uso de HMAC-MD5-96 dentro de ESP y AH.

RFC 2404: Uso de HMAC-SHA-1-96 dentro de ESP y AH.

RFC 2405: Algoritmo de cifrado ESP DES-CBC con IV explícito.

RFC 2406: Carga de Seguridad de Encapsulamiento IP (ESP).

RFC 2407: Dominio de Interpretación de seguridad IP de Internet para ISAKMP.

⁴¹ Cfr. ORTEGA 2003:65

⁴² Cfr. CEVALLOS 2006:26

RFC 2408: Asociación de Seguridad de Internet y Protocolo de Administración de Llave (ISAKMP).

RFC 2409: Intercambio de Llave de Internet (IKE).

RFC 2410: Algoritmo de Encriptación Nulo y su uso con IPSec.

RFC 2411: Guía de Documento de Seguridad IP.

RFC 2412: Protocolo de Determinación de Llave OAKLEY.

RFC 4301: Sustituye a RFC 2401: Arquitectura de seguridad para el Protocolo de Internet.

RFC 4302: Sustituye a RFC 2402: Cabecera de Autenticación IP.

RFC 4303: Sustituye a RFC 2406: Carga de Seguridad de Encapsulamiento IP (ESP).

RFC 4306: Sustituye a RFC 2407, RFC 2408, RFC 2409): Intercambio de Llave de Internet (IKEv2).

Finalmente como resumen se presenta la siguiente Tabla 1 que nos indica los principales protocolos de seguridad que componen IPSec:

Tabla 1
Protocolos que componen IPSec

Protocolo de Autenticación	Protocolo de Encriptación y Cifrado	Protocolo de Intercambio de Claves
Authentication Header (AH) Cabecera de Autenticación RFC 4302	Encapsulating Security Payload (ESP) Carga de Seguridad de Encapsulamiento RFC 4303	Internet Key Exchange (IKE) Intercambio de Claves de Internet RFC 4306
HMAC - MD5 HMAC - SHA1 HMAC - SHA256	DES (56 Bits) 3-DES (168 Bits) AES AES - CBC AES - CTR	ISAKMP OAKLEY X.509 con firma DSS Firma RSA Encriptación RSA

Fuente: Elaboración propia.

2.4.5 Combinación L2TP/IPsec

Debido a que L2TP e IPSec pertenecen a capas diferentes y contiguas como son la capa 2 y 3 respectivamente, resulta interesante y de mucha utilidad su combinación en las redes virtuales resultando ser sumamente efectiva en términos de seguridad.

Como ya se indicó IPsec opera en la capa 3 por lo que no especifica cómo construir un canal punto a punto (PPP), siendo esta función responsabilidad del protocolo de capa 2 L2TP, es entonces que IPsec asume que el canal punto a punto ya fue construido previamente, para luego invocar las funciones de seguridad adicionales que IPsec brinda. En consecuencia es de mucha utilidad el trabajo en conjunto de estos protocolos para crear, mantener y cerrar el canal punto a punto necesario para una red privada virtual.⁴³

Figura 9. Combinación de Protocolos L2TP / IPSEC

Fuente: Elaboración propia.

La efectividad de la combinación de estos protocolos resulta importante en términos de seguridad y compatibilidad de entornos de red, ya que por un lado IPsec otorga seguridad gracias a la encriptación y autenticación pero con la limitación de que solo opera en redes IP, sin embargo L2TP realiza túneles basados en PPP que soporta diferentes protocolos de red como IP, Frame Relay, X.25, ATM, siendo esta combinación muy eficiente para las redes privadas virtuales ya que se logra mayor seguridad y confiabilidad en diversos entornos de red.⁴⁴

2.5 Request For Comments (RFC)

Los RFC o Request For Comments son publicaciones del Grupo de Trabajo de Ingeniería de Internet (IETF), que es una organización internacional formada por investigadores, profesores, estudiantes, técnicos y profesionales de redes entre otros interesados en la evolución de la arquitectura de Internet y su buen funcionamiento. Es así que esta

⁴³ Cfr. TORRES 2002:34

⁴⁴ Cfr. LIMARI 2004:56

organización tiene como principal objetivo el mejor funcionamiento de Internet por medio de propuestas y estándares que describen como funciona internet y otras redes de computadoras conocidos como RFC con el fin de que influyan en como las personas diseñan, usan y gestionan Internet.⁴⁵ Así mismo esta importante organización tiene importantes RFC que son de gran utilidad para el presente proyecto como son:

2.5.1 RFC 1878: Variable Length Subnet Table for IPv4

El crecimiento de las redes ha dado como resultado una división de redes más grandes y más complejas por lo que es necesario segmentar las redes para aislar el tráfico de datos por área, departamento o sucursal para así evitar tormentas de broadcast que podría originar una congestión de red y finalmente su mal funcionamiento. Además la segmentación de red ofrece múltiples ventajas como la simplicidad en la administración de la red pues ayuda a poder gestionar y diferenciar las políticas de seguridad por área, departamento o sucursal. Así mismo es de gran utilidad para controlar el crecimiento de la red ya sea por nuevas áreas, departamento o sucursales.

La segmentación de red o VLSM (Variable Length Subnet) para IPv4 es tratada en el RFC 1878 donde aclara los problemas relacionados con las subredes de las redes IP al proporcionar una tabla de subred estándar. Esta tabla incluye número de subredes para redes de clase A, B y C, así como ID de red, rangos de host y direcciones IP. Además este documento detalla los valores potenciales para las subredes IPv4 donde se proporciona información adicional para los valores Decimal y Hexadecimal, los equivalentes de clase y el número de direcciones disponibles dentro del bloque indicado.⁴⁶

Es así que el RFC 1878 describe las subredes válidas y máscaras de subred que se pueden usar en redes TCP/IP y según su página 3: Subredes y Redes, indica:

⁴⁵ Cfr. IETF 2018

⁴⁶ Cfr. RFC1878 2018

“El número de direcciones de red y de host disponibles se deriva del número de bits utilizados para el enmascaramiento de subred. Las siguientes tablas representan el número de bits de subredes y la red resultante, direcciones de broadcast y direcciones de host. La Tabla 1-1 representa la división en subredes de una red clase B”

Tabla 2

Numero de Sub Redes de Red Clase B

Mascara Decimal	Mascara Binario	Nro. De Redes	Nro de Hosts
255.255.0.0	11111111.11111111.00000000.00000000	1	65534
255.255.128.0	11111111.11111111.10000000.00000000	2	32766
255.255.192.0	11111111.11111111.11000000.00000000	4	16382
255.255.224.0	11111111.11111111.11100000.00000000	8	8190
255.255.240.0	11111111.11111111.11110000.00000000	16	4094
255.255.248.0	11111111.11111111.11111000.00000000	32	2046
255.255.252.0	11111111.11111111.11111100.00000000	64	1022
255.255.254.0	11111111.11111111.11111110.00000000	128	510

Fuente: RFC 1878.

2.5.2 RFC 2764: Framework for IP based Virtual Private Networks

Este documento describe un marco para redes privadas virtuales (VPN) que se ejecutan en redes IP. Discute los diferentes tipos de VPN, sus respectivos requisitos y propone mecanismos específicos que podrían usarse para implementar cada tipo de VPN utilizando las especificaciones existentes o propuestas. El objetivo de este documento es servir como marco para el desarrollo de protocolos relacionados con el fin de desarrollar el conjunto completo de especificaciones necesarias para el despliegue generalizado de soluciones VPN interoperables.⁴⁷

Actualmente, existe un gran interés en el despliegue de redes privadas virtuales en las instalaciones de red troncal de IP. Sin embargo, el despliegue generalizado de las VPN se ha visto obstaculizado por la falta de implementaciones interoperables, que, a su vez, se deriva de la falta de un acuerdo general sobre la definición y el alcance de las VPN y la confusión sobre la gran variedad de soluciones descritas por El término VPN. En el contexto de este documento, una VPN se define simplemente como la 'emulación de una instalación de red de área amplia (WAN) privada que utiliza instalaciones de IP' (incluida la Internet pública o

⁴⁷ Cfr. RFC2764 2018

redes troncales de IP privadas). Como tales, hay tantos tipos de VPN como tipos de WAN, por lo tanto, la confusión sobre qué constituye exactamente una VPN.⁴⁸

En este documento, una VPN se modela como un objeto de conectividad. Los hosts pueden conectarse a una VPN, y las VPN pueden estar interconectadas juntas, de la misma manera que los hosts actuales se conectan a redes físicas, y las redes físicas están interconectadas entre sí (por ejemplo, a través de puentes o enrutadores). Muchos aspectos de las redes, como el direccionamiento, el mecanismo de reenvío, la calidad del servicio (QoS), la seguridad y el cortafuegos, tienen soluciones comunes tanto en las redes físicas como en las virtuales, y muchos de los problemas que surgen en la discusión de las VPN tienen análogos directos con aquellos problemas implementados en redes físicas. La introducción de VPN no crea la necesidad de reinventar la red, o de introducir paradigmas completamente nuevos que no tengan un análogo directo con las redes físicas existentes. En cambio, a menudo es útil examinar primero cómo se maneja un problema particular en un entorno de red física, y luego aplicar el mismo principio a un entorno que contiene redes virtuales y físicas, y desarrollar extensiones y mejoras apropiadas cuando sea necesario. Claramente, tener mecanismos que son comunes en las redes tanto físicas como virtuales facilita la introducción de redes privadas virtuales (VPN) en las redes existentes y también reduce el esfuerzo necesario tanto para el desarrollo de estándares como para el desarrollo de productos, ya que las soluciones existentes pueden aprovecharse.⁴⁹

CPE y redes basadas en VPNs

La mayoría de las implementaciones actuales de VPN se basan en equipos de CPE. Las capacidades de VPN se están integrando en una amplia variedad de dispositivos CPE, que van desde firewalls hasta enrutadores de borde WAN y dispositivos de terminación VPN especializados. Dichos equipos pueden ser adquiridos e implementados por los clientes, y pueden ser implementados (y, a menudo, administrados de forma remota) por los proveedores de servicios en un servicio de outsourcing.⁵⁰

⁴⁸ Cfr. RFC2764 2018

⁴⁹ Cfr. RFC2764 2018

⁵⁰ Cfr. RFC2764 2018

Requisitos Generales de VPN

En los últimos tiempos existe un creciente interés en el uso de VPN como un medio rentable de construir y desplegar redes de comunicación privada para la comunicación de múltiples sitios, a medida que las empresas han encontrado la necesidad de conexiones de Internet de alta velocidad para sus redes corporativas, ha habido un gran interés en la implementación de VPN basadas en CPE (Equipo Local del Cliente) que se ejecutan en Internet. Esto se debe principalmente a la ubicuidad y a los precios insensibles a la distancia de Internet, todo esto resulta en costos significativamente más bajos que los servicios típicos de líneas dedicadas o arrendadas a los ISP.⁵¹

La noción de utilizar Internet para las comunicaciones privadas no es nueva, y para este propósito se han utilizado muchas técnicas. Sin embargo, solo en los últimos tiempos se han reunido los mecanismos IP necesarios para cumplir con los requisitos VPN de los clientes. Estos requisitos incluyen los siguientes:

Transporte de Paquetes

El tráfico transportado dentro de una VPN puede no tener relación con el tráfico en la red troncal IP, ya sea porque el tráfico es multiprotocolo, o porque la red IP del cliente puede usar un direccionamiento IP no relacionado con el de la red troncal IP en la que se transporta el tráfico. En particular, la red IP del cliente puede utilizar direcciones IP privadas no únicas.⁵²

Seguridad de Datos

En general, los clientes que usan VPN requieren algún tipo de seguridad de datos, es así que existen diferentes modelos de confianza aplicables al uso de VPNs. Uno de esos modelos es donde el cliente no confía en que el proveedor de servicios ISP proporcione ningún tipo de seguridad, y en su lugar implementa una VPN utilizando dispositivos CPE que implementan la funcionalidad de firewall y que están conectados entre sí mediante túneles seguros. En este caso, el proveedor de servicios se utiliza únicamente para el transporte de paquetes IP.

⁵¹ Cfr. RFC2764 2018

⁵² Cfr. RFC2764 2018

Un modelo alternativo es donde el cliente confía en el proveedor de servicios ISP para proporcionar un servicio VPN administrado y seguro donde el cliente confía en que los paquetes no serán mal dirigidos, inyectados en la red de manera no autorizada, detenidos, modificados en tránsito o sujetos para el análisis del tráfico por partes no autorizadas.⁵³

Mecanismo de Tunelización

Juntos, los primeros dos de los requisitos mencionados anteriormente implican que las VPN deben implementarse a través de algún tipo de mecanismo de tunelización de IP, donde los paquetes formados y/o el direccionamiento utilizado dentro de la VPN pueden no estar relacionados con los utilizados para enrutar los paquetes tunelizados a través de la red troncal IP. Dichos túneles, dependiendo de su forma, pueden proporcionar cierto nivel de seguridad de datos intrínseca, o esto también puede mejorarse utilizando otros mecanismos como IPSec.⁵⁴

Garantías de Calidad de Servicio

Además de garantizar la privacidad de la comunicación, las técnicas de redes privadas existentes, basadas en mecanismos físicos o de capa de enlace, también ofrecen diversos tipos de garantías de calidad de servicio. En particular, las líneas arrendadas y de acceso telefónico ofrecen garantías de ancho de banda y latencia mediante el cumplimiento de SLAs del ISP. A medida que las VPN se despliegan más ampliamente, habrá una demanda en el mercado de garantías similares, a fin de garantizar la transparencia de la aplicación de extremo a extremo. Si bien la capacidad de las VPN para ofrecer tales garantías dependerá en gran medida de las capacidades proporcionales de las redes troncales IP subyacentes, un marco de VPN también debe abordar los medios por los cuales los sistemas VPN pueden utilizar dichas capacidades a medida que evolucionan.⁵⁵

⁵³ Cfr. RFC2764 2018

⁵⁴ Cfr. RFC2764 2018

⁵⁵ Cfr. RFC2764 2018

2.5.3 RFC 3193: Securing L2TP Using IPsec

El RFC 3193 explica cómo el Protocolo de túnel de capa dos (L2TP) puede utilizar IPsec para proporcionar autenticación de túnel, protección de privacidad, comprobación de integridad y protección de reproducción.

L2TP es un protocolo que crea un túnel entre un cliente y servidor (ambos L2TP) donde encapsula las tramas PPP para su envío a través de redes como IP, X.25, Frame Relay o ATM. Sin embargo, L2TP no define los mecanismos de protección del túnel.⁵⁶

IPsec es un conjunto de protocolos que se utiliza para asegurar la comunicación en la capa de red entre dos pares. Este protocolo está compuesto por el documento de arquitectura de seguridad IP, IKE, IPsec AH e IPsec ESP. IKE es el protocolo de administración de claves, mientras que AH y ESP se utilizan para proteger el tráfico IP.⁵⁷

Este documento propone el uso del conjunto de protocolos IPsec para proteger El tráfico L2TP a través de redes IP, y explica cómo IPsec y L2TP deben ser utilizados juntos. Este documento no intenta estandarizar la seguridad de extremo a extremo. Cuando se requiere seguridad de extremo a extremo, se recomienda que se utilicen mecanismos de seguridad adicionales como IPsec dentro del túnel, además de la seguridad del túnel L2TP.⁵⁸

Combinación L2TP/IPSEC

IPSec opera en la capa 3 por lo que no especifica cómo construir un canal punto a punto (PPP), siendo esta función responsabilidad del protocolo de capa 2 L2TP, es entonces que IPSec asume que el canal punto a punto ya fue construido previamente, para luego invocar las funciones de seguridad adicionales que IPSec brinda. En consecuencia es de mucha utilidad el trabajo en conjunto de estos protocolos para crear, mantener y cerrar el canal punto a punto necesario para una red privada virtual.⁵⁹

⁵⁶ Cfr. ORTEGA 2003:61

⁵⁷ Cfr. RFC3193 2018

⁵⁸ Cfr. RFC3193 2018

⁵⁹ Cfr. TORRES 2002:34

La combinación de estos protocolos resulta importante en términos de seguridad y compatibilidad de entornos de red, ya que por un lado IPSec otorga seguridad gracias a la encriptación y autenticación pero con la limitación de que solo opera en redes IP, sin embargo L2TP realiza túneles basados en PPP que soporta diferentes protocolos de red como IP, Frame Relay, X.25, ATM, siendo esta combinación muy eficiente para las redes privadas virtuales ya que se logra mayor seguridad y confiabilidad en diversos entornos de red.⁶⁰

2.6 Organismos Reguladores

Las redes de comunicación como las redes privadas virtuales son materia de diversas normas y protocolos que especifican su funcionamiento y características, estas a su vez son emitidas por diversas organizaciones interesadas en su desarrollo y uso con las mejores prácticas a nivel internacional.

2.6.1 Internet Engineering Task Force (IETF)

El Grupo de Trabajo de Ingeniería de Internet (IETF), es una organización internacional formada por investigadores, profesores, estudiantes, técnicos y profesionales de redes entre otros. Tiene como objetivo contribuir a la ingeniería de Internet aportando conocimiento a diversas áreas como transporte, encaminamiento y seguridad. IETF tiene como misión hacer que Internet funcione mejor mediante la regulación de propuestas y estándares de Internet conocidos como RFC con la finalidad de que estos documentos influyan en la manera como las personas diseñan, usan y gestionan Internet.⁶¹

2.6.2 Virtual Private Network Consortium (VPNC)

Este consorcio está formado por importantes compañías fabricantes en el mercado de VPNs como son: Checkpoint, Nokia, Alcatel. El consorcio declara tres protocolos como los principales protocolos de comunicación para VPN.⁶²

⁶⁰ Cfr. LIMARI 2004:56

⁶¹ Cfr. IETF 2018

⁶² Cfr. CALDERON 2001:54

- PPTP RFC 2637
- L2TP (bajo IPSec) RFC 2661
- IPSec RFC 4301

Entre los principales propósitos de VPNC se tiene la promoción de los productos de sus miembros a la prensa y potenciales clientes, aumentar la interoperabilidad entre los productos de sus miembros para ayudar a servir mejor a sus clientes, y ayudar a todos los interesados a entender las tecnologías y estándares VPN. Es preciso señalar que VPNC no crea normas o estándares, por el contrario se apoya fundamentalmente en los estándares y protocolos de la IETF conocidos como RFCs.⁶³

2.7 Comparación entre alternativas de solución

En el capítulo inicial se describió algunas soluciones para la conectividad entre sedes separadas geográficamente, siendo la diferencia entre ellas la tecnología a utilizar y principalmente el costo que estas conexiones significan. Es así que en el Perú las más populares son canales arrendados, enlaces satelitales, enlaces microondas y VPN a través de Internet. Entre estas últimas tres soluciones para la conectividad entre sedes separadas geográficamente como son: Conexión Satelital, Enlaces Microondas e Internet de Banda Ancha por Fibra Óptica, es evidente que esta última es la más económica y así lo señala el Colegio de Ingenieros del Perú a través del Ing. Carlos Sotelo López sostiene que:

“(…) el escaso desarrollo de redes de transporte, que trae como consecuencia precios exorbitantes en la comercialización de transporte de capacidad en Mbps entre Lima y provincias, entre los que podemos citar: 100 a 200 dólares el Mbps de Internet puro en Lima y 500 dólares el Mbps puro en provincias, cuando la conexión es a una red de fibra óptica, 800 a 1 200 dólares en los casos que la conexión es a una red de microondas y 6 000 dólares para 1 Mbps puro si la conexión es vía satélite.” (CIP 2013: 8)

⁶³ Cfr. VPNC 2016

La comunicación con posibles sedes al interior del país significaba un alto costo en comunicaciones sin embargo gracias a la Red Dorsal Nacional de Fibra Óptica (RDNFO) el acceso a Internet mejorara notablemente ya que se tendrá un precio de 27 dólares por transporte de 1 Mbps independiente de la distancia que recorra. Gracias a que el operador de la red dorsal no podrá comercializar Internet sino más bien proporcionar la infraestructura a operadores grandes y pequeños esto nos traerá como consecuencia que cualquier operador podrá tener un costo de 27 dólares de transporte más entre 100 a 200 dólares por la compra de Internet en Lima, dando finalmente un costo total de entre 127 a 227 dólares el Mbps de Internet.⁶⁴

Como resumen tenemos la siguiente Tabla 3 donde podemos ver las características de las soluciones de conectividad de banda ancha antes descritas:

Tabla 3

Comparación de Características de Soluciones de Conectividad

Medio de Transporte	Infraestructura	Costo de MBPS US.\$
Enlaces Satelitales	Satelites, Hub y Terminales Satelitales.	6.000
Enlaces Microondas	Torres de telecomunicaciones y antenas.	800 - 1.200 Provincias
Internet de Banda Ancha por Fibra Optica	Routers provistos por el ISP	100 - 200 en Lima 500 en Provincias

Fuente: Elaboración propia.

Es sabido que las VPN no son una tecnología nueva por el contrario se trata de una tecnología extensamente probada y eficaz que está en constante evolución por lo que esta solución es una forma simple y sobre todo económica de brindar conexiones seguras y privadas a través de Internet, siendo su principal ventaja que en la actualidad existen diversas ofertas de acceso a Internet por la alta competencia entre ISPs además de que hoy en día las velocidades de

⁶⁴ Cfr. CIP 2013:9

acceso a Internet se vienen incrementando constantemente gracias a la Red Dorsal Nacional de Fibra Óptica (RDNFO) siendo esto un gran factor de performance para las VPN.

Ventajas y Desventajas

Una de las principales ventajas en el uso de una VPN es que nos permite el uso de una red privada como lo podría ser una WAN dedicada pero con los costos de una red pública como lo es Internet. Donde podemos gozar de privilegios, accesos y permisos en nuestro ordenador de la misma forma como si estuviéramos físicamente en nuestra organización pudiendo acceder a documentos internos, base de datos, y acceso a Internet entre otros beneficios.⁶⁵

Es así que entre sus principales ventajas tenemos:

- Seguridad, confidencialidad e integridad de los datos transmitidos.
- Accesibilidad a todos los recursos de la red central.
- Reducción de costos de administración y soporte de la red.
- Aumenta la productividad del personal gracias al teletrabajo remoto.
- Provee de controles de acceso y autenticación basados en políticas centralizadas.
- Escalable por su sencilla integración de nuevas sedes.

Entre sus principales desventajas tenemos:

- Retardos por la encriptación de datos produciría lentitud en la red.
- Complejidad en el tráfico de paquetes por el encapsulamiento adicional.

Tipos de VPN

Actualmente existen diversas arquitecturas para realizar una VPN ya sea por hardware, software o la combinación de ambas, a continuación las principales soluciones VPN utilizadas en el mercado:

⁶⁵ Cfr. VIVANCO 2003:32

2.7.1 VPN Basadas en Cortafuegos o Firewalls

Las VPN basadas en firewall es quizás la forma más común de implementar una VPN, ya que en la mayoría de organizaciones se cuenta con un hardware o software firewall conectadas a Internet y en busca del ahorro en costos se hace uso de la infraestructura existente es así que este medio es utilizado, pues la mayoría de firewall cuentan con la capacidad para implementar cifrado VPN.⁶⁶ En la actualidad existen diversos proveedores de firewalls con capacidad VPN, donde un aspecto importante a evaluar es la seguridad del sistema operativo sobre el cual se ejecuta, es así que se debe evaluar las vulnerabilidades de dicho sistema operativo.⁶⁷

2.7.2 VPN Basadas en Enrutador y/o Proporcionadas por un ISP

Las VPN basadas en enrutador son adecuadas para organizaciones que realizan grandes inversiones en enrutadores que soporten esta tecnología y además su personal técnico tenga experiencia en la configuración de los mismos⁶⁸ o en su defecto dejar la administración y configuración de los enrutadores a cargo del proveedor ISP con lo que la solución pasaría a ser proporcionada por un ISP dejando el control, administración y seguridad en manos de un tercero.⁶⁹ Un punto importante a tener en cuenta es el desempeño de los enrutadores pues la adición del proceso de cifrado al enrutamiento podría complicar el performance del mismo.⁷⁰

2.7.3 VPN Basadas en Software

Tal como su nombre lo indica una VPN basada en software utiliza un programa para establecer túneles o encriptar datos entre dos puntos. Generalmente se utiliza entre un cliente y un servidor. Por ejemplo, en una VPN de PPTP o L2TP, es necesario que el software se encuentre cargado tanto en el cliente como en el servidor de esta manera se establece una sesión de VPN entre ambos puntos.⁷¹ Este tipo de VPN ofrece gran flexibilidad pues cuenta con amplia variedad de plataformas y de fácil instalación con un consecuente bajo costo para su implementación.

⁶⁶ Cfr. ORTEGA 2003:77

⁶⁷ Cfr. ORTEGA 2003:78

⁶⁸ Cfr. ORTEGA 2003:80

⁶⁹ Cfr. ORTEGA 2003:74

⁷⁰ Cfr. ORTEGA 2003:80

⁷¹ Cfr. ORTEGA 2003:84

La siguiente Tabla 4 indica las ventajas y desventajas de la implementación de la VPN utilizando diferentes arquitecturas, con lo que se podrá desarrollar un conjunto de requisitos, sobre los cuales basar una decisión sobre que VPN usar.⁷²

Tabla 4
Ventajas y Desventajas de Arquitecturas VPN

Arquitectura VPN	Ventajas	Desventajas
Firewall	Gran variedad de plataformas; uso del hardware o software existente.	Posibles brechas de seguridad por las vulnerabilidades del sistema operativo sobre el cual se ejecuta.
Enrutador	Bajo costo si se usa el hardware existente.	Podrian necesitar tarjetas adicionales, problemas de performance o requerir equipos mas robustos.
Software	Gran variedad de plataformas, facilidad de instalacion, buena para la gran mayoría de organizaciones por su bajo costo.	Posibles brechas de seguridad por las vulnerabilidades del sistema operativo sobre el cual se ejecuta.

Fuente: Elaboración propia.

2.8 Selección de alternativa de solución

Después de la evaluación técnica en cuanto a los requerimientos del proyecto y de factibilidad de las diversas soluciones existentes para VPN, y además de tomar en cuenta los recursos con lo que la organización objetivo dispone se determinó que la solución de VPN basada en software cumple con los requerimientos que la organización necesita, específicamente la utilización del sistema operativo Microsoft Windows Server, esta decisión se tomó entre otros motivos porque la organización tiene una política de estandarización en el uso de productos Microsoft, además de contar con las licencias correspondientes para la implementación y uso de este sistema operativo.

Así mismo cabe señalar que la organización objetivo tiene como prioridad explotar su recursos informáticos existentes es decir utilizar todo su potencial con el fin lograr la reducción de egresos.

⁷² Cfr. TORRES 2002:41

3 DEFINICION DEL PROBLEMA

3.1 El Problema

La organización presenta como problema principal la falta de comunicación en tiempo real entre la sede principal y sus sucursales, donde la red actual posee un direccionamiento IP no segmentado por sucursal lo que impide el crecimiento ordenado y la correcta administración de direcciones IP, así mismo la red actual no cuenta con medidas de seguridad que protejan el flujo de datos en sus comunicaciones, además la topología actual de red no permite la centralización de recursos TI lo cual afecta la disponibilidad de la información, consecuentemente a esto las sucursales no cuentan con acceso a la información e infraestructura que se encuentran en la sede principal como es el caso del ERP Microsoft Dynamics donde se registra información relevante propia del negocio como stock de los almacenes, ventas diarias y control diario de cajas por sucursal, es así que las sucursales no registran la información directamente al ERP, la información es enviada por correo electrónico generando casos de duplicidad y desactualización de hasta 3 días en fines de semana generando así información desactualizada en los sistemas de información de cada sucursal, lo cual origina errores y lentitud en la toma de decisiones importantes para la organización.

La organización cuenta con una oficina principal de 32 usuarios y cinco sucursales de 10 usuarios cada una, con un total de 82 usuarios en toda la organización. En la sede principal se cuenta con 7 usuarios críticos de las áreas de Gerencia, Finanzas y Almacén, quienes toman importantes decisiones diariamente en base a la información comercial recibida por cada sucursal, es así que es de vital importancia recibir la información de cada sucursal en tiempo real ya que con esta información se pueden tomar acciones que afectan directamente la economía de la organización, donde en algunos casos se puede llegar a perder hasta el 10% de ventas diarias por sucursal.

En general, la oficina principal y las sucursales se encuentran sin comunicación una de otra. Los procesos, registros, e información generada por cada sucursal son almacenados localmente en un tiempo determinado para posteriormente al final de cada jornada laboral sean enviadas vía correo electrónico y luego al día siguiente registrado en la base de datos de la sede principal de manera manual. Todo este proceso genera duplicidad de datos,

perdida de los mismos y retraso en la información de 1 día y hasta de 3 días los fines de semana. En resumen todo lo explicado genera problemas puntuales por área como:

En el área de Logística: No es posible contar con la información de stock de equipos en tiempo real de las diversas sucursales ya que esta gestión se realiza telefónicamente local por local con la consecuente demora que este medio representa, de esta manera no se aprovecha el uso del ERP Microsoft Dynamics (ubicada solo en la sede principal), lo que origina retardos en las coordinaciones de envíos, traslados e intercambios de mercadería entre los diversos locales.

En el área Comercial: No es posible contar con la información de ventas por producto en tiempo real de las diversas sucursales ya que esta gestión se realiza telefónicamente local por local con la consecuente demora que este medio representa, de esta manera no se aprovecha el uso del ERP Microsoft Dynamics (ubicada solo en la sede principal), lo que origina el retardo en toma de decisiones comerciales como lo son estrategias de mercado por medio de ofertas y/o promociones que permitan vender aquellos productos de poca rotación o movilizar productos a locales donde el segmento de mercado por ubicación geográfica requiera de algún producto en particular propio de la demanda del tipo de consumidor local.

En el área Finanzas: No es posible contar con la información del dinero recaudado por las cajas en tiempo real de las diversas sucursales ya que esta gestión se realiza telefónicamente local por local con la consecuente demora que este medio representa, de esta manera no se aprovecha el uso del ERP Microsoft Dynamics (ubicada solo en la sede principal), lo que origina el retardo en toma de decisiones económicas pues la liquidez de dinero es un tema crucial en las importantes decisiones financieras en toda organización, lo que permitirá saber con exactitud con cuánto dinero se cuenta en tiempo real para poder adquirir más productos y generar así la rotación efectiva del dinero recaudado día a día por cada local comercial.

En el área de Sistemas: La empresa tiene recursos limitados de sistemas de alta disponibilidad, si se produce una falla de hardware en algún servidor crítico o pérdida de energía en la sede principal puede afectar seriamente la productividad, lo cual significa un problema latente por resolver. Así mismo tampoco es posible aplicar los controles de seguridad de la sede principal a las sucursales, de la misma forma los usuarios solo pueden acceder a sus perfiles de usuario estando físicamente en la sede principal, teniendo un perfil

distinto y duplicado en las sucursales, y finalmente no se cuenta con replicación de servidores como base de datos y active directory para la alta disponibilidad, a pesar de contar con sucursales que operan continuamente pudiendo aprovechar su disponibilidad y espacio físico.

3.2 Descripción del Entorno de la Organización

Como se explicó anteriormente la carga administrativa para el control de las sucursales soportada por la sede principal es crítica más aun en fechas de alto transito comercial como son fiestas patrias y navidad, esto debido a que toda la organización se encuentra incomunicada entre sus diversos locales, por lo que la solución consiste en un sistema de comunicación de datos mediante redes privadas virtuales entre la sede principal y sus sucursales, es así que el campo de acción o entorno para el presente proyecto serán las áreas de Logística, Comercial, Finanzas y Sistemas, donde las soluciones propuestas para cada área impactaran en toda la organización gracias al diseño de un sistema de comunicación efectivo que interconectara a todos los locales de la organización.

La organización cuenta con una oficina principal y cinco sucursales siendo un total de 82 usuarios, así mismo dispone de los siguientes recursos informáticos distribuidos de la siguiente manera:

Tabla 5
Equipos y Usuarios en Oficina Principal

EQUIPOS Y USUARIOS EN OFICINA PRINCIPAL				
Grupo de Usuarios / Usuario	Nombre PC	Dirección IP	Equipo	Cant.
GERENCIA				3
Fernando Drago	GER-01	DHCP	Core I5 / 1Gb / 500GB	
Hugo Martel	GER-02	DHCP	Core I5 / 1Gb / 500GB	
Elizabeth Morales	GER-03	DHCP	Core I3 / 1Gb / 500GB	
FINANZAS				2
Luis Zender	FI-01	DHCP	Core I3 / 2Gb / 1TB	
Karen Rojas	FI-02	DHCP	Core I3 / 2Gb / 1TB	
ALMACÉN				2
Karina Pazos	AL-01	DHCP	Core I3 / 2Gb / 1TB	
Jaime Quenaya	AL-02	DHCP	Core I3 / 2Gb / 1TB	
CRÉDITOS				2
Pedro Solis	CRE-01	DHCP	Core I3 / 1Gb / 500GB	
Alberto Zurita	CRE-02	DHCP	Core I3 / 1Gb / 500GB	
JEFATURA DE VENTAS				2
Jaime Lopez Torres	JVEN-01	DHCP	Core I3 / 1Gb / 500GB	
Manuel Montiel	JVEN-02	DHCP	Core I3 / 1Gb / 500GB	
SOPORTE DE VENTAS				2
Cynthia Llanos	SVEN-01	DHCP	Core I3 / 1Gb / 500GB	
Roxana Carbonell	SVEN-02	DHCP	Core I3 / 1Gb / 500GB	

VENTAS CORPORATIVAS				10
Ivan Tamayo	VEN-01	DHCP	Pentium 4 3.00 / 512mb / 80GB	
Daniel Folezani	VEN-02	DHCP	Pentium 4 3.00 / 512mb / 80GB	
Marita Rodriguez	VEN-03	DHCP	Pentium 4 3.00 / 512mb / 80GB	
Katerine Lurquin	VEN-04	DHCP	Pentium 4 3.00 / 512mb / 80GB	
Fredy Moreno	VEN-05	DHCP	Pentium 4 3.00 / 512mb / 80GB	
Geson Bustamante	VEN-06	DHCP	Pentium 4 3.00 / 512mb / 80GB	
Fabio Sanchez	VEN-07	DHCP	Pentium 4 3.00 / 512mb / 80GB	
Vendedor Libre	VEN-08	DHCP	Pentium 4 3.00 / 512mb / 80GB	
Vendedor Libre	VEN-09	DHCP	Pentium 4 3.00 / 512mb / 80GB	
Vendedor Libre	VEN-10	DHCP	Pentium 4 3.00 / 512mb / 80GB	
CALL CENTER				5
Operador 01	CC-01	DHCP	Pentium 4 3.00 / 512mb / 80GB	
Operador 02	CC-02	DHCP	Pentium 4 3.00 / 512mb / 80GB	
Operador 03	CC-03	DHCP	Pentium 4 3.00 / 512mb / 80GB	
Operador 04	CC-04	DHCP	Pentium 4 3.00 / 512mb / 80GB	
Operador 05	CC-05	DHCP	Pentium 4 3.00 / 512mb / 80GB	
PROYECTOS				4
Proyecto 01	PR-01	DHCP	Core I3 / 1Gb / 500GB	
Proyecto 02	PR-02	DHCP	Core I3 / 1Gb / 500GB	
Proyecto 03	PR-03	DHCP	Core I3 / 1Gb / 500GB	
Proyecto 04	PR-04	DHCP	Core I3 / 1Gb / 500GB	

Fuente: Elaboración propia.

Así mismo dispone de las siguientes aplicaciones:

Tabla 6
Lista de Aplicaciones

LISTA DE APLICACIONES	
Microsoft Dynamics	Con licencia
Microsoft Office 2007	Con 20 licencias
Windows XP SP3	Con 40 licencias
Antivirus AVG Internet Security 2015	Licencia Free

Fuente: Elaboración propia.

El departamento de TI es responsable de los equipos de comunicaciones que tienen bajo su custodia, entre los cuales se tienen los siguientes:

Tabla 7
Dispositivos de Red.

DISPOSITIVOS DE RED	
Oficina principal	
Router Cisco 851	1
Switch D-Link 24 puertos 10/100 Modelo DES-1024D	2
Access Point TP-Link	2
Sucursales	
Router Zyxel P660 HW-T1V2	5
Switch D-Link 16 puertos 10/100 Modelo DES-1016D	5

Fuente: Elaboración propia.

Tabla 8
Internet y Ancho de Banda

INTERNET Y ANCHO DE BANDA	
Oficina principal	
Proveedor de Servicios: Movistar / Linea negocios	
Ancho de banda	1MB al 25%
Pool de IP públicas	200.110.28.72 /29
Sucursales	
Proveedor de Servicios: Movistar / Linea comercial	
Ancho de banda	1MB al 10%
Pool de IP públicas	----

Fuente: Elaboración propia.

Así también, se encargan de la gestión de los siguientes servidores, los cuales forman parte de la infraestructura y soporte de los servicios que emplean a diario los usuarios.

Tabla 9
Servidores de la Organización

SERVIDORES DE LA EMPRESA MEGA LINE SAC

Item	Value
Nombre de computadora	SRV-DC
Nombre de dominio	MEGALINESAC.COM
Roles	DC, DHCP, DNS, PRINT SERVER
Descripción	Servidor 01
Sistema operativo	Microsoft Windows Server 2003 Enterprise Edition SP2
Fabricante	HP
Modelo	ProLiant ML110
Numero de serial	
Numero de procesadores	1
Descripción del procesador	Intel® Pentium® 4 CPU 3.20 GHZ
Memoria RAM	1534MB
Memoria en disco duro	68.35GB (C: 19.53GB, D: 48.82GB)6.57GB y 1.19GB
Pantalla	SyncMaster 933, 18.5"
Versión de Bios	PhoenixBIOS 4.0 Release 6.0
Dirección IP	192.168.1.100
Dirección máscara de red	255.255.255.0
Dirección puerta de enlace	192.168.1.1

Item	Value
Nombre de computadora	SRV-BD
Nombre de dominio	MEGALINESAC.COM
Roles	Database Server
Descripción	Servidor 02
Sistema operativo	Microsoft Windows Server 2008 R2 STD 64-bit
Fabricante	IBM
Modelo	X3400 M3
Numero de serial	
Numero de procesadores	1
Descripción del procesador	Intel® Xeon® 4 CPU E5620 2.40 GHZ
Memoria RAM	4.00 GB
Memoria en disco duro	464.60GB (C: 195.31GB, D: 269.09GB)
	929.33GB (E: 273.44GB, F: 273.44GB, G: 382.46GB)
Pantalla	SyncMaster 933, 18.5"
Versión de Bios	PhoenixBIOS 4.0 Release 6.0
Dirección IP	192.168.1.101
Dirección máscara de red	255.255.255.0
Dirección puerta de enlace	192.168.1.1

Fuente: Elaboración propia.

3.3 Identificación de los Interesados

A continuación se muestra un cuadro con el detalle de los interesados de acuerdo al nivel de interés e influencia que tienen en el proyecto:

Tabla 10

Identificación de los Interesados

Nombre del Interesado	Organización a que pertenece	Categoría de interesado	Nivel interés (Bajo, Medio, Alto)	Nivel influencia (Bajo, Medio, Alto)
Fernando Drago	DAC - Mega Line	Patrocinador	Alto	Alto
Mega Line SAC	DAC - Mega Line	Cliente	Alto	Alto
Personal Tiendas	DAC - Mega Line	Usuario	Bajo	Bajo
Fernando Drago	DAC - Mega Line	Alta Dirección	Alto	Alto
Ing. Alvaro C.	América Movil	Proveedor	Alto	Medio
Hugo Martel V.	DAC - Mega Line	Director Proyecto	Alto	Alto
Luis Sanchez	DAC - Mega Line	Miembro proyecto	Alto	Medio

Fuente: Elaboración propia.

3.4 Requerimientos del Cliente

Después de definir los requerimientos de la organización, se estableció una serie de especificaciones de tal manera que se ajuste a las necesidades que se requieren cubrir en la

organización, por lo que se ha estructurado estos requerimientos en base a los objetivos específicos que a continuación explicaremos:

3.4.1 Segmentación de Red de Datos Escalable

Requerimiento: Establecer una segmentación de red escalable para las sucursales mediante el cálculo VLSM bajo el cumplimiento del RFC 1878, con las siguientes especificaciones:

- Se deberá tener como base el RFC 1878 que indica la división de sub redes por clase, donde a partir de la red de clase B se deberá realizar los cálculos VLSM que finalmente entreguen las sub redes por local con sus respectivas direcciones IP.
- Para el cálculo de sub redes se deberá contemplar con una sede principal y un mínimo de 9 sucursales es decir con 10 sub redes donde para el caso de la sede principal se deberá contemplar como mínimo 100 host y para cada una de las sucursales el mínimo de hosts requeridos será de 20.
- La tabla de direcciones IP deberá especificar la dirección y mascara de red por local, así como su puerta de enlace y su rango respectivo de direcciones IP válidas, además del número de hosts máximos permitidos por sub red.
- La clase de red elegida deberá contar con una disponibilidad mayor al 90% de redes disponibles para el crecimiento de futuros locales, donde cada sub red a su vez deberá contar con un mínimo de 20 hosts disponibles.

Entregable: Informe de la segmentación en sub redes y tabla de direcciones IP con Nivel de escalabilidad de la red clase B mayor al 90% del total de redes disponibles.

Justificación: Gracias a la segmentación de redes es posible aislar el tráfico de datos por área, departamento o sucursal de esta manera se evita posibles tormentas de broadcast que podría dar como resultado una congestión de red y por consecuencia su mal funcionamiento. Además la segmentación de red ofrece múltiples ventajas como la simplicidad en la administración de la red pues ayuda a poder gestionar y diferenciar las políticas de seguridad por área, departamento o sucursal. Así mismo es de gran utilidad para controlar el crecimiento de la red ya sea por nuevas áreas, departamento o sucursales.

3.4.2 Configuración de Red VPN que brinde Seguridad

Requerimiento: Desarrollar una configuración de red VPN que brinde seguridad de datos en el flujo de la información bajo el cumplimiento del RFC 3193, con las siguientes especificaciones:

- Se deberá tener como base el RFC 3193 que indica la utilización del protocolo L2TP para redes privadas virtuales conjuntamente con el protocolo IPSec con el fin de proporcionar autenticación de túnel, privacidad, control de integridad y protección de reproducción.
- La configuración de red VPN deberá proporcionar mayor seguridad en la red de datos reduciendo los riesgos que afecten la Confidencialidad e Integridad de la información que se transmita sobre ella.
- La guía de configuración deberá contemplar paso a paso las opciones y detalles de configuración con la entrega de imágenes que muestren la configuración realizada.
- La guía de configuración deberá contemplar los siguientes manuales VPN:
 - Configuración VPN Sitio a Sitio entre Servidores SRV-TMG1 y SRV TMG2.
 - Configuración VPN Sitio a Sitio entre Servidores SRV-TMG1 y SRV-VPN1.

Se entiende que para el caso del manual de configuración entre servidores SRV-TMG1 y SRV-VPN1 se deberá replicar la misma configuración a cada sucursal donde el servidor SRV-TMG1 se encuentra en la oficina principal y el servidor SRV-VPN1 corresponde al local 1, el mismo que será replicado en los servidores SRV-VPN2, SRV-VPN3, SRV-VPN4 respectivamente.

- Con el fin de brindar seguridad adicional se deberá entregar los siguientes manuales:
 - Configuración de Microsoft ForeFront TMG: Regla Acceso a Internet.
 - Configuración de Microsoft ForeFront TMG: Regla Internet Restringido.
 - Manual de Configuración Proxy para PC.
- Se deberá realizar una matriz de evaluación de riesgos en la seguridad de la información antes y después del funcionamiento de la red privada virtual con el fin de determinar la variación de riesgos de la seguridad de la información y determinar el nivel de riesgos minimizados, controlados o eliminados.

Entregable: Guía de configuración de protocolos de seguridad y matriz de evaluación de riesgos en la seguridad de la información con un nivel de riesgos bajos al 100% o con una reducción mayor al 60% de riesgos en la seguridad de la información.

Justificación: Por medio del uso de protocolos de seguridad se podrá contar con una red que proporcione confidencialidad e integridad en el flujo de la información entre sucursales garantizando así la veracidad de la misma lo que permitirá tomar buenas decisiones en base a información real integra y segura.

3.4.3 Topología de Red con Distribución Centralizada

Requerimiento: Presentar un diseño de topología de red lógica centralizada con accesibilidad a la infraestructura y optimización de recursos TI para la disponibilidad de la información con las siguientes especificaciones:

- La topología deberá ser presentada de manera gráfica con la identificación de los elementos de red involucrados así como sus respectivos nombres y tipo de enlaces por sucursal.
- Se deberá contemplar en la topología la red IP y número de hosts por sucursal de acuerdo al cálculo realizado en el primer requerimiento: Establecer una segmentación de red escalable para las sucursales mediante el cálculo VLSM.
- Se deberá especificar una sucursal como centro de datos alternativo en el cual se ubicaran los servidores: AD, BD y Firewall secundarios.
- Para asegurar la disponibilidad de recursos se deberá entregar los siguientes manuales:
 - Configuración de Controlador de Dominio Secundario.
 - Instalación de SQL Server en Servidor Secundario.
 - Configuración de Replicación de Base de Datos.
 - Configuración de Microsoft ForeFront TMG: Regla VPN Acceso Remoto.

Entregable: Gráfico con topología de red y distribución centralizada con el cálculo de disponibilidad de la información mayor al 90% mensual.

Justificación: Gracias a una distribución de red centralizada todas las sucursales podrán tener acceso a los recursos TI e información lo que permitirá tomar buenas decisiones en base a información actualizada en tiempo real y en todo momento.

3.5 EDT del Proyecto

A continuación se presenta la Estructura del Desglose del Trabajo (EDT), donde se encuentra el detalle de lo que se realizará en el presente proyecto, además se visualizan las etapas del proyecto y los entregables de cada una de ellas.

Figura 10. EDT del Proyecto

Fuente: Elaboración propia.

Tabla 11

Tabla Resumen de Objetivos Específicos y Requerimientos

TABLA RESUMEN DE OBJETIVOS ESPECIFICOS Y REQUERIMIENTOS	
Objetivo Especifico 1:	Establecer una segmentación de red escalable para las sucursales mediante el cálculo VLSM bajo el cumplimiento del RFC 1878.
RFC 2764:	Requisito: Distribución de Direcciones IP
RFC 1878: En su página 3: Subredes y Redes, indica: “El número de direcciones de red y de host disponibles se deriva del número de bits utilizados para el enmascaramiento de subred. Las siguientes tablas representan el número de bits de subredes y la red resultante, direcciones de broadcast y direcciones de host.	Se deberá tener como base el RFC 1878 que indica la división de sub redes por clase, donde a partir de la red de clase B se deberá realizar los cálculos VLSM que finalmente entreguen las sub redes por local con sus respectivas direcciones IP.
	Para el cálculo de sub redes se deberá contemplar con una sede principal y un mínimo de 9 sucursales es decir con 10 sub redes donde para el caso de la sede principal se deberá contemplar como mínimo 100 host y para cada una de las sucursales el mínimo de hosts requeridos será de 20.
	La tabla de direcciones IP deberá especificar la dirección y mascara de red por local, así como su puerta de enlace y su rango respectivo de direcciones IP válidas, además del número de hosts máximos permitidos por sub red.
	La clase de red elegida deberá contar con una disponibilidad mayor al 90% de redes disponibles para el crecimiento de futuros locales, donde cada su red a su vez deberá contar con un mínimo de 20 hosts disponibles.
Objetivo Especifico 2:	Desarrollar una configuración VPN que brinde seguridad de datos en el flujo de su información mediante el uso protocolos L2TP/IPSec bajo el cumplimiento del RFC 3193.
RFC 2764:	Requisito: Seguridad y Mecanismo de Tunnelización
RFC 3193: En su página 2: Introducción, indica: “Este documento propone el uso del conjunto de protocolos IPsec para proteger El tráfico L2TP a través de redes IP, y explica cómo IPsec y L2TP deben ser utilizados juntos.”	Se deberá tener como base el RFC 3193 que indica la utilización del protocolo L2TP para redes privadas virtuales conjuntamente con el protocolo IPsec con el fin de proporcionar autenticación de túnel, privacidad, control de integridad y protección de reproducción.
	La configuración de red VPN deberá proporcionar mayor seguridad en la red de datos reduciendo los riesgos que afecten la Confidencialidad e Integridad de la información que se transmita sobre ella.
	La guía de configuración deberá contemplar paso a paso las opciones y detalles de configuración con la entrega de imágenes que muestren la configuración realizada.
	Se deberá realizar una matriz de evaluación de riesgos en la seguridad de la información antes y después del funcionamiento de la red privada virtual con el fin de determinar la variación de riesgos de la seguridad de la información y determinar el nivel de riesgos minimizados, controlados o eliminados.

<p>Objetivo Especifico 3:</p> <p>Presentar una topología de red lógica centralizada que permita proponer medidas de optimización de recursos TI para la disponibilidad de la información.</p>	<p>La topología deberá ser presentada de manera gráfica con la identificación de los elementos de red involucrados así como sus respectivos nombres y tipo de enlaces por sucursal.</p> <p>Se deberá contemplar en la topología la red IP y número de hosts por sucursal de acuerdo al cálculo realizado en el primer requerimiento: Diseñar una segmentación de red escalable para las sucursales mediante el cálculo VLSM.</p> <p>Se deberá especificar una sucursal como centro de datos alternativo en el cual se ubicaran los servidores: AD, BD y Firewall secundarios.</p>
<p>Adicionales</p>	<p>Con el fin de brindar seguridad adicional se deberá entregar los siguientes manuales:</p> <ul style="list-style-type: none"> - Configuración de Microsoft ForeFront TMG: Regla Acceso a Internet. - Configuración de Microsoft ForeFront TMG: Regla Internet Restringido. - Manual de Configuración Proxy para PC. <p>Para asegurar la disponibilidad de recursos se deberá entregar los siguiente manuales:</p> <ul style="list-style-type: none"> - Configuración de Controlador de Dominio Secundario. - Instalación de SQL Server en Servidor Secundario. - Configuración de Replicación de Base de Datos. - Configuración de Microsoft ForeFront TMG: Regla VPN Acceso Remoto.

Fuente: Elaboración propia.

4 DISEÑO DE LA SOLUCION

4.1 Descripción del Diseño de la Solución

Actualmente la empresa tiene cinco sucursales las cuales trabajan de manera independiente sin comunicación directa a los sistemas que se alojan en la oficina principal, es así que siendo un problema el acceso a la información y recursos de la oficina principal. La solución propuesta consiste en el diseño de una red de comunicación mediante redes privadas virtuales entre las sucursales y la sede principal con el fin de optimizar recursos y agilizar las transacciones diarias propias del giro del negocio, para lo cual el eje principal de la solución es la interconexión de la sede principal y sus sucursales, para dicho fin se consideraron diversas soluciones de comunicación entre locales, las cuales fueron explicadas, detalladas y analizadas en el capítulo anterior. En dicho análisis se buscó que la solución responda a criterios como: escalabilidad, fácil implementación, control interno, y sobre todo economía para cumplir con dichos conceptos se contó con aplicativos de software con los que la organización ya dispone, además de convenios institucionales con un importante socio estratégico en comunicaciones como lo es América Móvil Perú SAC.

Es así que la solución consiste en el diseño de una red de comunicación mediante redes privadas virtuales a través de Internet, gracias a esta solución será posible conseguir lo siguiente:

- La interconexión de las redes de cada sucursal con la oficina principal permitiendo la agilización de los procesos y el intercambio de la información en tiempo real entre los usuarios.
- El acceso a la base de datos desde cualquiera de las sucursales logrando que los usuarios tengan disponible la información inmediata y en tiempo real.
- Controle de acceso y seguridad a las sucursales desde la sede principal haciendo uso de las políticas de seguridad, tales como prohibiciones de las páginas web comúnmente conocidas, que contribuirán en la productividad laboral de los empleados.
- Respaldo y replicación de datos en tiempo real con lo que se podrá estar preparado ante alguna incidencia y retomar las operaciones inmediatamente.

4.2 Justificación del Recurso Humano para la Solución

Para la implementación del proyecto se requerirá en primer lugar un jefe de proyectos para liderar el despliegue de la solución, así mismo se requiere de personal especializado en soluciones VPN de Microsoft así como personal interno que este monitoreando constantemente el desempeño de la solución. Este grupo de trabajo tendrá la siguiente estructura:

Figura 11. Estructura del Recurso Humano

Fuente: Elaboración propia.

- **Jefe de Proyecto:** Responsable de reportar a la Gerencia los avances del proyecto, así como la de organizar y solicitar la documentación de cada una de las etapas realizadas.
- **Ingeniero de Redes (ISP):** Encargado de coordinar con el cliente los enlaces de internet dedicado a cada una de las sedes para poder disponer de las capacidades solicitadas según SLAs. Además de dejar operativos los dispositivos de red con sus respectivas IPs públicas en cada sede.
- **Ingeniero de Redes:** Responsable del diseño de red y conexión VPN entre la oficina principal y cada una de las sedes, además de establecer el direccionamiento de red de todas las sedes, así mismo supervisara el trabajo del técnico especialista VPN Microsoft.
- **Técnico de Redes (VPN):** Responsable de instalar y configurar cada enlace VPN de las sucursales, así mismo realizara las conexiones del cableado entre los routers ISP y los servidores VPN.
- **Soporte Técnico:** Encargado de toda el área de sistemas de la organización objetivo quien tendrá como función principal monitorear la solución una vez haya concluido quien además deberá ser capacitado previamente en los detalles y funciones de la solución implementada.

4.3 Recursos Disponibles en la Organización Objetivo

4.3.1 Recurso Humano Disponible

En el punto anterior se identificó el recurso humano necesario para la implementación del proyecto, sin embargo la organización objetivo dispone de personal en sistemas a un nivel básico es así que se requerirá de personal externo especializado para la ejecución del proyecto. En la actualidad la organización objetivo cuenta con un técnico de sistemas que se hace cargo de dar soporte técnico TI a toda la organización en sus diversos locales. Este personal podría cumplir con la labor de monitorear la solución una vez que haya sido implementada para lo cual requerirá de una capacitación previa en cuanto a las configuraciones y funciones de la solución. Según lo expuesto a continuación se detalla el personal interno con el que se dispone así como externo que deberá ser adquirido para completar el equipo de trabajo:

Tabla 12

Recurso Humano Disponible y por Adquirir

Interno/Externo	Cargo	Justificación
Interno - DAC Claro	Jefe de Proyecto	La jefatura del proyecto sera liderada por el Gerente de Operaciones de la organización quien tendra como responsabilidad realizar las coordinaciones necesarias que el proyecto requiera.
Externo - America Movil	Ingeniero de Redes	Se debera contar con personal del ISP para la coordinacion de detalles tecnicos de conexión de enlaces en cada sede de la organización.
Externo	Ingeniero de Redes	Tendra como funcion el diseño y direccion tecnica del proyecto a implementar asi como la coordinacion operativa con el tecnico especialista en redes.
Externo	Tecnico de Redes	Debera ser personal con amplio conocimiento de soluciones VPN de Microsoft, para instalar y configurar la solucion.
Interno - DAC Claro	Soporte Tecnico	Responsable de la monitorizacion de la solucion una vez que haya sido implementada, ademas de realizar las configuraciones necesarias para la replicacion de servidores.

Fuente: Elaboración propia.

4.3.2 Recurso Material Disponible

En la actualidad la organización objetivo cuenta con dos servidores que cumplen funciones de servidor de controlador de dominio y servidor de base de datos, a continuación se detallan:

Tabla 13
Servidores Organización DAC

Item	Value
Nombre de computadora	SRV-DC
Nombre de dominio	MEGALINESAC.COM
Roles	DC, DHCP, DNS, PRINT SERVER
Descripción	Servidor 01
Sistema operativo	Microsoft Windows Server 2003 Enterprise Edition SP2
Fabricante	HP
Modelo	ProLiant ML110
Numero de serial	
Numero de procesadores	1
Descripción del procesador	Intel® Pentium® 4 CPU 3.20 GHZ
Memoria RAM	1534MB
Memoria en disco duro	68.35GB (C: 19.53GB, D: 48.82GB)6.57GB y 1.19GB
Pantalla	SyncMaster 933, 18.5"
Versión de Bios	PhoenixBIOS 4.0 Release 6.0
Dirección IP	192.168.1.100
Dirección máscara de red	255.255.255.0
Dirección puerta de enlace	192.168.1.1

Item	Value
Nombre de computadora	SRV-BD
Nombre de dominio	MEGALINESAC.COM
Roles	Database Server
Descripción	Servidor 02
Sistema operativo	Microsoft Windows Server 2008 R2 STD 64-bit
Fabricante	IBM
Modelo	X3400 M3
Numero de serial	
Numero de procesadores	1
Descripción del procesador	Intel® Xeon® 4 CPU E5620 2.40 GHZ
Memoria RAM	4.00 GB
Memoria en disco duro	464.60GB (C: 195.31GB, D: 269.09GB) 929.33GB (E: 273.44GB, F: 273.44GB, G: 382.46GB)
Pantalla	SyncMaster 933, 18.5"
Versión de Bios	PhoenixBIOS 4.0 Release 6.0
Dirección IP	192.168.1.101
Dirección máscara de red	255.255.255.0
Dirección puerta de enlace	192.168.1.1

Fuente: Elaboración propia.

Sin embargo para el desarrollo e implementación de la solución se requerirá de servidores adicionales que deberán ser adquiridos y cuyas características se detallan a continuación:

Tabla 14

Características de Servidor HP Proliant

CARACTERISTICAS :			
MODELO	ProLiant ML110 G7		
PROCESADOR(GHZ)	INTEL	Intel® Xeon® E3-1220 (3.10 GHz, 8M Cache)	
MEMORIA	2 GB DDR3		
	NÚMERO DE RANURAS:	4	
	CAPACIDAD MAXIMA HASTA (GB)	16GB	
UNIDADES DE ALMACENAMIENTO	DISCO DURO (GB)		500 GB
	Controlador de almacenamiento:		
	SATA RAID de 6 puertos integrado		
INCORPORA	RED	Ethernet 10/100/1000 (Gigabit)	
PUERTOS	POSTERIOR: FRONTAL:	SERIAL(ES) :	1
		RJ-45:	2
		DB-15:	1
		USB:	4
		USB:	4
		USB:	4
FACTOR DE FORMA	4U		

Fuente: DELTRON - HP.

4.4 Especificaciones del Diseño de la Solución

Según RFC 2764 describe algunos conceptos muy importantes que se deberá considerar para establecer los lineamientos del Diseño de la Red, dichos conceptos explicados a detalle en el marco teórico dejan claro como es considerada una red privada virtual y por consecuencia indican su tratamiento para el diseño de la misma, a continuación se citara dichos conceptos:

“En el contexto de este documento, una VPN se define simplemente como la emulación de una instalación de red de área amplia (WAN) privada que utiliza instalaciones de IP (incluida la Internet pública o redes troncales de IP privadas).” (RFC2764 2018:4)

“Muchos aspectos de las redes, como el direccionamiento, el mecanismo de reenvío, la calidad del servicio (QoS), la seguridad y el cortafuegos, tienen soluciones comunes tanto en las redes físicas como en las virtuales, y muchos de los problemas que surgen en la discusión de las VPN tienen análogos directos con aquellos

problemas implementados en redes físicas. La introducción de VPN no crea la necesidad de reinventar la red, o de introducir paradigmas completamente nuevos que no tengan un análogo directo con las redes físicas existentes.” (RFC2764 2018:4)

“Claramente, tener mecanismos que son comunes en las redes tanto físicas como virtuales facilita la introducción de redes privadas virtuales (VPN) en las redes existentes y también reduce el esfuerzo necesario tanto para el desarrollo de estándares como para el desarrollo de productos, ya que las soluciones existentes pueden aprovecharse.” (RFC2764 2018:5)

Por lo que gracias a estos conceptos podemos determinar que para el Diseño de la red se deberá definir los mismos componentes de una red WAN, así mismo se sabe una red WAN es la unión de dos o más redes de área local (LANs), además el RFC 2764 propone los siguientes requisitos generales VPN:

- **Transporte de Paquetes:** El tráfico transportado dentro de una VPN puede no tener relación con el tráfico en la red troncal IP, ya sea porque el tráfico es multiprotocolo, o porque la red IP del cliente puede usar un direccionamiento IP no relacionado con el de la red troncal IP en la que se transporta el tráfico.⁷³

Es así que la red IP del cliente u organización puede utilizar direcciones IP privadas no únicas, por lo que será necesario definir un direccionamiento de red para las sucursales, esta segmentación de red será definida a detalle en el Objetivo específico 1: Establecer una segmentación de red escalable para las sucursales mediante el cálculo VLSM bajo el cumplimiento del RFC 1878.

- **Seguridad de Datos:** Una VPN requiere algún tipo de seguridad de datos, es así que existen diferentes modelos de confianza aplicables al uso de VPNs. Uno de esos modelos es donde el cliente no confía en que el proveedor de servicios ISP proporcione ningún tipo de seguridad, y en su lugar implementa una VPN utilizando dispositivos CPE que implementan la funcionalidad de firewall y que están conectados entre sí mediante túneles seguros. En este caso, el proveedor de servicios se utiliza únicamente para el transporte de paquetes IP.⁷⁴

⁷³ Cfr. RFC2764 2018

⁷⁴ Cfr. RFC2764 2018

Para el cumplimiento de este requisito se ha definido la utilización dispositivos CPE como son los servidores VPN y TMG donde se realizaran las configuraciones necesarias para el funcionamiento VPN, esto será definido a detalle en el Objetivo específico 2: Desarrollar una configuración VPN que brinde seguridad de datos en el flujo de sus comunicaciones mediante el uso protocolos L2TP/IPsec bajo el cumplimiento del RFC 3193.

- **Mecanismos de Tunnelización:** Las VPN deben implementarse a través de algún tipo de mecanismo de tunnelización de IP, donde los paquetes formatos y/o el direccionamiento utilizado dentro de la VPN pueden no estar relacionados con los utilizados para enrutar los paquetes tunnelizados a través de la red troncal IP. Dichos túneles, dependiendo de su forma, pueden proporcionar cierto nivel de seguridad de datos intrínseca, o esto también puede mejorarse utilizando otros mecanismos como IPsec.⁷⁵

Los mecanismos de tunnelización son proporcionados por la utilización en conjunto de L2TP/IPsec cuyas especificaciones de su uso se detallan en el Objetivo específico 2: Desarrollar una configuración VPN que brinde seguridad de datos en el flujo de sus comunicaciones mediante el uso protocolos L2TP/IPsec bajo el cumplimiento del RFC 3193.

- **Garantía de Calidad de Servicio:** Además de garantizar la privacidad de la comunicación, las técnicas de redes privadas existentes, basadas en mecanismos físicos o de capa de enlace, también ofrecen diversos tipos de garantías de calidad de servicio. En particular, las líneas arrendadas y de acceso telefónico ofrecen garantías de ancho de banda y latencia mediante el cumplimiento de SLAs del ISP.⁷⁶

Para el cumplimiento de este requisito se ha definido la exigencia del estricto cumplimiento de las métricas ofrecidas a través de los SLAs del ISP, así mismo con el fin de brindar un servicio de calidad se han definido medidas de optimización de recursos TI para la disponibilidad de la información, estas son explicadas a detalle en el Objetivo

⁷⁵ Cfr. RFC2764 2018

⁷⁶ Cfr. RFC2764 2018

específico 3: Presentar una topología de red lógica centralizada que permita proponer medidas de optimización de recursos TI para la disponibilidad de la información.

Dado que se definió el tratamiento de una VPN de la misma manera que una red física podemos alinear los componentes de red al cumplimiento de los objetivos específicos y a manera de resumen presentamos la Tabla 15 donde además de los componentes de red podemos observar los requisitos establecidos por el RFC 2764.

Tabla 15
Requisitos y Componentes VPN

Requisito RFC 2764 / Componente de Red	Objetivo Especifico
<ul style="list-style-type: none"> - Transporte de Paquetes (RFC 2764) - Segmentacion de Red. - Distribucion de Direcciones IP. 	<p>OE1: Establecer una segmentación de red escalable para las sucursales mediante el cálculo VLSM bajo el cumplimiento del RFC 1878.</p>
<ul style="list-style-type: none"> - Seguridad de Datos (RFC 2764) - Mecanismo de Tunelizacion (RFC 2764) - Configuración de red y S.O. - Protocolos de Red. - Servidor de Autenticacion. 	<p>OE2: Desarrollar una configuración VPN que brinde seguridad de datos en el flujo de sus comunicaciones mediante el uso protocolos L2TP/IPsec bajo el cumplimiento del RFC 3193.</p>
<ul style="list-style-type: none"> - Calidad de Servicio (RFC 2764) - Topologia de Red. 	<p>OE3: Presentar una topología de red lógica centralizada que permita proponer medidas de optimización de recursos TI para la disponibilidad de la información.</p>

Fuente: Elaboración propia.

Es así que después de definir los requerimientos de la organización se estableció una serie de soluciones de tal manera que se ajuste a las necesidades que se requiere cubrir en la organización, por lo que se ha estructurado estas necesidades en base a los objetivos específicos del proyecto que a continuación explicaremos:

4.4.1 Segmentación de Red de Datos Escalable

Según RFC 1878 describe las subredes válidas y máscaras de subred que se pueden usar en redes TCP/IP y según su página 3: Subredes y Redes, indica:

“El número de direcciones de red y de host disponibles se deriva del número de bits utilizados para el enmascaramiento de subred. Las siguientes tablas representan el número de bits de subredes y la red resultante, direcciones de broadcast y direcciones de host. La Tabla 1-1 representa la división en subredes de una red clase B” (RFC1878 2018:3)

Según RFC 1878 en su tabla 1-1 solo se especifica el número de sub redes desde 65534 hasta 510 hosts, por lo que se realizó el cálculo adicional de las siguientes sub redes desde 254 a 2 hosts, ya que para el presente proyecto se necesitara y utilizaran las redes de 126 y 30 hosts.

Tabla 16

Numero de Sub Redes de Red Clase B

Mascara Decimal	Mascara Binario	Nro. De Redes	Nro de Hosts
255.255.0.0	11111111.11111111.00000000.00000000	1	65534
255.255.128.0	11111111.11111111.10000000.00000000	2	32766
255.255.192.0	11111111.11111111.11000000.00000000	4	16382
255.255.224.0	11111111.11111111.11100000.00000000	8	8190
255.255.240.0	11111111.11111111.11110000.00000000	16	4094
255.255.248.0	11111111.11111111.11111000.00000000	32	2046
255.255.252.0	11111111.11111111.11111100.00000000	64	1022
255.255.254.0	11111111.11111111.11111110.00000000	128	510
255.255.255.0	11111111.11111111.11111111.00000000	256	254
255.255.255.128	11111111.11111111.11111111.10000000	512	126
255.255.255.192	11111111.11111111.11111111.11000000	1024	62
255.255.255.224	11111111.11111111.11111111.11100000	2048	30
255.255.255.240	11111111.11111111.11111111.11110000	4096	14
255.255.255.248	11111111.11111111.11111111.11111000	8192	6
255.255.255.252	11111111.11111111.11111111.11111100	16384	2

Fuente: RFC 1878.

Para lograr una red de comunicación entre los locales se diseñaran redes VPN Site to Site entre la sede principal y cada una de las 5 sucursales, para lo cual se contara con 5 conexiones VPN una por cada sucursal (S1, S2, S3, S4 y S5) según se muestra en la Tabla 17, donde se especifica la dirección IP para cada servidor por sucursal, además se muestra la dirección IP de los principales servidores.

Tabla 17
Asignación de direcciones IP para Servidores

SITIO	Servidor	Dirección IP	Máscara de subred
Oficina principal	Controlador de dominio primario	172.16.1.100	255.255.255.128
	Base de datos primario	172.16.1.101	255.255.255.128
	Servidor firewall / VPN (Red interna)	172.16.1.1	255.255.255.128
S1 - Plaza Lima Sur (Chorrillos)	Servidor VPN (Red Interna)	172.16.1.129	255.255.255.224
	Controlador de dominio secundario	172.16.1.130	255.255.255.224
	Base de datos secundario	172.16.1.132	255.255.255.224
S2 - Minka (Callao)	Servidor VPN (Red Interna)	172.16.1.161	255.255.255.224
S3 - Chacarilla (Surco)	Servidor VPN (Red Interna)	172.16.1.193	255.255.255.224
S4 - Av. Venezuela (Breña)	Servidor VPN (Red Interna)	172.16.1.225	255.255.255.224
S5 - Plaza Lima Norte (Los Olivos)	Servidor VPN (Red Interna)	172.16.2.1	255.255.255.224

Fuente: Elaboración propia.

Así mismo se diseñara un nuevo direccionamiento que permita la correcta administración de IPs para cada sucursal, identificando cada local por un segmento distinto con la posibilidad de seguir creciendo en número de locales y usuarios según se muestra en la Tabla 18, donde se detalla la segmentación de red por cada sucursal detallando el rango de IPs validas así como el número de host permitidos por red.

Tabla 18
Direccionamiento IP para Sucursales

SITIOS	Dirección de Red	Máscara de subred	Dirección puerta de enlace	Rango de direcciones IP validas		Nº de direcciones IP validas
Oficina Principal	172.16.1.0	255.255.255.128	172.16.1.1	172.16.1.2	172.16.1.127	126 host
S1 - Plaza Lima Sur (Chorrillos)	172.16.1.128	255.255.255.224	172.16.1.129	172.16.1.130	172.16.1.159	30 host
S2 - Minka (Callao)	172.16.1.160	255.255.255.224	172.16.1.161	172.16.1.162	172.16.1.191	30 host
S3 - Chacarilla (Surco)	172.16.1.192	255.255.255.224	172.16.1.193	172.16.1.194	172.16.1.223	30 host
S4 - Av. Venezuela (Breña)	172.16.1.224	255.255.255.224	172.16.1.225	172.16.1.226	172.16.1.255	30 host
S5 - Plaza Lima Norte (Los Olivos)	172.16.2.0	255.255.255.224	172.16.2.1	172.16.2.2	172.16.2.31	30 host

Fuente: Elaboración propia.

Después de especificar el direccionamiento IP por sucursal así como la asignación de IPs para sus respectivos servidores, se puede observar en la Figura 12 de manera gráfica la asignación de direcciones IP a la oficina principal así como también a cada una de las sucursales.

Figura 12. Segmentación de Red por Sucursal

Fuente: Elaboración propia.

4.4.2 Configuración de Red VPN que brinde Seguridad

Según RFC 3193 indica la utilización del protocolo L2TP para redes privadas virtuales conjuntamente con el protocolo IPSec con el fin de proporcionar autenticación de túnel, privacidad, control de integridad y protección de reproducción y según su página 2: Introducción, indica:

“Este documento propone el uso del conjunto de protocolos IPsec para proteger El tráfico L2TP a través de redes IP, y explica cómo IPsec y L2TP deben ser utilizados juntos.” (RFC3193 2018:2)

Gracias a el uso de estos protocolos se podrá contar con una red VPN segura que proporcione confidencialidad e integridad en el flujo de la información entre sucursales garantizando así

la veracidad de la misma lo que permitirá tomar buenas decisiones en base a información real integra y segura.

Para conseguir una red VPN segura es necesario seguir las recomendaciones del RFC 3193 que indica que los protocolos IPsec y L2TP deben ser utilizados juntos en la configuración de la red VPN, es así que al momento de realizar la configuración se deberá tener en cuenta estas recomendaciones y realizar la selección correcta de protocolos según se detalla en las guías de configuración:

Configuración VPN sitio a sitio servidores SRV-TMG1 y SRV-TMG2

Esta guía de configuración se encuentra paso a paso en el Anexo 11.2 sin embargo es preciso detallar la configuración de protocolos en los pasos 49 y 62 de la guía de configuración:

Paso 49: En la selección de protocolos se deberá seleccionar las opciones *Habilitar L2TP/IPSec* y *Habilitar PPTP*.

Paso 62: Al finalizar la configuración se deberá tener como resumen de protocolos los siguientes valores:

Nombre: tmg1
Protocolo: L2TP/IPsec
Propietario de Conexión: SRV-TMG2

Figura 13. Valores de Configuración TMG1

Fuente: Elaboración propia Anexo 11.2

Configuración VPN sitio a sitio entre SRV-TMG1 Y SRV-VPN1

Esta guía de configuración se encuentra paso a paso en el Anexo 11.3 sin embargo es preciso detallar la configuración de protocolos en los pasos 2 y 11 de la guía de configuración:

Paso 2: En la selección de protocolos se deberá seleccionar la opción *Protocolo de túnel de capa dos (L2TP) a través de IPSec*.

Paso 11: Al finalizar la configuración se deberá tener como resumen de protocolos los siguientes valores:

Nombre: tmg21
Protocolo: L2TP/IPsec
Propietario de Conexión: SRV-TMG1

Figura 14. Valores de Configuración TMG21

Fuente: Elaboración propia Anexo 11.3.

Así mismo gracias a la configuración VPN segura se podrá montar sobre ella mecanismos de seguridad como extender los controles de acceso y seguridad a las sucursales desde la sede principal: Así como los usuarios de la sede principal son controlados por el software Microsoft Forefront TMG (Red LAN), se requiere que también sea posible el control de cualquier usuario ubicado en cualquier otro local de la organización, por tal motivo se necesita que toda la organización pertenezca a la misma red para que de esta manera el firewall Microsoft Forefront TMG restrinja y controle los accesos para todos los usuarios de

la organización independientemente de la ubicación física en la que se encuentre, es así que gracias a la comunicación entre locales lograda por el cumplimiento del objetivo inicial será posible lograr dicho control. Es así que se desarrollaron las siguientes Guías de Configuración:

- Configuración Microsoft ForeFront TMG: Regla VPN Acceso Remoto.
- Configuración Microsoft ForeFront TMG: Regla Acceso Internet.
- Configuración Microsoft ForeFront TMG: Regla Internet Restringido.

Las guías de configuración completa para este punto serán incluidas al final del documento como un Anexo el cual contiene 50 páginas de configuración paso a paso.

4.4.3 Topología de red con Distribución Centralizada

Gracias a una distribución de red centralizada todas las sucursales podrán tener acceso a los recursos TI e información lo que permitirá tomar buenas decisiones en base a información actualizada en tiempo real y en todo momento.

Según se muestra en la Figura 15, podemos observar la topología de red propuesta donde tenemos como eje o centro de información e infraestructura la Oficina Principal de la organización hasta donde cada una de las sucursales se conecta vía VPN para enviar y recibir información en tiempo real, información que es producida por cada una de las sucursales diariamente, así mismo podemos observar que se tienen servidores alternos o secundarios en la sucursal Plaza Lima Sur esto debido a que dicha sucursal se encuentra en un Centro Comercial que opera diariamente y posee en su estructura disponibilidad de energía eléctrica las 24 horas lo que asegura la replicación de los servidores secundarios ante una posible caída de los servidores principales ubicados en la Oficina Principal de la organización.

Figura 15. Distribución Centralizada

Fuente: Elaboración propia.

A continuación algunas funciones importantes que nos brindara la distribución de red centralizada:

- **Brindar la accesibilidad a la base de datos central desde las sucursales:**

Se requiere que desde la misma forma en que los usuarios de la sede principal acceden al ERP Microsoft Dynamics (Red LAN), también sea posible el acceso desde cualquier otro local de la organización, por tal motivo se requiere que toda la organización pertenezca a la misma red para que de esta manera el acceso a la BD del aplicativo sea transparente para el usuario, es así que gracias a la comunicación entre locales lograda por el cumplimiento del objetivo anterior será posible acceder desde cualquier local a la BD del ERP Microsoft Dynamics (ubicada en la sede principal).

- **Extender los controles de acceso y seguridad a las sucursales desde la sede principal:**

Así como los usuarios de la sede principal son controlados por el software Microsoft Forefront TMG (Red LAN), se requiere que también sea posible el control de cualquier

usuario ubicado en cualquier otro local de la organización, por tal motivo se necesita que toda la organización pertenezca a la misma red para que de esta manera el firewall Microsoft Forefront TMG restrinja y controle los accesos para todos los usuarios de la organización independientemente de la ubicación física en la que se encuentre, es así que gracias a la comunicación entre locales lograda por el cumplimiento del objetivo inicial será posible lograr dicho control.

- **Establecer una solución de replicación y/o alta disponibilidad en los servidores:**

Gracias a la comunicación entre locales lograda por el cumplimiento del objetivo inicial será posible la replicación de los servidores Active Directory y SQL Server (BD), de tal manera que estos puedan replicarse automáticamente y en tiempo real con sus pares ubicados en un local diferente a la sede principal. Para cumplir este requerimiento es necesaria la configuración de las opciones de replicación con la que cuentan cada sistema en particular como es el caso de Replicación de Active Directory y Replicación de SQL Server.

4.5 Costo de la Solución

Actualmente la organización objetivo ya dispone de dos servidores (HP ProLiant ML110 G7) con sus respectivos sistemas operativos destinados para la replicación de sus servidores principales, por lo que solo se está considerando los servidores faltantes para la implementación de la solución que a continuación detallamos:

Tabla 19

Costo de Hardware y Software

Cantidad	Descripción	Precio unitario	Precio total
5	Servidores HP ProLiant ML110 G7 Procesador Intel® Xeon® E3-1220 (3.10 GHz, 8M Cache L3) Memoria 2GB Disco duro 500 GB 2 puertos Ethernet Gigabit Controlador de almacenamiento SATA / RAID	\$ 663,00	\$ 3.315,00
5	Licencias para Windows Server 2008	\$ 701,15	\$ 3.505,75
Subtotal			\$ 6.820,75
IGV (18%)			\$ 1.227,74
Total US			\$ 8.048,49

Fuente: Elaboración propia.

Así mismo se detalla el presupuesto del recurso humano técnico para las configuraciones necesarias:

Tabla 20
Costo de Instalación y Configuración

Cantidad	Descripción	Precio unitario	Precio total
5	Instalación de Windows Server 2008	\$ 80,00	\$ 400,00
5	Configuración VPN Site-to-Site	\$ 300,00	\$ 1.500,00
1	Configuración VPN Client-to-Site	\$ 120,00	\$ 120,00
1	Configuración de replicación DC - AD	\$ 150,00	\$ 150,00
1	Configuración de replicación SQL	\$ 150,00	\$ 150,00
1	Capacitación, Pruebas y Entrega de Manuales	\$ 800,00	\$ 800,00
Total US			\$ 3.120,00

Fuente: Elaboración propia.

Por lo tanto el presupuesto final para la implementación de la solución que incluye tanto hardware, software, configuraciones necesarias y dirección profesional en ingeniería, se resume en el siguiente detalle:

Tabla 21
Inversión Total

Descripción	Precio total
Hardware y Software	\$ 8.048,49
Instalación y Configuraciones	\$ 3.120,00
Dirección de Ingeniería	\$ 1.200,00
Total US	\$ 12.368,49

Fuente: Elaboración propia.

Finalmente podemos resumir que para la implementación específica de este proyecto solo se considera la inversión inicial (CAPEX) que asciende a la suma de US.\$ 12.368,49 sin embargo no se está considerando el costo de operatividad (OPEX), esto debido a que el mantenimiento, monitorización y control de la solución estará a cargo del personal interno de la organización quien deberá ser debidamente capacitado en el desarrollo de la implementación de la solución, quien además contará con los manuales de configuración necesarios.

5 PRUEBAS, RESULTADOS Y VALIDACION

5.1 Plan de Pruebas

El presente proyecto: “Diseño de una red de comunicación VPN sobre internet para un Distribuidor Autorizado de Claro basado en el RFC 2764” consiste en realizar un diseño que nos permita lograr los objetivos establecidos de la organización mediante VPN, es así que para demostrar que es posible lograr dicho objetivo las pruebas serán realizadas en entornos virtuales donde se realizaran las mismas instalaciones y configuraciones necesarias para demostrar su operatividad y funcionamiento, por lo que a continuación se describe el escenario con los aplicativos necesarios para realizar dichas pruebas:

- GNS3: Simulador de red que nos ayudara a virtualizar topologías de red.
- VMware Workstation: Software que nos ayudara a virtualizar los diversos servidores que intervienen en el proyecto.

A continuación se describen las características del entorno virtualizado:

- **Máquinas Virtuales:**

- 6 máquinas virtuales con sistema operativo Windows Server 2003/2008:
512mb de RAM / CD / HD 20GB (2 con 10GB) / Tarjeta de red.
- 2 máquinas virtuales con sistema operativo Windows XP
256mb de RAM / CD / HD 10GB / Tarjeta de red.

- **Funciones:**

- a) 1 Máquina Virtual con SO Windows Server 2008, Función: Firewall/VPN
- b) 1 Máquina Virtual con SO Windows Server 2003, Función: VPN
- c) 1 Máquina Virtual con SO Windows Server 2003, Función: DC Primario.
- d) 1 Máquina Virtual con SO Windows Server 2003, Función: DC Secundario.
- e) 1 Máquina Virtual con SO Windows Server 2003, Función: BD Primario.
- f) 1 Máquina Virtual con SO Windows Server 2003, Función: BD Secundario.
- g) 2 Máquinas Virtuales con SO Windows XP, Función: Cliente / Conectividad.

- **Aplicaciones a utilizar:**

- a) Microsoft Forefront TMG 2010: Aplicación que permite el filtro de paquetes antes de salir a internet, al igual que la conexión VPN Site-to-Site y Client-to-Server.
- b) Microsoft SQL Server 2005: Aplicación que permite crear una base de datos de la empresa, a la cual los usuarios tienen acceso.
- c) Active Directory: Característica del sistema operativo Windows Server 2003, que permite la creación de un directorio personalizable en red. Cada usuario tiene su propia cuenta y con password.
- d) Enrutamiento y Acceso Remoto: Característica del sistema operativo Windows Server 2003, que permite la creación de una red VPN con otro servidor, permitiendo la interoperabilidad entre dos redes lejanas, que pertenezcan a una misma empresa.

- **Demo:**

1. Configuración de servidor firewall para salir a internet: Prueba con el cliente.
2. Configuración VPN Site-to-Site en servidor firewall: Prueba con el cliente
3. Configuración VPN Site-to-Site en servidor VPN: Pruebas con el cliente.
4. Configuración de Replicación de Controlador de Dominio: Pruebas con el cliente.
5. Configuración de Replicación de base de datos: Pruebas con el cliente.

Para las pruebas será necesario verificar el direccionamiento IP de cada equipo mediante el comando ipconfig, que permitirá conocer cuál es la configuración IP de cada equipo cuyo resultado proporcionara la configuración de cada interfaz de red. En el caso de los servidores, que funcionan como firewall, cuentan con dos tarjetas de red, que es igual a 2 interfaces de red, cada una con su propia configuración. Para probar que una red funcione de manera adecuada y por lo tanto los servicios de cada servidor funcionen de manera óptima, se utiliza el comando ping. El comando ping le permite enviar paquetes de datos a un equipo en una red y evaluar el tiempo de respuesta. Para visualizar el funcionamiento del comando ping, solo debe abrir la ventana de comandos de Windows (CMD) y ejecutar el comando: ping seguido de la dirección IP remota.

Se desarrollaran pruebas de acuerdo a los objetivos específicos con el fin de verificar su respectivo funcionamiento y validar los resultados obtenidos, a continuación se describirán y ejecutaran las pruebas con sus respectivos resultados para finalmente verificar y validar su correcto funcionamiento.

5.1.1 Plan de Pruebas por Objetivo Específico

- **OE1: Segmentación de red de datos**

Se realizaran pruebas de conectividad (Ping) entre servidores DC y DB primarios con secundarios utilizando las direcciones IP privadas clase B calculadas en el Capítulo IV, con lo que se podrá probar el estado de la red así como el correcto direccionamiento IP.

- **OE2: Configuración de red VPN**

Como pruebas iniciales se realizaran pruebas de conectividad (Ping) entre servidores TMG1 y VPN1 de cada sucursal utilizando las direcciones IP publicas asignadas por el ISP, con lo que se podrá posteriormente realizar pruebas de conectividad y funcionamiento VPN entre los servidores DC y BD probando así la conexión VPN ya que para lograr conectividad entre IPs privados primero se deberá tener conectividad entre los IPs públicos de cada servidor VPN.

- **OE3: Topología de red centralizada**

Se realizaran pruebas de acceso y replicación de servidores DC y BD con el fin de probar la disponibilidad de servidores entre sucursales.

A continuación se muestra las pruebas, donde las direcciones IP e imágenes mostradas pertenecen a un entorno virtual por lo que se recomienda utilizar el mismo procedimiento en implementación real.

5.2 Ejecución de Pruebas Objetivo Especifico 1

Establecer una segmentación de red escalable para las sucursales mediante el cálculo VLSM bajo el cumplimiento del RFC 1878, se calculó el direccionamiento con sus respectivas rangos IPs por sucursal, así como IPs específicos para los servidores según se detalló en el Capítulo IV, es así que para verificar su funcionamiento será necesario realizar pruebas de conectividad entre servidores DC con DC2 y BD con BD2, sin embargo este tipo de pruebas requiere que la configuración VPN entre sucursales se encuentre en funcionamiento.

Prueba 1: Conectividad Servidor SRV-DC Y SRV-DC2

Se realizara las pruebas de conectividad entre servidores SRV-DC y SRV-DC2 sin embargo es preciso señalar que para realizar estas pruebas será necesario que previamente se realice la configuración de la VPN Sitio a Sitio entre los servidores SRV-TMG1 y SRV-TMG2 (Ver Anexos), en este manual de configuración se detallan paso a paso en un total de 67 pasos, las configuraciones previas necesarias para realizar dicha prueba; todo esto debido a que las pruebas de conectividad serán realizadas con los IPs privados de cada servidor por lo que resulta necesario contar con la conexión VPN establecida previamente, como se muestra a continuación en la Figura 16:

Figura 16. Diagrama Red SRV-DC

Fuente: Elaboración propia.

Resultado de Prueba de Conectividad 1:

Como se muestra en las Figuras 17 y 18, se realizó pruebas (ping) entre los servidores SRV-DC y SRV-DC2 con el fin de encontrar conectividad entre ambas interfaces de red, esto confirma que efectivamente existe conectividad entre ambos servidores y que el servidor SRV-DC está listo para la replicación usuarios y equipos de Active Directory al servidor SRV-DC2.

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrador>ipconfig /all

Configuración IP de Windows

Nombre del host . . . . . : SRV-DC
Sufijo DNS principal . . . . : megaline.com
Tipo de nodo . . . . . : desconocido
Enrutamiento habilitado . . . : No
Proxy WINS habilitado . . . . : No
Lista de búsqueda sufijo DNS : megaline.com

Adaptador Ethernet Conexión de área local:

Sufijo conexión específica DNS:
Descripción . . . . . : VMware Accelerated AMD PCNet Adapter
Dirección física. . . . . : 00-0C-29-09-02-C8
DHCP habilitado . . . . . : No
Dirección IP. . . . . : 172.16.1.100
Máscara de subred . . . . . : 255.255.255.128
Puerta de enlace predet. . . : 172.16.1.1
Servidores DNS. . . . . : 127.0.0.1

C:\Documents and Settings\Administrador>ping SRV-DC2

Haciendo ping a SRV-DC2.megaline.com [172.16.1.130] con 32 bytes de datos:

Respuesta desde 172.16.1.130: bytes=32 tiempo=2ms TTL=126
Respuesta desde 172.16.1.130: bytes=32 tiempo=3ms TTL=126
Respuesta desde 172.16.1.130: bytes=32 tiempo=3ms TTL=126
Respuesta desde 172.16.1.130: bytes=32 tiempo=3ms TTL=126

Estadísticas de ping para 172.16.1.130:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 2ms, Máximo = 3ms, Media = 2ms

C:\Documents and Settings\Administrador>
```

Figura 17. Ping exitoso de servidor SRV-DC

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrador>ipconfig /all

Configuración IP de Windows

Nombre del host . . . . . : SRV-DC2
Sufijo DNS principal . . . . : megaline.com
Tipo de nodo . . . . . : desconocido
Enrutamiento habilitado . . . : No
Proxy WINS habilitado . . . . : No
Lista de búsqueda sufijo DNS : megaline.com

Adaptador Ethernet Conexión de área local:

Sufijo conexión específica DNS:
Descripción . . . . . : VMware Accelerated AMD PCNet Adapter
Dirección física. . . . . : 00-0C-29-C9-CE-CB
DHCP habilitado . . . . . : No
Dirección IP. . . . . : 172.16.1.130
Máscara de subred . . . . . : 255.255.255.224
Puerta de enlace predet. . . : 172.16.1.129
Servidores DNS. . . . . : 172.16.1.100

C:\Documents and Settings\Administrador>ping SRV-DC

Haciendo ping a SRV-DC.megaline.com [172.16.1.100] con 32 bytes de datos:

Respuesta desde 172.16.1.100: bytes=32 tiempo=1ms TTL=126
Respuesta desde 172.16.1.100: bytes=32 tiempo=3ms TTL=126
Respuesta desde 172.16.1.100: bytes=32 tiempo=3ms TTL=126
Respuesta desde 172.16.1.100: bytes=32 tiempo=3ms TTL=126

Estadísticas de ping para 172.16.1.100:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 1ms, Máximo = 3ms, Media = 2ms

C:\Documents and Settings\Administrador>
```

Figura 18. Ping exitoso de servidor SRV-DC2

Prueba 2: Conectividad Servidor SRV-BD Y SRV-BD2

Se realizara las pruebas de conectividad entre servidores SRV-BD y SRV-BD2 sin embargo es preciso señalar que para realizar estas pruebas será necesario que previamente se realice la configuración de la VPN Sitio a Sitio entre los servidores SRV-TMG1 y SRV-TMG2 (Ver Anexos), en este manual de configuración se detallan paso a paso en un total de 67 pasos, las configuraciones previas necesarias para realizar dicha prueba; todo esto debido a que las pruebas de conectividad serán realizadas con los IPs privados de cada servidor por lo que resulta necesario contar con la conexión VPN establecida previamente, como se muestra a continuación en la Figura 19:

Figura 19. Diagrama Red SRV-BD

Fuente: Elaboración propia.

Resultado de Prueba de Conectividad 2:

Como se muestra en las Figuras 20 y 21 , se realizó pruebas (ping) entre los servidores SRV-BD y SRV-BD2 con el fin de encontrar conectividad entre ambas interfaces de red, esto confirma que efectivamente existe conectividad y que el servidor SRV-BD está listo para la replicación de tablas y filas a la base de datos del servidor SRV-BD2.

```

C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrador.MEGALINE>ipconfig /all

Configuración IP de Windows

    Nombre del host . . . . . : SRV-BD
    Sufijo DNS principal . . . . : megaline.com
    Tipo de nodo . . . . . : desconocido
    Enrutamiento habilitado . . . : No
    Proxy WINS habilitado . . . . : No
    Lista de búsqueda sufijo DNS : megaline.com

Adaptador Ethernet Conexión de área local:

    Sufijo conexión específica DNS:
    Descripción . . . . . : VMware Accelerated AMD PCNet Adapter
    Dirección física. . . . . : 00-0C-29-57-C6-37
    DHCP habilitado . . . . . : No
    Dirección IP. . . . . : 172.16.1.101
    Máscara de subred . . . . . : 255.255.255.128
    Puerta de enlace predet. . . : 172.16.1.1
    Servidores DNS. . . . . : 172.16.1.100

C:\Documents and Settings\Administrador.MEGALINE>ping SRV-BD2.megaline.com

Haciendo ping a SRV-BD2.megaline.com [172.16.1.132] con 32 bytes de datos:

Respuesta desde 172.16.1.132: bytes=32 tiempo=2ms TTL=126
Respuesta desde 172.16.1.132: bytes=32 tiempo=1ms TTL=126
Respuesta desde 172.16.1.132: bytes=32 tiempo=1ms TTL=126
Respuesta desde 172.16.1.132: bytes=32 tiempo=1ms TTL=126

Estadísticas de ping para 172.16.1.132:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 1ms, Máximo = 2ms, Media = 1ms

C:\Documents and Settings\Administrador.MEGALINE>

```

Figura 20. Ping exitoso del servidor SRV-BD

Fuente: Elaboración propia.

```

C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrador.MEGALINE>ipconfig /all

Configuración IP de Windows

    Nombre del host . . . . . : SRV-BD2
    Sufijo DNS principal . . . . : megaline.com
    Tipo de nodo . . . . . : desconocido
    Enrutamiento habilitado . . . : No
    Proxy WINS habilitado . . . . : No
    Lista de búsqueda sufijo DNS : megaline.com

Adaptador Ethernet Conexión de área local:

    Sufijo conexión específica DNS:
    Descripción . . . . . : VMware Accelerated AMD PCNet Adapter
    Dirección física. . . . . : 00-0C-29-24-83-37
    DHCP habilitado . . . . . : No
    Dirección IP. . . . . : 172.16.1.132
    Máscara de subred . . . . . : 255.255.255.224
    Puerta de enlace predet. . . : 172.16.1.129
    Servidores DNS. . . . . : 172.16.1.100

C:\Documents and Settings\Administrador.MEGALINE>ping SRV-BD.megaline.com

Haciendo ping a SRV-BD.megaline.com [172.16.1.101] con 32 bytes de datos:

Respuesta desde 172.16.1.101: bytes=32 tiempo=1ms TTL=126
Respuesta desde 172.16.1.101: bytes=32 tiempo=3ms TTL=126
Respuesta desde 172.16.1.101: bytes=32 tiempo=1ms TTL=126
Respuesta desde 172.16.1.101: bytes=32 tiempo=1ms TTL=126

Estadísticas de ping para 172.16.1.101:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 1ms, Máximo = 3ms, Media = 1ms

C:\Documents and Settings\Administrador.MEGALINE>

```

Figura 21. Ping exitoso del servidor SRV-DB2

Fuente: Elaboración propia.

5.2.1 Resultados y Validación Objetivo Especifico 1

Según los resultados obtenidos se pudo demostrar el correcto direccionamiento IP así como la segmentación entre sucursales, esto gracias a la utilización del indicador de logro: **Informe de la segmentación en sub redes y tabla con direccionamiento IP**, el mismo que se detalló en el capítulo anterior, por lo que ahora necesitamos validar el cumplimiento de su respectiva métrica que es: **Nivel de escalabilidad de la red clase B mayor al 90% del total de redes disponibles.**

En la siguiente tabla se muestra el cálculo de Sub Redes a partir de la red de clase B 172.16.1.0/8, donde podemos observar las redes a utilizar y las redes disponibles para futuros locales:

Tabla 22
Direcciones IP Disponibles

Nro de Redes	Hosts	Direccion de Red	Mascara de Red	Sede o Sucursal
1	126	172.16.1.0 /25	255.255.255.128	Oficina Principal
1	30	172.16.1.128 /27	255.255.255.224	S1 - Plaza Lima Sur (Chorrillos)
2	30	172.16.1.160 /27	255.255.255.224	S2 - Minka (Callao)
3	30	172.16.1.192 /27	255.255.255.224	S3 - Chacarilla (Surco)
4	30	172.16.1.224 /27	255.255.255.224	S4 - Av. Venezuela (Breña)
5	30	172.16.2.0 /27	255.255.255.224	S5 - Plaza Lima Norte (Los Olivos)
6	30	172.16.2.32 /27	255.255.255.224	Disponible
7	30	172.16.2.64 /27	255.255.255.224	Disponible
8	30	172.16.2.96 /27	255.255.255.224	Disponible
9	30	172.16.2.128 /27	255.255.255.224	Disponible
10	30	172.16.2.160 /27	255.255.255.224	Disponible
11	30	172.16.2.192 /27	255.255.255.224	Disponible
12	30	172.16.2.224 /27	255.255.255.224	Disponible
13	30	172.16.3.0 /27	255.255.255.224	Disponible
14	30	172.16.3.32 /27	255.255.255.224	Disponible
15	30	172.16.3.64 /27	255.255.255.224	Disponible
16	30	172.16.3.96 /27	255.255.255.224	Disponible
17	30	172.16.3.128 /27	255.255.255.224	Disponible
18	30	172.16.3.160 /27	255.255.255.224	Disponible
19	30	172.16.3.192 /27	255.255.255.224	Disponible
20	30	172.16.3.224 /27	255.255.255.224	Disponible
21	30	172.16.4.0 /27	255.255.255.224	Disponible
22	30	172.16.4.32 /27	255.255.255.224	Disponible
23	30	172.16.4.64 /27	255.255.255.224	Disponible
24	30	172.16.4.96 /27	255.255.255.224	Disponible
25	30	172.16.4.128 /27	255.255.255.224	Disponible
26	30	172.16.4.160 /27	255.255.255.224	Disponible
27	30	172.16.4.192 /27	255.255.255.224	Disponible
28	30	172.16.4.224 /27	255.255.255.224	Disponible

Fuente: Elaboración propia.

Como se observa en la Tabla 22 tenemos 1 red de 126 hosts y 28 redes de 30 hosts, para este último solo se calculó las primeras 28 redes con el fin de demostrar la disponibilidad con las que se puede contar a partir de la red 172.16.1.0/8, sin embargo la red de Clase B dispone de 2048 redes de 30 hosts según el cálculo de redes disponibles obtenidos de la tabla 1-1 del RFC 1878, que a continuación se presenta:

Tabla 23
Sub Redes de Red Clase B

Mascara Decimal	Mascara Binario	Nro. De Redes	Nro de Hosts
255.255.0.0	11111111.11111111.00000000.00000000	1	65534
255.255.128.0	11111111.11111111.10000000.00000000	2	32766
255.255.192.0	11111111.11111111.11000000.00000000	4	16382
255.255.224.0	11111111.11111111.11100000.00000000	8	8190
255.255.240.0	11111111.11111111.11110000.00000000	16	4094
255.255.248.0	11111111.11111111.11111000.00000000	32	2046
255.255.252.0	11111111.11111111.11111100.00000000	64	1022
255.255.254.0	11111111.11111111.11111110.00000000	128	510
255.255.255.0	11111111.11111111.11111111.00000000	256	254
255.255.255.128	11111111.11111111.11111111.10000000	512	126
255.255.255.192	11111111.11111111.11111111.11000000	1024	62
255.255.255.224	11111111.11111111.11111111.11100000	2048	30
255.255.255.240	11111111.11111111.11111111.11110000	4096	14
255.255.255.248	11111111.11111111.11111111.11111000	8192	6
255.255.255.252	11111111.11111111.11111111.11111100	16384	2

Fuente: RFC 1878.

Es así según la Tabla 23 tenemos 2048 redes disponibles de 30 Hosts y solo estamos usando 5, teniendo disponibles 2043 redes libres, por lo que el siguiente calculo brinda el porcentaje de redes disponibles para su asignación a futuros locales.

$$\% = \frac{100 \times 2043}{2048} = 99.75 \% \quad 99.755859$$

5.3 Ejecución de Pruebas Objetivo Especifico 2

Desarrollar una configuración VPN que brinde seguridad de datos en el flujo de sus comunicaciones mediante el uso protocolos L2TP/IPSec bajo el cumplimiento del RFC 3193, para este caso se realizaron pruebas de conectividad entre IPs internos de los servidores por sucursal, con lo que se estaría probando el funcionamiento de la configuración VPN en donde primeramente se probó conectividad entre IPs públicos los mismos que fueron mapeados a IPs privados para poder lograr la conectividad necesaria entre sucursales.

Prueba 1: Conectividad Routers R1 y R2

Se realizara las pruebas de conectividad entre los IPs públicos de los routers R1 y R2 sin embargo es preciso señalar que después de realizar estas pruebas es necesario que el proveedor ISP América Móvil Perú SAC, realice las configuraciones de NAT respectivas en cada uno de los routers correspondientes a cada local según se muestra a continuación en la Figura 22:

Figura 22. Diagrama Red Routers

Fuente: Elaboración propia.

Resultado de Prueba de Conectividad 1:

Según se muestra en las Figuras 23 y 24, se realizó pruebas de conectividad (ping) entre los routers R1 y R2 con el fin de encontrar conectividad entre ambas interfaces de red, esto confirma que efectivamente existe conectividad entre ambos routers y que se encuentran listos para el nateo de IP pública a IP privado.

```
CA. Administrador: C:\Windows\system32\cmd.exe

C:\Users\Administrador>hostname
SRU-TMG1

C:\Users\Administrador>ping 200.110.28.74

Haciendo ping a 200.110.28.74 con 32 bytes de datos:
Respuesta desde 200.110.28.74: bytes=32 tiempo<1m TTL=128
Respuesta desde 200.110.28.74: bytes=32 tiempo<1m TTL=128
Respuesta desde 200.110.28.74: bytes=32 tiempo<1m TTL=128
Respuesta desde 200.110.28.74: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 200.110.28.74:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Administrador>_
```

Figura 23. Ping exitoso de servidor R1

Fuente: Elaboración propia.

```
CA. Administrador: C:\Windows\system32\cmd.exe

C:\Users\Administrador>hostname
SRU-TMG2

C:\Users\Administrador>ping 200.110.28.73

Haciendo ping a 200.110.28.73 con 32 bytes de datos:
Respuesta desde 200.110.28.73: bytes=32 tiempo=1ms TTL=128
Respuesta desde 200.110.28.73: bytes=32 tiempo<1m TTL=128
Respuesta desde 200.110.28.73: bytes=32 tiempo=1ms TTL=128
Respuesta desde 200.110.28.73: bytes=32 tiempo=1ms TTL=128

Estadísticas de ping para 200.110.28.73:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\Administrador>_
```

Figura 24. Ping exitoso de servidor R2

Fuente: Elaboración propia.

Prueba 2: Conectividad Servidor SRV-TMG1 Y SRV-TMG2

Se realizara las pruebas de conectividad entre servidores SRV-TMG1 y SRV-TMG2 sin embargo es preciso señalar que para realizar estas pruebas es necesario que el proveedor ISP América Móvil Perú SAC, haya realizado las configuraciones de NAT respectivas en cada uno de los routers correspondientes a cada local según se muestra a continuación en la Figura 25:

Figura 25. Diagrama Red SRV-TMG

Fuente: Elaboración propia.

Resultado de Prueba de Conectividad 2:

Según se muestra en las Figuras 26 y 27, se realizó pruebas de conectividad (ping) entre los servidores SRV-TMG1 y SRV-TMG2 con el fin de encontrar conectividad entre ambas interfaces de red, esto confirma el funcionamiento VPN y que efectivamente existe conectividad entre ambos servidores firewall y que nuestras interfaces de red externas e internas están listas para la conexión de servidores internos AD y BD.

```
Administrador: C:\Windows\system32\cmd.exe
C:\Users\Administrador>hostname
SRV-TMG1
C:\Users\Administrador>ping 172.16.1.129
Haciendo ping a 172.16.1.129 con 32 bytes de datos:
Respuesta desde 172.16.1.129: bytes=32 tiempo=2ms TTL=126
Respuesta desde 172.16.1.129: bytes=32 tiempo=1ms TTL=126
Respuesta desde 172.16.1.129: bytes=32 tiempo=1ms TTL=126
Respuesta desde 172.16.1.129: bytes=32 tiempo=1ms TTL=126
Estadísticas de ping para 172.16.1.129:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
C:\Users\Administrador>_
```

Figura 26. Ping exitoso de servidor SRV-TMG1

Fuente: Elaboración propia.

```
Administrador: C:\Windows\system32\cmd.exe
C:\Users\Administrador>hostname
SRV-TMG2
C:\Users\Administrador>ping 172.16.1.1
Haciendo ping a 172.16.1.1 con 32 bytes de datos:
Respuesta desde 172.16.1.1: bytes=32 tiempo=2ms TTL=126
Respuesta desde 172.16.1.1: bytes=32 tiempo=1ms TTL=126
Respuesta desde 172.16.1.1: bytes=32 tiempo=1ms TTL=126
Respuesta desde 172.16.1.1: bytes=32 tiempo=1ms TTL=126
Estadísticas de ping para 172.16.1.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms
C:\Users\Administrador>_
```

Figura 27. Ping exitoso de servidor SRV-TMG2

Fuente: Elaboración propia.

Prueba 3: Protocolo IPsec Servidor SRV-TMG1 Y SRV-TMG2

Se realizara las pruebas de conectividad entre los routers R1 y R2 con el fin de capturar el tráfico entre routers y verificar la utilización del protocolo IPsec, para lo que se analizara la siguiente topología que se muestra a continuación en la Figura 28:

Figura 28. Diagrama Red Routers R1 y R2

Resultado de Prueba de Protocolo 3:

Según se muestra en las Figura 29, se puede observar la utilización IPsec, donde figura el protocolo de encriptación AES-CBC, protocolo de autenticación SHA y el protocolo de intercambio de claves IKE, que pertenecen a los protocolos de seguridad IPsec.

```

Ethernet II, Src: Cisco_ed:7a:f0 (00:17:5a:ed:7a:f0), Dst: Cisco_8b:36:d0 (00:1d:a1:8b:36:d0)
Internet Protocol Version 4, Src: 192.168.1.39 (192.168.1.39), Dst: 192.168.1.38 (192.168.1.38)
User Datagram Protocol, Src Port: 500 (500), Dst Port: 500 (500)
Internet Security Association and Key Management Protocol
  Initiator SPI: e47a591fd057587f
  Responder SPI: a00b8ef0902bb8ec
  Next payload: Security Association (1)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 108
  Type Payload: Security Association (1)
    Next payload: Vendor ID (13)
    Payload length: 60
    Domain of interpretation: IPSEC (1)
  Situation: 00000001
  Type Payload: Proposal (2) # 1
    Next payload: NONE / No Next Payload (0)
    Payload length: 48
    Proposal number: 1
    Protocol ID: ISAKMP (1)
    SPI Size: 0
    Proposal transforms: 1
  Type Payload: Transform (3) # 1
    Next payload: NONE / No Next Payload (0)
    Payload length: 40
    Transform number: 1
    Transform ID: KEY_IKE (1)
    Transform IKE Attribute Type (t=1,l=2) Encryption-Algorithm : AES-CBC
    Transform IKE Attribute Type (t=14,l=2) Key-Length : 128
    Transform IKE Attribute Type (t=2,l=2) Hash-Algorithm : SHA
    Transform IKE Attribute Type (t=4,l=2) Group-Description : Alternate 1024-bit MODP group
    Transform IKE Attribute Type (t=3,l=2) Authentication-Method : PSK
    Transform IKE Attribute Type (t=11,l=2) Life-Type : Seconds

```

Figura 29. Protocolos IPsec

5.3.1 Resultados y Validación Objetivo Especifico 2

Según los resultados obtenidos se pudo demostrar la correcta configuración VPN además de validar la utilización del protocolo de seguridad IPsec, esto gracias a la utilización del indicador de logro: **Guía de configuración de protocolos de seguridad** el cual se detalló en el capítulo anterior, por lo que ahora necesitamos validar el cumplimiento de su respectiva métrica que es: **Nivel de riesgos bajos de la seguridad de la información al 100%** para lo cual se deberá elaborar una **Matriz de evaluación de riesgos de seguridad de la información**.

Para la validación de este objetivo es necesario identificar vulnerabilidades, amenazas y posibles consecuencias de la materialización de una amenaza sobre alguna vulnerabilidad, por lo que se presenta la Tabla 24 donde previamente se identificó los activos de información con sus respectivas vulnerabilidades, amenazas y el impacto que esto ocasionaría.

Tabla 24
Vulnerabilidades Amenazas e Impacto

CONTENIDOR Y/O ACTIVO DE INFORMACION SELECCIONADO PARA EL ANALISIS DE RIESGOS	CAUSAS		CONSECUENCIAS (IMPACTO)
	VULNERABILIDADES	AMENAZAS	
Servidores AD y BD	<ul style="list-style-type: none"> El respaldo de backup se encuentra ubicado en los mismos servidores a los cuales les establecen las copias de respaldo. La configuración y administración de los servidores no se encuentra centralizada. No existen configuraciones de seguridad establecidas en los servidores o en los servicios de red que han sido implementados a través de la red corporativa. 	<ul style="list-style-type: none"> Indisponibilidad temporal en el acceso la información contenida en los servidores generada por un tercero no autorizado. 	<ul style="list-style-type: none"> Eliminación de información clave para el negocio afectando la disponibilidad de la misma para el desarrollo de las actividades concernientes al negocio. Pérdida de información que puede conllevar a la afectación del negocio y pérdida de clientes y negocios importantes para la entidad. Afectación de la operación de la organización debido a la indisponibilidad de la información.
Cuarto de Equipos Tecnológicos	<ul style="list-style-type: none"> No poseen un sistema de detección de humo, fuego y/o humedad instalado en el centro de cómputo. No poseen un centro de cómputo alternativo independiente de energía eléctrica y conexión ISP. 	<ul style="list-style-type: none"> Afectación temporal de la disponibilidad de la información y/o aplicativos alojados en los servidores causados por una falla no intencionada de un empleado de la organización. Fuego – Posibilidad de que un incendio destruya los recursos y activos de la organización. Daños causados por Agua – Escape, fuga o inundación que ocasione el daño de los recursos de la organización. 	<ul style="list-style-type: none"> Eliminación de información clave para el negocio afectando la disponibilidad de la misma para el desarrollo de las actividades concernientes al negocio. Pérdida de información que puede conllevar a la afectación del negocio y pérdida de clientes y negocios importantes para la entidad. Afectación de la operación de la organización debido a la indisponibilidad de la información por daño de los contenedores de información (Servidores).

Red Corporativa	<ul style="list-style-type: none"> Deficiencias en las configuraciones de seguridad de la red, empleando un cifrado débil. Ausencia de un administrador de red que configure, administre y gestione la red bajo criterios de seguridad de la información. Perdida de confidencialidad de información que puede ser sensible para la entidad debido a que es compartida a través de la infraestructura de red de la organización, permitiendo su visualización a personas no autorizadas. 	<ul style="list-style-type: none"> Fuga de información debido al acceso de usuarios no autorizados a la infraestructura de red de la organización. Terceros realizan procesos de suplantación de identidad para acceder a los aplicativos tecnológicos de la entidad que se encuentran disponibles a través de la red de datos corporativa. Empleados descontentos pueden hacer uso de usuarios y contraseñas de personal que ya no labora en la entidad para visualizar y/o sustraer información confidencial de la entidad. 	<ul style="list-style-type: none"> Perdida de disponibilidad, integridad y confidencialidad de la información de la entidad, generando un impacto negativo en la continuidad del negocio. Afectación en los ingresos económicos de la organización debido a la pérdida de clientes a causa de la divulgación no autorizada de información a la competencia. Indisponibilidad de los servicios que se brindan a través de la red ocasionando tiempos no productivos del equipo comercial de la organización. Desprestigio de la imagen corporativa debido a la divulgación no autorizada de información confidencial por parte del personal interno y/o externo de la entidad.
Unidades de almacenamiento de información	<ul style="list-style-type: none"> No se establece ninguna restricción de información en unidades de almacenamiento externas como USB, discos duros (internos y/o externos). Ausencia de niveles de protección física sobre los dispositivos de almacenamiento externo. 	<ul style="list-style-type: none"> Pérdida y/o fuga de información confidencial de la organización por hurto de unidades de almacenamiento de información externas. 	<ul style="list-style-type: none"> Divulgación por terceros de información confidencial de la organización generando problemas de índole legal y reputacional a la entidad. Perdida de información ocasionada accidentalmente, generando pérdida de imagen corporativa ante terceros.

Para la validación de este objetivo es necesario realizar dos Matrices de Análisis de Riesgo las mismas que son producto de la identificación y valoración de los riesgos de seguridad, la primera de la situación actual de la organización y la segunda después de que se realice la configuración de protocolos y medidas de seguridad para la red privada virtual, de esta manera establecer diferencias. Antes es necesario establecer los criterios de evaluación según se muestran a continuación en las Tablas 25, 26 y 27:

Tabla 25
Medición de Impacto y Probabilidad

Tabla 26

Valoración de Probabilidad de Ocurrencia

Alto (4)	Cuando la probabilidad de ocurrencia es frecuente (Ej: al menos una vez al mes)
Medio (3)	Cuando la probabilidad de ocurrencia es regular (Ej: al menos una vez al año)
Bajo (2)	Cuando la probabilidad de ocurrencia es baja (Ej: al menos una vez cada 5 años)
Muy Bajo (1)	Cuando la probabilidad de ocurrencia es muy baja (Ej: cada 20 años o más)

Tabla 27

Valoración del Impacto

Crítico (4)	Afecta irreversiblemente la operatividad, competitividad, rentabilidad o imagen de la empresa.
Serio (3)	Afecta seriamente la operatividad, competitividad, rentabilidad o imagen de la empresa.
Medio (2)	Afecta considerablemente la operatividad, competitividad, rentabilidad o imagen de la empresa.
Mínimo (1)	No afecta considerablemente la operatividad, competitividad, rentabilidad o imagen de la empresa.

A continuación la Tabla 28 con la primera Matriz de Análisis de Riesgos de Seguridad de la Información correspondiente a la situación actual de la organización donde podemos observar que tenemos riesgos altos y riesgos medio esto debido a que no existen controles de seguridad ni mecanismos que ayuden a mitigar los riesgos.

Tabla 28
Matriz de Riesgo 1

Matriz de Analisis de Riesgo		Probabilidad de Amenaza					
Elementos de Informacion	Magnitud de Daño (Impacto)	Criminalidad		Sucesos Fisicos		Negligencia	
		Robo	Virus	Incendio	Falta de Energia	Compartir contraseñas	No cifrar datos criticos
		3	4	1	3	4	4
Datos e Informacion							
Logistica	2	6	8	2	6	8	8
Comercial	2	6	8	2	6	8	8
Finanzas	2	6	8	2	6	8	8
Sistemas e Informacion							
Cuarto de Equipos	3	9	12	3	9	12	12
Red Corporativa	3	9	12	3	9	12	12
Servidor AD y BD	3	9	12	3	9	12	12

Fuente: Elaboración propia.

Después de identificar las vulnerabilidades y amenazas sobre los activos seleccionados, se establecen los riesgos de seguridad a los que están expuestos, es así que se presenta la siguiente Tabla 29 donde se definen los riesgos de seguridad y se les da una valoración para determinar el nivel del riesgo al que están expuestos.

Tabla 29
Valoración de Riesgos de Seguridad

CONTENEDOR Y/O ACTIVO DE INFORMACION SELECCIONADO PARA EL ANALISIS DE RIESGOS	RIESGOS DE SEGURIDAD	VALORACION DEL RIESGO			
		Impacto	Probabilidad	Calificación	NIVEL DEL RIESGO
Servidores AD y BD	R1 - Pérdida de información de la organización debido a la ausencia de procedimientos que establezcan los lineamientos y buenas prácticas de seguridad para realizar backup de la información.	3	4	12	Alto
	R2 - Afectación de la confidencialidad e integridad de la información a causa de una inadecuada gestión de identidades y control de acceso a los recursos y repositorios de información de la organización.	3	4	12	Alto
	R3 - Tiempos laborales muertos causados por la indisponibilidad de la información y servicios debido a la ausencia de configuraciones de seguridad en los servidores.	3	4	12	Alto
Cuarto de Equipos Tecnológicos	R4 - Tiempos de inactividad en las operaciones de la organización, debido al daño o ausencia de sistemas de respaldo eléctrico a la infraestructura de red de la organización.	3	3	9	Medio
	R5 - Deterioro parcial y/o total de la infraestructura tecnológica del centro de cómputo causada por la presencia de fuego en el recinto.	3	1	3	Bajo
Red Corporativa	R6 - Sustracción y/o pérdida de información sensible de la organización debido a la ausencia de políticas y controles en el establecimiento de contraseñas de acceso a los dispositivos tecnológicos de la entidad.	3	4	12	Alto
	R7 - Indisponibilidad de la información y/o servicios que se acceden a través de la red corporativa por deficiencias en su diseño e implementación.	3	4	12	Alto
Unidades de almacenamiento de Información	R8 - Pérdida de clientes por divulgación no autorizada de información debido a la ausencia de mecanismos de cifrado de información sobre unidades de almacenamiento electrónico.	3	4	12	Alto

Ahora presentamos la Tabla 30 con la segunda Matriz de Análisis de Riesgos de Seguridad de la Información correspondiente la situación donde se ejecute la guía de configuración de protocolos de seguridad en la red VPN, donde podemos observar que el total de riesgos es decir el 100% tiene nivel de riesgo bajo.

Tabla 30
Matriz de Riesgo 2

Matriz de Analisis de Riesgo		Probabilidad de Amenaza					
Elementos de Informacion	Magnitud de Daño (Impacto)	Criminalidad		Sucesos Fisicos		Negligencia	
		Robo	Virus	Incendio	Falta de Energia	Compartir contraseñas	No cifrar datos criticos
		2	2	1	3	2	1
Datos e Informacion							
Logistica	1	2	2	1	3	2	1
Comercial	1	2	2	1	3	2	1
Finanzas	1	2	2	1	3	2	1
Sistemas e Informacion							
Cuarto de Equipos	1	2	2	1	3	2	1
Red Corporativa	1	2	2	1	3	2	1
Servidor AD y BD	1	2	2	1	3	2	1

Fuente: Elaboración propia.

5.4 Ejecución de Pruebas Objetivo Especifico 3

Presentar una topología de red lógica centralizada que permita proponer medidas de optimización de recursos TI para la disponibilidad de la información, en este caso se tiene que probar que los recursos TI tengan disponibilidad para toda la organización es así que se deberá probar que los servidores principales que son: AD y BD puedan replicar la información en tiempo real a sus respectivos servidores secundarios o de respaldo para poder estar disponibles en todo momento.

Prueba 1: Replicación Dominio megaline.com

Se realizara las pruebas de replicación entre servidores SRV-DC y SRV-DC2 sin embargo es preciso señalar que para realizar estas pruebas será necesario que previamente se realice las siguientes configuraciones:

- Configuración VPN sitio a sitio Servidores SRV-TMG1 Y SRV-TMG2

En este manual de configuración se detallan paso a paso en un total de 67 pasos, las configuraciones previas necesarias para realizar dicha prueba; todo esto debido a que las pruebas serán realizadas con los IPs privados de cada servidor por lo que resulta necesario contar con la conexión VPN establecida previamente. (Ver Anexos)

- Configuración de Controlador de Dominio Adicional

En este manual de configuración se detallan paso a paso en un total de 23 pasos, las configuraciones previas necesarias para realizar dicha prueba; todo esto debido a que se necesita un servidor de controlador de dominio secundario para que sea el receptor de la replicación del servidor de controlador de dominio principal. (Ver Anexos)

Resultado de Prueba de Replicación 1:

Se realizó la prueba de replicación de controlador de dominio entre los servidores SRV-DC y SRV-DC2. Para la prueba, se realizó la creación de un usuario *user01* en el servidor SRV-DC y luego se verificó que el mismo usuario se haya replicado en el servidor SRV-DC2, tal como se puede apreciar a continuación en las Figuras 30 y 31:

Figura 30. Usuario user01 en servidor SRV-DC

Fuente: Elaboración propia.

Figura 31. Usuario user01 en servidor SRV-DC2

Fuente: Elaboración propia.

Prueba de Replicación 2: Base de Datos Megaline

Se realizara las pruebas de replicación entre servidores SRV-BD y SRV-BD2 sin embargo es preciso señalar que para realizar estas pruebas será necesario que previamente se realice las siguientes configuraciones:

- Configuración VPN sitio a sitio Servidores SRV-TMG1 Y SRV-TMG2

En este manual de configuración se detallan paso a paso en un total de 67 pasos, las configuraciones previas necesarias para realizar dicha prueba; todo esto debido a que las pruebas serán realizadas con los IPs privados de cada servidor por lo que resulta necesario contar con la conexión VPN establecida previamente. (Ver Anexos)

- Manual de Instalación de SQL server

En este manual de configuración se detallan paso a paso en un total de 23 pasos, las configuraciones previas necesarias para realizar dicha prueba; todo esto debido a se necesita un servidor SQL secundario para que sea el receptor de la replicación del servidor SQL principal. (Ver Anexos)

- Configuración de Replicación de Base de Datos

En este manual de configuración se detallan paso a paso en un total de 70 pasos, las configuraciones previas necesarias para realizar dicha prueba; todo esto debido a se necesita un servidor SQL secundario configurado correctamente para que sea el receptor de la replicación del servidor SQL principal. (Ver Anexos)

Resultado de Prueba de Replicación 2:

Se realizó la prueba de replicación de base de datos entre los servidores SRV-BD y SRV-BD2. Para la prueba, se realizó la creación de una base de datos MEGALINEBAK, en el servidor SRV-BD2, el cual recibirá las tablas Clientes y Vendedor de la base de datos MEGALINE del servidor SRV-BD. Se verificó que las mismas tablas y filas se hayan replicado en el servidor SRV-BD2, tal como se puede apreciar a continuación en las Figuras 32 y 33:

Figura 32. Base de datos MEGALINE en servidor SRV-BD

Fuente: Elaboración propia.

Figura 33. Base de datos MegalineBak en servidor SRV-BD2

Fuente: Elaboración propia.

5.4.1 Resultados y Validación Objetivo Especifico 3

Según los resultados obtenidos se pudo demostrar la replicación de servidores AD y BD con lo que podemos decir que se cuenta con respaldo y centralización de la infraestructura TI, esto gracias a la utilización del indicador de logro: **Diseño de topología de red y distribución centralizada con disponibilidad de Infraestructura TI**, el mismo que se detalló en el capítulo anterior, por lo que ahora necesitamos demostrar el cumplimiento de su respectiva métrica que es: **Nivel de disponibilidad de la red mayor al 90% mensual**.

Con el fin de determinar el nivel de disponibilidad de la red VPN es necesario precisar que se considera el cumplimiento de los SLA establecidos por el proveedor ISP América Móvil Perú.

Es así que basados en el cumplimiento de los SLA de la Tabla 30, que incluso indican cumplimiento al 99.98% de disponibilidad del backbone de red de Internet, es posible validar que nuestros resultados podrán ser cumplidos en un escenario real tal como se demostró en un entorno virtualizado explicado y graficado anteriormente.

Tabla 31
Métricas América Móvil

ITEM	MÉTRICA	DEFINICIÓN	OBJETIVO
1	Disponibilidad del Backbone de Red Internet	Porcentaje de tiempo durante un mes en el cual el backbone de la red se encuentra disponible.	99.98%
2	Disponibilidad de Enlace De Última Milla	Porcentaje de tiempo durante un mes en el cual la última milla de la red del cliente se encuentra disponible.	99.50%
3	Packet Transit Delay (Latencia)	Tiempo total que le toma a un paquete ICMP viajar entre dos puntos (Puntos de Presencia POPS) definidos en la red de Internet de Telmex (round trip).	Lima < 80 ms Provincia < 680 ms
4	Packet Delivery Loss	Es el porcentaje de diferencia entre los paquetes ICMP transmitidos y recibidos.	< 1%

Fuente: América Móvil.

Dicho esto con el fin de demostrar el cumplimiento de la métrica establecida nos basamos en métodos propuestos por ITIL V3 donde establece que la disponibilidad es una actividad cuyo fin es evitar la pérdida de la disponibilidad de los servicios TI. Es así que para definir la disponibilidad en porcentaje se usará la siguiente ecuación porcentual de disponibilidad:

$$Availability = \frac{AST - DT}{AST} \times 100\%$$

AST: Corresponde al tiempo acordado de servicio TI ofrecido por la red VPN.

DT: Es el tiempo de interrupción del servicio TI durante los horarios de disponibilidad.

Para aplicar la fórmula es necesario precisar los tiempos de operatividad de la organización que detallamos a continuación:

Horas de Trabajo al día de cada sucursal: 12 Horas.

Días de trabajo a la semana: 7 Días.

$$\% \text{ Disponibilidad} = \frac{12 - 1}{12} = 91.66 \%$$

Es así que se logra demostrar un nivel de disponibilidad mayor al 90% mensual.

6 CONCLUSIONES

Como conclusión general podemos afirmar que las redes privadas virtuales son al fin y al cabo redes de comunicación y en consecuencia su análisis y estudio no crea la necesidad de reinventar la red, o de introducir paradigmas completamente nuevos que no tengan un análogo directo con las redes físicas existentes. En consecuencia queda claro que tener mecanismos que son comunes en las redes tanto físicas como virtuales facilita la introducción de redes privadas virtuales en las redes existentes y también reduce el esfuerzo necesario tanto para el desarrollo de estándares como para el desarrollo de productos, ya que las soluciones existentes pueden aprovecharse. Estos argumentos dejan claro como es considerada una red privada virtual y por consecuencia indican su tratamiento para el diseño de la misma.

Las redes privadas virtuales son sin duda una solución muy flexible y sobre todo económica para las organizaciones que necesiten tener una comunicación segura con sus proveedores, clientes, y/o sucursales, prescindiendo así de la implementación de costosas redes dedicadas de comunicación que permitirían conseguir el mismo fin. Después de estudiar las ventajas en cuanto a infraestructura y costos que ofrece la implementación de redes privadas virtuales resulta innegable considerar a esta solución como una de las mejores opciones de comunicación para el Distribuidor Autorizado Claro pues además de su bajo costo ofrece seguridad en la transmisión de datos, así mismo nos ofrece escalabilidad pues nos permitirá a futuro crear conexiones virtuales con otros puntos de venta cuando la organización así lo requiera y con una mínima inversión con el ISP América Móvil Perú SAC.

A continuación se presentan las conclusiones por cada objetivo específico:

- **OE1:** De acuerdo a las subredes válidas y máscaras de subred indicadas en el RFC 1878 se puede concluir que efectivamente la red clase B nos brinda hasta 2048 redes disponibles de 30 hosts lo cual nos permite tener un amplio margen de direcciones IP para futuros locales. Es así que gracias al cálculo VLSM efectuado se dispone de hasta 23 redes disponibles y de 2020 redes disponibles por calcular con lo que definitivamente aseguramos una gran cantidad de redes, con más de 90% de redes disponibles para un futuro crecimiento.

- **OE2:** Según indica el RFC 3193 la utilización de protocolos L2TP/IPSec en la configuración VPN nos brinda seguridad en el flujo de comunicaciones es así que gracias a la Matriz de evaluación de riesgos de seguridad de la información realizada se puede concluir que la configuración VPN nos brinda de manera directa confidencialidad e integridad en el flujo de la información entre sucursales la misma que permitirá tomar buenas decisiones en base a información real integra y segura, además de forma indirecta al contar con una red privada virtual segura se podrá montar sobre ella mecanismos de autenticación y control de acceso a usuarios con lo que toda la organización será controlada por políticas GPO del AD y restricciones del Firewall ubicados en la sede principal con alcance a todas las sucursales de la organización.
- **OE3:** Las pruebas de la red privada virtual fueron satisfactorias, lo que demuestra que las VPN son una gran solución que permite una topología de red centralizada entre sucursales donde es posible tener acceso a los recursos TI en tiempo real permitiendo así la disponibilidad de la información en todo momento con el fin de tomar las mejores decisiones comerciales que el negocio necesita. Logrando un nivel de disponibilidad mayor al 90% mensual.

Es así que además gracias a la topología centralizada también podemos contar con:

- Accesibilidad a la base de datos central desde las sucursales.
- Controles de acceso y seguridad a las sucursales desde la sede principal.
- Una solución de replicación y/o alta disponibilidad en los servidores.

Se demuestra la necesidad de una interconexión permanente para la mejor administración de cualquier empresa, más aun si los precios y stock de sus productos están sujetos a cambios y las ventas son representativas en intervalos menores a un día, como es el caso del Distribuidor Autorizado de Claro.

Finalmente las VPN significan una importante solución para la organización en cuanto a confiabilidad, integridad y disponibilidad de su información, que son los tres pilares fundamentales de la seguridad de la información que toda organización necesita. Así mismo gracias a la integración permanente de sus redes LAN y la consecuente conexión a una única

base de datos mejorara notablemente la calidad de servicio de la empresa en cuanto a atención al cliente, ya que la información de la empresa se actualizara constantemente y tendrá una mejor integridad. Es así que el presente estudio realizado cumplió los objetivos propuestos inicialmente donde se logró la interconexión de la sede principal con sus sucursales de manera segura, económica y sobre todo logrando la disponibilidad de su información.

7 RECOMENDACIONES

Como recomendación general es útil analizar primero como es tratado un problema particular en un entorno de red física, y luego aplicar el mismo principio a un entorno que contiene redes virtuales, para finalmente desarrollar extensiones y mejoras apropiadas cuando sea necesario. Esto debido a que muchos aspectos de las redes, como el direccionamiento, el mecanismo de reenvío, la calidad del servicio (QoS), la seguridad y firewall, tienen soluciones comunes tanto en las redes físicas como en las virtuales, y muchos de los problemas que surgen en la discusión de las VPN tienen análogos directos con aquellos problemas implementados en redes físicas.

A continuación se presentan recomendaciones por cada objetivo específico:

OE1: Es necesario seguir estrictamente el cuadro de direcciones IPs calculados en el Capítulo IV, pues esto asegura la conectividad entre servidores críticos como son AD y BD, además se recomienda llevar un control de las direcciones IPs entregadas a cada host con el fin de no repetir direcciones IPs, evitando así conflictos IP.

Así mismo se deberá identificar cada host con un número de IP único para de esta manera con solo saber el IP poder identificar su ubicación tanto física como lógica y poder tomar acciones de acuerdo al tratamiento que le corresponda al usuario del terminal.

OE2: Se recomienda que el personal encargado de manejar y realizar el monitoreo de los servidores VPN de la organización, establezcan políticas de seguridad necesarias para evitar el acceso a usuarios no autorizados a la información y de esta manera evitar modificaciones en las mismas.

Se recomienda a los administradores de la VPN hacer un monitoreo continuo de logs que genera la VPN, así mismo se recomienda utilizar un puerto de switch dedicado que permita monitorear el tráfico cursado a través del enlace al ISP y de esta manera comparar con los informes que el proveedor periódicamente entregue, esto es necesario para tener la certeza de que el ancho de banda contratado es realmente el acordado al inicio.

Es necesario hacer un seguimiento en las horas de mayor tráfico para determinar momentos en los que se produzca mayor congestión, y de esta manera poder prever posibles ampliaciones del ancho de banda contratado con el proveedor ISP.

OE3: Se deberá realizar pruebas regulares de replicación entre servidores AD y BD con el fin de verificar su replicación en tiempo real para de esta manera garantizar su disponibilidad para cuando la organización lo necesite.

Así mismo se recomienda realizar simulacros donde se ponga en uso los servidores alternos esto con el fin de evaluar el tiempo que le toma a los usuarios finales poder continuar con sus labores diarias, para de esta manera identificar posibles problemas o contratiempos los mismos que deberán ser tratados para minimizar su impacto.

8 REFERENCIAS

- [1] **BANCO INTERAMERICANO DE DESARROLLO (BID)** 2013 Estrategia de Infraestructura para la Competitividad. Washington BID.
- [2] **BROLLO, Gerardo (2010)** Nuevas Tendencias en Redes Virtuales Privadas (Trabajo de Adscripción para el curso de Teleproceso y Sistemas Distribuidos). Corrientes: Universidad Nacional del Nordeste.
- [3] **BROWN, Steven R. (2001)** Implementación de Redes Privadas Virtuales (RPV) México: McGraw-Hill Interamericana.
- [4] **CALDERON RODRIGUEZ, Calixto (2001)** Implementación de una VPN (Virtual Private Network) Usando el estándar IPSEC (Proyecto de fin de carrera como especialista en Informática). Valencia: Universidad Politécnica de Valencia.
- [5] **CEVALLOS RODRIGUEZ, Mario Roberto (2006)** Diseño e Implementación de una Red Virtual Privada entre las oficina de INFONET ubicadas en las ciudades de Quito y Miami (Tesis para el Título de Ingeniero en Electrónica y Telecomunicaciones). Sangolqui: Escuela Politécnica del Ejercito.
- [6] **CISCO SYSTEMS (2018)** Red Privada Virtual (consulta: 13 de agosto de 2018) https://www.cisco.com/c/es_mx/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html
- [7] **COLEGIO DE INGENIEROS DEL PERU (CIP)** 2013 Banda ancha para la inclusión. Lima CIP.
- [8] **FLORES MERCADO, Miguel Angel (2007)** Diseño de un enlace de microondas dedicado entre las radio bases de Acajete, Cuacnopala, Esperanza y una central en Puebla (Tesis para el Título de Ingeniero en Comunicaciones y Electrónica). México DF: Escuela Superior de Ingeniería Mecánica y Eléctrica.
- [9] **FONSECA Ch, ROMERO G, y MEDELLIN S. (2014)** Investigaciones en Tecnologías de Información Informática y Computación. EEUU: Palibrio LLC.
- [10] **GUGLIELMO GARCIA, Miguel Eduardo (2012)** Modelo de interconexión de los ambulatorios que conformar el servicio de salud del municipio de El Hatillo con el centro médico docente La Trinidad (Tesis para el Título de Ingeniero en Telecomunicaciones). Caracas: Universidad Católica Andrés Bello.
- [11] **GUTIERREZ GOZALEZ, María Nieves (2006)** Estudio sobre las VPN (Tesis para el Título de Ingeniero en Informática). Valladolid: Universidad de Valladolid.
- [12] **GUZMAN VITE, Marcos (2008)** Implementación de una Red Privada Virtual en Presidencia Municipal de Pachuca de Soto Hidalgo (Tesis para el Título de Ingeniero en Electrónica y Telecomunicaciones). Pachuca de Soto: Instituto de Ciencias de Pachuca de Soto Hidalgo.

- [13] **INTERNET ENGINEERING TASK FORCE (IETF) (2018)** Sitio web oficial de la IETF; contiene información sobre la institución y enlaces de interés (consulta: 20 de agosto de 2018) <https://www.ietf.org/>
- [14] **REQUEST FOR COMMENTS (RFC1878) (2018)** RFC 1878 (consulta: 20 de agosto de 2018) <https://tools.ietf.org/html/rfc1878>
- [15] **REQUEST FOR COMMENTS (RFC2764) (2018)** RFC 2764 (consulta: 20 de agosto de 2018) <https://tools.ietf.org/html/rfc2764>
- [16] **REQUEST FOR COMMENTS (RFC3193) (2018)** RFC 3193 (consulta: 20 de agosto de 2018) <https://tools.ietf.org/html/rfc3193>
- [17] **LIMARI RAMIREZ, Víctor Humberto (2004)** Protocolos de Seguridad para Redes Privadas Virtuales (VPN) (Tesis para el Título de Ingeniero Electrónico). Valdivia: Universidad Austral de Chile.
- [18] **MENENDEZ AVILA, Ricardo Armando (2012)** Estudio del Desempeño e Implementación de una solución MPLS-VPN sobre Múltiples Sistemas Autónomos. (Tesis para optar el Título de Ingeniero de las Telecomunicaciones). Lima: Pontificia Universidad Católica del Perú.
- [19] **OROZCO LARA, Fausto Raúl (2014)** Diseño de una Red Virtual con tecnología MPLS para la Carrera de Ingeniería de Networking de la Universidad de Guayaquil. (Tesis para el Título de Magister en Telecomunicaciones). Guayaquil: Universidad Católica de Santiago de Guayaquil.
- [20] **ORTEGA BUSTAMANTE, Cosme MacArthur (2003)** Metodología para la Implementación de Redes Privadas Virtuales, con Internet como red de enlace (Tesis para el Título de Ingeniero en Sistemas Computacionales). Ibarra: Universidad Técnica del Norte.
- [21] **REYES MORENO, Enevis Rafael (2005)** Lineamientos para la creación de una VPN (Virtual Private Network) Red Privada Virtual (Tesis para el Título de especialista en Telemática). Medellín: Universidad de Antioquia.
- [22] **RODRIGUEZ ORE, Daniel (2012)** Gestión de disponibilidad de los servicios TI en la empresa virtual IT-Expert (Tesis para el Título de Ingeniero de Sistemas de Información). Lima: Universidad Peruana de Ciencias Aplicadas - UPC.
- [23] **SANTAMARIA SILUPU, Jorge Luis (2016)** Estudio de los Diferentes Modelos de Inter-AS MPLS-VPNs para brindar una propuesta Técnica que permita la comunicación entre Múltiples Proveedores de Servicios. (Tesis para el Título de Ingeniero Electrónico y Telecomunicaciones). Piura: Universidad Nacional de Piura.
- [24] **SCOTT Ch., WOLFE P. y ERWIN M. (1998)** Virtual Private Networks California: O'Reilly Media.

- [25] **TORRES ABRIL, Walter Vinicio (2002)** Estudio y diseño de una red privada virtual para INGELSI utilizando sistemas operativos Microsoft Windows 2000. (Tesis para el Título de Ingeniero en Electrónica y Telecomunicaciones). Quito: Escuela Politécnica Nacional.
- [26] **TRUJILLO MACHADO, Edison Rafael (2006)** Diseño e Implementación de una VPN en una empresa comercializadora utilizando IPSEC. (Tesis para el Título de Ingeniero en Informática). Quito: Escuela Politécnica Nacional.
- [27] **UNIVERSIDAD DE VALENCIA (2018)** Red y Comunicaciones: Red Privada Virtual (consulta: 13 de agosto de 2018) <http://www.uv.es/uvweb/servicio-informatica/es/servicios/generales/red-comunicaciones/red-privada-virtual-vpn/-es-vpn-1285903202284.html>
- [28] **VASQUEZ, Jorge (2014)** Investigaciones en tecnologías de información informática y computación USA: Palibrio.
- [29] **VIVANCO MUÑOZ, Percy (2003)** Desarrollo de una virtual private network (VPN) para la interconexión de una empresa con sus sucursales en provincias. (Tesis para el Título de Ingeniero de Sistemas). Lima: Universidad Nacional Mayor de San Marcos.
- [30] **VIRTUAL PRIVATE NETWORK CONSORTIUM (VPNC) (2016)** Sitio web oficial de VPNC; contiene información sobre la institución (consulta: 20 de febrero de 2016) <https://www.vpnc.org/>

9 GLOSARIO

A

ACTIVE DIRECTORY.- Término que utiliza Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores.

ACCESO REMOTO.- La capacidad de un ordenador en un emplazamiento para conectarse a un dispositivo en otro emplazamiento.

ANCHO DE BANDA.- La gama de frecuencias disponible para señalar la diferencia entre las frecuencias más altas y las más bajas de una banda, se miden en Hertz.

AUTENTICACIÓN.- Determinar si un usuario tiene permiso de acceso a un recurso o para realizar una operación.

F

FOREFRONT TMG.- Gateway de seguridad web desarrollado por Microsoft que ayuda a proteger a las empresas de las amenazas que existen actualmente en Internet.

I

ISP (INTERNET SERVICE PROVIDER).- Es una entidad, habitualmente con ánimo de lucro, que además de dar acceso a Internet a personas físicas y/o jurídicas, les ofrece una serie de servicios (páginas web, consultoría de webs e Intranets, etc.).

INTERNET.- Red global de equipos cuyas comunicaciones se realizan mediante un protocolo común, TCP/IP.

L

LATENCIA.- 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.

P

PERFIL DE USUARIO.- Es una colección de opciones de configuración que hacen que el equipo tenga el aspecto y funcione de la manera que el usuario desea.

PROXY.- Servidor especial encargado, entre otras cosas, de centralizar el tráfico entre Internet y una red privada, de forma que evita que cada una de las máquinas de la red interior tenga que disponer necesariamente de una conexión directa a la red. Al mismo tiempo contiene mecanismos de seguridad (firewall o cortafuegos) los cuales impiden accesos no autorizados desde el exterior hacia la red privada.

R

RED PRIVADA VIRTUAL.- Es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet.

S

SERVIDOR.- Máquina conectada a otras que ejecuta una acción a solicitud de las otras (clientes).

10 SIGLARIO

- 3DES Triple Data Encryption Standard
- AD Active Directory
- BID Banco Interamericano de Desarrollo
- CPE Customer Premisess Equipment
- DAC Distribuidor Autorizado de Claro
- GPO Group Policy Object
- IPSEC Internet Protocol Security
- ISP Internet Service Provider
- LAN Local Area Network
- L2TP Layer 2 Tunneling Protocol
- MPLS Multiprotocol Label Switching
- OSI Open System Interconnection
- PPTP Point to Point Tunneling Protocol
- RDNFO Red Dorsal Nacional de Fibra Óptica
- SLA Service Level Agreement
- TIC Tecnologías de la Información y Comunicación
- VPN Virtual Private Network
- WAN Wide Area Nework

11 ANEXOS

Anexo 1. Situación actual de la Organización

11.1 Instalación de Microsoft Forefront TMG 2010

1. Verificar que tenemos las tarjetas de red configuradas apropiadamente para la instalación

2. Tras ejecutarse el disco de instalación, la pantalla de inicio de Forefront TMG 2010 aparece

3. Clic en 'Ejecutar la herramienta de preparación'

4. Pantalla de inicio de 'Herramientas de preparación'

5. Aceptar los términos y condiciones. Clic en Siguiente

6. Escoger el tipo de instalación, escoger 'Servicios y Administración de Forefront TMG'. Clic en Siguiente

7. Empieza la preparación para instalar el sistema

8. La preparación ha finalizado. Clic en Finalizar para iniciar el Asistente para la instalación de Forefront TMG

9. El Asistente de instalación comienza. Clic en Siguiente

10. Aceptar el Contrato de Licencia. Clic en Siguiente

11. Escribir nombre de usuario y organización. Escribir número de serie. Clic en Siguiente

The screenshot shows the 'Forefront TMG Empresa Asistente para la instalación' window. The title bar is blue with the Microsoft logo and the text 'Forefront TMG Empresa Asistente para la instalación'. The main area has a light gray background. At the top, the section is titled 'Información del cliente' in bold. Below it, the instruction 'Escriba los detalles del cliente.' is displayed. There are three input fields: 'Nombre de usuario:' with the text 'MEGALINE', 'Organización:' with the text 'MEGALINE', and 'Número de serie del producto:' which is split into five boxes containing 'YTDT9', 'WR9Y6', 'WF2W6', 'J6V4G', and 'D2FF7'. At the bottom, there are three buttons: '< Atrás', 'Siguiente >', and 'Cancelar'. A mouse cursor is pointing at the 'Siguiente >' button.

12. Ruta de instalación. Clic en Siguiente

The screenshot shows the 'Forefront TMG Empresa Asistente para la instalación' window. The title bar is blue with the Microsoft logo and the text 'Forefront TMG Empresa Asistente para la instalación'. The main area has a light gray background. At the top, the section is titled 'Ruta de acceso de instalación' in bold. Below it, the instruction 'Puede cambiar la ruta de acceso de instalación o haga clic en Siguiente para aceptar la ruta de acceso predeterminada.' is displayed. There is a text box labeled 'Ruta de acceso de instalación para Forefront TMG:' containing the path 'C:\Program Files\Microsoft Forefront Threat Management Gateway\'. To the right of the text box is a 'Cambiar...' button. At the bottom, there are three buttons: '< Atrás', 'Siguiente >', and 'Cancelar'. A mouse cursor is pointing at the 'Siguiente >' button.

13. Agregar red interna. Clic en Agregar

14. Aquí agregar el rango de direcciones IP a asignar a la red interna o asignar un adaptador de red del servidor. Clic en Agregar adaptador.

15. Marcar la opción de la interfaz de red INTERNA. Clic en Aceptar

16. Aceptamos nuevamente

17. Habiendo agregado la red interna. Clic en Siguiente

18. Advertencia de algunos servicios que se reiniciarán. Clic en Siguiente

19. Clic en Instalar para empezar la instalación

20. La instalación en proceso

21. La instalación continúa instalando componentes principales y secundarios

22. La instalación finaliza

23. Tras abrir la consola de Administración de Forefront, vemos este asistente para configurar rápidamente el servicio. Clic en Cerrar

24. Confirmamos que queremos cerrar el Asistente. Clic en Si

25. Aquí finaliza la instalación de Forefront TMG

11.2 Configuración VPN sitio a sitio Servidores SRV-TMG1 Y SRV-TMG2

Para los manuales mostrados a continuación, se utilizaron la siguiente configuración de red:

SRV-TMG1

RED INTERNA:

IP: 172.16.1.1

MASK: 255.255.255.128

PE: ----

DNS: 172.16.1.100

RED EXTERNA

IP: 192.168.1.38

SRV-TMG2

RED INTERNA

IP: 172.16.1.129

MASK: 255.255.255.224

PE: ----

DNS: 172.16.1.130

RED EXTERNA

IP: 192.168.1.39

• CONFIGURACIÓN VPN SITIO A SITIO: SRV-TMG1

1. Administración de Forefront TMG. Ir a *Directiva de acceso remoto*

2. Clic derecho. Clic en *Configurar propiedades de VPN*

3. Seleccionar redes desde las cuales los clientes pueden iniciar conexiones VPN. Marcar la opción *Externa*

4. Seleccionar método de asignación de direcciones IP. Marcar la opción *Grupo de direcciones estáticas*. Clic en Agregar

5. Seleccionar el servidor SRV-TMG1 y escribir la dirección inicial y final asignada a las conexiones VPN. Clic en Aceptar

6. Clic en Aplicar

7. En pestaña Autenticación, marcar *Autenticación cifrada de Microsoft versión 2 (MS-CHAPv2)*

8. En pestaña RADIUS, desmarcar todas las opciones. Clic en Aceptar

9. Tareas de clientes de VPN. Ir a *Configurar acceso de cliente de VPN*

10. En la ventana Propiedades: Clientes de VPN. Ir a pestaña *General*

11. Marcar la opción *Habilitar acceso de clientes VPN*. Agregar el número de conexiones VPN permitidos.

12. Clic en Aceptar

13. Clic en Aplicar para guardar los cambios

14. Clic en *Comprobar propiedades de VPN*

15. En pestaña *Protocolos*, marcar las opciones *Habilitar L2TP/IPSec* y *Habilitar PPTP*.
Clic en *Aceptar*

16. En pestaña *Sitios remotos*

17. Clic en *Crear conexiones VPN de sitio a sitio*

NOTA: Tomar en cuenta la siguiente configuración para configurar las reglas VPN:

Para SRV-TMG1

Usuario local a crear: tmg2

Nombre de regla: tmg2

Usuario para autenticación remota: tmg1

Para SRV-TMG2

Usuario local a crear: tmg1

Nombre de regla: tmg1

Usuario para autenticación remota: tmg2

18. Asistente para la creación de nueva red VPN sitio a sitio. Escribir nombre de regla *tmg2*

19. Marcar la opción *Protocolo de túnel de capa dos (L2TP) a través de IPSec*. Clic en Siguiete

20. Mensaje que indica que debemos crear un usuario para autenticación. Lo crearemos luego. Clic en Aceptar

21. Escribir la dirección IP del servidor VPN de sitio remoto

22. Autenticación remota. Escribir el nombre del usuario con el que se autenticara al sitio remoto (Ver NOTA)

The screenshot shows a Windows XP-style dialog box titled 'Asistente para crear conexión de sitio a sitio'. The main heading is 'Autenticación remota'. Below it, a text box explains: 'Para que el sitio local inicie una conexión al sitio remoto, se requiere una cuenta de usuario en el sitio remoto para la autenticación.' There is a checked checkbox labeled 'Permitir que el sitio local inicie conexiones al sitio remoto con esta cuenta de usuario:'. Below this are four input fields: 'Nombre de usuario:' with the text 'tmg1', 'Dominio:', 'Contraseña:' (masked with dots), and 'Confirmar contraseña:' (also masked with dots). A yellow warning icon is next to a note: 'La cuenta de usuario debe coincidir con el nombre de la conexión VPN de sitio a sitio creada en el sitio remoto.' At the bottom are three buttons: '< Atrás', 'Siguiete >' (with a mouse cursor pointing to it), and 'Cancelar'.

23. Autenticación saliente L2TP/IPsec. Marcar la opción *Autenticación de clave previamente compartida*. Escribir clave *megaline123*

The screenshot shows the same dialog box, but the step is 'Autenticación saliente L2TP/IPsec'. The text box says: 'Especifique el método de autenticación IPsec usado para conectar al sitio remoto.' There are two radio button options. The first is 'Autenticación de certificado (recomendado)' with a description: 'La autenticación de certificado es el método de autenticación predeterminado y es el recomendado. Este método requiere que los servidores VPN de ambos sitios tengan certificados digitales emitidos por la misma entidad de certificación de confianza.' The second option, 'Autenticación de clave previamente compartida', is selected. Below it is a text field labeled 'Clave previamente compartida:' containing the text 'megaline123'. At the bottom are the same three buttons: '< Atrás', 'Siguiete >' (with a mouse cursor pointing to it), and 'Cancelar'.

24. Direcciones de red. Clic en Agregar intervalo...

25. Escribir dirección inicial y final de sitio remoto. Clic en Aceptar

26. Clic en Siguiente

Asistente para crear conexión de sitio a sitio

Direcciones de red
Especifique los intervalos de direcciones IP de la red de sitio remoto. Los intervalos normalmente coinciden con los intervalos internos en el otro extremo del túnel.

Intervalos de direcciones:

Dirección inicial	Dirección final
172.16.1.128	172.16.1.159

Editar...
Quitar
Agregar intervalo...

< Atrás Siguiente > Cancelar

27. Desmarcar la opción *El sitio remoto está habilitado para el equilibrio de carga de red*.

Clic en Siguiente

Asistente para crear conexión de sitio a sitio

Equilibrio de carga en la red remoto
Si el equilibrio de carga de red está habilitado en el sitio remoto, especifique las direcciones IP dedicadas (DIP) de la puerta de enlace del sitio remoto.

☐ El sitio remoto está habilitado para el equilibrio de carga de red

Especifique las direcciones IP dedicadas en la puerta de enlace remota:

Dirección inicial	Dirección final
-------------------	-----------------

Agregar intervalo...
Editar...
Quitar

Ayuda acerca de las [matrices remotas habilitadas para NLB](#).

< Atrás Siguiente > Cancelar

28. Marcar la opción *Crear una regla de red que especifique una relación de ruta*. Nombre de red por defecto. Clic en Siguiente

Asistente para crear conexión de sitio a sitio

Regla de red de sitio a sitio
Se requiere una regla de red para que el tráfico se enrute a la nueva red de sitio a sitio VPN y desde ella.

☒ Crear una regla de red que especifique una relación de ruta

Nombre de la regla de red: tmg2 a red interna

Enrutar el tráfico entre la nueva red y estos destinos:

Nombre
Interna

Agregar...
Editar...
Quitar...

☐ Crearé una regla de red más adelante
Si elige esta opción, debe crear una regla de red para esta red de sitio a sitio. De lo contrario, el tráfico no se enrutará a esta red ni desde ella.

< Atrás Siguiente > Cancelar

29. Marcar la opción *Crear una regla de acceso permitido...* Aplicar la regla a todo el tráfico saliente.

Asistente para crear conexión de sitio a sitio

Regla de acceso a red de sitio a sitio
Se requiere una regla de acceso para permitir el tráfico a la nueva red de sitio a sitio VPN y desde ella.

☒ Crear una regla de acceso permitido. Esta regla permitirá el tráfico entre la red interna y la nueva red de sitio a sitio para todos los usuarios.

Nombre de la regla de acceso: Permitir el acceso entre tmg2 e interna

Aplicar la regla a estos protocolos:

Protocolos seleccionados
Todo el tráfico saliente
Protocolos seleccionados
Todo el tráfico saliente excepto el seleccionado

Agregar...
Editar...
Quitar

☐ Cambiaré la directiva de acceso más adelante
Si elige esta opción, debe cambiar la directiva de acceso para esta red de sitio a sitio. De lo contrario, se denegará el tráfico a esta red y desde ella.

< Atrás Siguiente > Cancelar

30. Clic en Siguiente

31. Clic en Finalizar

32. Clic en Aceptar para reiniciar todas las conexiones de Enrutamiento y Acceso Remoto

33. Mensaje que indica que debemos crear un usuario tmg2 con acceso telefónico permitido.
Clic en Aceptar

34. Ir a Administrador del servidor > Usuarios y grupos locales

35. Acción > Usuario nuevo

36. Creamos el usuario tmg2, con contraseña respectiva. Clic en Crear

37. Doble clic sobre usuario tmg2. Propiedades de usuario tmg2. Ir a pestaña Marcado

38. Marcar la opción *Permitir Acceso* en Permiso de acceso a redes. Clic en Aceptar

- **CONFIGURACION VPN SITIO A SITIO: SRV-TMG2**

NOTA:

Para SRV-TMG1

Para SRV-TMG2

Usuario local a crear: tmg2

Usuario local a crear: tmg1

Nombre de regla: tmg2

Nombre de regla: tmg1

*Usuario para autenticación remota: tmg1
tmg2*

Usuario para autenticación remota:

39. Administración de Forefront TMG. Ir a *Directiva de acceso remoto*

40. Clientes VPN. Clic en Configuración de método de asignación de direcciones

41. Clic en Agregar

42. Seleccionar el servidor SRV-TMG2 y escribir la dirección inicial y final asignada a las conexiones VPN. Clic en Aceptar

43. Clic en Aceptar

44. Tareas. Clic en Configurar acceso de cliente VPN

45. Ir a pestaña General

46. Marcar opción *Habilitar acceso de clientes VPN*

47. Clic en Aceptar

48. Clic en Comprobar propiedades de VPN

49. En pestaña Protocolos, marcar las opciones *Habilitar L2TP/IPSec* y *Habilitar PPTP*.

Clic en Aceptar

50. En pestaña *Sitios remotos*. Clic en *Crear conexiones VPN de sitio a sitio*

Cientes de VPN Sitios remotos

Sitios remotos VPN

Para permitir conexiones VPN de sitio a sitio, primero debe crear una red de sitio remoto. La red de sitio remoto especifica las propiedades para la conexión de sitio a sitio, como los protocolos usados para el tráfico VPN, los servidores VPN, los métodos de autenticación y las direcciones IP de la red VPN.

Para crear una red VPN de sitio remoto, en el panel de tareas, haga clic en [Crear conexión VPN de sitio a sitio](#).

[Ayuda acerca de las redes privadas virtuales de sitio a sitio.](#)

51. Asistente para la creación de nueva red VPN sitio a sitio. Escribir nombre de regla *tmg1*

52. Marcar la opción *Protocolo de túnel de capa dos (L2TP) a través de IPSec*. Clic en *Siguiente*

53. Mensaje que indica que debemos crear un usuario para autenticación. Lo crearemos luego. Clic en Aceptar

54. Escribir la dirección IP del servidor VPN de sitio remoto

55. Autenticación remota. Escribir el nombre del usuario con el que se autenticara al sitio remoto (Ver NOTA)

The screenshot shows a Windows XP-style dialog box titled 'Asistente para crear conexión de sitio a sitio'. The main heading is 'Autenticación remota'. Below it, a text box explains: 'Para que el sitio local inicie una conexión al sitio remoto, se requiere una cuenta de usuario en el sitio remoto para la autenticación.' There is a checked checkbox labeled 'Permitir que el sitio local inicie conexiones al sitio remoto con esta cuenta de usuario:'. Below this are four input fields: 'Nombre de usuario:' containing 'tmg2', 'Dominio:', 'Contraseña:' (masked with dots), and 'Confirmar contraseña:' (also masked with dots). A yellow warning icon is next to a note: 'La cuenta de usuario debe coincidir con el nombre de la conexión VPN de sitio a sitio creada en el sitio remoto.' At the bottom are three buttons: '< Atrás', 'Siguiete >' (with a mouse cursor pointing to it), and 'Cancelar'.

56. Marcar la opción *Autenticación de clave previamente compartida*

The screenshot shows the same dialog box, but at the 'Autenticación saliente L2TP/IPsec' step. The text says: 'Especifique el método de autenticación IPsec usado para conectar al sitio remoto.' There are two radio button options. The first is 'Autenticación de certificado (recomendado)' with a description: 'La autenticación de certificado es el método de autenticación predeterminado y es el recomendado. Este método requiere que los servidores VPN de ambos sitios tengan certificados digitales emitidos por la misma entidad de certificación de confianza.' The second option, 'Autenticación de clave previamente compartida', is selected. Below it is a text field labeled 'Clave previamente compartida:' containing the text 'megaline123'. At the bottom are the same three buttons: '< Atrás', 'Siguiete >' (with a mouse cursor pointing to it), and 'Cancelar'.

57. Marcar la opción *Permitir la autenticación de clave compartida...*

58. Clic en Agregar intervalo... Escribir dirección inicial y final de sitio remoto. Clic en Aceptar

59. Desmarcar la opción *El sitio remoto está habilitado para el equilibrio de carga de red*.

Clic en Siguiente

Asistente para crear conexión de sitio a sitio

Equilibrio de carga en la red remoto
Si el equilibrio de carga de red está habilitado en el sitio remoto, especifique las direcciones IP dedicadas (DIP) de la puerta de enlace del sitio remoto.

☐ El sitio remoto está habilitado para el equilibrio de carga de red

Especifique las direcciones IP dedicadas en la puerta de enlace remota:

Dirección inicial	Dirección final
-------------------	-----------------

Agregar intervalo...
Editar...
Quitar...

Ayuda acerca de las [matrices remotas habilitadas para NLB](#).

< Atrás **Siguiente >** Cancelar

60. Marcar la opción *Crear una regla de red que especifique una relación de ruta*. Nombre de red por defecto. Clic en Siguiente

Asistente para crear conexión de sitio a sitio

Regla de red de sitio a sitio
Se requiere una regla de red para que el tráfico se enrute a la nueva red de sitio a sitio VPN y desde ella.

☒ Crear una regla de red que especifique una relación de ruta

Nombre de la regla de red: tmg1 a red interna

Enrutar el tráfico entre la nueva red y estos destinos:

Nombre
Interna

Agregar...
Editar...
Quitar...

☐ Crearé una regla de red más adelante
Si elige esta opción, debe crear una regla de red para esta red de sitio a sitio. De lo contrario, el tráfico no se enrutará a esta red ni desde ella.

< Atrás **Siguiente >** Cancelar

61. Marcar la opción *Crear una regla de acceso permitido...* Aplicar la regla a todo el tráfico saliente. Clic en Siguiente

62. Clic en Finalizar

63. Clic en Aceptar para reiniciar todas las conexiones de Enrutamiento y Acceso Remoto

64. Mensaje que indica que debemos crear un usuario tmg2 con acceso telefónico permitido.

Clic en Aceptar

65. Aplicar los cambios en Administración de Forefront TMG

66. En Administrador de Servidor, crear un nuevo usuario *tmg1*

67. En Propiedades de usuario *tmg1*. Marcar la opción *Permitir Acceso* en Permiso de acceso a redes. Clic en Aceptar

11.3 Configuración VPN sitio a sitio entre SRV-TMG1 Y SRV-VPN1

- **CONFIGURACIÓN VPN SITIO A SITIO: SRV-TMG1**

A continuación se muestran los pasos para configurar la regla de acceso en el servidor SRV-TMG1. Para información más detallada, revisar los manuales previos.

1. Asistente para la creación de nueva red VPN sitio a sitio. Escribir nombre de regla *tmg21*

2. Marcar la opción *Protocolo de túnel de capa dos (L2TP) a través de IPSec*. Clic en Siguiente

3. Mensaje que indica que debemos crear un usuario para autenticación. Lo crearemos luego.

Clic en Aceptar

4. Escribir la dirección IP del servidor VPN de sitio remoto

5. Autenticación remota. Escribir el nombre del usuario con el que se autenticara al sitio remoto (Ver NOTA)

The screenshot shows a Windows XP-style dialog box titled "Asistente para crear conexión de sitio a sitio". The main heading is "Autenticación remota". Below it, a text box explains: "Para que el sitio local inicie una conexión al sitio remoto, se requiere una cuenta de usuario en el sitio remoto para la autenticación." There is a checked checkbox labeled "Permitir que el sitio local inicie conexiones al sitio remoto con esta cuenta de usuario:". Below this are four input fields: "Nombre de usuario:" with the text "tmg12", "Dominio:" (empty), "Contraseña:" (masked with dots), and "Confirmar contraseña:" (masked with dots). A yellow warning icon is next to a note: "La cuenta de usuario debe coincidir con el nombre de la conexión VPN de sitio a sitio creada en el sitio remoto." At the bottom are three buttons: "< Atrás", "Siguiente >", and "Cancelar".

6. Autenticación saliente L2TP/IPsec. Marcar la opción Autenticación de clave previamente compartida. Escribir clave *megaline123*

The screenshot shows the same dialog box, but the main heading is "Autenticación saliente L2TP/IPsec". The text box says: "Especifique el método de autenticación IPsec usado para conectar al sitio remoto." There are two radio button options. The first is "Autenticación de certificado (recomendado)" with a description: "La autenticación de certificado es el método de autenticación predeterminado y es el recomendado. Este método requiere que los servidores VPN de ambos sitios tengan certificados digitales emitidos por la misma entidad de certificación de confianza." The second option, "Autenticación de clave previamente compartida", is selected. Below it is a text box labeled "Clave previamente compartida:" containing the text "megaline123". The same three buttons are at the bottom: "< Atrás", "Siguiente >", and "Cancelar".

7. Clic en Agregar intervalo... Escribir dirección inicial y final de sitio remoto. Clic en Aceptar

Dirección inicial	Dirección final
172.16.1.160	172.16.1.191

8. Desmarcar la opción *El sitio remoto está habilitado para el equilibrio de carga de red*. Clic en Siguiete

☐ El sitio remoto está habilitado para el equilibrio de carga de red

Especifique las direcciones IP dedicadas en la puerta de enlace remota:

Dirección inicial	Dirección final
-------------------	-----------------

9. Marcar la opción *Crear una regla de red que especifique una relación de ruta*. Nombre de red por defecto. Clic en Siguiente

The screenshot shows the 'Asistente para crear conexión de sitio a sitio' (Site-to-Site Connection Wizard) window. The title bar reads 'Asistente para crear conexión de sitio a sitio'. The main heading is 'Regla de red de sitio a sitio' (Site-to-Site Network Rule). Below the heading, a descriptive text states: 'Se requiere una regla de red para que el tráfico se enrute a la nueva red de sitio a sitio VPN y desde ella.' (A network rule is required for traffic to be routed to the new site-to-site VPN network and from it). There are two radio button options. The first option, 'Crear una regla de red que especifique una relación de ruta' (Create a network rule that specifies a route relationship), is selected. Below this option, there is a text field for 'Nombre de la regla de red:' (Network rule name) containing the text 'tmg21 a red interna'. Below that, a section titled 'Enrutar el tráfico entre la nueva red y estos destinos:' (Route traffic between the new network and these destinations:) contains a list box with the entry 'Interna' (Internal) and three buttons: 'Agregar...' (Add...), 'Editar...' (Edit...), and 'Quitar...' (Remove...). The second radio button option is 'Crearé una regla de red más adelante' (I will create a network rule later), with a descriptive text: 'Si elige esta opción, debe crear una regla de red para esta red de sitio a sitio. De lo contrario, el tráfico no se enrutará a esta red ni desde ella.' (If you choose this option, you must create a network rule for this site-to-site network. Otherwise, traffic will not be routed to this network or from it). At the bottom of the window are three buttons: '< Atrás' (Back), 'Siguiente >' (Next), and 'Cancelar' (Cancel).

10. Marcar la opción *Crear una regla de acceso permitido...* Aplicar la regla a todo el tráfico saliente. Clic en Siguiente

The screenshot shows the 'Asistente para crear conexión de sitio a sitio' (Site-to-Site Connection Wizard) window, Step 2: 'Regla de acceso a red de sitio a sitio' (Site-to-Site Network Access Rule). The title bar reads 'Asistente para crear conexión de sitio a sitio'. The main heading is 'Regla de acceso a red de sitio a sitio' (Site-to-Site Network Access Rule). Below the heading, a descriptive text states: 'Se requiere una regla de acceso para permitir el tráfico a la nueva red de sitio a sitio VPN y desde ella.' (A network access rule is required to allow traffic to the new site-to-site VPN network and from it). There are two radio button options. The first option, 'Crear una regla de acceso permitido. Esta regla permitirá el tráfico entre la red interna y la nueva red de sitio a sitio para todos los usuarios.' (Create an access rule. This rule will allow traffic between the internal network and the new site-to-site network for all users.), is selected. Below this option, there is a text field for 'Nombre de la regla de acceso:' (Access rule name) containing the text 'Permitir el acceso entre tmg21 e interna' (Allow access between tmg21 and internal). Below that, a section titled 'Aplicar la regla a estos protocolos:' (Apply the rule to these protocols:) contains a dropdown menu with 'Todo el tráfico saliente' (All outgoing traffic) selected. Below the dropdown is an empty list box and three buttons: 'Agregar...' (Add...), 'Editar...' (Edit...), and 'Quitar' (Remove). The second radio button option is 'Cambiaré la directiva de acceso más adelante' (I will change the access rule later), with a descriptive text: 'Si elige esta opción, debe cambiar la directiva de acceso para esta red de sitio a sitio. De lo contrario, se denegará el tráfico a esta red y desde ella.' (If you choose this option, you must change the access rule for this site-to-site network. Otherwise, traffic will be denied to this network and from it). At the bottom of the window are three buttons: '< Atrás' (Back), 'Siguiente >' (Next), and 'Cancelar' (Cancel).

11. Clic en Finalizar

12. Mensaje que indica que debemos crear un usuario tmg2 con acceso telefónico permitido.

Clic en Aceptar

- **CONFIGURACIÓN VPN SITIO A SITIO: SRV-VPN1**

A continuación se muestran los pasos para configurar. Para información más detallada, revisar los manuales previos. Abrir el servicio **Enrutamiento y Acceso Remoto**

13. Clic derecho en nombre del servidor SRV-VPN1, clic en *Configurar Enrutamiento y acceso remoto*

14. Asistente para instalación de servidor de Enrutamiento y acceso remoto. Clic en Siguiente.

15. Marcar la opción Acceso remoto (acceso telefónico o red privada virtual)

Asistente para la instalación del servidor de enrutamiento y acceso remoto

Configuración
Puede habilitar cualesquiera de las siguientes combinaciones de servicios o puede personalizar este servidor.

☒ Acceso remoto (acceso telefónico o red privada virtual)
Permitir a clientes remotos conectarse a este servidor a través de una conexión de acceso telefónico o una conexión segura a Internet de red privada virtual (VPN).

☐ Traducción de direcciones de red (NAT)
Permitir a clientes internos conectarse a Internet usando una dirección IP pública.

☐ Acceso a red privada virtual (VPN) y NAT
Permitir que los clientes remotos se conecten a este servidor a través de Internet y que los clientes locales se conecten a Internet usando una sola dirección IP pública.

☐ Conexión segura entre dos redes privadas
Conectar esta red a una red remota, como a una oficina sucursal.

☐ Configuración personalizada
Seleccionar cualquier combinación de características disponibles en Enrutamiento y acceso remoto.

[Para obtener más información.](#)

< Atrás Siguiente > Cancelar

16. Seleccionar la interfaz donde ingresaran las conexiones VPN. Seleccionar EXTERNA

Asistente para instalación del servidor de enrutamiento y acceso remoto

Conexión VPN
Para permitir que los clientes VPN se conecten a este servidor, al menos una interfaz de red debe estar conectada a Internet.

Seleccione la interfaz de red que conecta este servidor a Internet.

Interfaces de red:

Nombre	Descripción	Dirección IP
EXTERNA	Conexión de red Intel(R)...	192.168.1.67
INTERNA	Conexión de red Intel(R)...	172.16.1.161

☒ Habilitar seguridad en la interfaz seleccionada configurando filtros de paquetes estát
Los filtros de paquetes estáticos sólo permiten que el tráfico VPN obtenga acceso a este servidor mediante la interfaz seleccionada.

[Para obtener más información sobre las interfaces de red.](#)
[Para obtener más información sobre el filtrado de paquetes.](#)

< Atrás Siguiente > Cancelar

17. Asignaciones de direcciones IP. Marcar la opción *De un intervalo de direcciones especificado*

Asistente para instalación del servidor de enrutamiento y acceso remoto

Asignación de direcciones IP
Puede seleccionar el método para asignar direcciones IP a clientes remotos.

¿Cómo desea que se asignen las direcciones IP a los clientes remotos?

☐ Automáticamente
Si usa un servidor DHCP para asignar direcciones asegúrese de que está configurado correctamente. Si no utiliza un servidor DHCP, este servidor generará las direcciones.

☒ De un intervalo de direcciones especificado

[Para obtener más información](#)

< Atrás Siguiente > Cancelar

18. Escribir rango de direcciones IP a asignar a conexiones VPN

Asistente para instalación del servidor de enrutamiento y acceso remoto

Asignación de intervalo de direcciones
Puede especificar los intervalos de direcciones que este servidor usará para asignar direcciones a clientes remotos.

Escriba los intervalos de direcciones (conjuntos estáticos) que desea usar. Este servidor asignará todas las direcciones del primer intervalo antes de pasar al siguiente.

Inte

Editar intervalo de direcciones IPv4 ? x

Escriba una dirección IP inicial, y una dirección IP final o la cantidad de direcciones en el intervalo.

Dirección IP inicial: 200 . 200 . 200 . 41

Dirección IP final: 200 . 200 . 200 . 60

Número de direcciones: 20

Aceptar Cancelar

< Atrás Siguiente > Cancelar

19. Clic en Siguiente

Asistente para instalación del servidor de enrutamiento y acceso remoto

Asignación de intervalo de direcciones

Puede especificar los intervalos de direcciones que este servidor usará para asignar direcciones a clientes remotos.

Escriba los intervalos de direcciones (conjuntos estáticos) que desea usar. Este servidor asignará todas las direcciones del primer intervalo antes de pasar al siguiente.

Intervalos de direcciones:

De	Hasta	Número
200.200.200.41	200.200.200.60	20

Nuevo... Modificar... Eliminar

< Atrás Siguiente > Cancelar

20. Clic en la opción *No, usar Enrutamiento y Acceso Remoto*

Asistente para instalación del servidor de enrutamiento y acceso remoto

Administrar servidores de acceso remoto múltiples

Las solicitudes de conexión pueden autenticarse localmente o reenviarse a un servidor de Servicio de usuario de acceso telefónico de autenticación remota (RADIUS) para su autenticación.

Aunque Enrutamiento y acceso remoto puede autenticar solicitudes de conexión, grandes redes que incluyen varios servidores de acceso remoto usan a menudo un servidor RADIUS para realizar la autenticación central.

Si está usando un servidor RADIUS en su red, puede configurar este servidor para reenviar solicitudes de autenticación al servidor RADIUS.

¿Desea configurar este servidor para que trabaje con un servidor RADIUS?

☒ No, usar Enrutamiento y acceso remoto para autenticar las solicitudes de conexión

☐ Sí, configurar este servidor para que trabaje con un servidor RADIUS

[Para obtener más información](#)

< Atrás Siguiente > Cancelar

21. Clic en Finalizar

22. Clic en Aceptar

23. Acción > Interfaz de marcado a petición nueva

24. Asistente para interfaz de marcado a pedido. Clic en Siguiente

25. Nombre de interfaz: *tmg12*

26. Marcar la opción *Conectar usando red privada virtual (VPN)*

27. Marcar la opción *Protocolo de túnel de nivel 2 (L2TP)*

28. Escribir la dirección remota del servidor VPN

The screenshot shows a Windows XP-style dialog box titled "Asistente para interfaz de marcado a petición". The main heading is "Dirección de destino" with the question "¿Cuál es el nombre o la dirección del enrutador remoto?". Below this, it says "Escriba el nombre o la dirección IP del enrutador al que se está conectando." and "Nombre del host o dirección IP (como p.ej. microsoft.com, 157.54.0.1 o 3ffe:1234::1111):". A text input field contains "192.168.1.65". At the bottom are buttons for "< Atrás", "Siguiente >", and "Cancelar".

29. Marcar la opción *Enrutar paquetes a la interfaz IP* y *Agregar cuenta de usuario...*

The screenshot shows the same dialog box, but at the "Protocolos y Seguridad" step. It asks to "Seleccionar el transporte y las opciones de seguridad para esta conexión." and "Seleccione las opciones que correspondan:". There are four checkboxes: "Enrutar paquetes IP en esta interfaz." (checked), "Agregar una cuenta de usuario para que un enrutador remoto pueda conectarse" (checked), "Enviar una contraseña de texto sin formato si ésta es la única manera de conectar" (unchecked), and "Usar scripting para completar la conexión con el enrutador remoto" (unchecked). A link "Para obtener más información" is at the bottom left. Navigation buttons "< Atrás", "Siguiente >", and "Cancelar" are at the bottom right.

30. Agregar rutas estáticas, a la red remota

Asistente para interfaz de marcado a petición

Rutas estáticas para redes remotas
Una ruta estática es una ruta permanente entre dos redes definida manualmente.

Para activar esta conexión de marcado a petición, deberá agregar una ruta estática a la red. Especifique la dirección IP de las redes remotas con las que se comunicará esta red.

Rutas estáticas:

Destino	Máscara de red o longitud ...	Métrico
---------	-------------------------------	---------

31. Agregar la dirección IP, máscara y métrica de red de la red remota

Asistente para interfaz de marcado a petición

Ruta estática

☒ Compatibilidad con redes remotas que usan IPv4

Destino: 172 . 16 . 1 . 0
Máscara de red: 255 . 255 . 255 . 128
Métrica: 1

☐ Compatibilidad con redes remotas que usan IPv6

Destino:
Longitud del prefijo:
Métrica:

32. Clic en Siguiente

Asistente para interfaz de marcado a petición

Rutas estáticas para redes remotas
Una ruta estática es una ruta permanente entre dos redes definida manualmente.

Para activar esta conexión de marcado a petición, deberá agregar una ruta estática a la red. Especifique la dirección IP de las redes remotas con las que se comunicará esta red.

Rutas estáticas:

Destino	Máscara de red o longitud ...	Métrico
172.16.1.0	255.255.255.128	1

33. Escribir la contraseña del usuario que se creará localmente

Asistente para interfaz de marcado a petición

Credenciales de llamada entrante
Configure el nombre de usuario y la contraseña que el enrutador remoto usará al llamar a este servidor.

Tendrá que establecer las credenciales de marcado que usarán los enrutadores remotos al conectarse a esta interfaz. Se creará una cuenta de usuario en este enrutador con la información que escribió aquí.

Nombre de usuario:

Contraseña:

Confirmar contraseña:

34. Escribir el nombre y contraseña de usuario con el que se autenticara a servidor remoto

35. Clic en Finalizar

36. Buscar interfaz de red creada *tmg12*. Clic derecho. Clic en Propiedades

37. En pestaña Funciones de red, clic en Configuración IPsec

38. Marcar la opción *Usar clave previamente compartida...* y escribir la clave

39. Clic en Aceptar

40. Ir a Administrador del servidor > Usuarios y grupos locales. Crear un usuario *tmg21*

41. En Propiedades de usuario *tmg21*, Marcar la opción *Permitir Acceso* en Permiso de acceso a redes. Clic en Aceptar

11.4 Configuración de Controlador de Dominio Adicional

1. Configurar el direccionamiento IP adecuado para el equipo

2. Configurar el equipo a dominio. Clic derecho en Mi PC. Clic en Propiedades

3. Ir a pestaña Nombre de equipo

4. Clic en Cambiar

5. Marcar Dominio, escribir el nombre de dominio. Clic en Aceptar

6. Autenticarse con un usuario de dominio. Clic en Aceptar

7. Un mensaje nos confirma que estamos en el dominio. Clic en Aceptar

8. Clic en Aceptar para reiniciar y guardar los cambios

9. Después de reiniciar, clic en Inicio > Ejecutar y escribir dcpromo

10. El asistente de instalación de dominio. Clic en Siguiente

11. Compatibilidad del sistema operativo. Clic en Siguiente

12. Tipo de controlador de dominio. Aquí escogemos *Controlador de dominio adicional para un dominio existente*. Clic en Siguiente

13. Escribir el usuario de dominio con el que nos autenticaremos. Clic en Siguiente

The screenshot shows the 'Asistente para instalación de Active Directory' window. The title bar reads 'Asistente para instalación de Active Directory'. The main heading is 'Credenciales de red' with a subinstruction: 'Especifique un nombre de usuario de red y una contraseña.' Below this, a larger instruction states: 'Escriba el nombre de usuario, la contraseña y el dominio de usuario de una cuenta con suficientes privilegios para instalar Active Directory en este equipo.' There are three input fields: 'Usuario:' with a dropdown menu showing 'Administrador', 'Contraseña:' with masked characters (dots), and 'Dominio:' with the text 'megaline.com'. At the bottom right, there are three buttons: '< Atrás', 'Siguiente >', and 'Cancelar'. A mouse cursor is pointing at the 'Siguiente >' button.

14. Escribir el nombre completo de dominio. Clic en Siguiente

The screenshot shows the 'Asistente para instalación de Active Directory' window. The title bar reads 'Asistente para instalación de Active Directory'. The main heading is 'Controlador de dominio adicional' with a subinstruction: 'Especifique el nombre del dominio en el que este servidor será un controlador de dominio adicional.' Below this, a larger instruction states: 'Escriba el nombre DNS completo del dominio existente para el cual este servidor será un controlador de dominio adicional (por ejemplo, oficinacentral.ejemplo.microsoft.com).' There is a text field labeled 'Nombre de dominio:' containing the text 'megaline.com'. To the right of the text field is a button labeled 'Examinar...'. At the bottom right, there are three buttons: '< Atrás', 'Siguiente >', and 'Cancelar'. A mouse cursor is pointing at the 'Siguiente >' button.

15. Carpeta de base de datos y del registro. Clic en Siguiente

16. Volumen de sistema compartido. Clic en Siguiente

17. Escribir contraseña para restauración. Clic en Siguiente

Asistente para instalación de Active Directory

Contraseña de admin. del Modo de restauración de servicios de directorio
Esta contraseña se utiliza cuando inicie el equipo en el Modo de restauración de servicios de directorio.

Escriba y confirme la contraseña que desea asignar a la cuenta de Administrador que se utilizará cuando se inicie este servidor en el modo de restauración de servicios de directorio. La cuenta de administrador del modo de restauración es diferente de la cuenta de administrador del dominio. Las contraseñas de estas cuentas debe ser diferentes, asegúrese de recordar ambas.

Contraseña de modo remoto: [Masked Password]

Confirmar contraseña: [Masked Password]

Para obtener más información acerca del modo de restauración de servicios de directorio, vea la [Ayuda de Active Directory](#).

< Atrás Siguiente > Cancelar

18. Resumen de todo lo marcado en pasos anteriores. Clic en Siguiente

Asistente para instalación de Active Directory

Resumen
Revise y confirme las opciones seleccionadas.

Ha elegido:
Configurar este servidor como un controlador de dominio adicional para el dominio megaline.com.

Carpeta de la base de datos: C:\WINDOWS\NTDS
Carpeta del archivo de registro: C:\WINDOWS\NTDS
Carpeta de la carpeta SYSVOL: C:\WINDOWS\SYSVOL\

Para cambiar una opción, haga clic en Atrás. Para comenzar la operación, haga clic en Siguiente.

< Atrás Siguiente > Cancelar

19. Instalación

20. Finaliza la instalación. Clic en Finalizar.

21. Clic en 'Reiniciar Ahora' para guardar cambios

22. Al iniciar el sistema, autenticarse con usuario de dominio.

23. Ir a Inicio > Programas > Herramientas Administrativas > Usuarios y Equipos de Active Directory. Verificar que tenemos el dominio megaline.com.

11.5 Manual de Instalación de SQL Server

1. Tras ejecutarse el disco de instalación, la pantalla de inicio de SQL Server 2005 aparece

2. Clic en 'Componentes de servidor, herramientas, Libros en pantallas y ejemplos'

3. Marcar en 'Acepto términos y condiciones de la licencia'. Clic en Siguiente

4. Clic en Instalar para instalar los requisitos previos

5. Finalizada la instalación previa. Clic en Siguiente

6. Inicia el asistente de instalación. Clic en Siguiente

7. Tras comprobar la configuración, verificar que está instalado los servicios de IIS

NOTA: Si no está instalado IIS, instalar

8. Tras comprobar que si está instalado los servicios de IIS, clic en Siguiente

9. Ingresar nombre de la empresa, al igual que el número de serie. Clic en Siguiente

The screenshot shows the 'Programa de instalación de Microsoft SQL Server 2005' window. The title bar is blue with the Microsoft logo and the text 'Programa de instalación de Microsoft SQL Server 2005'. The main window has a light gray background. At the top, there's a section titled 'Información de registro' with a small icon of a server and a box. Below this, a message says: 'La siguiente información se utilizará para personalizar la instalación.' and 'Debe rellenar el campo Nombre para poder continuar. El campo Compañía es opcional.' There are two text input fields: 'Nombre:' with the value 'MEGALINE' and 'Compañía:' with the value 'MEGALINE'. Below these, a message says: 'Escriba la clave del producto de 25 caracteres que encontrará en la etiqueta amarilla en las notas o la funda del CD.' There is a product key field with the value 'WXGDG - DJ8DJ - CC77F - 8FDJV - DFBYG'. At the bottom, there are four buttons: 'Ayuda', '< Atrás', 'Siguiente >', and 'Cancelar'.

10. Clic en Avanzadas, para escoger más opciones de instalación

The screenshot shows the 'Programa de instalación de Microsoft SQL Server 2005' window. The title bar is blue with the Microsoft logo and the text 'Programa de instalación de Microsoft SQL Server 2005'. The main window has a light gray background. At the top, there's a section titled 'Cuenta de servicio' with a small icon of a server and a box. Below this, a message says: 'Las cuentas de servicio definen las cuentas con las que debe iniciarse sesión.' There is a checkbox labeled 'Personalizar para cada cuenta de servicio' which is unchecked. Below this, there is a 'Servicio:' dropdown menu. There are two radio buttons: 'Usar la cuenta del sistema integrada' (unchecked) and 'Usar una cuenta de usuario de dominio' (checked). The 'Usar una cuenta de usuario de dominio' option has three text input fields: 'Nombre de usuario:', 'Contraseña:', and 'Dominio:'. Below these, there is a section titled 'Iniciar los servicios cuando finalice la instalación' with four checkboxes: 'SQL Server' (checked), 'Agente SQL Server' (unchecked), 'Analysis Services' (checked), and 'Reporting Services' (checked). There is also an unchecked checkbox for 'Explorador de SQL'. At the bottom, there are four buttons: 'Ayuda', '< Atrás', 'Siguiente >', and 'Cancelar'.

11. Asegurar que todas las opciones están marcadas. Clic en Siguiente

12. Escoger un nombre de instancia, o escribir un nombre. Clic en Siguiente

13. Escoger el tipo usuario y marcar los servicios a iniciar al finalizar la instalación. Escoger 'Usar la cuenta del sistema integrada'. Clic en Siguiente.

Programa de instalación de Microsoft SQL Server 2005

Cuenta de servicio
Las cuentas de servicio definen las cuentas con las que debe iniciarse sesión.

☐ Personalizar para cada cuenta de servicio

Servicio:

☐ Usar la cuenta del sistema integrada Sistema local

☒ Usar una cuenta de usuario de dominio

Nombre de usuario:

Contraseña:

Dominio:

Iniciar los servicios cuando finalice la instalación

☒ SQL Server ☒ Reporting Services

☐ Agente SQL Server ☐ Explorador de SQL

☒ Analysis Services

Ayuda < Atrás Siguiente > Cancelar

14. Elegir el modo de autenticación, Windows o de SQL.

Programa de instalación de Microsoft SQL Server 2005

Modo de autenticación
El modo de autenticación especifica la seguridad utilizada para la conexión con SQL Server.

Seleccione el modo de autenticación que se utilizará para la instalación.

☒ Modo de autenticación de Windows

☐ Modo mixto (autenticación de Windows y autenticación de SQL Server)

Especifique a continuación la contraseña de inicio de sesión de sa:

Escribir contraseña:

Confirmar contraseña:

Ayuda < Atrás Siguiente > Cancelar

15. Configuración de intercalación. Clic en Siguiente

16. Opciones de instalación de servidor de informes. Clic en Siguiente

17. Configuración de informes de errores y uso. Clic en Siguiente

18. Verificar todo lo que se instalará. Clic en Instalar

19. La instalación continúa

20. Tras terminar la instalación, clic en Siguiente

21. Para finalizar la instalación, clic en Finalizar

22. Inicio >Ejecutar> SQL Server 2005 > SQL Management Studio y autenticarse con el usuario local. Clic en Conectar

23. Veremos la interfaz de SQL Server Management Studio. Aquí finaliza la instalación.

11.6 Configuración de Replicación de Base de Datos

Agentes en el proceso de replicación de base de datos:

- **DISTRIBUIDOR:** Agente que maneja todo los tramites de replicación
- **PUBLICADOR:** Agente quien ofrece su base de datos para transmitir o publicarla.
También se encarga de crear el artículo a replicar
- **SUSCRIPTORES:** Agentes quienes reciben los datos en la base de datos secundaria.

1. Configurar el direccionamiento IP adecuado para el servidor SRV-DB

2. Configurar el direccionamiento IP adecuado para el servidor SRV-DB2

EN PUBLICADOR (SRV-DB)

3. Ir a *Inicio > Programas > SQL Server 2005 > SQL Server Manager*

4. Ir a *Configuración de red de SQL Server 2005 > Protocolos de MSSQLServer*

5. Doble clic en *TCP/IP*

6. Pestaña *Protocolo*, verificar que *Habilitado* = *Si*

7. Pestaña *Direcciones IP*, verificar que la dirección IP del servidor sea la correcta. También verificar que *Habilitado* = *Si*

8. Mensaje que indica que debemos detener e iniciar el servicio

9. Doble clic en *Canalizaciones con Nombre*

10. Pestaña *Protocolo*, verificar que *Habilitado* = Si

11. Mensaje que indica que debemos detener e iniciar el servicio

12. Clic en *Servicios de SQL Server 2005*

13. Clic derecho sobre *SQL Server (MSSQLSERVER)*. Clic en *Detener*

14. Deteniendo Servicio

15. Clic derecho sobre *SQL Server (MSSQLSERVER)*. Clic en *Iniciar*

16. Iniciando Servicio

EN SUSCRIPTOR (SRV-DB2)

17. Ir a *SQL Server Manager > Configuración de red de SQL Server 2005 > Protocolos de MSSQLServer*

18. Doble clic en TCP/IP. Habilitar TCP/IP. Verificar el direccionamiento IP. (Ver pasos 5, 6 y 7)

19. Doble clic en *Canalizaciones con Nombre*. *Habilitar*. (Ver pasos 9 y 10)

20. Detener y reiniciar el servicio *SQL Server (MSSQLSERVER)* (Ver pasos 13, 14, 15, y 16)

EN AMBOS SERVIDORES SRV-DB y SRV-DB2

21. Ir a SQL Server Manager > Servicios de SQL Server

22. Clic Derecho sobre SQL Server Agent. Clic en Iniciar

23. Iniciando el servicio

CONFIGURAR DISTRIBUCIÓN EN SRV-DB

24. Crear una carpeta

25. En Propiedades de carpeta > Compartir > Habilitar los permisos de lectura y escritura

26. Comprobar que podemos acceder a carpeta creada vía la dirección IP.

27. Ir a Inicio > Programas > Microsoft SQL Server 2005 > SQL Server Management Studio

28. Autenticarse con las credenciales apropiadas. Clic en Conectar

29. En ventana *Explorador de objetos*, ir a carpeta *Replica*

30. Clic derecho. Clic en *Configurar distribución*

31. Asistente para configurar la distribución. Clic en Siguiente

32. Verificamos la opción marcada: '*SRV-DB actuara como su propio distribuidor*'. Clic en Siguiente

33. Inicio de Agente SQL Server. Marcar la opción '*Si, configurar el servicio del Agente SQL Server para que se inicie automáticamente*'. Clic en Siguiente

34. Carpeta de instantáneas. Escribir la ruta de la carpeta compartida (Ver pasos 24, 25 y 26). Clic en Siguiente

35. Base de datos de la distribución. Clic en Siguiente

Asistente para configurar la distribución

Base de datos de distribución
Seleccione el nombre y la ubicación de la base de datos de distribución y de los archivos de registro.

La base de datos de distribución almacena los cambios de las publicaciones transaccionales hasta que se pueden actualizar los suscriptores. También almacena información histórica de las publicaciones de mezcla y de instantáneas.

Nombre de base de datos de distribución:

Carpeta para el archivo de la base de datos de distribución:

Carpeta para el archivo de registro de la base de datos de distribución:

Las rutas de acceso deben hacer referencia a discos locales del distribuidor y deben comenzar con una letra de unidad local seguida de dos puntos (por ejemplo, C:). Las letras de unidades asignadas y las rutas de acceso de red no son válidas.

36. Publicadores. Marcar *SRV-DB*. Clic en Siguiente

Asistente para configurar la distribución

Publicadores
Habilite los servidores para que usen este distribuidor cuando se conviertan en publicadores.

Publicadores:

Publicador	Base de datos de distribución
☒ SRV-DB	distribución

37. Acciones del asistente. Marcar *Configurar distribución*. Clic en Siguiente

38. Finalización del asistente. Clic en Finalizar

39. Al terminar, las tres acciones deben salir *Correcto*

CREANDO PUBLICACIÓN EN SRV-DB

40. En *SQL Server Management Studio*, ubicar cual es la base de datos de la cual se publicará los datos

En ventana *Explorador de objetos*, carpeta *Replica*, subcarpeta *Publicaciones Locales*.

41. Clic derecho. Clic en *Nueva Publicación*

42. Asistente para nueva publicación. Clic en Siguiente

43. Base de datos de publicaciones. Elegir la base de datos a publicar. Clic en Siguiente

44. Tipo de publicación. Escoger el tipo de publicación: *publicación transaccional*. Clic en Siguiente

45. Artículos. Escoger las tablas que deseamos replicar

46. Filtro de filas de tabla. Clic en Siguiente

47. Agente de instantáneas. Marcar la opción “*Crear una instantánea inmediatamente y mantenerla disponible para inicializar la suscripción*”. Clic en Siguiente.

48. Seguridad de agente. Clic en *Configuración de seguridad*

49. Marcar *Ejecutar la siguiente cuenta de Windows*. Escribir el usuario y contraseña de Administrador. Marcar *Mediante la suplantación de la cuenta de proceso*

50. Seguridad de agente. Clic en Siguiente

51. Acciones de Asistente. Marcar *Crear publicación*. Clic en Siguiente

52. Finalización del Asistente. Escribir nombre de publicación. Clic en Finalizar

53. Al terminar, las tres acciones deben salir *Correcto*

CREANDO LA SUSCRIPCION

EN EL SUSCRIPTOR:

54. Crear la base de datos en la cual se replicara los datos

55. Ventana *Explorador de objetos*, carpeta *Replica*, subcarpeta *Suscripciones Locales*.

56. Asistente para nueva configuración. Clic derecho, *Nuevas suscripciones*

57. Publicación. Clic en pestaña Publicación y clic en <Buscar publicación de SQL Server>

58. Autenticarse con las credenciales donde está el servidor de base de datos publicador

59. Publicación. En pestaña Base de datos, escoger la publicación creada en SRV-DB. Clic en Siguiente

60. Ubicación del Agente de distribución. Marcar *Ejecutar cada agente en su suscriptor*. Clic en Siguiente

61. Suscriptores. En pestaña, escoger la base de datos a la cual se replicara los datos. Clic en Siguiente

62. Seguridad del Agente de distribución. Clic en botón....

63. Marcar *Ejecutar la siguiente cuenta de Windows*. Escribir el usuario y contraseña de Administrador. Marcar *Mediante la suplantación de la cuenta de proceso*

64. Seguridad del Agente de distribución. Clic en Siguiente

65. Programación de sincronización. Escoger en la pestaña *Elegir Ejecutar continuamente*.

66. Inicializar suscripciones. Escoger en la pestaña *Inmediatamente*

67. Acciones de Asistente. Marcar *Crear las suscripciones*. Clic en Siguiete

68. Finalización del Asistente. Clic en Finalizar

69. Al terminar, la acción debe salir *Correcto*

COMPROBAR REPLICACION EN SRV-DB2

70. En ventana *Explorador de objetos*, en base de datos MEGALINEBAK, carpeta *Tabla*, verificar que las tablas Clientes y Vendedor han replicado.

The screenshot shows the Microsoft SQL Server Management Studio interface. The left pane displays the 'Explorador de objetos' (Object Explorer) for the 'SRV-DB2 (SQL Server 9.0.1399 - SRV-DB2\Adri)' server. The 'Bases de datos' (Databases) folder is expanded, showing 'MEGALINEBAK'. Under 'MEGALINEBAK', the 'Tablas' (Tables) folder is expanded, showing 'dbo.Clientes' and 'dbo.Vendedor'. The right pane shows a query window with the following SQL code:

```
create database MEGALINEBAK

select * from Clientes
```

The 'Resultados' (Results) tab is active, displaying a table with 10 rows and 7 columns. The columns are: 'Cli_codigo', 'Cli_nombre', 'Cli_telefono', 'cli_ruc', 'cli_direccion', and 'Estado'. The data is as follows:

	Cli_codigo	Cli_nombre	Cli_telefono	cli_ruc	cli_direccion	Estado
1	C0001	Laura Moreno Lee	1234567	10085931801	Av. La Marina 1234	1
2	C0002	Alejandro Moreno	6584503	10085931801	Av. Pardo 456	1
3	C0003	Claudia Lee	1237833	10085931801	Av. Principal 123	1
4	C0004	Castañeda Blas	7862542	10085931801	Av. Jose 456	1
5	C0005	Percy Obando	4523872	10085931801	Av. Enrique 456	1
6	C0006	Martin Aparicio	6584503	10085931801	Av. Colonial 456	1
7	C0007	Miguel Narva	6584503	10085931801	Av. Eduardo 456	1
8	C0008	Claudio Pardo	6584503	10085931801	Av. Coronel 456	1
9	C0009	Monica Gonzales	6584503	10085931801	Av. Brazil 456	1
10	C0010	Enrique LLagaz	6584503	10085931801	Av. Eduardo 456	1

The status bar at the bottom indicates 'Consulta ejecutada correctamente.' (Query executed successfully).

11.7 Configuración Forefront TMG: Regla VPN Acceso Remoto

A continuación se muestran los pasos para configurar la regla de acceso remoto en el servidor SRV-TMG1. Para información más detallada, revisar los manuales previos.

1. Asistente para nueva regla de acceso. Escribir nombre de regla. Clic en Siguiente

2. Acción de regla. Marcar Permitir

3. Protocolos. Seleccionar *Todo el tráfico saliente*

4. Marcar la opción *No habilitar la inspección de malware para esta regla*

5. Orígenes de regla de acceso. Agregar *Cientes VPN*

6. Destinos de regla de acceso. Agregar *Interna*

7. Conjunto de usuarios. Todos los usuarios

8. Clic en Finalizar

9. Verificar que la regla está creada. Clic en *Aplicar*, para guardar los cambios

10. Guardar los cambios. Clic en Aceptar

11.8 Configuración Forefront TMG: Regla Acceso Internet

1. Asistente para nueva regla de acceso. Escribir nombre de regla. Clic en Siguiente

Asistente para nueva regla de acceso

Éste es el Asistente para nueva regla de acceso

Este asistente le ayudará a crear una nueva regla de acceso. Las reglas de acceso definen las acciones realizadas y los protocolos usados cuando los clientes especificados de una red intentan tener acceso a destinos o contenido específico en otra red.

Nombre de la regla de acceso:

Permitir Internet

Haga clic en Siguiente para continuar:

< Atrás Siguiente > Cancelar

2. Acción de regla. Marcar Permitir

Asistente para nueva regla de acceso

Acción de la regla

Seleccione la forma en que se tratan las solicitudes de cliente para contenido del destino especificado, si se cumplen las condiciones especificadas en la regla.

Acción por realizar cuando se cumplen las condiciones de la regla:

☒ Permitir

☐ Denegar

< Atrás Siguiente > Cancelar

3. Protocolos. Seleccionar *DNS*, *HTTP*, *HTTPS*

4. Verificar protocolos. Clic en Siguiente

5. Marcar la opción No habilitar la inspección de malware para esta regla

6. Orígenes de regla de acceso. Agregar *Interna*

7. Verificar origen de acceso. Clic en Siguiente

8. Destinos de regla de acceso. Agregar *Externa*

9. Conjunto de usuarios. Todos los usuarios

10. Clic en Finalizar

11. Verificar que la regla está creada. Clic en *Aplicar*, para guardar los cambios

12. Clic en Aceptar. Los cambios se guardaron.

11.9 Configuración Forefront TMG: Regla Internet Restringido

1. Asistente para nueva regla de acceso. Escribir nombre de regla. Clic en Siguiente

Asistente para nueva regla de acceso

Éste es el Asistente para nueva regla de acceso

Este asistente le ayudará a crear una nueva regla de acceso. Las reglas de acceso definen las acciones realizadas y los protocolos usados cuando los clientes especificados de una red intentan tener acceso a destinos o contenido específico en otra red.

Nombre de la regla de acceso:

Permitir Internet Restringido

Haga clic en Siguiente para continuar.

< Atrás Siguiente > Cancelar

2. Acción de regla. Marcar Permitir

Asistente para nueva regla de acceso

Acción de la regla

Seleccione la forma en que se tratan las solicitudes de cliente para contenido del destino especificado, si se cumplen las condiciones especificadas en la regla.

Acción por realizar cuando se cumplen las condiciones de la regla:

☒ Permitir

☐ Denegar

< Atrás Siguiente > Cancelar

3. Protocolos. Seleccionar *DNS*, *HTTP*, *HTTPS*

4. Verificar protocolos. Clic en Siguiente

5. Marcar la opción No habilitar la inspección de malware para esta regla

6. Orígenes de regla de acceso. Agregar *Interna*

7. Verificar origen de acceso. Clic en Siguiente

8. Destinos de regla de acceso. Clic en Agregar. Escogeremos *Conjuntos de Direcciones de URL*. Clic en Nuevo

9. *Nuevo elemento de directiva.* Escribiremos un nombre y agregaremos las direcciones web a las cuales se permitirán el acceso. Clic en Aceptar.

10. Agregar el nuevo elemento

11. Conjunto de usuarios. Aquí se pueden especificar los usuarios que se les desea aplicar la regla. Para efectos de prueba, agregar todos los usuarios.

12. Clic en Finalizar

13. Clic en Aceptar. Los cambios se guardaron.

11.10 Manual de Configuración Proxy en PC

1. Abrir Internet Explorer

2. Herramientas > Opciones de Internet

3. Pestaña *Conexiones*, clic en Configuración de LAN

4. Marcar la opción *Utilizar un servidor proxy para su LAN*. Escribir la dirección IP y el puerto del servidor firewall

5. Ir a www.google.com.pe. La página resolverá exitosamente