UNIVERSIDAD NACIONAL DEL ALTIPLANO

FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA, ELECTRÓNICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

DISEÑO E IMPLEMENTACIÓN DE RED PRIVADA VIRTUAL IPSEC PARA LA COMUNICACIÓN DE SUCURSALES DE CAJA RURAL DE AHORRO Y CRÉDITO LOS ANDES SA, PUNO – 2019.

TESIS

PRESENTADA POR:

Bach. WILMER ALVARO MAMANI QUISPE

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

PUNO – PERÚ

2022

DEDICATORIA

A mis padres, en especial a mi madre Sabina por su apoyo incondicional, sin ella no hubiera logrado realizar el presente proyecto, a mis hermanas y hermano, Vilma, Roxana y Clodomiro por el apoyo brindado durante mi etapa como estudiante y también en la realización de la presente tesis.

Wilmer Álvaro.

AGRADECIMIENTO

A la Universidad Nacional del Altiplano, por darme la oportunidad de desarrollarme como profesional, especialmente a la Escuela profesional de Ingeniería de Sistemas, así como a todos sus académicos, compañeros de grado y amigos, quienes me acompañaron durante mi etapa de estudiante brindando sus conocimientos y apoyo.

A los miembros del jurado, (M.Sc.) William Eusebio Arcaya Coaquira, (D.Sc.) Fidel Ernesto Ticona Yanqui y (M.Sc.) Cristian Augusto Romero Goyzueta, por sus sugerencias y correcciones para mejorar el proyecto; así también mi especial agradecimiento a mi asesor (Mg.) Robert Antonio Romero Flores, por el apoyo y la exigencia para lograr el objetivo de concluir la tesis.

A mis compañeros y amigos de trabajo de la Caja Rural de Ahorro y Crédito los Andes SA, Sub-Gerencia de Tecnologías de Información, quienes me brindaron su apoyo, tiempo y paciencia durante el desarrollo del presente proyecto de tesis.

INDICE GENERAL

DEDICATORIA

AGRADECIMIENTO

INDICE GENERAL

INDICE DE TABLAS

INDICE DE FIGURAS

ÍNDICE DE ACRÓNIMOS

RESUMEN **14**

ABSTRACT **15**

CAPITULO I

INTRODUCCIÓN

1.1. PLANTEAMIENTO DEL PROBLEMA **17**

1.2. FORMULACIÓN DEL PROBLEMA **18**

1.2.1. Problema General 18

1.2.2. Problemas Específicos 18

1.3. JUSTIFICACIÓN **18**

1.4. OBJETIVOS DE LA INVESTIGACIÓN **20**

1.4.1. Objetivo General 20

1.4.2. Objetivos Específicos 20

1.5. HIPÓTESIS DE LA INVESTIGACIÓN **20**

1.5.1. Hipótesis General 20

1.5.2. Hipótesis Especifico 21

CAPITULO II

REVISIÓN DE LITERATURA

2.1. ANTECEDENTES DE INVESTIGACIÓN **22**

2.1.1. Internacionales 22

2.1.2. Nacional 23

2.1.3. Local 23

2.2. SUSTENTO TEÓRICO 25

2.2.1. Red De Área Local (LAN)..... 25

2.2.1.1. Topologías de LAN. 26

2.2.1.1.1. Estrella. 26

2.2.1.1.2. Estrella Extendida. 26

2.2.1.1.3. Anillo. 27

2.2.1.1.4. Malla. 27

2.2.1.1.5. Bus. 27

2.2.2. Red De Área Amplia (Wan) 28

2.2.2.1. Tipos de conexiones WAN 29

2.2.3. Diagramas De Topologías De Red 30

2.2.3.1. Topología Física. 30

2.2.3.2. Topología Lógica. 30

2.2.4. Red Privada Virtual (VPN)..... 31

2.2.4.1. Funcionamiento de una VPN. 32

2.2.4.2. Utilidad de la VPN. 33

2.2.4.3. Ventajas y Desventajas de una VPN. 34

2.2.5. Tipos De VPN..... 34

2.2.5.1. Acceso Remoto. 34

2.2.5.2. Sitio a Sitio..... 35

2.2.6. Protocolos De VPN..... 35

2.2.6.1. IPSec. 35

2.2.6.2. L2TP. 36

2.2.6.3. PPTP. 36

2.2.6.4. VPN SSL..... 37

2.2.7. IPSec 37
2.2.7.1. Funciones Esenciales de Seguridad. 38
2.2.7.1.1. Confidencialidad. 38
2.2.7.1.2. Integridad. 39
2.2.7.1.3. Autenticación. 40
2.2.7.2. Intercambio seguro de claves 41
2.2.7.3. Protocolos de seguridad IPSEC. 42
2.2.7.3.1. Authentication Header (AH). 42
2.2.7.3.2. ESP. 43
2.2.7.3.3. Modo transporte. 45
2.2.7.3.4. Modo túnel. 45
2.2.7.4. Intercambios de claves en Internet (IKE). 46
2.2.7.4.1. Asociaciones de seguridad (SA). 46
2.2.8. Cisco IOS 51
2.2.8.1. Ubicación de IOS. 52
2.2.8.2. Funciones de IOS. 53
2.2.8.3. Método de acceso a la consola. 53
2.2.8.3.1. Consola. 53
2.2.8.3.2. Telnet. 54
2.2.8.3.3. SSH. 54
2.2.8.3.4. Puerto Auxiliary. 54
2.2.8.4. Modos de funcionamiento de Cisco IOS. 54
2.2.9. Modelo OSI 55
2.2.10. Modelo TCP/IP 56
2.2.11. Comparación entre modelo OSI y TCP/IP 57
2.3. DEFINICIÓN DE TÉRMINOS BÁSICOS 58
2.3.1. VPN 58

2.3.2. IPSec 59
2.3.3. Modo tunnel 59
2.3.4. Intercambios de claves en Internet (IKE) 59
2.3.5. Asociaciones de seguridad (SA) 59

CAPITULO III

MATERIALES Y MÉTODOS

3.1. TIPO Y DISEÑO DE INVESTIGACIÓN 60
3.1.1. Tipo De Investigación 60
3.1.2. Diseño De Investigación 60
3.2. POBLACIÓN Y MUESTRA DE INVESTIGACIÓN 61
3.2.1. Población 61
3.2.2. Muestra 61
3.2.3. Ubicación De La Población 62
3.3. MATERIAL EXPERIMENTAL 63
3.3.1. Hardware 63
3.3.2. Software 69
3.3.3. Recursos Y Materiales 70
3.3.4. Servicios 70
3.3.5. Presupuesto 71

CAPITULO IV

RESULTADOS Y DISCUSIÓN

4.1. ANÁLISIS DE LA SITUACIÓN ACTUAL 72
4.1.1. Análisis de Costo de Instalación Proveedor 72
4.1.2. Análisis de Tiempo de Instalación Proveedor 73
4.2. PROCESO DE DISEÑO E IMPLEMENTACIÓN 74
4.2.1. Diseño de Topología Física 74
4.2.2. Diseño de Topología Lógica. 75

4.2.3. Asignación de Direccionamiento IP 76
4.2.4. Proceso De Instalación Y Configuración..... 77
4.2.4.1. Instalación. 77
4.2.4.2. Configuración. 79
4.2.5. Verificación de la conectividad 82
4.3. ANÁLISIS DEL PROCESO DE IMPLEMENTACIÓN. 89
4.3.1. Tiempo de Instalación. 89
4.3.2. Costo de implementación. 90
4.3.3. Análisis de la conectividad VPN. 90
4.4. RESULTADOS DEL INSTRUMENTO DE INVESTIGACIÓN..... 96
4.5. CONTRASTE DE LA HIPÓTESIS 96
4.5.1. Contraste de Hipótesis Tiempo 96
4.5.2. Contraste de Hipótesis Costo 98
4.6. DISCUSIÓN 101
V. CONCLUSIONES..... 102
VI. RECOMENDACIONES 104
VII. REFERENCIAS BIBLIOGRAFICAS..... 105
ANEXOS 109

ÁREA : REDES Y TELEMATICA

TEMA : Red Privada Virtual

FECHA DE SUSTENTACION: 05 de Agosto del 2022

INDICE DE TABLAS

Tabla 1: Presupuesto utilizado para la implementación. 71

Tabla 2: Costo instalación y servicio Proveedor. 72

Tabla 3: Tiempo Instalación Proveedor. 73

Tabla 4: Direccionamiento de IP. 76

Tabla 5: Descripción de configuración sede principal. 79

Tabla 6: Descripción de configuración sede remota. 80

Tabla 7: Actividades de Implementación Sede Principal. 89

Tabla 8: Actividades de Implementación Sucursal Acora, Coata y Taraco. 89

Tabla 9: Actividades de Implementación Sucursal Yunguyo. 89

Tabla 10: Costo Implementación por entidad. 90

Tabla 11: Descripción de sh crypto isakmp sa. 91

Tabla 12: Costo promedio de instalación y servicio. 96

Tabla 13: Tiempo proveedor y entidad de instalación. 97

Tabla 14: Prueba t para tiempo de instalacion. 97

Tabla 15: Costo proveedor y entidad de instalación. 99

Tabla 16: Prueba t para costos de instalación. 100

INDICE DE FIGURAS

Figura 1: Red de Área Local (LAN). 26

Figura 2: Topologías Físicas. 28

Figura 3: Red de Área Amplia (WAN). 29

Figura 4: Topología Física. 30

Figura 5: Topología Lógica. 30

Figura 6: Red Privada Virtual (VPN). 32

Figura 7: Red Privada Virtual IPSec. 33

Figura 8: Estructura IPSec. 38

Figura 9: Confidencialidad IPSec. 39

Figura 10: Integridad IPSec. 40

Figura 11: Autenticación IPSec. 41

Figura 12: Intercambio Seguro de Claves. 42

Figura 13: Authentication Header. 43

Figura 14: ESP. 44

Figura 15: Modo Transporte. 44

Figura 16: Modo Túnel. 46

Figura 17: Asociaciones de seguridad (SA). 47

Figura 18: Fase 1 de IKE. 48

Figura 19: Intercambio 1 de IKE. 48

Figura 20: Intercambio 2 de IKE. 49

Figura 21: Intercambio 3 de IKE. 50

Figura 22: Intercambio 1 de DH. 51

Figura 23: Sistema Operativo Cisco IOS. 52

Figura 24: Estructura IOS. 55

Figura 25: Modelo OSI. 56

Figura 26: Modelo TCP/IP. 57

Figura 27: Modelo OSI vs TCP/IP. 58

Figura 28: Ubicación de las sucursales. 63

Figura 29: Cisco 800 Series. 65

Figura 30: Router TP-LINK 3420. 66

Figura 31: Características de Laptop. 68

Figura 32: Diseño de Topología Física. 74

Figura 33: Diseño de Topología Lógica. 75

Figura 34: Instalación Sucursal Acora. 77

Figura 35: Instalación Sucursal Coata. 77

Figura 36: Instalación Sucursal Taraco. 78

Figura 37: Instalación Sucursal Yunguyo. 78

Figura 38: Ping extendido desde router Acora hasta router Cabecera. 82

Figura 39: Ping desde el servidor hasta la Pc de la sede Acora. 83

Figura 40: Tracert desde el servidor hasta la PC de la sede Acora 83

Figura 41: Ping extendido desde Router Coata hasta Router cabecera. 84

Figura 42: Ping desde servidor hasta PC de Coata. 84

Figura 43: Tracert desde servidor hasta PC de Coata. 85

Figura 44: Ping desde Router Taraco hasta Router Cabecera. 85

Figura 45: Ping desde Servidor hasta PC Taraco. 86

Figura 46: Tracert desde Servidor hasta PC Taraco. 86

Figura 47: Ping extendido desde Router Yunguyo hasta Router Cabecera. 87

Figura 48: Ping desde Servidor hasta Pc de Yunguyo. 87

Figura 49: Tracert desde Servidor hasta PC Yunguyo. 88

Figura 50: Asociaciones de Seguridad Activas. 88

Figura 51: IPSec SA creada en router de cabecera sucursal Acora. 92

Figura 52: IPSec SA creada en router de cabecera sucursal Coata. 93

Figura 53: IPSec SA creada en router de cabecera sucursal Taraco. 94

Figura 54: IPSec SA creada en router de cabecera sucursal Yunguyo. 95

Figura 55: Distribución T-student tiempo de instalación. 98

Figura 56: Distribución T-student costos de servicio. 100

ÍNDICE DE ACRÓNIMOS

CISCO IOS : Sistema Operativo de Cisco.

DH : Diffie Hellman

ESP : (Encapsulating Security Payload) Carga útil de seguridad encapsulada.

FIREWALL : Los firewalls son programas de software o dispositivos de hardware que filtran y examinan la información que viene a través de su conexión a Internet.

IKE : (Internet key Exchange) Intercambio de claves de Internet.

IP : (Internet Protocol) protocolo de Internet.

IPSec : (Internet Protocol Security) Seguridad del protocolo de Internet.

ISAKMP : Es un protocolo criptográfico que constituye la base del protocolo de intercambio de claves.

LAN : (Local Area Network) Red de área local.

MD5 : Es un algoritmo de reducción criptográfico de 128-bits

NAT : (Network Address Translation) Traducción de Direcciones de Red.

PKI : (Public Key Infrastructure) Infraestructura de clave pública.

PPTP : (Point to Point) Punto a punto.

PSK : (pre-shared key) Clave precompartida.

QoS : (Quality of Service) Calidad de servicio.

SHA : (Secure Hash Algorithm, Algoritmo de Hash Seguro) Es una familia de funciones hash de cifrado

Tunel : Es una técnica que permite a los usuarios de acceso remoto para conectarse a una variedad de recursos de red a través de una red pública de datos.

VPN : (Virtual Private Network) Red Privada Virtual.

WAN : (Wide Area Network) Red de Área Amplia.

RESUMEN

El presente trabajo de investigación tiene lugar en la Caja Rural de Ahorro y Crédito los Andes SA, el cual pretende dar solución a un problema específico que se tiene al momento de requerir una conexión de Red Priva Virtual en sus sucursales en tiempos cortos y costos razonables, ya que un proveedor de este tipo servicio puede o no tener factibilidad para brindarlo donde la empresa lo requiera, es por ello que se tiene como objetivo general diseñar e implementar un Red Privada Virtual IPSec con IP Dinámica en Routers Cisco que permita la comunicación de las sucursales remotas con la sede principal en un menor tiempo y costo en comparación a un proveedor externo del servicio de Red Privada Virtual, para la cual se utiliza la investigación tipo aplicada y el diseño de método cuasi-experimental que permite abordar de mejor manera ya que la implementación se realizara en equipos reales y sucursales seleccionas a conveniencia, y también permiten realizar pruebas de diseño e implementación propuestas pre y post, al finalizar el proyecto se obtuvo como resultado que el diseño e implementación de una Red Privada Virtual IPSec con IP dinámica permite reducir los tiempos del promedio tomada de muestras en 41 días por cada sucursal y respecto al costo la disminución es de s/ 3,868.89 mensuales por las 4 sucursales, por lo cual se concluye que el presente proyecto disminuye los tiempos y costos de instalación para la red de comunicación de las sucursales con la sede principal de la Caja Rural de Ahorro y Crédito los Andes SA 2019.

Palabras Clave: VPN, IPSec, IP Dinámica y Routers Cisco.

ABSTRACT

The present research work takes place in the Caja Rural de Ahorro y Crédito los Andes SA, which aims to solve a specific problem that occurs when requiring a Virtual Private Network connection in its branches in short times and reasonable costs. , since a provider of this type of service may or may not have the feasibility to provide it where the company requires it, that is why the general objective is to design and implement an IPSec Virtual Private Network with Dynamic IP in Cisco Routers that allows the communication of remote branches with the main headquarters in a lower time and cost compared to an external provider of the Virtual Private Network service, for which applied type research and the design of a quasi-experimental method are used that allow to better address already that the implementation be carried out in real equipment and selected branches at convenience, and also allow design and implementation tests pre and post proposals, at the end of the project it was obtained as a result that the design and implementation of an IPSec Virtual Private Network with dynamic IP allows to reduce the times of the average taken of samples in 41 days for each branch and regarding the cost the decrease is of s/ 3,868.89 per month for the 4 branches, for which it is concluded that this project reduces the installation times and costs for the communication network of the branches with the main headquarters of the Caja Rural de Ahorro y Crédito los Andes SA 2019.

Keywords: VPN, IPSec, Dynamic IP y Routers Cisco.

CAPITULO I

INTRODUCCIÓN

La red de comunicación de una institución dedicada al sistema financiero es de vital importancia, ya que es la base para la administración de sus operaciones bancarias, por ello se debe contar con una conexión de Red Privada Virtual entre las sucursales remotas y la sede principal, por ello la entidad financiera Caja Rural de Ahorro y Crédito Los Andes SA que se dedica a las micro finanzas orientada al área rural tiene como uno de sus objetivos la expansión territorial a nivel nacional, en especial a las zonas rurales, para ofrecer sus productos y/o servicios en las distintas regiones del país, por este motivo la entidad realiza las instalación de sus sucursales de atención al público general en los pueblos o ciudades más cercanas a las zonas rurales, estas sucursales requieren contar con una conexión de Red Privada Virtual para realizar sus transacciones mediante su CORE (aplicación de intercambio en tiempo real centralizado) Financiero, y para ello la entidad contrata una Red Privada Virtual del proveedor Claro Empresas, el proveedor realiza la instalación del servicio solicitado cumpliendo una serie actividades y procedimientos donde se contemplan los plazos y costos de instalación, siendo estos plazos dependientes de la factibilidad técnica y permisos de instalación como el tendido de cable de fibra óptica o de obtener permisos para la instalación de una antena microondas en las sucursales de la entidad, también se consideran montos elevados para las instalaciones; siendo los plazos de instalación el principal problema para contar con un servicio Red Privada Virtual en las sucursales, es por ello que se plantea la presente investigación de “Diseño e Implementación de una VPN IPSec con IP dinámica con routers cisco”, la cual tiene como principal objetivo disminuir el tiempo y costo de instalación de una Red Privada Virtual entre las sedes remotas y la sede principal de Caja Rural de Ahorro y Credito los Andes SA SA, para ello se contemplaran como objetivos

específicos el análisis del servicio contratado, el diseño, la implementación, la verificación y finalmente el análisis de la disminución del tiempo y costo.

1.1. PLANTEAMIENTO DEL PROBLEMA

La entidad Caja Rural de Ahorro y Crédito los Andes SA, se encuentra en un proceso de expansión en la instalación de sucursales en las distintas regiones del país, estas sucursales requieren contar con un servicio de Red Privada Virtual para realizar operaciones y/o transacciones en tiempo real, sin embargo la instalación de este servicio de Red Privada Virtual por el proveedor contratado presenta un problema en cuanto al tiempo que requiere para su instalación completa, así también la contratación del servicio tiene un costo de instalación de pago único, así como el costo de mensual por el servicio brindado; de lo descrito, el tiempo que requiere el proveedor para la instalación de la Red Privada Virtual es un problema para la entidad, porque en ocasiones se quiere contar con el servicio en plazos menores a los dispuestos por el proveedor, y para ello se plantea el "Diseño e Implementación de Red Privada virtual IPSec para la comunicación de las sucursales de la Caja Rural de Ahorro y crédito los Andes SA", Utilizando Internet Móvil y proveedores de servicio de internet (ISP) que cuenta con factibilidad de instalación en la sucursales requeridas, ya que estas ofrecen el servicio básico de acceso a internet y también el plazo de instalación es de un máximo de 7 días.

La implementación de la Red Privada Virtual propuesta resolverá el problema que tiene la entidad para disponer con una conexión entre las sucursales remotas con la sede principal en menor tiempo y costo comparado a proveedor.

1.2. FORMULACIÓN DEL PROBLEMA

1.2.1. Problema General

¿Cómo y en qué medida el diseño e implementación de una VPN IPSec con IP Dinámica con Routers Cisco permite disminuir el tiempo y costo en la red de comunicación de las sucursales de Caja Rural de Ahorro y Crédito los Andes SA?

1.2.2. Problemas Específicos

- ¿A qué se debe el tiempo y costo de servicio tan elevados para la instalación de la red privada virtual en las sucursales por parte del proveedor de la Caja Rural de Ahorro y crédito los Andes SA?
- ¿Como el diseño de la topología física y lógica de una VPN IPSec con IP Dinámica con Router Cisco permite disminuir el tiempo y costo en las sucursales de la Caja Rural de Ahorro y crédito los Andes SA?
- ¿Por qué la implementación de una Red Privada Virtual IPSec con IP Dinámica con Routers Cisco permitirá conectividad entre las sucursales de la Caja Rural de Ahorro y Crédito los Andes SA?
- ¿Cuál es el impacto de la implementación de una VPN IPSec con IP dinámica con routers cisco en el tiempo y costo de instalación en la red de comunicación de las sucursales de Caja Rural de Ahorro y crédito los Andes SA?

1.3. JUSTIFICACIÓN

La entidad financiera Caja Rural de Ahorro y Crédito los Andes SA, dedicada a las micro finanzas, orientada al área rural, tiene como uno de sus objetivos la expansión territorial a nivel nacional, en especial a las zonas rurales, para poder ofrecer sus productos y/o servicios en las distintas regiones del país, para lo cual la entidad realiza la instalación de sus sucursales de atención en los pueblos o ciudades más cercanas a las zonas rurales, estas sucursales de atención requieren contar con una conexión de Red

Privada Virtual para realizar de forma segura sus transacciones mediante su CORE Bancario (Aplicación de intercambio en tiempo real centralizado), para ello la entidad contrata el servicio de red privada virtual a la empresa CLARO, quien realiza la instalación del servicio cumpliendo una serie de actividades y procedimientos donde contemplan plazos que van desde los 30 hasta 90 días, y teniendo un costo fijo de instalación y pagos mensuales del servicio. Siendo los plazos establecidos para la instalación un problema perjudicial para la entidad, ya que si no se cuenta con el servicio no puede realizar sus operaciones, por este motivo surge la necesidad de contar con el servicio de una Red Privada Virtual alterna que pueda ser implementada en un menor plazo y a menor costo.

Esta implementación tiene como principal propósito ser una alternativa permanente para cuando se requiera en alguna sucursal de la Entidad, donde el proveedor CLARO del servicio de Red Privada Virtual no cuente con factibilidad técnica o el plazo requerido para la implementación de servicio sea muy largo, lo cual no es conveniente para la entidad. Por ello, la implementación de una Red Privada Virtual IPSec con IP dinámica con Routers Cisco resulta ser una buena alternativa, ya que puede ser implementada por el personal de la gerencia de Tecnologías de información de la entidad en un plazo mucho más corto y aun menor costo en comparación con el proveedor CLARO, ya que este puede ser realizado utilizando internet ADSL o Móvil y equipos propios.

1.4. OBJETIVOS DE LA INVESTIGACIÓN

1.4.1. Objetivo General

- Diseñar e Implementar una Red Privada Virtual IPSec con IP Dinámica con Routers Cisco que permita disminuir el tiempo y costo para la red de comunicación de las sucursales de la Caja Rural de Ahorro y Crédito los Andes SA.

1.4.2. Objetivos Específicos

- Analizar la situación actual del tiempo y costo de instalación del servicio de Red Privada Virtual contratado por la Entidad en las sucursales de Caja Rural de Ahorro y Crédito Los Andes SA.
- Diseñar la topología física y lógica de una Red Privada Virtual IPSec con IP Dinámica para disminuir el tiempo y costo de instalación en las sucursales de Caja Rural de ahorro y crédito los andes SA.
- Implementar la Red Privada Virtual con IP Dinámica con Routers Cisco y verificar la conectividad de las sucursales de la Caja Rural de Ahorro y crédito los Andes SA.
- Evaluar la disminución de tiempo y costo en la red de comunicación de las sucursales de la Caja Rural de Ahorro y crédito los Andes SA.

1.5. HIPÓTESIS DE LA INVESTIGACIÓN

1.5.1. Hipótesis General

El diseño e implementación de una Red Privada Virtual IPSec con IP Dinámica con Routers Cisco permite disminuir el tiempo y costo para la red de comunicación de las sucursales de la Caja Rural de Ahorro y Crédito los Andes SA.

1.5.2. Hipótesis Especifico

- El Análisis de la situación actual del servicio contratado por la entidad permite obtener los tiempos y costos de instalación del servicio.
- El diseño de la topología física y lógica de una Red Privada Virtual IPSec con IP Dinámica con routers Cisco permite disminuir el tiempo y costo para la red de comunicación en las sucursales de Caja Rural de Ahorro y Crédito los Andes SA.
- La implementación de una Red Privada Virtual IPSec con IP Dinámica con Routers Cisco permite la conectividad entre las sucursales de Caja Rural de Ahorro y Crédito los Andes SA.
- La evaluación muestra la disminución del tiempo y costo de instalación y servicio en la red de comunicación de las sucursales de la Caja Rural de Ahorro y crédito los Andes SA.

CAPITULO II

REVISIÓN DE LITERATURA

2.1. ANTECEDENTES DE INVESTIGACIÓN

2.1.1. Internacionales

En su tesis (Zapata Rodríguez, 2016) Evaluación de Parámetros de Calidad de Servicio (QoS) para el Diseño de una Red VPN con MPLS, que tuvo como objetivo diseñar y simular en un laboratorio una red VPN/MPSL, donde se recolecta la información mediante procedimientos inductivos y experimentales para evaluar los parámetros de QoS y garantizar la disponibilidad y escalabilidad en la red, también en base a ello definir los parámetros de QoS más críticos en el diseño y evaluación, para esto se utiliza la herramienta de simulación GNS3 y D-ITG que inyecta el tráfico de voz, datos y streaming que utilizan protocolo de la capa de transporte TCP o UDP, y se obtuvo como conclusión que las redes VPN/MPLS con mecanismos DiffServ ofrecen garantías en QoS para los diferentes tipos de tráfico como son VoIP, Streaming y Datos.

(Romero López & Romero López, 2016), en su trabajo que consiste en la elaboración de un documento basado en la investigación sobre la temática de redes privadas virtuales, como son las VPNs, donde se analizan su seguridad y la importancia que tienen en una organización, para ello se describen los protocolos de seguridad de VPN, amenazas en la red y las formas de mitigar las vulnerabilidades, de esta forma las organización puedan realizar una correcta selección de la VPN a implementar según sus necesidades, en su conclusión nos indican que existen diferentes modelos de implementación de VPNs, los cuales se basan en el software y hardware a utilizar, siendo el hardware el más óptimo en cuanto al proceso de autenticación y cifrado, pero también nos indican que se requiere realizar una correcta combinación en estos dos aspectos para prevenir riesgos de ataque y acceso de intrusos, ya que las redes privadas virtuales se ha

convertido en la solución para la comunicación entre sucursales, clientes interno y externos, debido a ello se han desarrollado los protocolos de seguridad como IPSec, PPTP,SSL, entre otros.

2.1.2. Nacional

Para (Mar Segundo, 2016) en su "trabajo de investigación se basa en emplear la tecnología de red Virtual Private Network (VPN), con la finalidad de mejorar la confidencialidad del intercambio de información entre las sedes Lima - Cusco del Instituto Nacional de Estadística e Informática (INEI)" (Pág. 15),y también se da solución a un problema de seguridad utilizando internet a través de una VPN, esto debido a que el personal de la institución ha reportado inconvenientes en sus cuentas de correo personal que utilizan para comunicarse en la institución, también se ha visto por conveniente implementar un dominio para el correo "inei.com" por la cual se enviara y recibirá los correos entre el personal de la sede lima y cusco de esta forma se ayuda a garantizar la confidencialidad en el intercambio de información, y para verificar la seguridad se realizaron pruebas de ataques man in the middle con una conexión a la intranet via VPN y otra sin conexión a la misma.

2.1.3. Local

(Huarcaya Ramos & Muñoz Apaza, 2022) en su proyecto de investigación titulado Diseño de la red de área local aplicando la metodología del ciclo de vida de red de cisco para mejorar la calidad de los servicios, el índice de transferencia de datos y la estabilidad de los sistemas de información de la Municipalidad distrital de Santa Rosa, debido a que las instituciones del gobierno han sido afectadas por las medidas de confinamiento producto de la pandemia, que impiden el normal funcionamiento de los tramites de forma presencial, se plantea como objetivo diseñar un modelo de red estructurado aplicando metodología del ciclo de vida de cisco para mejorar la calidad de los servicios, velocidad

de intercambio de datos y dar mayor estabilidad al sistema de información de la institución, aprovechando el uso de dispositivos tecnológicos de información y comunicación, esta investigación es del tipo descriptivo aplicado orientada a la investigación aplicada, y se realiza en la municipalidad con 54 funcionarios, donde se realizaron la recaudación de datos utilizando entrevistas y encuestas, y se concluyó que se requiere la implementación de una nueva red de datos para mejorar la transferencia de datos y la estabilidad de los servicios, esto mediante una simulación realizada en Packet Tracer.

(Atencio Mendoza & Mamani Figueroa, 2017), en su tesis "Diseño e Implementación de un Prototipo de Red Privada Virtual en Capa 3 Utilizando Cisco IOS para la Universidad Nacional del Altiplano" donde se realiza el diseño e implementación de un prototipo de red privada virtual, utilizando Cisco IOS para lograr su funcionamiento se realizaron diferentes diseños que permitan una implementación real y adecuada para la información que se requiera enviar, utilizando protocolos de cifrado de datos, y los resultados obtenidos mostraron que la red transmite los datos de punto a punto cifrados y encapsulados con el conjunto de protocolos de IPSec que trabajan en la capa 3, también los resultados obtenidos con los programas Packet Tracer y Wireshark fueron satisfactorios, y se concluyó en base a los resultados que el prototipo de red privada virtual brinda autenticación, integridad y confidencialidad al transmitir datos entre las oficinas de Tecnología Informática y las coordinaciones académicas, teniendo como rendimiento mínimo de 89.29 % de un total de 56 datos trasmitidos durante las pruebas realizadas, quedando demostrado que el prototipo diseñado dentro de los laboratorios de Cisco puede ser implementada en equipos reales en todas las oficinas de la Institución.

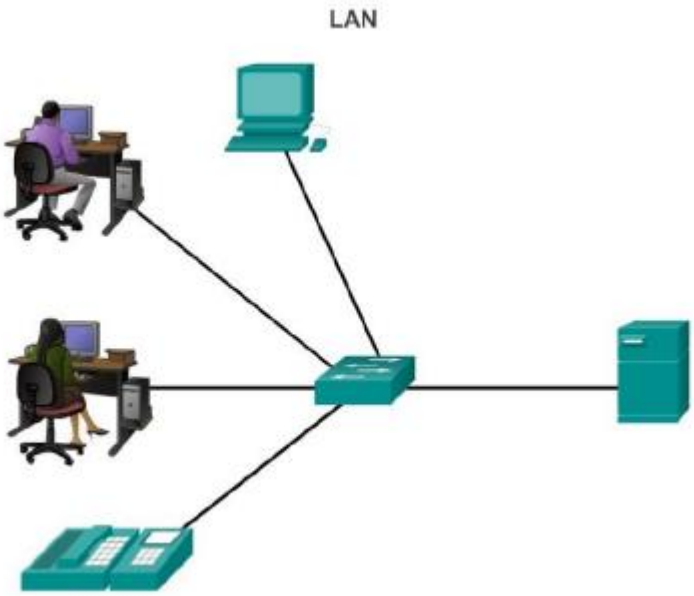
2.2. SUSTENTO TEÓRICO

2.2.1. Red De Área Local (LAN)

Según (Hwang, 2021) dice que una red de área local o LAN (por las siglas en inglés Local Area Network) es una red de computadoras ubicadas en un área reducida a una casa, un departamento o un edificio y define dos principales tipos de LAN: las inalámbricas WLAN y las cableadas, la cableadas son las más comunes y utilizan conmutadores y cableado Ethernet para conectar los dispositivos finales, en pequeñas instituciones una LAN cableada puede constar solamente de un dispositivo no administrado a comparación de una de mayor dimensión que puede requerir mayor cantidad de conmutares con software para su administración y garantizar el funcionamiento óptimo de la red LAN. De la misma manera (Editorial Etecé, 2021) afirma que una red LAN es una red informática cuyo alcance se limita a un espacio físico reducido, como son los edificios, departamentos y casas, también indica que a través de una red LAN puede compartirse información y recurso entre los dispositivos conectados que pueden ser computadoras, servidores, teléfonos celulares, tableta, impresoras, proyectores, etc. Esto incluso estando en diferentes pisos o habitaciones.

Las redes LAN nos permiten conectar dispositivos para transmitir y recibir información entre dispositivos conectados a una misma red, como son servidores, portátiles e impresoras, también en una red LAN los dispositivos conectados comparten una sola conexión de internet o VPN.

Figura 1: Red de Área Local (LAN).



Fuente: Cisco Networking Academy (2017)

2.2.1.1. Topologías de LAN.

Existen distintas topologías de LAN, a continuación, se describen las más populares:

2.2.1.1.1. Estrella.

Según (Cisco Networking Academy, 2017) la topología estrella conecta dispositivos finales a un dispositivo intermediario central, la topología en estrella es la más común porque es fácil de instalar muy escalable y de fácil resolución de problemas. También, según (Editorial Etecé, 2021) la topología en estrella es la que conecta a un servidor central de red que administra los recursos y asigna según se le solicite.

2.2.1.1.2. Estrella Extendida.

(Cisco Networking Academy, 2017) Nos dice que la topología estrella extendida o hibrida es aquella donde los dispositivos intermediarios centrales interconectan otras topologías en estrella.

2.2.1.1.3. Anillo.

Para la topología en Anillo (Editorial Etecé, 2021) nos indica que todos los computadores están conectados con sus vecinos mediante una transmisión unidireccional, donde si se produce un fallo se interrumpe la red. Para (Cisco Networking Academy, 2017) la topología en Anillo los dispositivos finales se conectan a su vecino y forman un anillo.

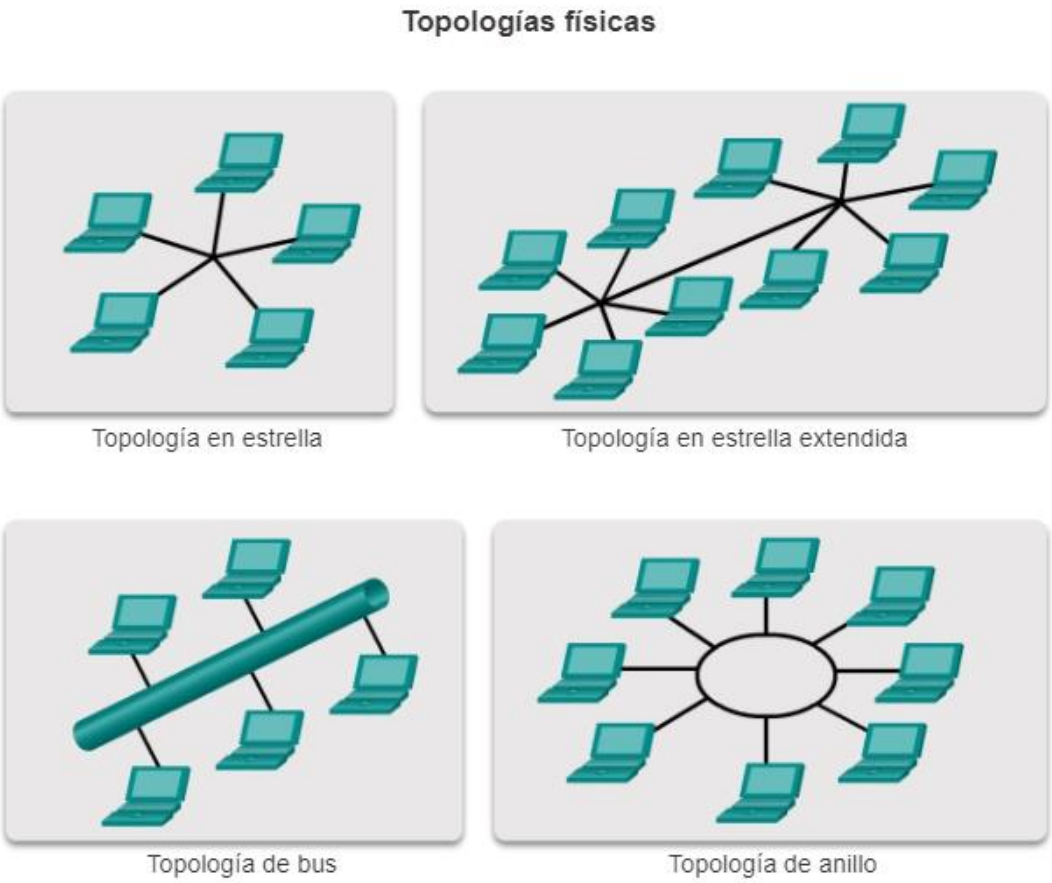
2.2.1.1.4. Malla.

Para (Nolle & Gillis, 2022) son las que crean múltiples rutas para que la información viaje entre los dispositivos conectados, se enfoca en crear una red a prueba de fallos porque si un nodo falla existe otro camino para que la información llegue a su destino, una malla puede incluir cientos de nodos.

2.2.1.1.5. Bus.

La topología en bus según (Cisco Networking Academy, 2017) todos los sistemas se encadenan y terminan de algún modo en cada extremo, y no se requieren dispositivos intermediarios como switches para interconectar los dispositivos. Y según (Editorial Etecé, 2021) la topología en bus permite la transmisión de datos en línea recta porque se usa mismo camino para interconectar los dispositivos esto hace susceptible a daños de cable o a la interrupción del tráfico.

Figura 2: Topologías Físicas.

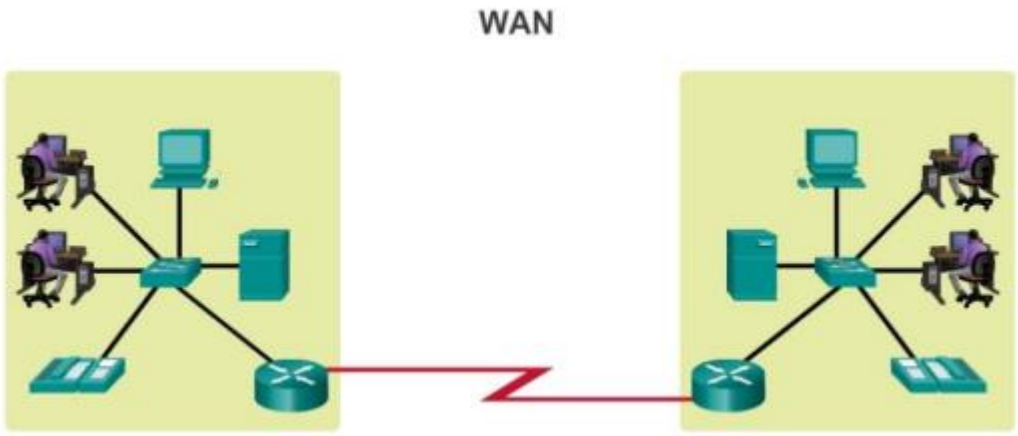


Fuente: Cisco Networking Academy (2017)

2.2.2. Red De Área Amplia (Wan)

Para (Rouse, 2016) una Red de Área Amplia (WAN) interconecta múltiples redes LAN que están distribuidas en distintas ubicaciones geográficamente, para una empresa la WAN puede la sede principal con sus sucursales, asi como con sus servicios en la nube, esto elimina la necesidad de instalar dispositivos como firewall o un servidor en cada una de sus sedes. Y (Digital Guide IONOS, 2020) nos dice que WAN es una red de gran escala que abarca países e incluso continentes, que interconecta redes LAN o MAN y no ordenadores individuales, las WAN puede ser públicas o administradas por empresas para conectar distintas sedes ubicadas a grandes distancias para usar sus servicios en la nube y conectar las sedes remotas, las públicas son operadas por ISP para permitir acceso a este servicio.

Figura 3: Red de Área Amplia (WAN).



Fuente: Cisco Networking Academy (2017)

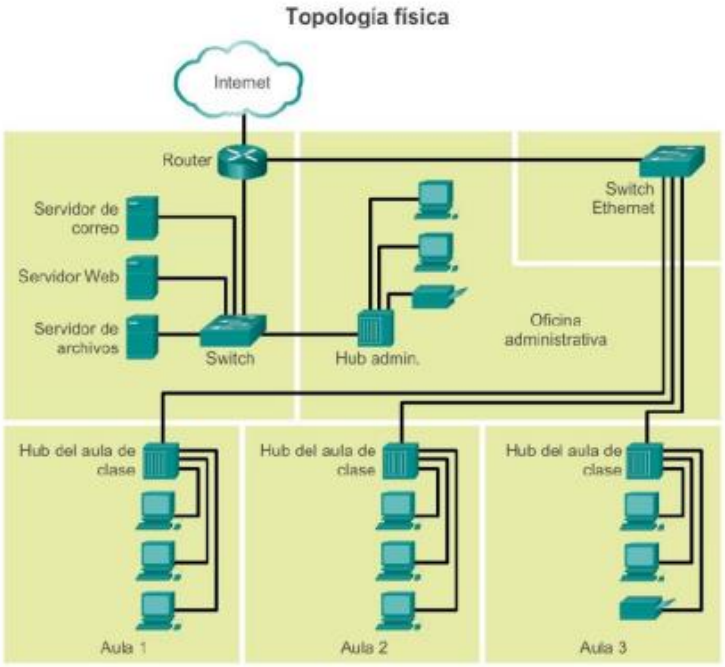
2.2.2.1. Tipos de conexiones WAN

Según (Rouse, 2016) Las conexiones WAN pueden incluir tecnologías cableadas e inalámbricas, las tecnologías inalámbricas pueden ser las redes basadas en el estándar 4G LTE que están ganando terreno así como las redes públicas Wi-Fi o satelitales, sin embargo las WAN con conexiones de red cableadas todavía siguen siendo de uso preferido para la gran mayoría de las empresas, Una infraestructura WAN puede ser de propiedad privada o arrendad a un ISP, si es servicio funciona por una conexión dedicada y privada esta debe contar con un servicio de (SLA).

2.2.3. Diagramas De Topologías De Red

2.2.3.1. Topología Física.

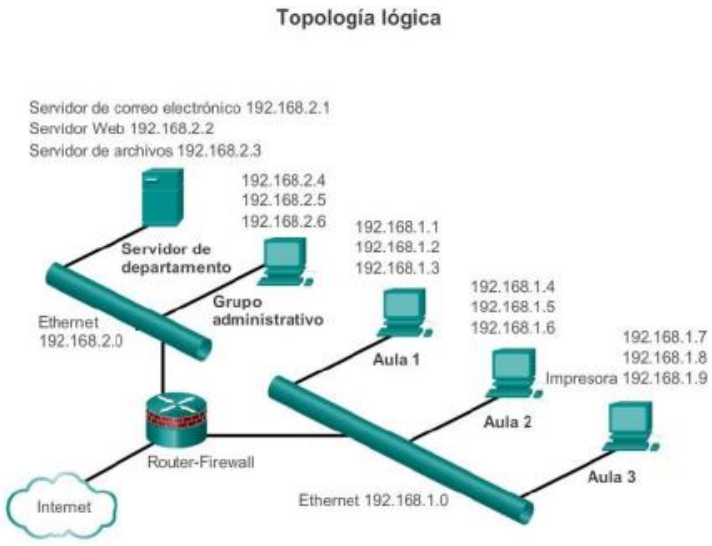
Figura 4: Topología Física.



Fuente: Cisco Networking Academy (2016)

2.2.3.2. Topología Lógica.

Figura 5: Topología Lógica.



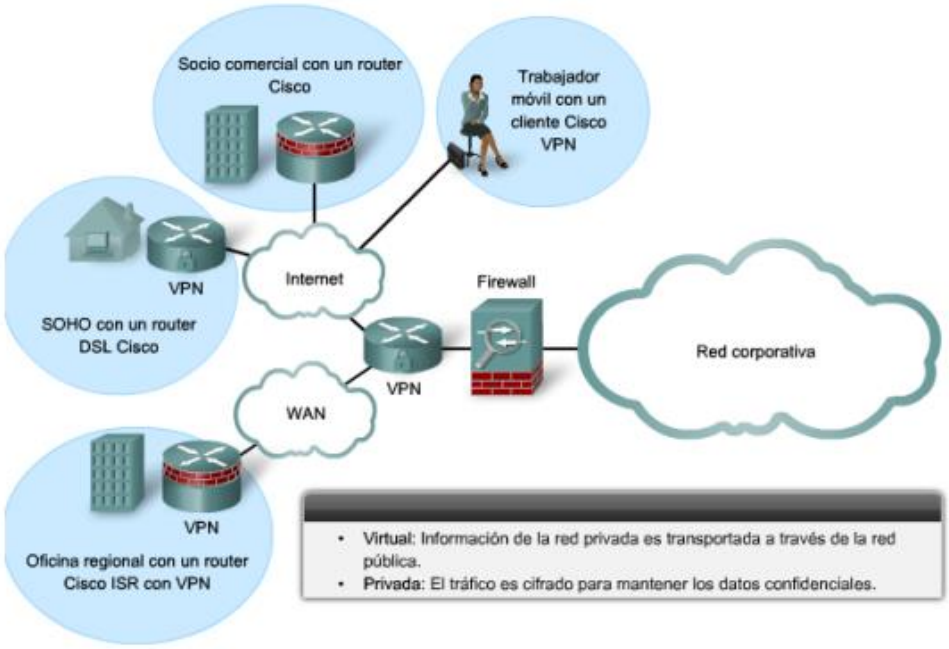
Fuente: Cisco Networking Academy (2017)

2.2.4. Red Privada Virtual (VPN)

Para (Gillis, 2021) Una red privada virtual es un servicio que crea una conexión en línea segura y cifrada, donde los usuarios pueden tener más privacidad y anonimato y no tener inconvenientes como la censura basados en la ubicación geográfica, la VPN es una red privada a través de una red pública, que permitir al usuario enviar y recibir datos de forma segura a través de internet. Y de la misma forma (Cisco, 2021) nos dice que una red privada virtual es una conexión cifrada a Internet desde un dispositivo a una red, esta conexión cifrada garantiza una transmisión de datos segura y confidencial, y evita que personas no autorizadas tengan acceso y espíen la información enviada, también permiten el trabajo remoto de usuarios ligados a empresas.

Las VPNs utilizan en una red menos segura, como el internet público, mediante los cuales generan un túnel de conexión de tipo LAN entre sedes ubicadas en distintas partes geográficamente, esto realizan utilizando protocolos de tunelización que envían los datos cifrados de extremo a extremo, para de esta manera evitar cualquier intrusión en la privacidad de los usuarios. Y tampoco los proveedores de servicios de internet (ISP) que normalmente tienen una gran cantidad de información sobre las actividades de un cliente pueden tener acceso a los datos enviados por una VPN.

Figura 6: Red Privada Virtual (VPN).



Fuente: Cisco Networking Academy (2017)

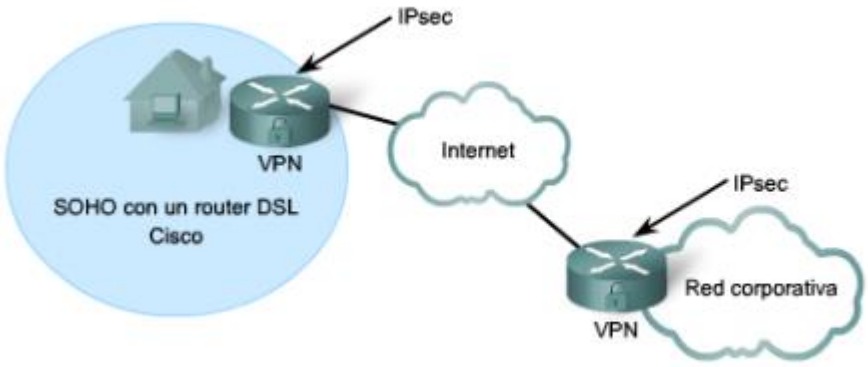
2.2.4.1. Funcionamiento de una VPN.

Para (Gillis, 2021) un túnel VPN en su definición básica es una conexión punto a punto a la que solo acceden usuario autorizados, para la creación del túnel se utiliza un protocolo de túnel, que puede ser OpenVPN o SSTP, el protocolo utilizado dependerá de la plataforma en la que se quiera utilizar la VPN, como por ejemplo SSTP se utiliza en el sistema operativo Windows y proporciona cifrado de datos con distintas potencias, el VPN la puede ejecutar localmente o en la nube pero el cliente se ejecuta en segundo plano y el usuario final no nota a menos que haya bajo rendimiento. Para (Cisco, 2021) una red privada virtual extiende la red corporativa a través de conexiones cifradas por internet, el recorrido del tráfico es privado porque está cifrado entre el dispositivo y la red, también un empleado puede conectarse a la red corporativa y trabajar fuera de la oficina, la conexión puede realizarse incluso utilizando smartphones y tables.

Al utilizar un túnel VPN, el dispositivo de un usuario podrá conectarse a otra red mientras los datos están encriptados y la dirección IP está oculta, de esta forma los atacantes u otras personas que esperan tener acceso a las actividades del cliente no podrán ver los datos.

También, cuando se utiliza una VPN por Internet este puede verse afectado en su rendimiento si tiene mucha carga en su conexión, ya que el servicio de internet domestico es Asimétrico, para ello lo más recomendable es implementar calidad de servicio (QoS).

Figura 7: Red Privada Virtual IPSec.



Fuente: Cisco Networking Academy (2017)

2.2.4.2. Utilidad de la VPN.

La utilidad de la VPN para (Gillis, 2021) es tanto para los usuarios normales de Internet como para las organizaciones que la utilizan para la privacidad virtual, ya que las utilizan para acceder a su centro de datos desde cualquier extremo utilizando canales cifrados, la VPN también se usa para conectarse a una base de datos de la misma organización ubicada en un área diferente, también la utilidad más productiva es para que pueda ser utilizada por los trabajadores remotos, trabajadores independientes y viajeros que necesitan acceder a aplicaciones alojadas en las redes de la organización, para ello un usuario debe estar autorizado para esto se puede utilizar contraseñas, tokens de seguridad o datos biométricos.

Una VPN puede brindar al usuario para utilizar servicios alojados en sedes corporativas, ya que la comunicación está cifrada.

2.2.4.3. Ventajas y Desventajas de una VPN.

Para (SmartyDNS, 2019) hay muchas cosas que se deben considerar para comprender los beneficios y desventajas de una VPN, por ello empieza con enumerando las desventajas: las mejores VPN son pagadas, no funcionan de forma nativa en todas las plataformas, su uso puede disminuir la velocidad de conexiones y algunos proveedores de VPN tienden a registrar los datos de los usuarios, y las ventajas son: no existen restricción geográfica, la privacidad no está en riesgo, protegen de ataques cibernéticos, mantienen a salvo de la censura en línea, es perfecto para trabajos remotos, no se reduce el ancho de banda, pueden ayudar a ahorrar dinero, las descargas de Torrents ya no son arriesgadas y mejoran la experiencia de juego.

2.2.5. Tipos De VPN

2.2.5.1. Acceso Remoto.

(Cisco, 2021) Una VPN de acceso remoto conecta un dispositivo de forma segura fuera de la oficina corporativa, **estas pueden** ser computadoras portátiles, tables o smartphones, se puede pensar que el acceso remoto como si se tuviera la computadora en la red a la que se está accediendo, los avances tecnológicos en la VPN ya permiten realizar comprobaciones a las terminales antes de la conexión para garantizar que cumplan con ciertos estados para realizar la conexión. También (Gillis, 2021) nos dice que el acceso remoto conecta los clientes con un servidor en la red de la organización mediante una puerta de enlace que autentique su identidad antes de otorgar **los accesos** a la red interna, y este tipo se basa en IPsec o SSL para asegurar la conexión.

2.2.5.2. Sitio a Sitio.

Según (Gillis, 2021) una VPN de sitio a sitio utiliza un dispositivo de puerta de enlace para conectar una red completa en una ubicación a una red en otra ubicación, porque los dispositivos en la ubicación remota no necesitan clientes VPN, la mayoría de las VPN sitio a sitio utilizan IPSec atreves de Internet, pero también es común que utilicen de conmutación de etiquetas multiprotocolo de operador (MPLS) en lugar de la internet para el transporte de las VPN sitio a sitio, también es posible obtener conectividad de capa 3 (MPLS IP VPN) o capa 2 (servicio de red de área local privada). También (Cisco, 2021) nos dice que una VPN sitio a sitio se usan cuando se requieran conectar una oficina corporativa con las sucursales por internet y no sea posible por la distancia entre estas, por ello se usan equipo dedicados para estableces y mantener la conexión, se puede interpretar como un acceso de red a red.

2.2.6. Protocolos De VPN

Según (OSTEC Seguridad Digital de Resultados, 2016) con el propósito de atender una comunicación segura y confiable durante la transmisión de datos se utiliza diferentes protocolos y cada uno de ellos funciona de diferente manera, a continuación, se describen las más populares:

2.2.6.1. IPSec.

Para (OSTEC Seguridad Digital de Resultados, 2016) IPSec (Internet Protocol Security) es una extensión del protocolo IP (Internet Protocol) y tiene por objetivo garantizar comunicaciones privadas y seguras utilizando servicios de seguridad criptográficos, en una implementación de VPN estándar de IPSec entre sus principales atributos es la seguridad que satisface los requisitos de una empresa para la conexión entre sus sucursales o usuarios remotos a sus sedes principales,

también podemos destacar la privacidad, integridad de los datos y la autenticidad de la información. Para (Grupo de Sistemas Operativos DATSI FI UPM, 2022) IPSec actúa en la capa de red, la capa 3 del modelo OSI, así como otros protocolos que operan en la capa de transporte son el SSL, TLS y SSH, esto hace más flexible a IPSec, ya que es utilizado para proteger los protocolos de la capa 4 incluyendo TCP y UDP, para que una aplicación utilice IPSec no se requiere hacer cambios en ella como en SSL y otros protocolos que requieren modificar su código, por ello IPSec tiene una ventaja sobre estos.

2.2.6.2. L2TP.

Para (OSTEC Seguridad Digital de Resultados, 2016) L2TP (Layer 2 Tunneling Protocol) es un protocolo de encapsulación que se basa en un protocolo de criptografía IPSec, aunque no ofrece ninguna confidencialidad o autenticación por sí mismo, también son conocidas como líneas virtuales que proporcionan acceso de bajo costo a los usuarios, porque permite gestionar al servidor de una empresa las direcciones IP a sus usuarios remotos, de esta forma L2TP busca garantizar la confidencialidad, autenticidad e integridad.

2.2.6.3. PPTP.

Para PPTP (Point-to-Point Tunneling Protocol) se tiene la definición de (OSTEC Seguridad Digital de Resultados, 2016) que lo define como un protocolo VPN desarrollado como una extensión del PPP (Point-to-Point Protocol) por tener una criptografía básica, ya que PPTP encapsula los protocolos IP en datagramas del PPP y tiene una sobrecarga relativamente baja, haciendo que el servidor de encapsulación realice las comprobaciones de seguridad para un envió más seguro, lo que lo hace más rápido que los otros protocolos VPN.

2.2.6.4. VPN SSL.

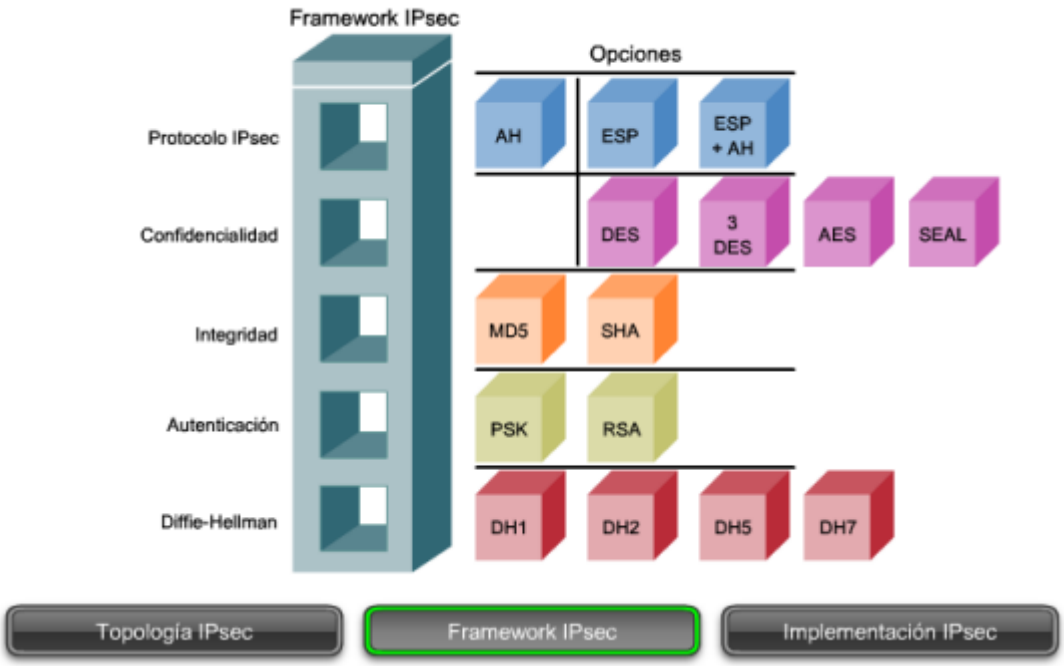
VPN SSL (Secure Sockets Layer) es definido por (OSTEC Seguridad Digital de Resultados, 2016) como un formato que puede ser utilizado de dos maneras, con acceso directamente a la web sin necesidad de instalación de cliente de conexión, y otra, mediante un cliente, la manera de proteger el transporte de información la realiza a través del SSL y sus sub protocolos, que garantizan la comunicación y seguridad entre los involucrados, este tipo de VPN viene ganando mayor cantidad de usuarios por la facilidad de uso e interoperabilidad con dispositivos móviles que cada vez son más utilizados por los empleados para acceder de manera segura a la información de una organización.

2.2.7. IPSec

Para (Cisco Networking Academy, 2016) IPsec es un estándar IETF (RFC 2401-2412) que define cómo debe configurarse una VPN utilizando el protocolo de direccionamiento IP, es un framework de estándares abiertos donde se definen reglas de comunicación segura, IPSec no está asociado a un tipo de cifrado, autenticación algoritmo de seguridad o tecnología de claves, IPSec se basa en algoritmos existentes para implementar el cifrado, el intercambio de claves y la autenticación; esta funciona en la capa de red, protegiendo y autenticando los paquetes IP los pares IPSec participantes, el framework IPSec se compone de cinco bloques: primero el protocolo IPSec que incluyen las opciones ESP o AH, segundo algoritmos de cifrado como DES, 3DES, AES, SEAL, el elección depende del nivel de seguridad requerido, en el tercero se representa la integridad utilizando MD5 o SHA, el cuarto es la clave secreta compartida, dos métodos posibles son pre-compartida y firma digital utilizando RSA y por último el quinto

es el grupo de algoritmos HD, existen cuatro algoritmos posibles para elección: DH Grupo 1, DH Grupo 2, DH Grupo 5 y DH Grupo 7.

Figura 8: Estructura IPSec.



Fuente: Cisco Networking Academy

2.2.7.1. Funciones Esenciales de Seguridad.

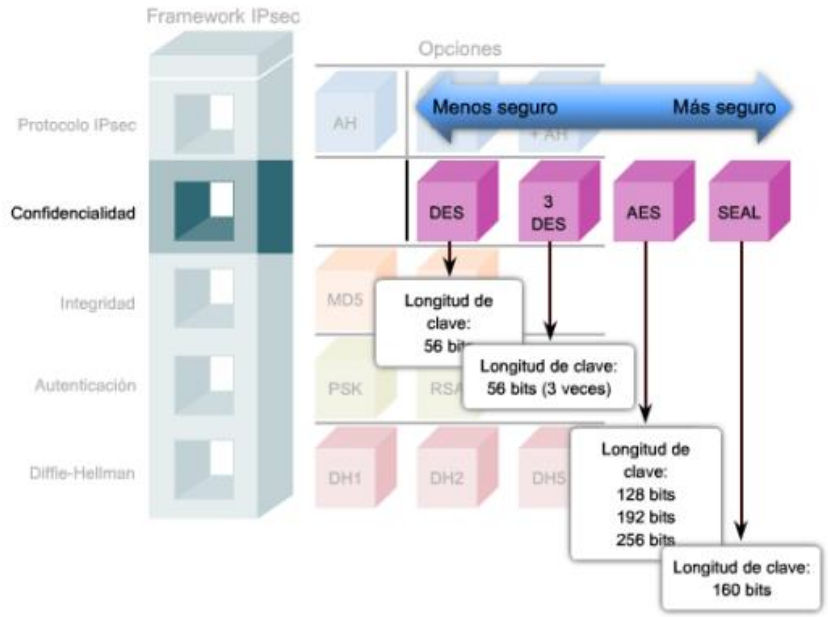
Para (Cisco Networking Academy, 2016) IPsec puede asegurar un camino entre un Gateway y un host, par de hosts y un par de gateways, IPSec provee funciones esenciales de seguridad.

2.2.7.1.1. Confidencialidad.

La confidencialidad se obtiene utilizando cifrando el tráfico que transita por la VPN, si alguien intenta obtener la clave mediante un ataque de fuerza bruta, el número de posibilidades a probar está en función a la longitud de la clave, por ello el grado de seguridad depende de la longitud de la clave utilizada por el algoritmo de cifrado, por ejemplo una clave de 64 bits puede llevar romperla

aproximadamente un año y una calve de 128 bits puede tomar 10^19 años con una computadora relativamente sofisticada (Cisco Networking Academy, 2016).

Figura 9: Confidencialidad IPSec.

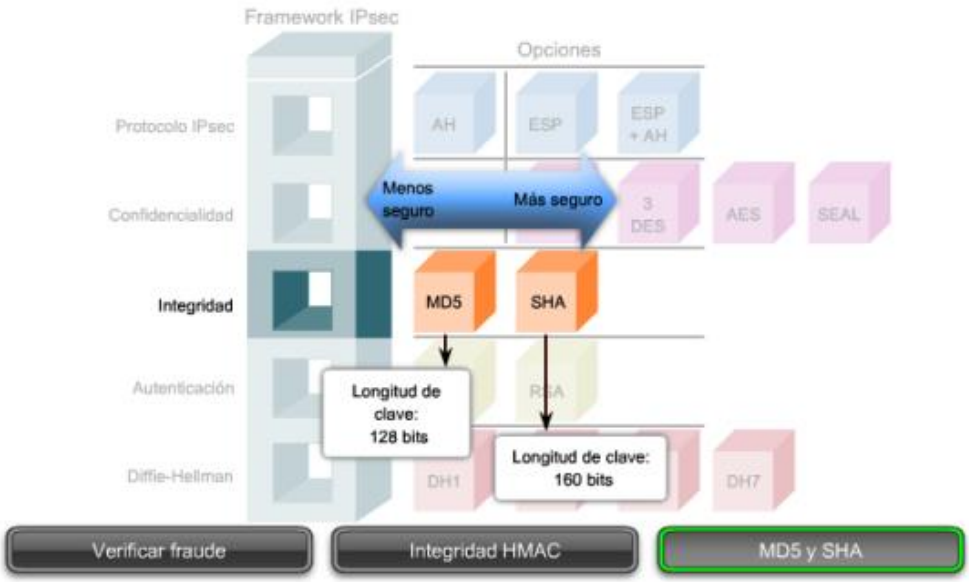


Fuente: Cisco Networking Academy (2017)

2.2.7.1.2. Integridad.

IPsec asegura que los datos llegan a destino sin modificaciones, utilizando algoritmos de hash como MD5 y SHA (Cisco Networking Academy, 2016).

Figura 10: Integridad IPSec.

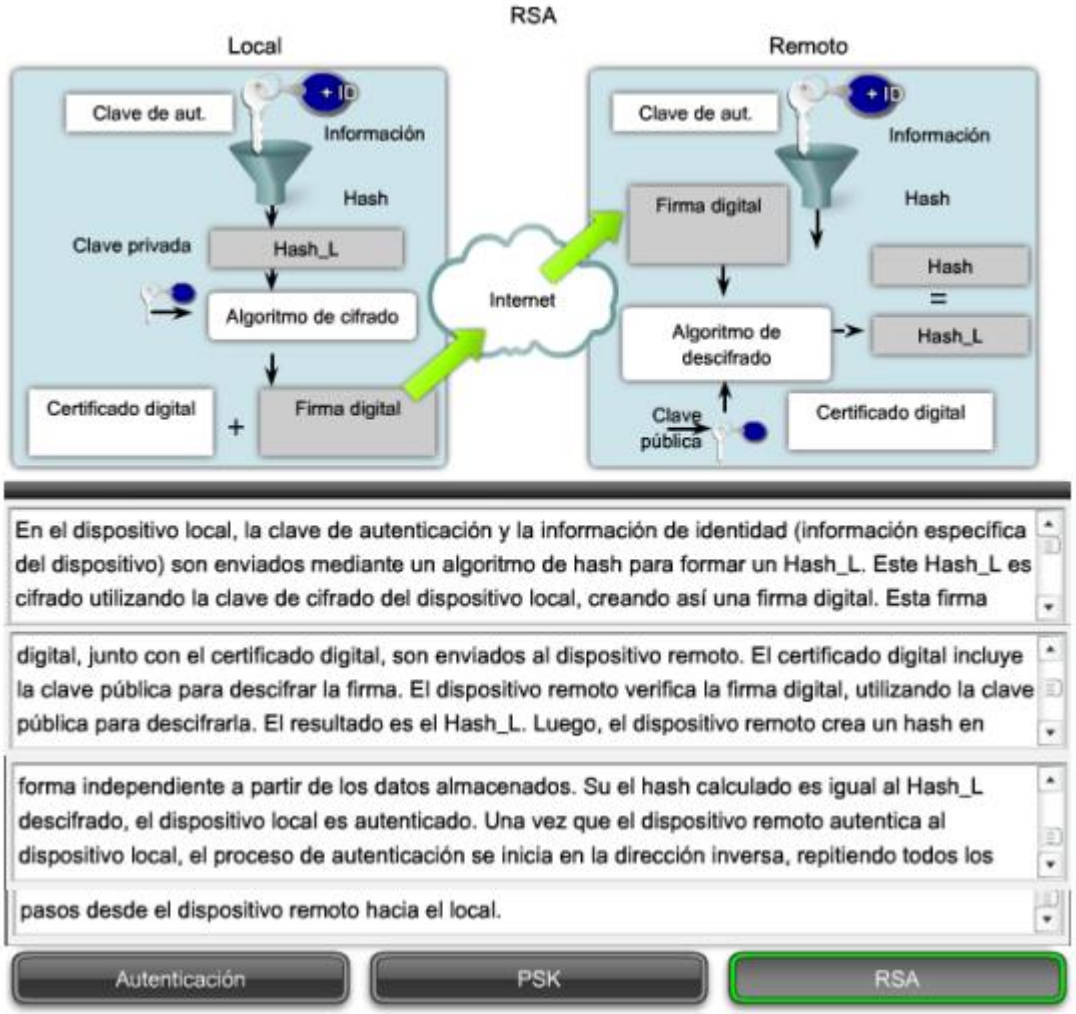


Fuente: Cisco Networking Academy (2017)

2.2.7.1.3. Autenticación.

(Cisco Networking Academy, 2016) Dice que IPsec utiliza IKE (Internet Key Exchange) para autenticar a los usuarios y dispositivos y que estos puedan llevar a cabo comunicaciones en forma independiente, también en IKE se utilizan varios tipos de autenticación como nombre de usuario y contraseña, esta contraseña es de uso único, biométrica, pre-compartidas y certificados digitales.

Figura 11: Autenticación IPSec.

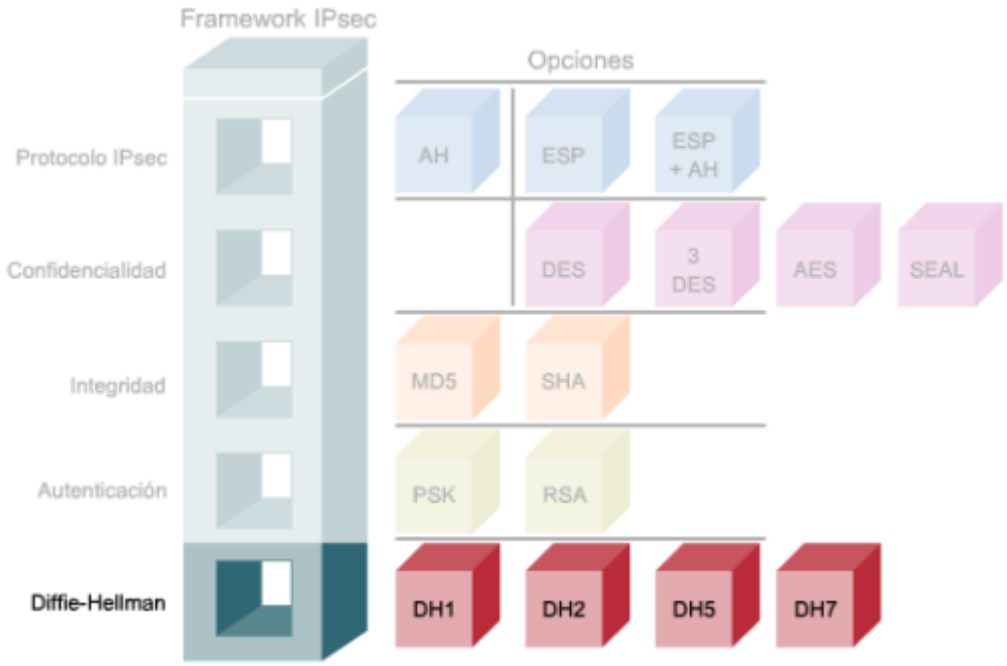


Fuente: Cisco Networking Academy (2017)

2.2.7.2. Intercambio seguro de claves

(Cisco Networking Academy, 2016). indica que IPsec utiliza el algoritmo DH para proveer un método de intercambio de claves públicas entre los pares, para establecer una clave compartida secreta.

Figura 12: Intercambio Seguro de Claves.



Fuente: Cisco Networking Academy (2017)

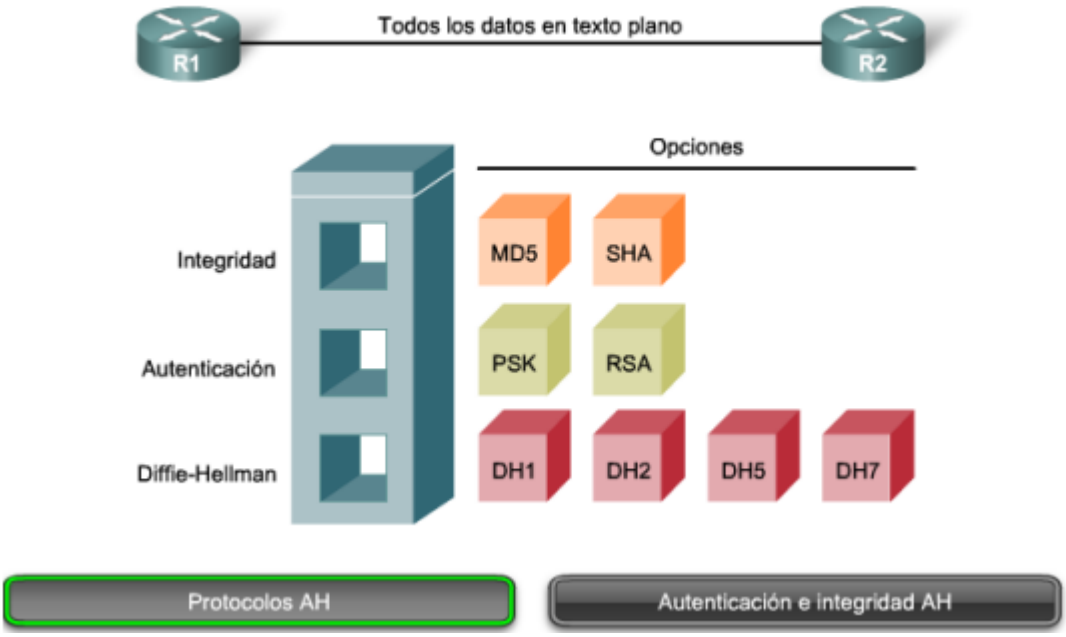
2.2.7.3. Protocolos de seguridad IPSEC.

"IPsec es un framework de estándares abiertos que detalla los mensajes para asegurar las comunicaciones, pero se basa en algoritmos existentes dos protocolos principales del framework IPsec son AH y ESP" (Cisco Networking Academy, 2016, pág. 587).

2.2.7.3.1. Authentication Header (AH).

AH aplica funciones hash de una vía con clave al paquete y crear el hash correspondiente y para lograr la autenticación, donde el hash creado se combina con el texto y se transmite, el receptor realiza la detección de cambios en cualquier parte del paquete durante su transmisión, realizando la misma función hash de una vía en el paquete recibido, y comparando el resultado con el valor del hash recibido, el que el hash involucre una clave secreta compartida asegura la autenticidad (Cisco Networking Academy, 2016).

Figura 13: Authentication Header.

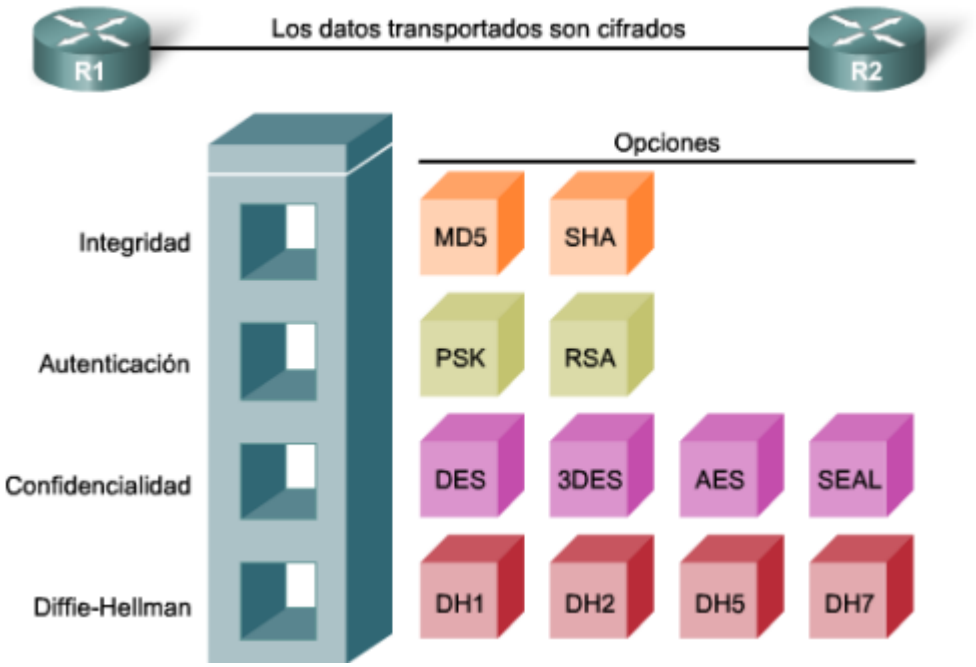


Fuente: Cisco Networking Academy (2017)

2.2.7.3.2. ESP.

Para (Cisco Networking Academy, 2016) ESP provee confidencialidad cifrando los datos, se selecciona ESP como protocolo de IPSec porque soporta una variedad de algoritmos de cifrado simétricos, los productos de Cisco soportan el uso de 3DES, AES, y SEAL, para un cifrado más seguro, pero el algoritmo por defecto para IPSec es DES de 56 bits.

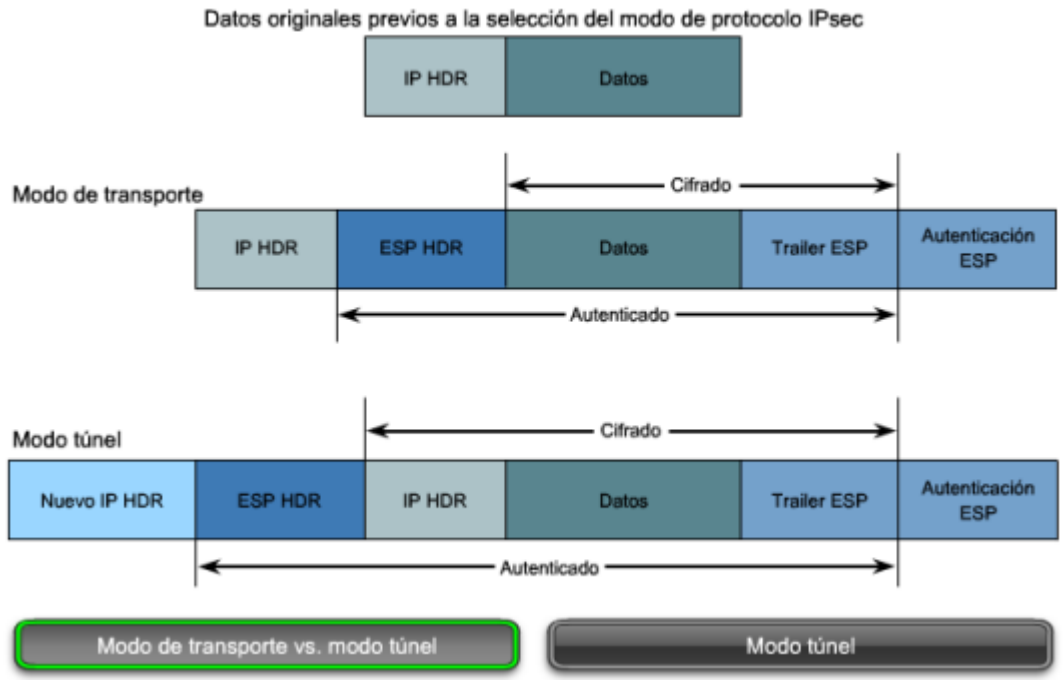
Figura 14: ESP.



Fuente: Cisco Networking Academy (2017)

ESP y AH pueden aplicarse a los paquetes IP de dos formas diferentes, en modo transporte y en modo túnel.

Figura 15: Modo Transporte.



Fuente: Cisco Networking Academy (2017)

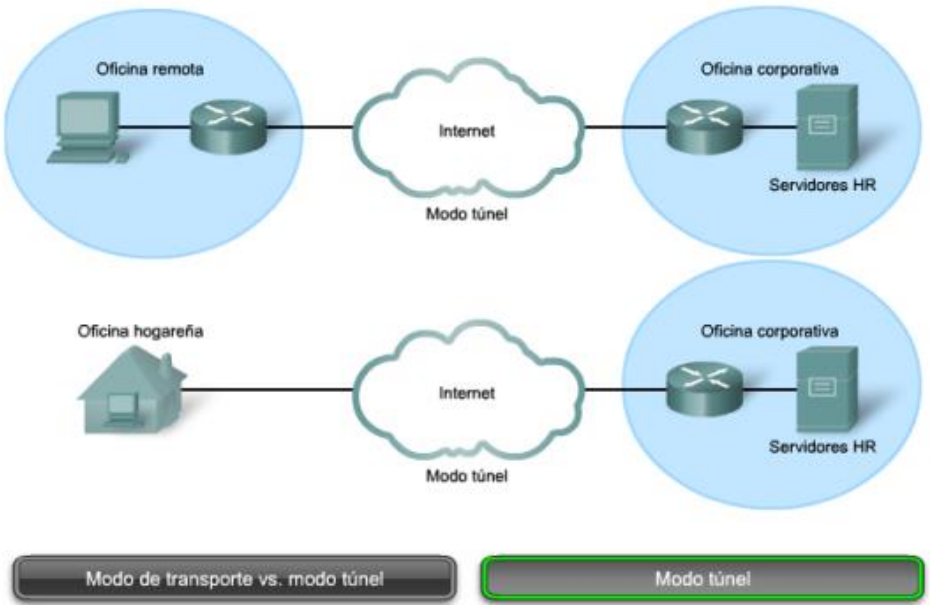
2.2.7.3.3. Modo transporte.

El modo transporte protege los datos del paquete pero mantiene la dirección IP original en texto plano, porque la seguridad la provee a partir de la capa de transporte del modelo OSI y capas superiores, ya que la dirección IP original puede utilizarse para encaminar el paquete a través de Internet, el modo de transporte ESP se utiliza entre hosts y funciona bien con GRE, porque esconde las direcciones de los dispositivos finales agregando su propia IP (Cisco Networking Academy, 2016).

2.2.7.3.4. Modo túnel.

El modo túnel es el que se utilizara en el presente proyecto y según (Cisco Networking Academy, 2016) este modo provee seguridad para el paquete IP original completo, porque es cifrado y encapsulado en otro paquete, también como conocido como “Cifrado de IP en IP”; para lo cual la dirección IP del paquete IP extremo se utiliza para en rutar a través de Internet, cuando se utiliza el modo túnel ESP en IPSec de acceso remoto el cliente IPSec en la Pc realiza el cifrado y encapsulación para luego en la oficina corporativa se router lo des encapsule y descifre el paquete.

Figura 16: Modo Túnel.



Fuente: Cisco Networking Academy (2017)

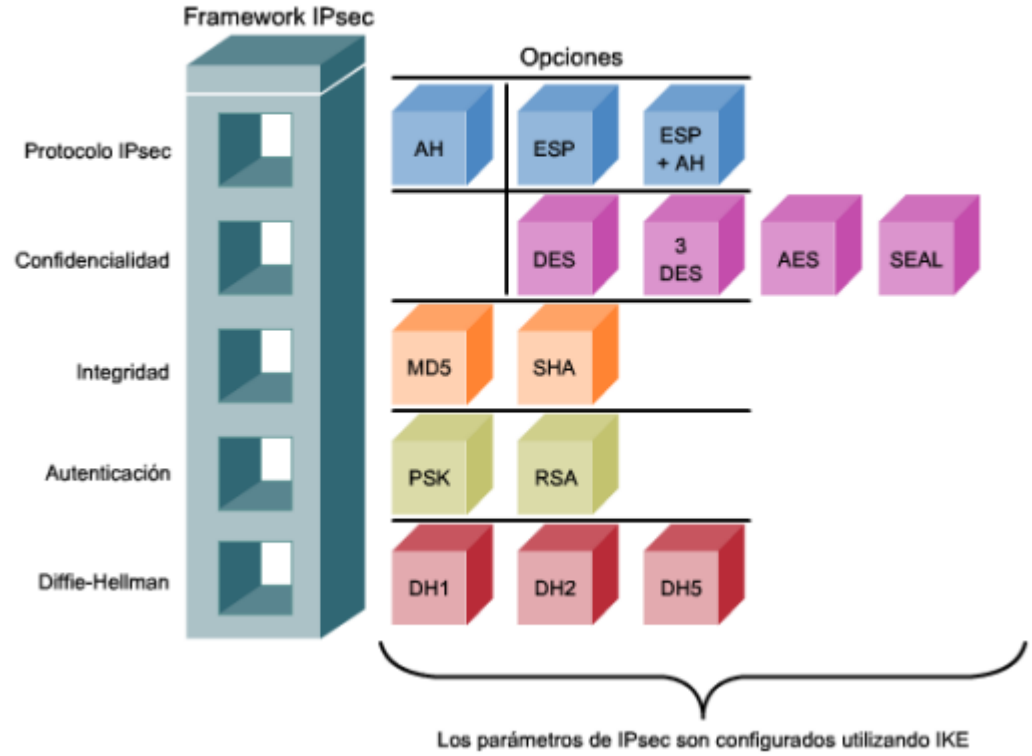
2.2.7.4. Intercambios de claves en Internet (IKE).

IPsec negocia los parámetros de intercambio de claves, establece una clave compartida, autentica al otro extremo y negocia los parámetros de cifrado y los parámetros negociados entre los dispositivos se conocen como asociación de seguridad (Security Association - SA)" (Cisco Networking Academy, 2016, pág. 594)

2.2.7.4.1. Asociaciones de seguridad (SA).

Un SA es un bloque de construcción básico de IPsec, estas asociaciones de seguridad se mantienen dentro de una base de datos SADB en cada dispositivo, una VPN IPsec tiene registros SA que definen los parámetros de cifrado IPSec y registros SA donde se definen los parámetros de intercambio de claves (Cisco Networking Academy, 2016).

Figura 17: Asociaciones de seguridad (SA).

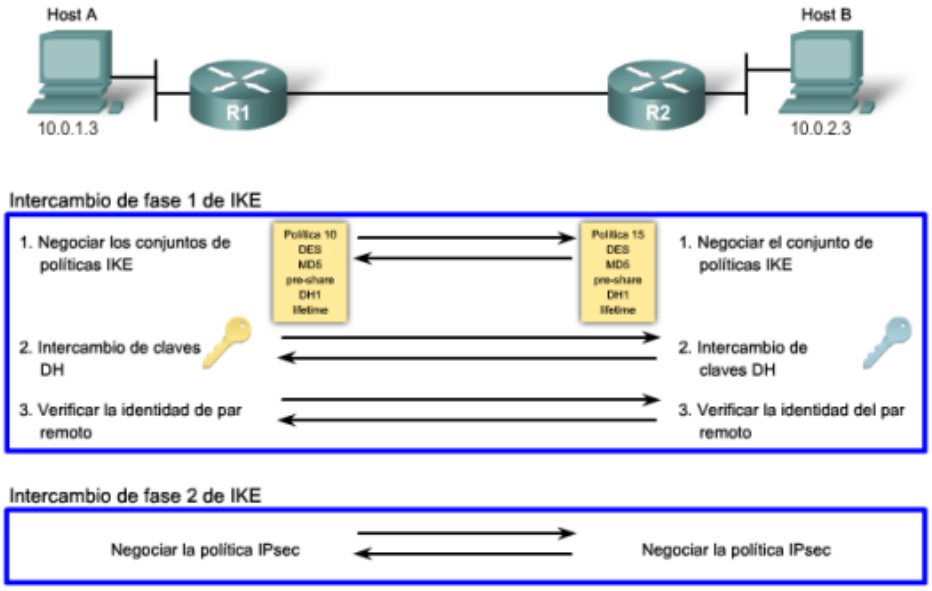


Fuente: Cisco Networking Academy (2017)

De acuerdo con (Cisco Networking Academy, 2016) para establecer un canal de comunicación segura entre dos pares, el protocolo IKE ejecuta dos fases:

"Fase 1. Dos pares IPsec realizan la negociación inicial de SAs. El propósito básico de la fase 1 es negociar los conjuntos de políticas IKE, y autenticar a los pares y establecer un canal seguro entre ellos" (Cisco Networking Academy, 2016, pág. 595). Durante el intercambio de fase 1 de IKE ocurren tres intercambios:

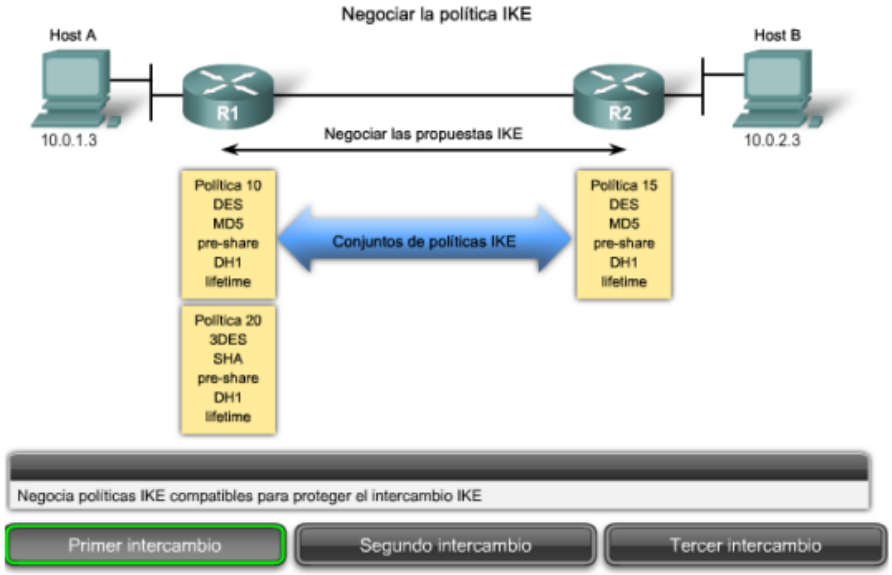
Figura 18: Fase 1 de IKE.



Fuente: Cisco Networking Academy (2017)

Nota: Primer intercambio. Se estable en un iniciador y el receptor para obtener la política básica de seguridad, los pares negocian y acuerdan los algoritmos y hashes que se utilizaran para asegurar las comunicaciones IKA, los llamados conjunto de políticas IKA son los primeros que se intercambian.

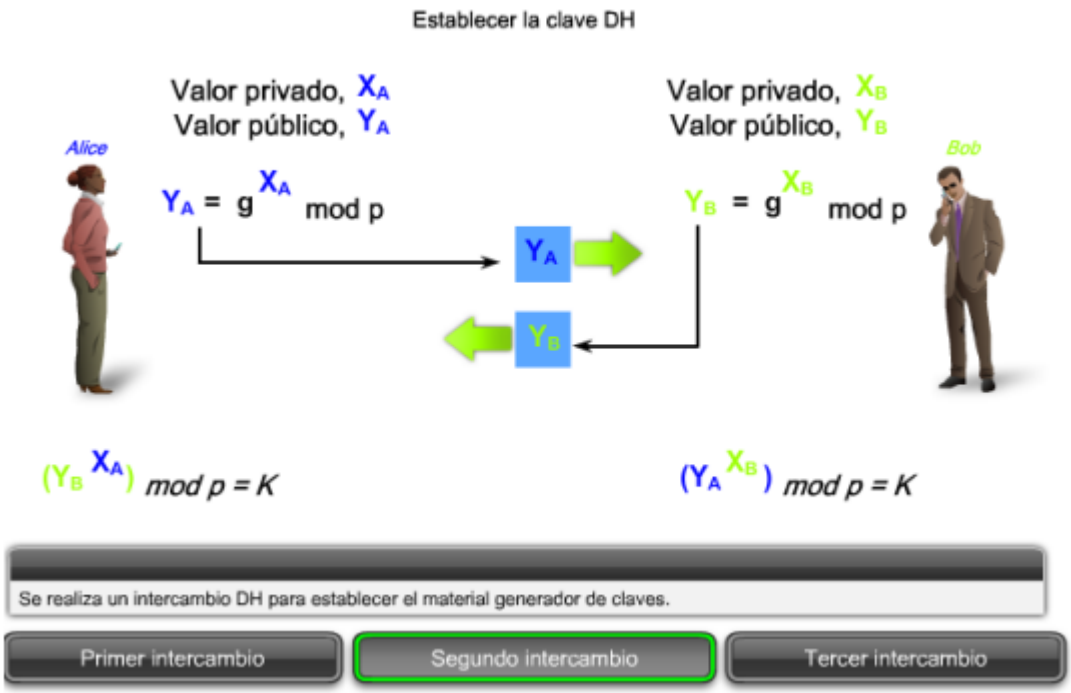
Figura 19: Intercambio 1 de IKE.



Fuente: Cisco Networking Academy (2017)

Nota: Segundo intercambio. Durante el segundo intercambio se crean e intercambian las claves publicas DH, estas permiten a los extremos participantes estableces una clave secreta compartida sobre un canal de comunicación no seguro, al ejecutar el protocolo de intercambio de claves DH se adquiere lo necesario para el cifrado y hashing por los algoritmos para que IKE e IPSec se pongan de acuerdo.

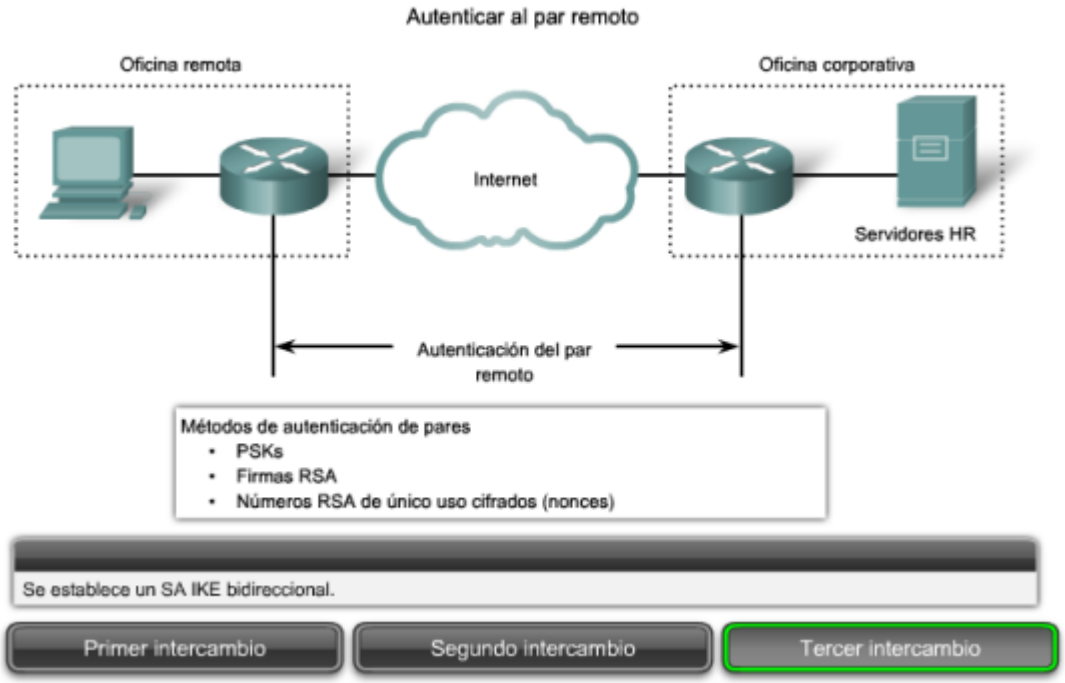
Figura 20: Intercambio 2 de IKE.



Fuente: Cisco Networking Academy (2017)

Tercer intercambio. En este último intercambio de la fase 1 de IKE un dispositivo debe autenticar al otro extremo antes de considerar seguro el camino de la comunicación, esto lo realizan utilizando uno de los tres métodos de autenticación de datos de origen: PSK firma RSA número cifrado de un solo uso RSA.

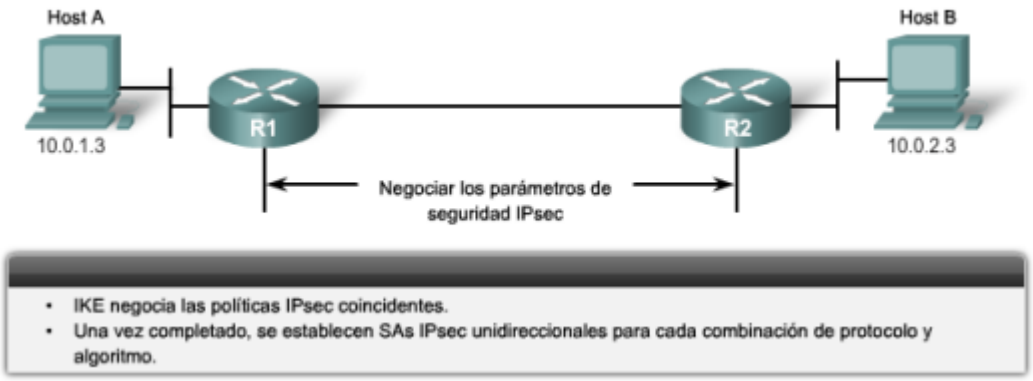
Figura 21: Intercambio 3 de IKE.



Fuente: Cisco Networking Academy (2017)

Fase 2. (Cisco Networking Academy, 2016) Nos dice que en esta fase el proceso IKE ISAKMP en esta fase negocia los SAs en nombre de IPsec, para ello IKE ejecuta la negociación de los parámetros de seguridad IPSec, establece las SAs IPSec y las renegocia periódicamente, para asegurar la seguridad realizando un intercambio DH adicional, el modo rápido también renegocia una nueva SA IPSec cuando el tiempo de vida de una SA expira, es decir el modo rápido refresca los datos de generación de claves que crea la clave secreta compartida, esto basada en los datos de generación de claves derivados del intercambio DH en la fase 1.

Figura 22: Intercambio 1 de DH.



Fuente: Cisco Networking Academy (2017)

2.2.8. Cisco IOS

Según (Cisco Networking Academy, 2017) el sistema operativo Internetwork (IOS, Internetwork Operating System) de Cisco es un término genérico para la colección de sistemas operativos de red que se utilizan en la mayoría de los dispositivos de red Cisco independientemente de su tamaño o el tipo, los dispositivos de red utilizados para conectar a Internet requieren un sistema operativo que los ayude a realizar sus funciones, la forma de interactuar con los sistemas operativos de un dispositivo puede realizarse mediante la interfaz de línea de comandos CLI o la interfaz gráfica, cuando se emplea CLI se interactúa con el sistema introduciendo comandos con el teclado mediante una ventana de petición de entrada de comandos, esto se ejecuta y proporciona una respuesta en forma de texto, pero este modo requiere de mayor conocimiento de la sintaxis a utilizar, en comparación el modo GUI que es más fácil de usar y requiere un menor conocimiento de la estructura de comandos a utilizar.

Figura 23: Sistema Operativo Cisco IOS.

Fuente: Cisco Networking Academy (2017)

2.2.8.1. Ubicación de IOS.

El archivo IOS en si tiene un tamaño en Mb y se encuentra almacenado en un área de memoria llamada flash, la cual provee un almacenamiento no volátil, si bien no se borra al apagarse esta puede ser modificada o sobrescribirse a necesidad, esto permite actualizar el IOS a una versión más reciente agregándole nuevas características sin reemplazar el hardware, y también esta memoria sirve para almacenar varias versiones del IOS, y cuando se enciende el dispositivo el IOS se copia a la RAM y se ejecuta desde ahí, de esta forma aumenta el rendimiento del dispositivo, es posible que los requisitos de las versiones más recientes de IOS exijan más memoria RAM y flash de la que puede instalarse en algunos dispositivos (Cisco Networking Academy, 2017).

2.2.8.2. Funciones de IOS.

Los dispositivos como routers y switches que utilizan Cisco IOS realizan funciones de las cuales dependen los profesionales de red para hacer que sus redes funcionen de la forma correcta y las principales funciones son: seguridad de la red, direccionamiento IP de interfaces virtuales y físicas, optimización de la conectividad, enrutamiento, habilitación de tecnologías como QoS y compatibilidad con otras tecnologías de administración de red (Cisco Networking Academy, 2017).

2.2.8.3. Método de acceso a la consola.

"Existen varias formas de acceder al entorno de la CLI" (Cisco Networking Academy, 2017, pág. 74). Los métodos más comunes son los siguientes: Consola, Telnet, **SSH o** Puerto auxiliary.

2.2.8.3.1. Consola.

El puerto consola en el puerto de administración que proporciona acceso fuera de banda a los dispositivos de Cisco, esto se refiere que es un acceso mediante un canal de administración dedicado y que se utiliza únicamente para el mantenimiento del dispositivo, la ventaja de este puerto es que posible acceder al dispositivo incluso sin haber configurado ningún servicio, para acceder también se requiere de un software de emulación de terminal que se instala en una PC, también este puerto se utiliza cuando fallan los servicios de red y no es posible acceder al dispositivo de manera remota, para mayor seguridad este puerto consola también se le debe configurar una contraseña para evitar accesos no autorizados (Cisco Networking Academy, 2017).

2.2.8.3.2. Telnet.

Es un método para establecer una sesión de CLI en un dispositivo de forma remota a diferencia de la conexión de consola, la sesión Telnet requiere servicios de red activos en el dispositivo, es decir debe tener al menos una interfaz configurada para el acceso por Telnet, para ello se requiere la asignación de una dirección IP a dicha interfaz, un dispositivo Cisco IOS contiene clientes Telnet, esto permite acceder a otros dispositivos que admitan el proceso de servidor Telnet (Cisco Networking Academy, 2017).

2.2.8.3.3. SSH.

El protocolo Shell Seguro (SSH) proporciona un acceso remoto similar al de Telnet, porque proporciona autenticación de contraseña y usa encriptación cuando transporta datos de la sesión, y es la más recomendad para el acceso a los dispositivos Cisco IOS, la mayoría de las versiones de Cisco IOS incluyen un servido SSH, otros requieren que se habilite de forma manual, también se incluyen un cliente SSH (Cisco Networking Academy, 2017).

2.2.8.3.4. Puerto Auxiliary.

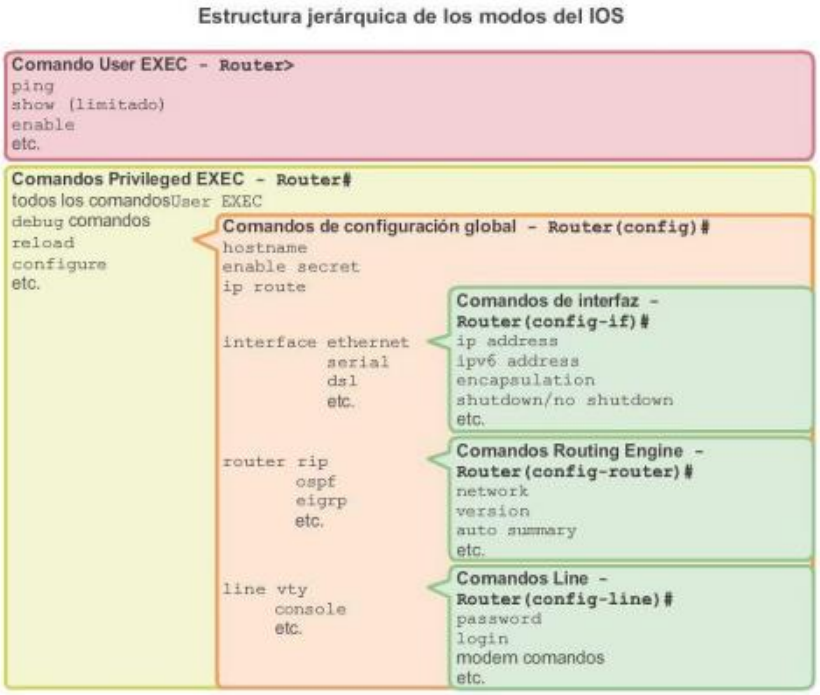
Es una forma antigua de establecer una sesión CLI de manera remota, por una conexión telefónica de dial-up con un modem conectado al puerto auxiliar del dispositivo router, al igual que la conexión de consola este método también es una conexión fuera de banda y no requiere la configuración ni la disponibilidad de ningún servicio de red en el dispositivo (Cisco Networking Academy, 2017).

2.2.8.4. Modos de funcionamiento de Cisco IOS.

Una vez que se conecta a un dispositivo un técnico puedo navegar por diversos modos del IOS, se utiliza una estructura jerárquica para los modos, desde el más básico hasta el más especializado y los modos principales son: Modo de usuario

EXEC de usuario, modo de ejecución privilegiado EXEC privilegiado, modo de configuración global y otros modos de configuración (Cisco Networking Academy, 2017).

Figura 24: Estructura IOS.



Fuente: Cisco Networking Academy (2017)

2.2.9. Modelo OSI

El modelo OSI fue diseñado por la ISO para proporcionar un marco sobre el cual crear una suite de protocolos de sistemas abiertos, se tenía la visión de que este conjunto de protocolos se utilizara para desarrollar una red mundial que no dependa de sistemas exclusivos, la velocidad a la que fue adoptada Internet basada en TCP/IP y la proporción en la que se expandió ocasionaron que el desarrollo y la aceptación de la suite de protocolos OSI quedaran atrás, aunque estos protocolos que se crearon con las especificaciones OSI se utilizan ampliamente en la actualidad, este modelo de siete capas hizo más contribuciones al desarrollo que otros protocolos y productos, OSI proporciona una amplia lista de funciones

y servicios que se pueden presentar en cada capa, y describen la interacción de cada capa con las capas directamente por encima y debajo de él (Cisco Networking Academy, 2017).

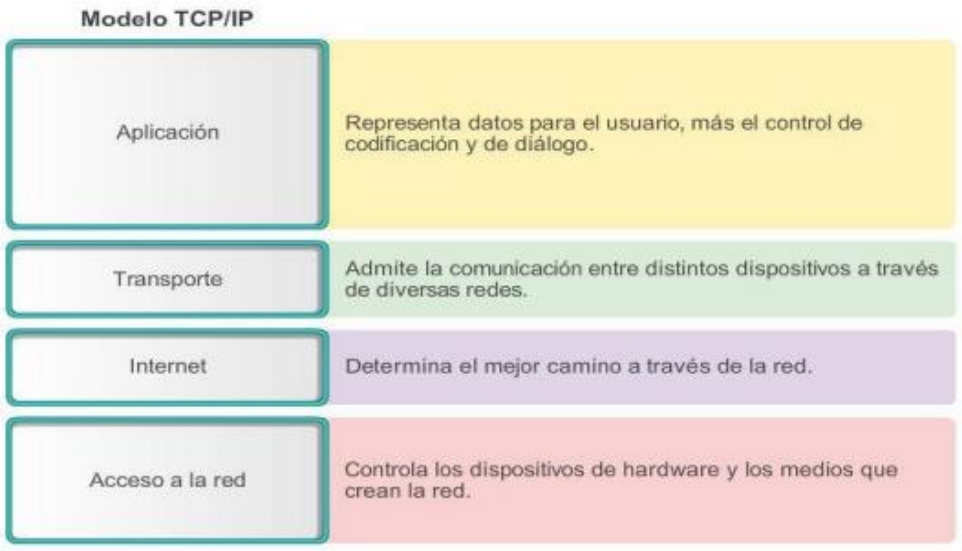
Figura 25: Modelo OSI.

Fuente: Cisco Networking Academy (2017)

2.2.10. Modelo TCP/IP

Este modelo TCP/IP se creó a principios de la década de los setenta y se conoce con el nombre de modelo de Internet, y se define cuatro categorías de funciones que deben ocurrir para que las comunicaciones se lleven a cabo correctamente, esta suite de protocolos TCP/IP es un estándar abierto, es decir ninguna compañía controla la definición del modelo, sus definiciones y protocolos TCP/IP se explican en un foro público en conjunto con la RFC disponibles al público, estas RFC contienen las especificaciones formales de los protocolos de comunicación de datos y los recursos que describen su uso, las RFC también contienen documentos técnicos y organizacionales sobre internet, que incluyen especificaciones técnicas y documentos de las políticas elaboradas por la IETF (Cisco Networking Academy, 2017).

Figura 26: Modelo TCP/IP.



Fuente: Cisco Networking Academy (2017)

2.2.11. Comparación entre modelo OSI y TCP/IP

La suite de protocolos TCP/IP se pueden describir en términos del modelo de referencia OSI, en el modelo OSI, la capa de acceso a la red y la capa de aplicación de modelo TCP/IP están subdivididas a fin de describir funciones que deben producirse en estas capas, la capa de acceso a la red en TPC/IP no especifica que protocolos deben utilizar cuando se transmite por un medio físico, y solo se describe la transferencia desde la capa de Internet hacia los protocolos de red física, en las capas 1 y 2 del modelo OSI se trata los procedimientos necesarios para acceder a los medios y las maneras físicas de enviar los datos a través de una red, en la capa de red o capa 3 del modelo OSI, se utiliza de manera casi universal para describir el alcance de los procesos que ocurren en todas las redes que se encargan de dirigir y enrutar los mensajes a través de una internetwork, mientras que IP es el protocolo de TCP/IP que incluye la funcionalidad descrita en la capa 3 de modelo OSI, en la capa 4 o capa de transporte de OSI se describen los

servicios y funciones que proporcionan la entrega ordenada y confiable de datos entre el origen y destino, estas funciones incluyen acuse de recibo, recuperación de errores y secuenciamiento, en TPC/IP el protocolo TCP y UDP proporcionan la funcionalidad necesaria, y para la capa de aplicación de TCP/IP se incluyen protocolos de funcionalidad específica a una variedad de aplicaciones del usuario, mientras en el modelo OSI las capas 5, 6 y 7 se utilizan como referencia para proveedores y desarrolladores de software de aplicación para fabricar productos que funcionan en redes (Cisco Networking Academy, 2017).

Figura 27: Modelo OSI vs TCP/IP.

Fuente: Cisco Networking Academy (2017)

2.3. DEFINICIÓN DE TÉRMINOS BÁSICOS

2.3.1. VPN

Según (Cisco, 2021), es una conexión cifrada que garantiza la transmisión de datos segura y confidencial, y evita que personas no autorizadas tengan acceso y espíen la información enviada, también permiten el trabajo remoto de usuarios ligados a empresas

2.3.2. IPSec

De acuerdo con (OSTEC Seguridad Digital de Resultados, 2016), es un protocolo que tiene por objetivo garantizar comunicaciones privadas y seguras utilizando servicios de seguridad criptográficos, que garantizan la privacidad, integridad y autenticidad de la información enviada.

2.3.3. Modo tunnel

(Cisco Networking Academy, 2016), nos indica que este modo provee seguridad para el paquete IP, por lo cifra y empaqueta en otro paquete, el cual es conocido como cifrado de IP en IP, que se utiliza el enrutamiento a través de internet.

2.3.4. Intercambios de claves en Internet (IKE)

Nos indica (Cisco Networking Academy, 2016), que es un componente fundamental de las VPNs Ipsec SSL.

2.3.5. Asociaciones de seguridad (SA)

Para (Cisco Networking Academy, 2016) las asociaciones de seguridad son un bloque de construcción básica de IPSec, que se mantiene en un base de datos en el dispositivo, y en esta se registran los parámetros de cifrado IPSec y el intercambio de claves.

CAPITULO III

MATERIALES Y MÉTODOS

3.1. TIPO Y DISEÑO DE INVESTIGACIÓN

3.1.1. Tipo De Investigación

La presente investigación es de tipo aplicada, ya que el propósito de la investigación es la implementación real de una Red Privada Virtual en las sucursales de la Caja Rural de Ahorro y Crédito los Andes SA para la conexión de estas hasta su sede principal.

Así como lo define (Lozada, 2014), La investigación aplicada busca la generación de conocimiento con aplicación directa a los problemas de la sociedad o el sector productivo. Esta se basa fundamentalmente en los hallazgos tecnológicos de la investigación básica, ocupándose del proceso de enlace entre la teoría y el producto.

3.1.2. Diseño De Investigación

De acuerdo con (Hernández Sampieri , Fernández Collado, & Baptista Lucio , 2014) “Los diseños cuasi experimentales manipulan deliberadamente al menos una variable independiente para ver su efecto y relación con una a más variables dependientes” (Pág. 184), es por ello por lo que el tipo de diseño de investigación que corresponde es cuasi experimental, ya que la implementación que se realiza es un grupo seleccionado, y el diseño tiene el siguiente diagrama:

G1 O1 X O2… (Ec.1)

Donde:

G1: Caja Rural de Ahorro y Crédito los Andes SA.

O1 y O2: Observación Pre y Post Prueba.

X: Diseño e Implementación de VPN IPSec

3.2. POBLACIÓN Y MUESTRA DE INVESTIGACIÓN

3.2.1. Población

La población es un "Conjunto de todos los casos que concuerdan con determinadas especificaciones" (Hernández Sampieri , Fernández Collado, & Baptista Lucio , 2014, pág. 174). La población que se manejara en el presente trabajo de investigación es finita, ya que Según (Ramirez, 2010, pág. 92) la población finita "es aquella cuyos elementos en su totalidad son identificables por el investigador, por lo menos desde el punto de vista del conocimiento que se tiene sobre su cantidad total".

Teniendo conocimiento de ello la población son las 103 sucursales remotas de la Caja Rural de Ahorro y Crédito los Andes SA.

3.2.2. Muestra

Para la presente investigación la muestra es dirigida, y según (Hernández Sampieri , Fernández Collado, & Baptista Lucio , 2014) "Las muestras no probabilísticas, también llamadas muestras dirigidas, suponen un procedimiento de selección orientado por las características de la investigación, más que por un criterio estadístico de generalización. Se utilizan en diversas investigaciones cuantitativas y cualitativas" (Pág. 189).

> Aquí el procedimiento no es mecánico ni se basa en fórmulas de probabilidad, sino que depende del proceso de toma de decisiones de un investigador o de un grupo de investigadores y, desde luego, las muestras seleccionadas obedecen a otros criterios de investigación. Elegir entre una muestra probabilística o una no probabilística depende del planteamiento del estudio, del diseño de investigación y de la contribución que se piensa hacer con ella, para la presente investigación la selección de la muestra será a conveniencia (Cosio Dueñas, 2016).

La muestra que se toma son 4 sucursales Acora, Coata, Taraco y Yunguyo de la Caja Rural de Ahorro y Crédito los Andes SA, seleccionadas a criterio por el investigador.

3.2.3. Ubicación De La Población

Caja Rural de Ahorro y Crédito Los Andes SA.

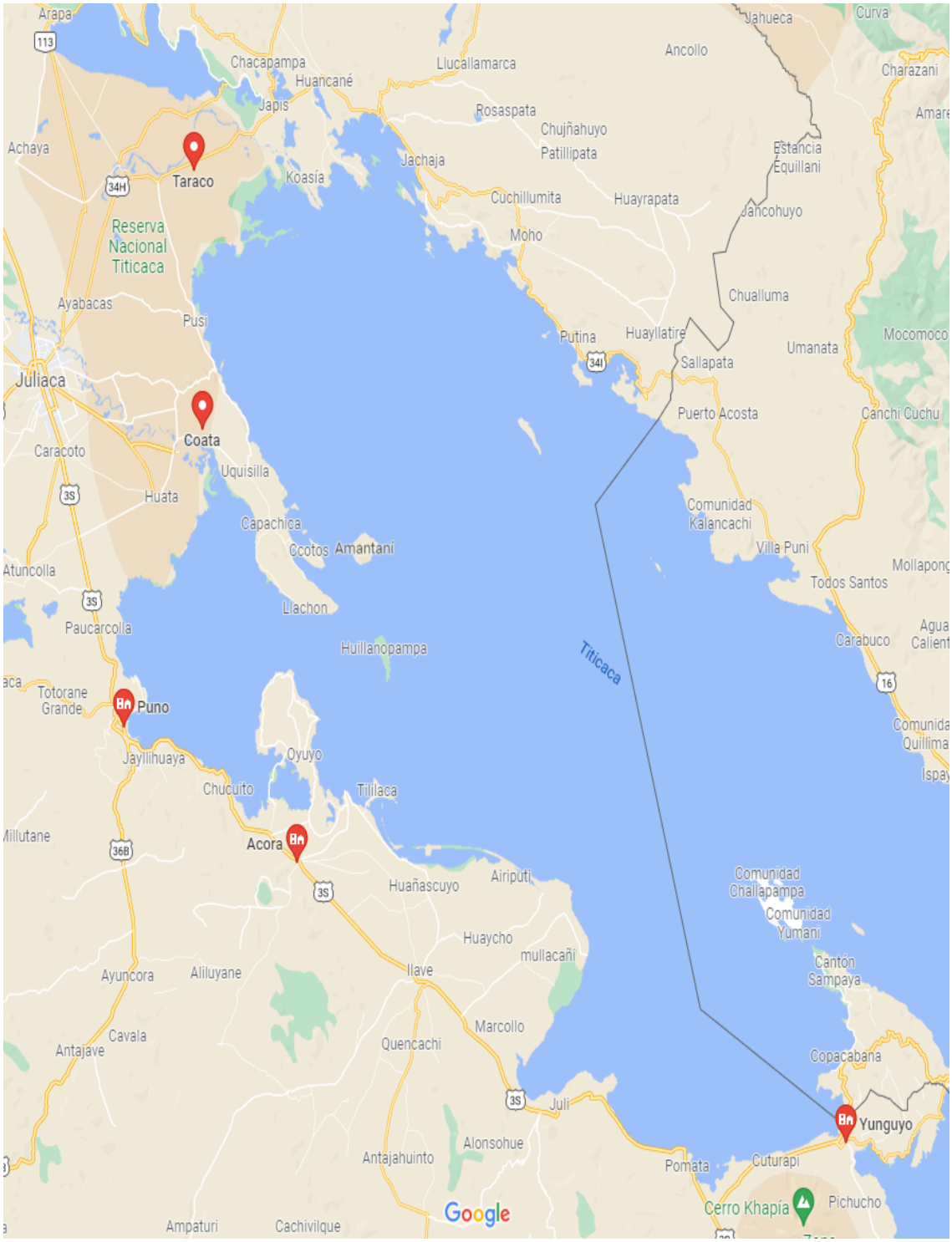
Gerencia de Tecnologías de Información.

Centro de Datos.

Dirección, Jr Junín 129, Puno

SUCURSAL PRINCIPAL	:	PUNO – PUNO – PUNO
SUCURSAL ACORA	:	ACORA – PUNO – PUNO
SUCURSAL COATA	:	COATA – PUNO – PUNO
SUCURSAL TARACO	:	TARACO – HUANCANE – PUNO
SUCURSAL YUNGUYO	:	YUNGUYO – YUNGUYO – PUNO

Figura 28: Ubicación de las sucursales.



Fuente: (google maps, 2022)

3.3. MATERIAL EXPERIMENTAL

3.3.1. Hardware

DISPOSITIVO: Router Cisco 800 Series

CANTIDAD: 05

DESCRIPCION: Cisco 881 Ethernet Security Router

Tipo de dispositivo: Encaminador + conmutador de 4 puertos (integrado), Factor de forma: Externo, Dimensiones (Ancho x Profundidad x Altura): 32.5 cm x 24.9 cm x 4.4 cm, Memoria RAM: 256 MB (instalados) / 768 MB (máx.), Memoria Flash: 128 MB, Protocolo de direccionamiento: OSPF, RIP-1, RIP-2, BGP, EIGRP, HSRP, VRRP, NHRP, GRE, Protocolo de interconexión de datos: Ethernet, Fast Ethernet, Red / Protocolo de transporte: L2TP, IPSec, Protocolo de gestión remota: Telnet, SNMP 3, HTTP, HTTPS, SSH, Características: Cisco IOS Advanced IP services , soporte de NAT, Puerto de estado de interrupción (ISP), soporte VLAN, señal ascendente automática (MDI/MDI-X automático), snooping IGMP, Stateful Packet Inspection (SPI), filtrado de contenido, filtrado de dirección MAC, soporte IPv6, Stateful Failover, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Fair Queuing (WFQ), soporte de Access Control List (ACL), Quality of Service (QoS), Dynamic Multipoint VPN (DMVPN), Servidor DHCP, Virtual Route Forwarding-Lite (VRF-Lite), DNS proxy, Cumplimiento de normas: IEEE 802.1D, IEEE 802.1Q, IEEE 802.1x, Alimentación: CA 120/230 V (50/60 Hz) (Intercompras Comercio Electrónico SA de CV, 2022).

Figura 29: Cisco 800 Series.

Fuente: Cisco Networking Academy (2017)

DISPOSITIVO : Router TP – Link TL-MR3420

CANTIDAD : 03

DESCRIPCION :

El Router TP-LINK TL-MR3420 le permite compartir una conexión móvil 3G / 4G en un área de cobertura 3G / 4G. Además, al conectar un módem USB UMTS/HSPA/EVDO a este router, se crea inmediatamente un punto de acceso público 3G. Conexión fiable y eficiente Gracias a su tecnología CCA, el router evita conflictos para garantizar la máxima estabilidad de la señal. Además, una segunda conexión "de reserva" permite a los usuarios permanecer conectados, incluso cuando se interrumpe la conexión principal.

Funciones avanzadas Fácil de usar y configurar, el TP-LINK TL-MR3420 tiene características avanzadas que son muy convenientes de usar: Con sólo pulsar un botón en el router, el cifrado WPA / WPA2 protege sus datos contra conexiones no autorizadas. Un sistema de control permite al administrador de la red determinar el ancho de banda asignado a cada ordenador.

Principales características

Router Wi-Fi N 300 Mbps y 3G / 4G

Compatible con módems 3G/4G USB UMTS/HSPA/EVDO

Cifrado de datos (WPA / WPA2) con sólo pulsar un botón

Control de ancho de banda: determinar el ancho de banda asignado a cada ordenador.

Segunda conexión “de reserva": los usuarios permanecen en línea incluso cuando se interrumpe una conexión.

Compatible con PPPoE, Dynamic IP, Static IP, PPTP y L2TP

Tecnología CCA para una máxima estabilidad y prevención de conflictos

Lista de compatibilidad de los módems USB 3G/3.75G

Figura 30: Router TP-LINK 3420.

Fuente: (Tp-Link, 2022)

DISPOSITIVO : Router ADSL

CANTIDAD : 01

DESCRIPCION :

El router ADSL o encaminador ADSL (Asymmetric Digital Subscriber Line) de línea de abonado digital asimétrica, es un dispositivo que permite conectar al mismo tiempo uno o varios equipos o incluso una o varias redes de área local (LAN).

DISPOSITIVO : Modem USB 3G/4G

CANTIDAD : 03

DESCRIPCION :

Un módem externo USB es un módem de aproximadamente el tamaño de una unidad flash que se conecta al ordenador a través del puerto USB. Estos módems se utilizan casi exclusivamente para conectar a las conexiones de banda ancha móvil, y también a veces se llaman dispositivos de seguridad. La banda ancha móvil le permite conectarse a Internet en cualquier lugar que usted puede conseguir la recepción de su proveedor de servicios móviles. Mientras que las características específicas varían entre los modelos y fabricantes.

El módem USB no es un simple dispositivo de almacenamiento de datos. Este aparato, el cual se conecta a tu computadora mediante un puerto USB, te permite acceder a Internet mediante tecnología 3G o 4G a través de una de las redes del operador de telefonía móvil con el que tengas suscrito el contrato, La llave 3G o el módem USB son compatible con las computadoras fijas y portátiles y con cualquier tipo de sistema operativo, Además, en la actualidad, también se pueden utilizar con tabletas, siempre y cuando estas dispongan de un puerto USB, Es importante que sepas que los módems USB usan la conexión 3G y 4G, por tanto, la navegación es bastante más rápida de lo que ocurría en sus inicios y se acerca bastante a lo que podría ser el ADSL (KillMyBill, 2017).

DISPOSITIVO : Laptop

CANTIDAD : 01

DESCRIPCION :

Figura 31: Características de Laptop.

Elemento	Valor
Nombre del SO	Microsoft Windows 10 Pro
Versión	10.0.19042 compilación 19042
Descripción adicional del SO	No disponible
Fabricante del SO	Microsoft Corporation
Nombre del sistema	LL241A1120BO
Fabricante del sistema	LENOVO
Modelo del sistema	20F5A0G600
Tipo de sistema	PC basado en x64
SKU del sistema	LENOVO_MT_20F5_BU_Think_FM_ThinkPad X260
Procesador	Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz, 2400 Mhz, 2 procesadores princi...
Versión y fecha de BIOS	LENOVO R02ET74W (1.47), 15/09/2020
Versión de SMBIOS	2.8
Versión de controladora integr...	1.15
Modo de BIOS	UEFI
Fabricante de la placa base	LENOVO
Producto de placa base	20F5A0G600
Versión de la placa base	SDK0J40697 WIN
Rol de plataforma	Móvil
Estado de arranque seguro	Activada
Configuración de PCR7	Enlace posible
Directorio de Windows	C:\WINDOWS
Directorio del sistema	C:\WINDOWS\system32
Dispositivo de arranque	\Device\HarddiskVolume2
Configuración regional	España
Capa de abstracción de hardw...	Versión = "10.0.19041.1151"
Nombre de usuario	LL241A1120BO\Administrador de Red
Zona horaria	Hora est. Pacífico, Sudamérica
Memoria física instalada (RAM)	8.00 GB

Elaboración Propia

OTROS : Adaptador DB9 USB a Serial

CANTIDAD : 01

DESCRIPCION :

Este adaptador se puede utilizar para transformar un puerto USB en un puerto de comunicación serie RS-232 con un conector DB9 macho. Es ideal para la conexión de módem, PDA, GPS, dispositivos de medición, máquinas, herramientas industriales, etc.

OTROS : Cable Consola Serial Hembra a RJ-45

CANTIDAD : 01

DESCRIPCION :

El cable serie tiene una distancia de transmisión corta debido al ruido que limita la transmisión de un alto número de bits por segundo cuando el cable tiene más de 15 m de longitud, su función es “la interconexión de datos entre dispositivos digitales se establece generalmente utilizando cables seriales que se utilizan para transferir datos entre dispositivos los cuales utilizan técnicas de comunicación de bits desde un puerto hasta otro” (odalysicas, 2014, párr. 1).

OTROS : CHIP Internet Móvil

CANTIDAD : 03

DESCRIPCION :

Para (Fernandez, 2019) “la tarjeta SIM o Subscriber Identity Module es una pequeña tarjeta de plástico que tiene un chip pegado a ella, y que tienes que insertar en tu teléfono móvil o smartphone” (Párr. 1). En este chip, almacena de manera segura tu número de teléfono, así como las claves de acceso de un usuario concreto en una operadora de telefonía.

OTROS : Cable de Red

CANTIDAD : 12 Unidades de 1.5 m.

DESCRIPCION :

Para (WIKIPEDIA, 2021) “Cable de conexión (patch cord) también llamado cable de red se usa en redes de computadoras o sistemas informáticos o electrónicos para conectar un dispositivo electrónico con otro. Está compuesto por cobre y cubierto de plástico” (párr. 1).

3.3.2. Software

- Sistema Operativo Windows 10 Pro x64
- Microsoft Office 2013.

- Microsoft Visio 2013.
- Cisco IOS
- Putty.

3.3.3. Recursos Y Materiales

- Textos CCNA v5 200-125
- Texto CCNA Security 1.0
- Internet.

3.3.4. Servicios

- Internet ADSL Movistar
- Internet móvil

3.3.5. Presupuesto

Tabla 1: Presupuesto utilizado para la implementación.

Descripción	Unidad de medida	Costo Unitario (S/.)	Cantidad	Costo total (S/.)
Material de escritorio				
Papel Bond 80 grs. (A4)	Millar	S/50.00	1	S/50.00
Folder manila (A4)	Unidad	S/0.50	2	S/1.00
Lapiceros	Unidad	S/1.50	2	S/3.00
Resaltador de texto	Unidad	S/2.00	1	S/2.00
Engrapador	Unidad	S/15.00	1	S/15.00
Perforador	Unidad	S/20.00	1	S/20.00
Tóner impresor laser	Unidad	S/210.00	1	S/210.00
Equipos, dispositivos y servicios				
Laptop	Unidad	S/1,899.00	1	S/1,899.00
Cisco IOS 800 Series	Unidad	S/1,815.00	5	S/9,075.00
Router TP LINK TL-MR3420	Unidad	S/140.00	3	S/420.00
Modem USB Internet Móvil	Unidad	S/100.00	3	S/300.00
Router Telefonica Movistar ADSL	Unidad	S/96.00	2	S/192.00
Servicio Internet ADSL	Meses	S/189.91	1	S/189.91
Chip Internet Movil Datos	Meses	S/99.00	3	S/297.00
Adaptador db9 USB a Serial	Unidad	S/45.00	1	S/45.00
Impresora HP laser	Unidad	S/390.00	1	S/390.00
USB	Unidad	S/30.00	1	S/30.00
Viáticos para traslado				
Pasajes	Dia	S/20.00	10	S/200.00
Alimentación	Dia	S/30.00	10	S/300.00
Suministros de información virtual				
Servicio de internet	Meses	S/129.00	3	S/387.00
Encuadernación y empastados				
Empastado de borrador de tesis	Empastado	S/5.00	5	S/25.00
Empastado de tesis	Empastado	S/20.00	5	S/100.00
	TOTAL			S/14,150.91

Elaboración Propia

CAPITULO IV

RESULTADOS Y DISCUSIÓN

4.1. ANÁLISIS DE LA SITUACIÓN ACTUAL

La Caja Rural de Ahorro y Crédito los Andes SA actualmente viene realizando sus operaciones financieras mediante su CORE Financiero, esta aplicación realiza la transmisión de datos de las transacciones mediante una conexión de Red Privada Virtual, es por ello la necesidad de contratar a un proveedor de servicio, y la Gerencia de Tecnologías de Información está encargada de coordinar la instalación de una conexión de Red Privada virtual en las sucursales de Caja Rural de Ahorro y Crédito los Andes SA, para lo cual el encargado coordina la contratación del servicio del servicio de Red Privada Virtual con proveedores, que alcanzan sus propuestas las cuales son analizadas y evaluadas antes de su contratación, y los puntos más importantes son los tiempos de instalaciones, el costo de instalación y el costo mensual a pagar, por ello a continuación se detallan los costos y tiempo del proveedor contratado en las sucursales seleccionadas:

4.1.1. Análisis de Costo de Instalación Proveedor

Los costos que se indican en la siguiente tabla, fueron extraídos de la propuesta comercial y contrato realizado entre la entidad y el proveedor del servicio, y se toman en cuenta el costo de instalación y el costo de mantenimiento mensual para un periodo de contrato de 36 meses para el análisis de la investigación. El detalle en el Anexo D.

Tabla 2: Costo instalación y servicio Proveedor.

SUCURSAL	Costo de Instalación	Costo Mensual	Costo 36 Meses
ACORA	S/800.00	S/1,208.60	S/43,509.60
COATA	S/800.00	S/970.80	S/34,948.80
TARACO	S/800.00	S/1,208.60	S/43,509.60
YUNGUYO	S/800.00	S/970.80	S/34,948.80
Total	S/3,200.00	S/4,358.80	S/156,916.80

Elaboración Propia

4.1.2. Análisis de Tiempo de Instalación Proveedor

A continuación, se muestra el detalle de las actividades y el tiempo en días que le tomó al proveedor realizar la instalación del servicio de Red Privada Virtual en las sucursales seleccionas de la Caja Rural de Ahorro y Crédito los Andes SA, los cuales se utilizaran para realizar la comparación con los tiempos obtenidos durante el desarrollo del proyecto.

Tabla 3: Tiempo Instalación Proveedor.

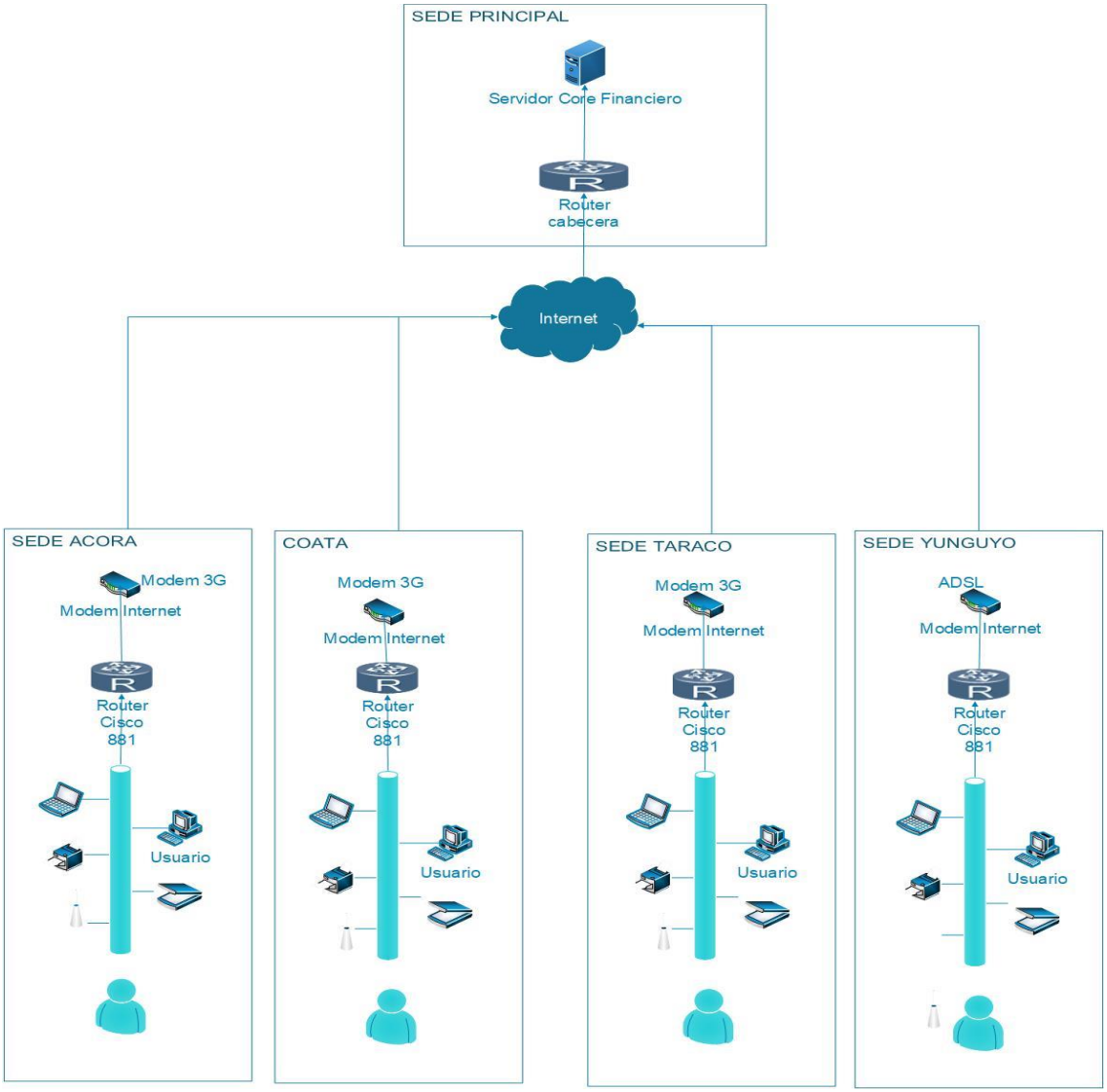
SUCURSAL	ACTIVIDAD	RESPONSABLE	TIEMPO DE INSTALACION PROVEEDOR (Días)
ACORA	Estudio de Factibilidad	CLARO	7
	Elaboración de Propuesta Técnica	CLARO	7
	Elaboración de contrato	CLARO	7
	Evaluación y aprobación para contratar el servicio	ENTIDAD	15
	Tiempo de instalación	CLARO	31
	Subtotal (Días)		**67**
COATA	Estudio de Factibilidad	CLARO	7
	Elaboración de Propuesta Técnica	CLARO	7
	Elaboración de contrato	CLARO	7
	Evaluación y aprobación para contratar el servicio	ENTIDAD	15
	Tiempo de instalación	CLARO	20
	Subtotal (Días)		**56**
TARACO	Estudio de Factibilidad	CLARO	7
	Elaboración de Propuesta Técnica	CLARO	7
	Elaboración de contrato	CLARO	7
	Evaluación y aprobación para contratar el servicio	ENTIDAD	15
	Tiempo de instalación	CLARO	20
	Subtotal (Días)		**56**
YUNGUYO	Estudio de Factibilidad	CLARO	7
	Elaboración de Propuesta Técnica	CLARO	7
	Elaboración de contrato	CLARO	7
	Evaluación y aprobación para contratar el servicio	ENTIDAD	15
	Tiempo de instalación	CLARO	25
	Subtotal (Días)		**61**

Elaboración Propia

4.2. PROCESO DE DISEÑO E IMPLEMENTACIÓN

4.2.1. Diseño de Topología Física

Figura 32: Diseño de Topología Física.

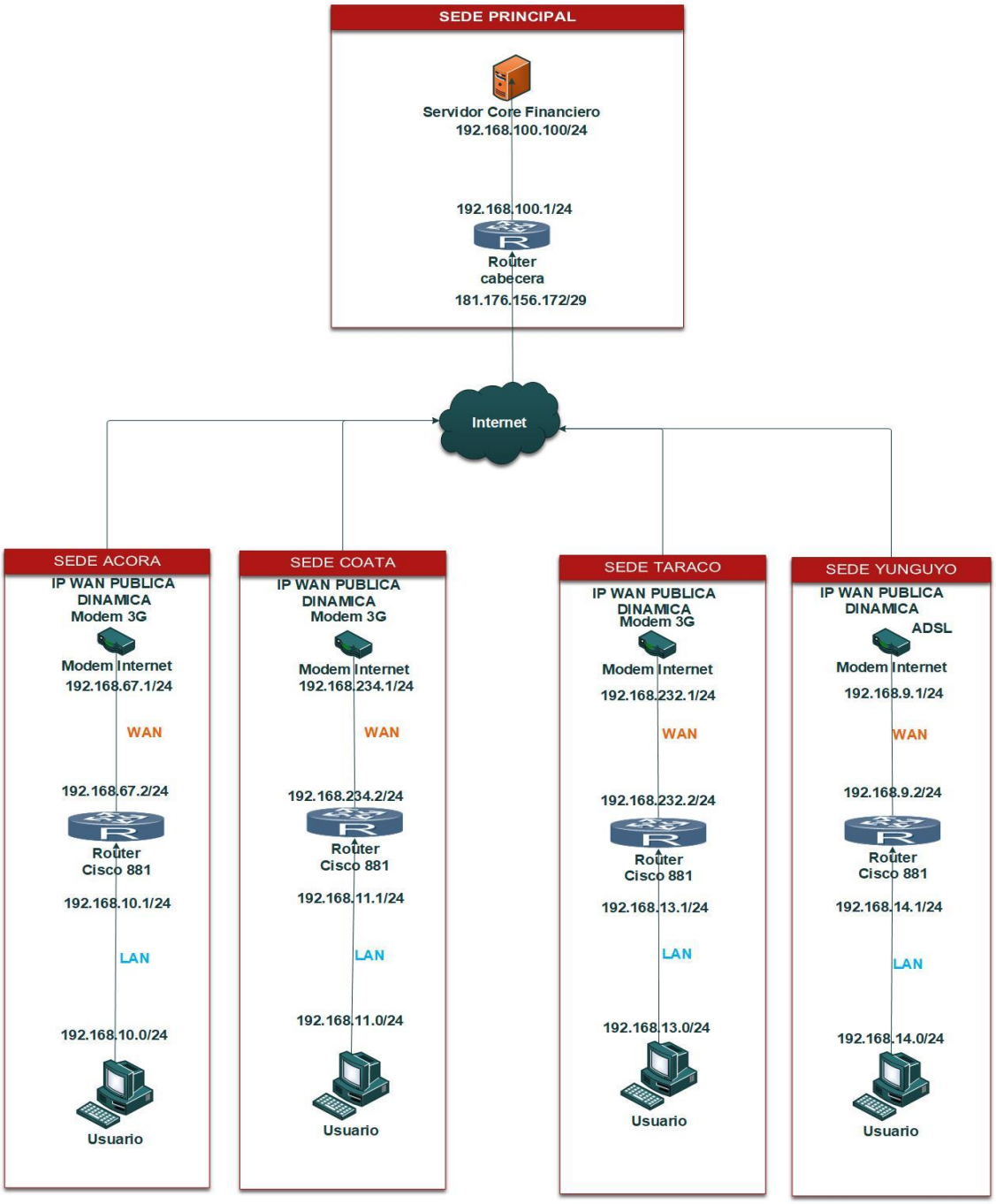


Elaboración Propia

Nota. La Figura representa el diseño de las instalaciones física de los equipos en las sucursales de la Caja Rural de Ahorro y Crédito los Andes SA.

4.2.2. Diseño de Topología Lógica.

Figura 33: Diseño de Topología Lógica.



Elaboración Propia

Nota. La Figura 33 indica la distribucion logica que sera implementada en las sucursales de la Caja Rural de Ahorro y Credito los Andes SA.

4.2.3. Asignación de Direccionamiento IP

Tabla 4: Direccionamiento de IP.

SUCURSAL	Dispositivo	Dirección IP	Mascara	Gateway	Puerto
SEDE PRINCIPAL	Router Cabecera	192.168.100.1	255.255.255.0		Fa 0
		181.176.156.172	255.255.255.248	181.168.156.169	Fa 0
	SERVER	192.168.100.100	255.255.255.0	192.168.100.1	NIC
ACORA	Router Cisco 881	192.168.10.1	255.255.255.0		Fa 0
		192.168.67.2	255.255.255.0	192.168.67.1	Fa 4
	Modem 3G Internet	192.168.67.1	255.255.255.0		Fe 1
		Publica			móvil 3G/4G
	Usuario	192.168.10.10	255.255.255.0	192.168.10.1	NIC
COATA	Router Cisco 881	192.168.11.1	255.255.255.0		Fa 0
		192.168.234.2	255.255.255.0	192.168.234.1	Fa 4
	Router Modem 3G/4G	192.168.234.1	255.255.255.0		Fe 1
		Publica			móvil 3G/4G
	PC	192.168.11.10	255.255.255.0	192.168.11.1	NIC
TARACO	Router Cisco 881	192.168.13.1	255.255.255.0		Fa 0
		192.168.232.2	255.255.255.0	192.168.232.1	Fa 4
	Router Modem 3G/4G	192.168.232.1	255.255.255.0		Fe 1
		Publica			3G/4G
	PC	192.168.13.10	255.255.255.0	192.168.13.1	NIC
YUNGUYO	Router Cisco 881	192.168.14.1	255.255.255.0		Fa 0
		192.168.9.2	255.255.255.0	192.168.9.1	Fa 4
	Router ADSL	192.168.9.1	255.255.255.0		Fe 1
		Publica			3G/4G
	PC	192.168.14.10	255.255.255.0	192.168.14.1	NIC

Elaboración Propia

4.2.4. Proceso De Instalación Y Configuración

4.2.4.1. Instalación.

Figura 34: Instalación Sucursal Acora.

Elaboración Propia

Nota. La Figura 34 muestra las instalaciones de los equipos routers cisco y demas equipos necesarios para el funcionamiento de la VPN IPSec, en la Sucursal de Acora.

Figura 35: Instalación Sucursal Coata.

Elaboración Propia

Nota. La Figura 35 muestra las instalaciones de los equipos routers cisco y demas equipos necesarios para el funcionamiento de la VPN IPSec, en la Sucursal de Coata.

Figura 36: Instalación Sucursal Taraco.

Elaboración Propia

Nota. La Figura 36 muestra las instalaciones de los equipos routers cisco y demas equipos necesarios para el funcionamiento de la VPN IPSec, en la sucursal de Taraco.

Figura 37: Instalación Sucursal Yunguyo.

Elaboración Propia

Nota. La Figura 37 muestra las instalaciones de los equipos routers cisco y demas equipos necesarios para el funcionamiento de la VPN IPSec en la sucursal de Yunguyo.

4.2.4.2. Configuración.

La configuración del router principal se encuentra en el ANEXO A, sin embargo, se presenta la configuración Principal y configuración genérica de las sucursales:

Tabla 5: Descripción de configuración sede principal.

Configuración Sucursal Principal	
Comando IOS	Descripción
crypto isakmp policy 1	Creación de política ISAKMP. Cada política se identifica de una única forma por el número de prioridad que se le asigna y para el caso es 1.
encr 3des	Algoritmo de cifrado. Triple DES (3DES), se utiliza cuando las longitudes de las claves son iguales, aunque AES es el estándar de cifrado más fuerte.
hash md5	Algoritmo Hash Utilizado. MD5 tiene una salida de 128 a diferencia que SHA-256 que tiene 256, sin embargo, MD5 se considera más rápido SHA-256, con MD5 se puede verificar rápidamente la integridad al usarlo como suma de verificación, podemos asegurar que el archivo en ambos lados es el mismo.
authentication pre-share	Método de autenticación de identidad. Se especifica una clave compartida y registrada en ambos lados de la conexión.
group 2	Identificador de grupo Diffie-Hellman. Se utiliza el grupo 2 por ser de 1024 bits, y a mayor numero el grupo más seguro, pero a la vez se requiere de mayor tiempo para computar la clave, y para el caso se recomienda el 2.
crypto isakmp key $$VPNIPsec#CRAC119$$ address 0.0.0.0 0.0.0.0	Contraseña compartida, y dirección IP de asociación, para el proyecto como no se tiene IP estática en las sucursales se configura aceptar cualquier origen.
crypto isakmp keepalive 60 30 periodic	Mantiene las conexiones de comunicación de una red que no están terminadas y se mantienen hasta que el cliente o servidor interrumpe la conexión.
crypto ipsec transform-set TS esp-3des esp-md5-hmac	Parte de la política donde se define parámetros de seguridad para la negociación de IPSec SA.
mode tunnel	El modo de túnel IPsec ESP cifra y encapsula los paquetes IP al tiempo que proporciona autenticación e integridad.

(continuación...)	
crypto dynamic-map hq-vpn 10 **set security-association lifetime seconds 86400** **set transform-set TS** **match address <<NOMBRE-SEDE>>**	Creación de mapas crypto dinámicos, que no exige parámetros como el par IP, se establece tiempo de renovación de SA, se asocia la lista de acceso a nombre de cada sucursal.
ip access-list extended <<NOMBRE-SEDE>> **permit ip 192.168.100.0 0.0.0.255 192.168.10.0 0.0.0.255**	Se crea la lista de acceso con el segmento de IP permito como destino para cada sucursal que se conectara de forma dinámica. Esta línea se repite por cada sucursal remota.
crypto map VPN-BO 1 ipsec-isakmp dynamic hq-vpn	Vincula el mapa dinámico a IPSec.
interface FastEthernet4 **ip address 181.176.156.172 255.255.255.248** **ip mtu 1400** **ip tcp adjust-mss 1300** **duplex auto** **speed auto** **crypto map VPN-BO**	Configuración de la interfaz WAN con ip publica estática y la asignación de crypto map creado.

Elaboración Propia

Nota. La Tabla 5 contiene la configuración realizada en el router de Cabecera que se encuentra en la sede principal.

Tabla 6: Descripción de configuración sede remota.

Configuración Sede Remota	
Comando IOS	Descripción
crypto isakmp policy 1	Creación de política ISAKMP. Cada política se identifica de una única forma por el número de prioridad que se le asigna y para el caso es 1.
encr 3des	Algoritmo de cifrado. Triple DES (3DES), se utiliza cuando las longitudes de las claves son iguales, aunque AES es el estándar de cifrado más fuerte.

(continuación...)	
hash md5	Algoritmo Hash Utilizado. MD5 tiene una salida de 128 a diferencia que SHA-256 que tiene 256, sin embargo, MD5 se considera más rápido SHA-256, con MD5 se puede verificar rápidamente la integridad al usarlo como suma de verificación, podemos asegurar que el archivo en ambos lados es el mismo.
authentication pre-share	Método de autenticación de identidad. Se especifica una clave compartida y registrada en ambos lados de la conexión.
group 2	Identificador de grupo Diffie-Hellman. Se utiliza el grupo 2 por ser de 1024 bits, y a mayor numero el grupo más seguro, pero a la vez se requiere de mayor tiempo para computar la clave, y para el caso se recomienda el 2.
crypto isakmp key $$VPNIPsec#CRAC119$$ address 181.176.156.172	Contraseña compartida, y dirección IP publica estática configurada en el router de cabecera a la cual se realizará la conexión.
crypto isakmp keepalive 60 30 periodic	Mantiene las conexiones de comunicación de una red que no están terminadas y se mantienen hasta que el cliente o servidor interrumpe la conexión.
crypto ipsec transform-set TS esp-3des esp-md5-hmac	Parte de la política donde se define parámetros de seguridad para la negociación de IPSec SA.
mode tunnel	El modo de túnel IPsec ESP cifra y encapsula los paquetes IP al tiempo que proporciona autenticación e integridad.
crypto map vpn-hq 10 ipsec-isakmp set peer 181.176.156.172 set transform-set TS match address VPN-TRAFFIC	Creación de mapas crypto, donde se indica la IP destino de conexión, y la lista de acceso permitida para la conexión asociada a un nombre.
ip access-list extended VPN-TRAFFIC permit ip 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255	Se crea la lista de acceso con el segmento de IP permito como destino para cada sucursal que se conectara de forma dinámica. Esta línea se repite por cada sucursal remota.
interface FastEthernet4 ip address 192.168.X.2 255.255.255.0 duplex auto speed auto crypto map vpn-hq	Configuración de la interfaz WAN con IP privada local y la asignación de crypto map creado a la interfaz de salida a internet.

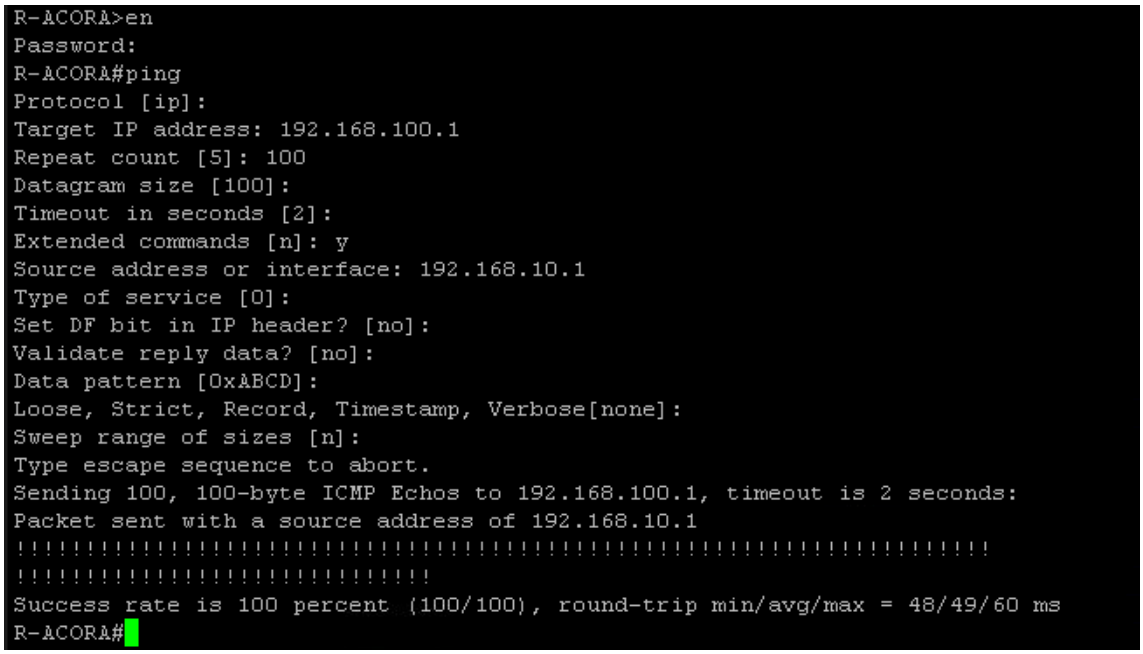
Elaboración Propia

Nota. La Tabla 6, contiene la configuración general en las sucursales.

4.2.5. Verificación de la conectividad

Para realizar las pruebas de conectividad entre las sedes de remotas seleccionadas de Caja Rural de Ahorro y Crédito los Andes SA hasta la sede principal se utilizó el comando ping desde PC en sede remota hasta Servidor en la sede principal y viceversa.

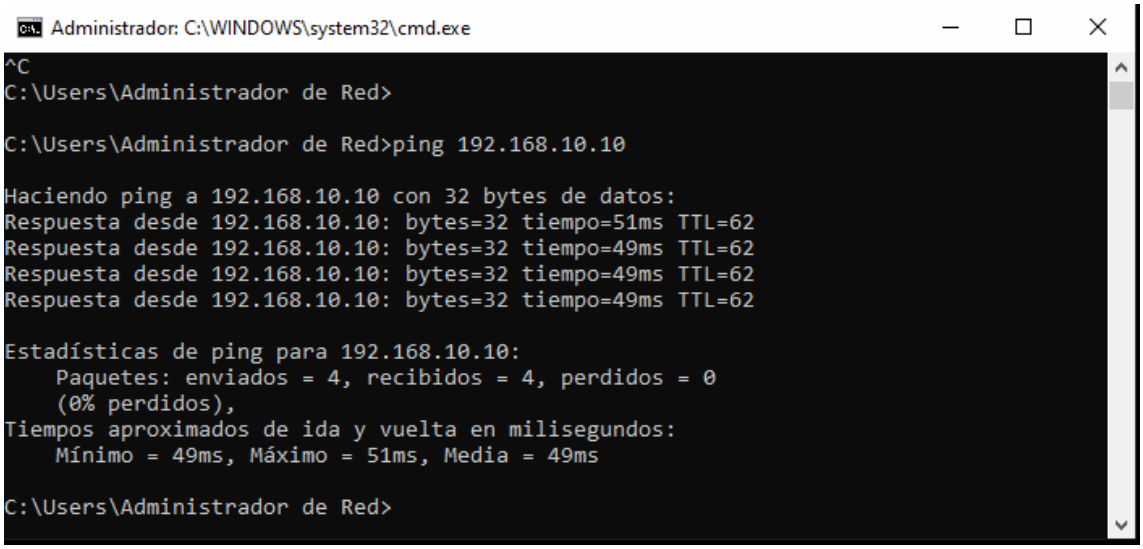
Figura 38: Ping extendido desde router Acora hasta router Cabecera.



Elaboración Propia

Nota, Figura 38 indica que la conexión establecida entre el router cisco instalado en la sede Acora y el Router en la sede central, sin pérdida de paquetes enviados con un tiempo promedio de 49 ms, que es un tiempo aceptable para operaciones en línea.

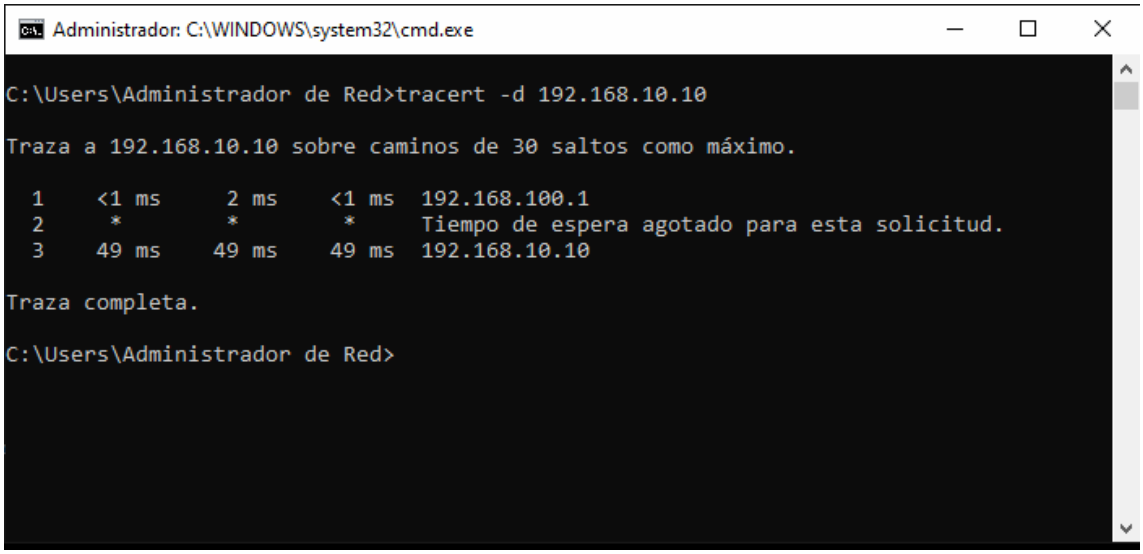
Figura 39: Ping desde el servidor hasta la Pc de la sede Acora.



Elaboración Propia

Nota. La Figura 39 muestra la conexión establecida entre el servidor que está ubicado en la sede principal hasta la computadora ubicado en la sede Acora con una media de 49 ms y es aceptable para las transacciones del sistema financiero de la entidad.

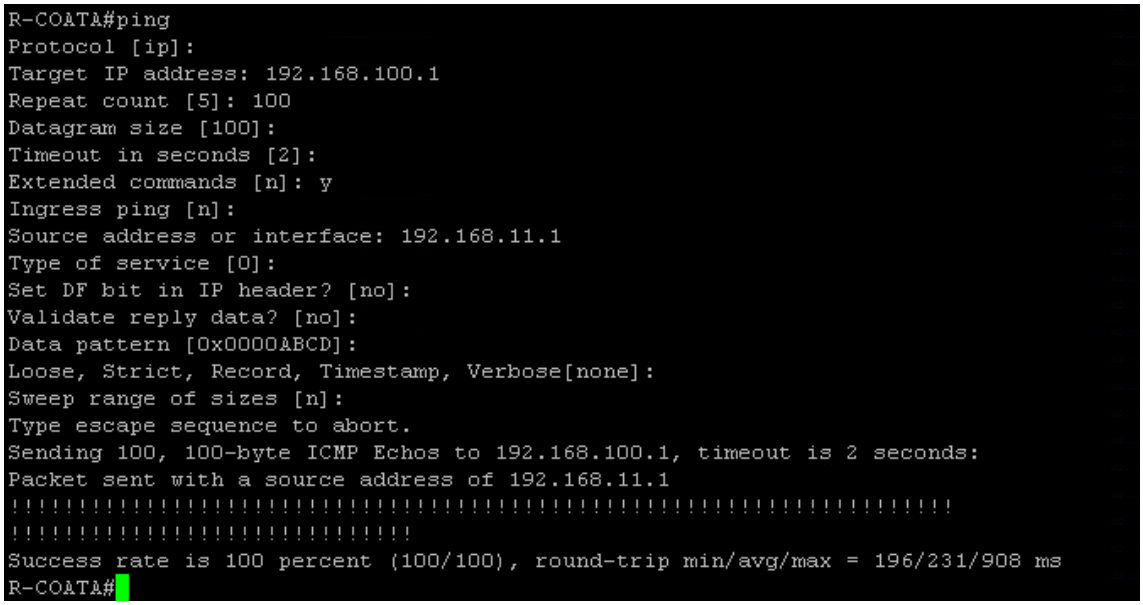
Figura 40: Tracert desde el servidor hasta la PC de la sede Acora



Elaboración Propia

Nota. por último, la Figura 40 muestra la ruta que realiza el tráfico enviado desde el servidor de la sede central hasta la computadora que se encuentra en la sede Acora.

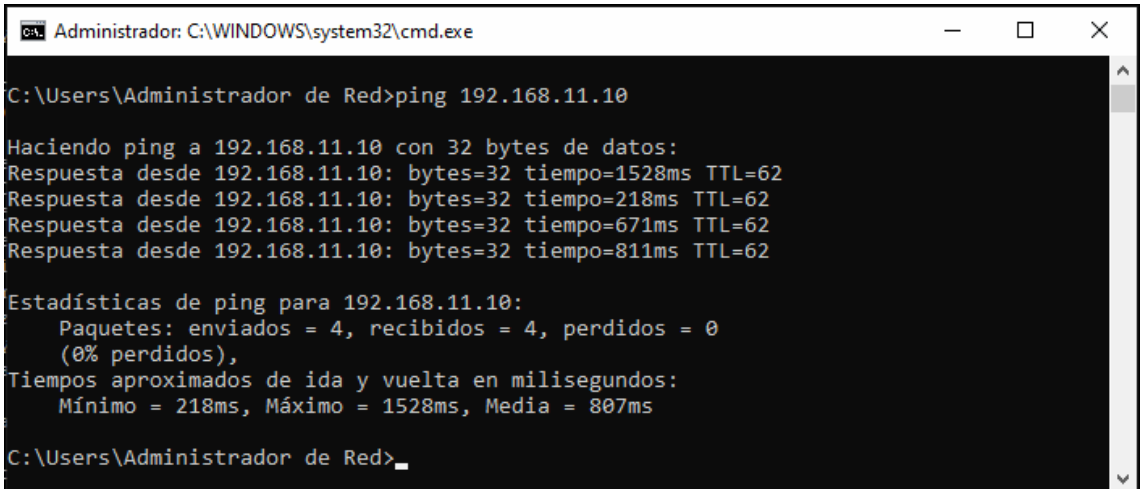
Figura 41: Ping extendido desde Router Coata hasta Router cabecera.



Elaboración Propia

Nota, Figura 41 indica que la conexión establecida entre el router cisco instalado en la sede Coata y el Router en la sede central, sin pérdida de paquetes enviados con un tiempo promedio de 231 ms, pero con un tiempo maximo de 908 ms lo cual no es aceptable para el funcionamiento de transacciones en linea.

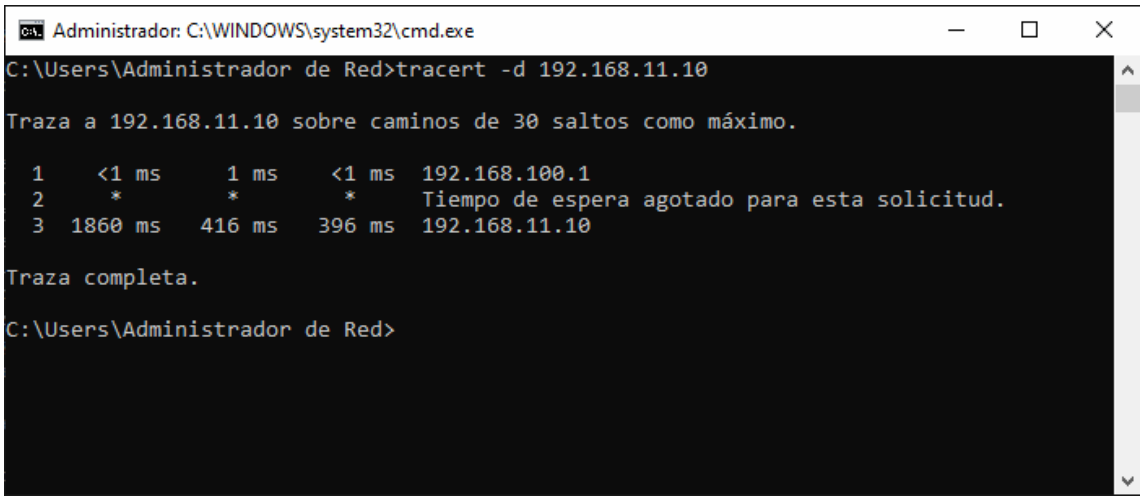
Figura 42: Ping desde servidor hasta PC de Coata.



Elaboración Propia

Nota. La Figura 42 muestra la conexión establecida entre el servidor que está ubicado en la sede principal hasta la computadora ubicado en la sede Coata con una media de 807 ms, lo cual no es aceptable para las operaciones bancarias de la entidad.

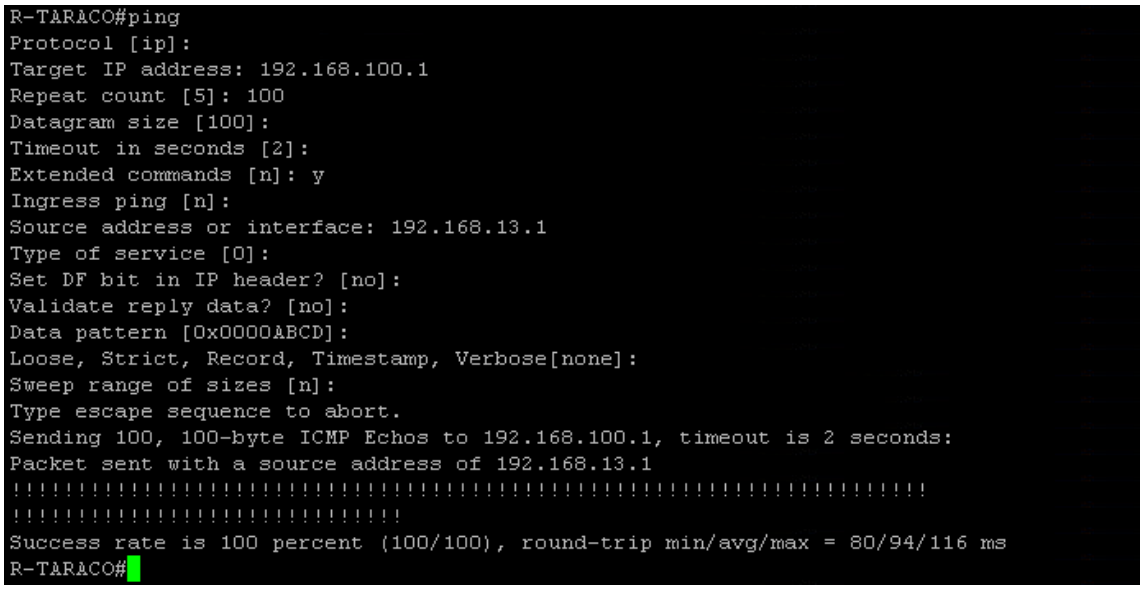
Figura 43: Tracert desde servidor hasta PC de Coata.



Elaboración Propia

Nota. por último, la Figura 43 muestra la ruta que realiza el tráfico enviado desde el servidor de la sede central hasta la computadora que se encuentra en la sede Coata.

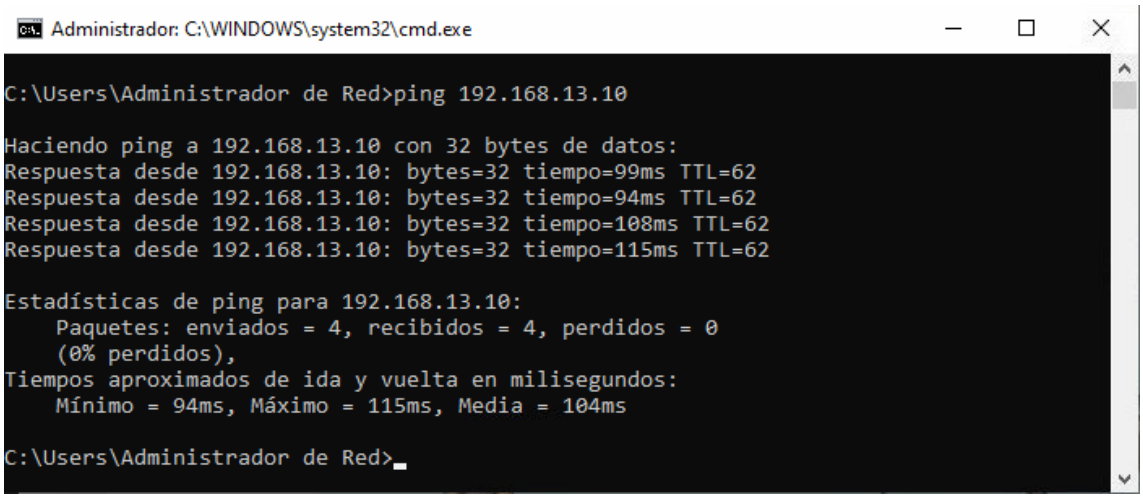
Figura 44: Ping desde Router Taraco hasta Router Cabecera.



Elaboración Propia

Nota, Figura 44 indica que la conexión establecida entre el router cisco instalado en la sede Taraco y el Router en la sede central, sin pérdida de paquetes enviados con un tiempo promedio de 94 ms, lo cual se encuentra al limite del tiempo aceptable para realizar operaciones en linea.

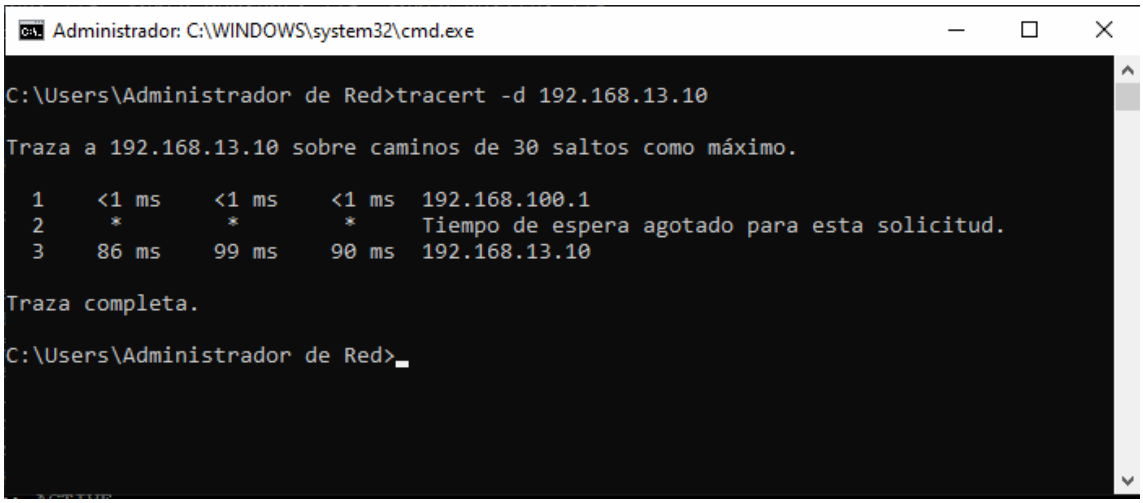
Figura 45: Ping desde Servidor hasta PC Taraco.



Elaboración Propia

Nota. La Figura 45 muestra la conexión establecida entre el servidor que está ubicado en la sede principal hasta la computadora ubicado en la sede Taraco con una media de 104 ms y es aceptable para las transacciones del sistema financiero de la entidad.

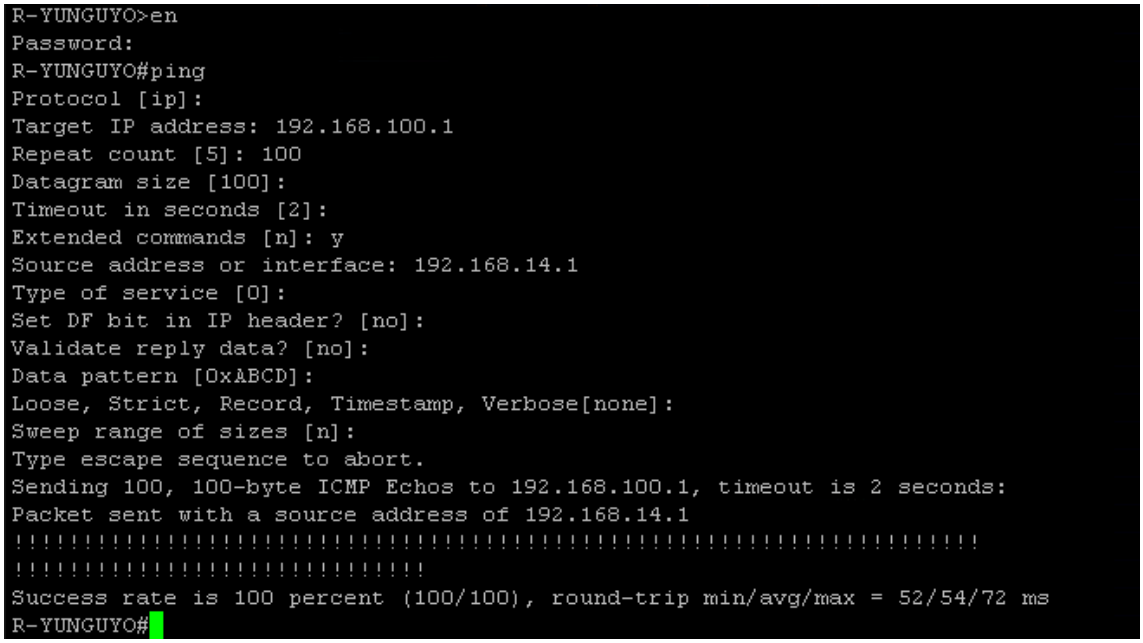
Figura 46: Tracert desde Servidor hasta PC Taraco.



Elaboración Propia

Nota. por último, la Figura 46 muestra la ruta que realiza el tráfico enviado desde el servidor de la sede central hasta la computadora que se encuentra en la sede Taraco.

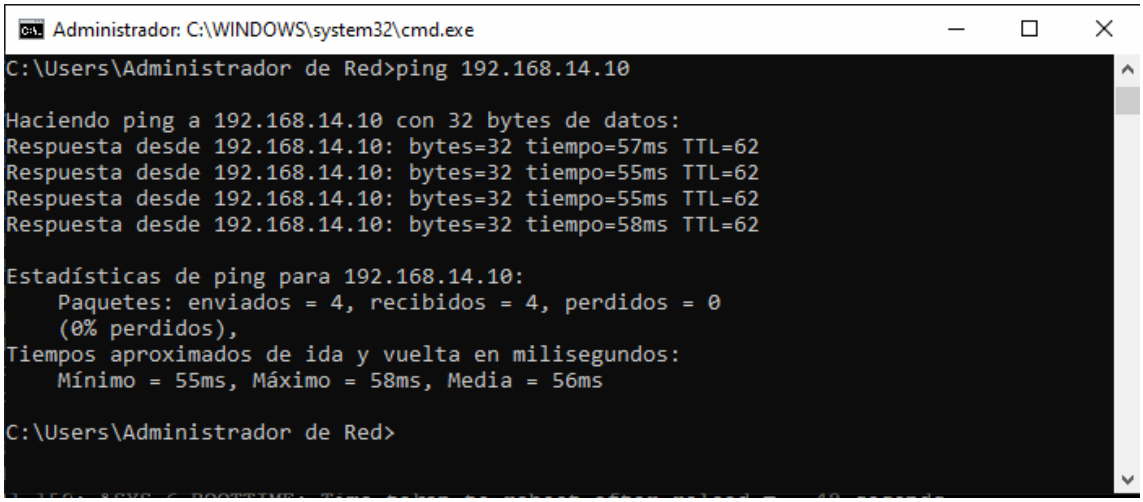
Figura 47: Ping extendido desde Router Yunguyo hasta Router Cabecera.



Elaboración Propia

Nota, Figura 47 indica que la conexión establecida entre el router cisco instalado en la sede Yunguyo y el Router en la sede central, sin pérdida de paquetes enviados con un tiempo promedio de 54 ms, que es un tiempo aceptable para operaciones en línea.

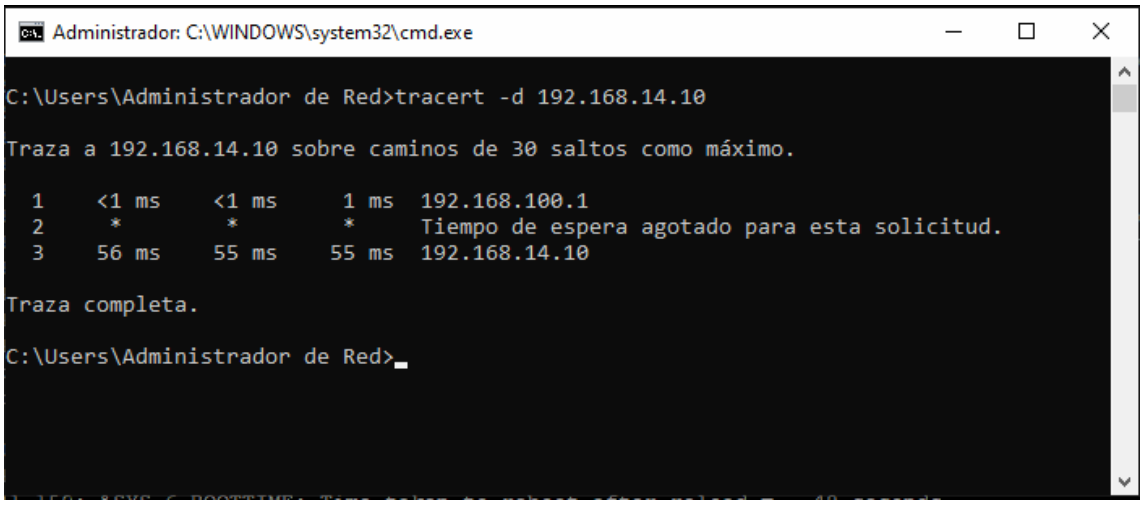
Figura 48: Ping desde Servidor hasta Pc de Yunguyo.



Elaboración Propia

Nota. La Figura 48 muestra la conexión establecida entre el servidor que está ubicado en la sede principal hasta la computadora ubicado en la sede Yunguyo con una media de 104 ms y es aceptable para las transacciones del sistema financiero de la entidad.

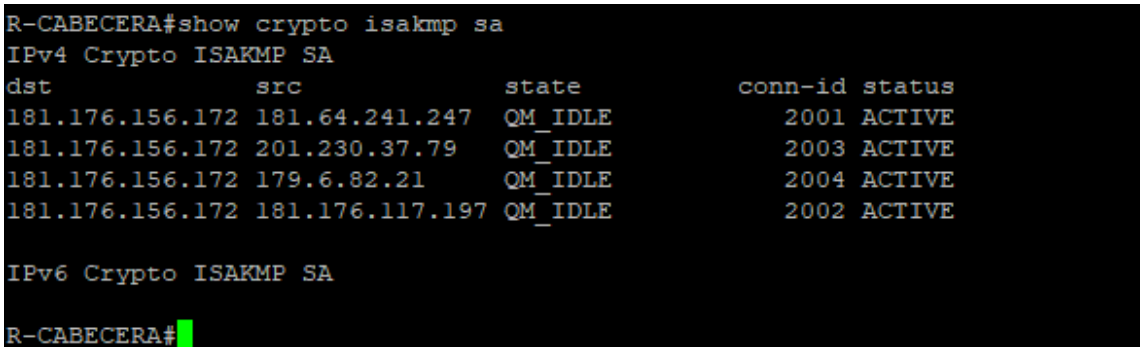
Figura 49: Tracert desde Servidor hasta PC Yunguyo.



Elaboración Propia

Nota. por último, la Figura 49 muestra la ruta que realiza el tráfico enviado desde el servidor de la sede central hasta la computadora que se encuentra en la sede Yunguyo.

Figura 50: Asociaciones de Seguridad Activas.



Elaboración Propia

Nota. Router Cabecera, como muestra la Figura 50 se tiene 4 conexiones establecidas que representan las 4 sedes donde se instalaron los router cisco, tambien el resumen de las conexiones establecidas se encuentran en el Anexo B.

4.3. ANÁLISIS DEL PROCESO DE IMPLEMENTACIÓN.

4.3.1. Tiempo de Instalación.

Tabla 7: Actividades de Implementación Sede Principal.

Sucursal Principal		
TAREA	TIEMPO (Días)	DESCRIPCION
Instalación y Configuración de Equipos	1	Se utiliza una IP Publica ya contratada por la Caja Rural de Ahorro y Crédito los Andes SA. Configuración ANEXO A

Elaboración Propia

Tabla 8: Actividades de Implementación Sucursal Acora, Coata y Taraco.

Sucursal Acora, Coata y Taraco		
Tarea	Tiempo (Días)	Descripción
Verificación de proveedor de Internet y Operador Móvil con mejor cobertura	1	El operador de internet móvil para esta sede es Claro
Realizar el requerimiento y compra de los equipos, Modem 3G/4G, Router TP Link y Router Cisco	15	La compra de equipos se realiza con la aprobación de la jefatura de Área y el departamento de Logística.
Instalación y configuración de equipos en la sucursal remota.	1	Configuración ANEXO A.

Elaboración Propia

Tabla 9: Actividades de Implementación Sucursal Yunguyo.

Sucursal Yunguyo		
Tarea	Tiempo (Días)	Descripción
Contratar servicio de internet ADSL	10	El operador de internet es Movistar
Realizar el requerimiento y compra de los equipos Router Cisco	15	La compra de equipos se realiza con la aprobación de la jefatura de Área y el departamento de Logística.
Instalación y configuración de equipos en la sucursal remota.	1	Configuración ANEXO A.

Elaboración Propia

4.3.2. Costo de implementación.

Tabla 10: Costo Implementación por entidad.

SEDE	instalación	Costo mensual	Costo x 36 Meses
ACORA	S/2,101.00	S/100.00	S/3,600.00
COATA	S/2,101.00	S/100.00	S/3,600.00
TARACO	S/2,101.00	S/100.00	S/3,600.00
YUNGUYO	S/2,101.00	S/189.91	S/6,836.76
Total	S/8,404.00	S/489.91	S/17,636.76

Elaboración Propia

Nota. La Tabla 10 muestra el costo de instalación y costo de servicio mensual para las 4 sedes utilizando lo indicado en el proyecto.

4.3.3. Análisis de la conectividad VPN.

La interpretación del resultado mostrado a la salida del comando sh crypto isakmp sa en el router de cabecera se realiza en base a la siguiente tabla de definiciones, la tabla completa en el Anexo C.

Tabla 11: Descripción de sh crypto isakmp sa.

N°	DESCRIPCION
1	La dirección IP del extremo del tráfico del túnel local protegido por esta SA.
2	Si se utiliza NAT transversal, se adjunta el número de puerto de encapsulación UDP.
3	La dirección IP y, opcionalmente, el nombre de host del interlocutor remoto. Se muestra un nombre de host si el par fue configurado por su FQDN.
4	Si se utiliza NAT transversal, se adjunta el número de puerto de encapsulación UDP.
5	La subred local protegida por esta SA, tal como se configuró en la regla de lista criptográfica. La subred se expresa como < *dirección* >/< *comodín* >.
6	La subred remota protegida por esta SA, tal como se configuró en la regla de lista criptográfica. La subred se expresa como <dirección>/<comodín>.
7	Total: el número total de paquetes entrantes recibidos
8	Total OK: el número total de paquetes entrantes recibidos y no descartados
9	Descifrar: el número total de paquetes descifrados con éxito
10	Verificar: el número total de paquetes verificados con éxito por HMAC
11	Decaps: la cantidad total de paquetes desencapsulados con éxito del encabezado del túnel IPSec
12	Descomprimido: el número total de paquetes descomprimidos con éxito por el proceso de compresión de carga IP (IPPCP)
13	Total: el número total de paquetes salientes enviados
14	Total OK: el número total de paquetes salientes enviados y no descartados
15	Cifrar: el número total de paquetes cifrados con éxito.
16	Resumen: el número total de paquetes adjuntos con éxito con un HMAC
17	Encaps: el número total de paquetes encapsulados con éxito con un encabezado de túnel IPSec
18	Sa caducado: la cantidad de paquetes descartados antes de transmitirse a través de este túnel debido a que SA caducó: la vida útil de KB de SA es menor que la longitud total del paquete IP externo
19	El modo de encapsulación: túnel o transporte

Elaboración Propia

Nota. La tabla contiene una parte de las definiciones de los resultados obtenidos durante la verificación de conectividad entre las sucursales remotas y la sede principal.

Figura 51: IPSec SA creada en router de cabecera sucursal Acora.

```
protected vrf: (none)
local  ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
current_peer 201.230.37.79 port 45097
  PERMIT, flags={}
 #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
 #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 0, #recv errors 0

  local crypto endpt.: 181.176.156.172, remote crypto endpt.: 201.230.37.79
  path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0
  current outbound spi: 0x4A284E6(77759718)
  PFS (Y/N): N, DH group: none

  inbound esp sas:
   spi: 0x5153D35C(1364448092)
     transform: esp-3des esp-md5-hmac ,
     in use settings ={Tunnel UDP-Encaps, }
     conn id: 5, flow_id: Onboard VPN:5, sibling_flags 80000046, crypto map: VPN-BO
     sa timing: remaining key lifetime (k/sec): (4558637/3563)
     IV size: 8 bytes
     replay detection support: Y
     Status: ACTIVE

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
   spi: 0x4A284E6(77759718)
     transform: esp-3des esp-md5-hmac ,
     in use settings ={Tunnel UDP-Encaps, }
     conn id: 6, flow_id: Onboard VPN:6, sibling_flags 80000046, crypto map: VPN-BO
     sa timing: remaining key lifetime (k/sec): (4558637/3563)
     IV size: 8 bytes
     replay detection support: Y
     Status: ACTIVE
```

Elaboración Propia

Nota. La Figura nos muestra el IPSec SA creada entre los pares de la sede remota Acora y la sede principal, la lista de acceso, crypto map creado VPN-BO y el estado de la conexión que se muestra como activa, donde el número de paquetes descifrados, verificados y desencapsulados son iguales a los paquetes cifrados, paquetes adjuntos y encapsulados con éxito con un encabezado de túnel IPSec, también el modo de encapsulación túnel.

Figura 52: IPSec SA creada en router de cabecera sucursal Coata.

```
protected vrf: (none)
local  ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.11.0/255.255.255.0/0/0)
current_peer 179.6.82.21 port 35245
  PERMIT, flags={}
 #pkts encaps: 154, #pkts encrypt: 154, #pkts digest: 154
 #pkts decaps: 253, #pkts decrypt: 253, #pkts verify: 253
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 0, #recv errors 0

  local crypto endpt.: 181.176.156.172, remote crypto endpt.: 179.6.82.21
  path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0
  current outbound spi: 0x47D77323(1205302051)
  PFS (Y/N): N, DH group: none

  inbound esp sas:
   spi: 0xC05C3C75(3227270261)
     transform: esp-3des esp-md5-hmac ,
     in use settings ={Tunnel UDP-Encaps, }
     conn id: 15, flow_id: Onboard VPN:15, sibling_flags 80000046, crypto map: VPN-BO
     sa timing: remaining key lifetime (k/sec): (4588500/1056)
     IV size: 8 bytes
     replay detection support: Y
     Status: ACTIVE

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
   spi: 0x47D77323(1205302051)
     transform: esp-3des esp-md5-hmac ,
     in use settings ={Tunnel UDP-Encaps, }
     conn id: 16, flow_id: Onboard VPN:16, sibling_flags 80000046, crypto map: VPN-BO
     sa timing: remaining key lifetime (k/sec): (4588508/1056)
     IV size: 8 bytes
     replay detection support: Y
     Status: ACTIVE
```

Elaboración Propia

Nota. La Figura nos muestra el IPSec SA creada entre los pares de la sede remota Coata y la sede principal, la lista de acceso, donde el número de paquetes descifrados, verificados y desencapsulados no son iguales a los paquetes cifrados, paquetes adjuntos y encapsulados con éxito con un encabezado de túnel IPSec, esto puede ser debido a que en esta sucursal se obtuvieron tiempos de respuesta muy alto y no aptos para uso de la entidad.

Figura 53: IPSec SA creada en router de cabecera sucursal Taraco.

```
protected vrf: (none)
local  ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.13.0/255.255.255.0/0/0)
current_peer 181.176.117.197 port 2270
  PERMIT, flags={}
 #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 7
 #pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 7
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 0, #recv errors 0

  local crypto endpt.: 181.176.156.172, remote crypto endpt.: 181.176.117.197
  path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0
  current outbound spi: 0xFF66086F(4284876911)
  PFS (Y/N): N, DH group: none

  inbound esp sas:
   spi: 0xF5CD0376(4123853686)
     transform: esp-3des esp-md5-hmac ,
     in use settings ={Tunnel UDP-Encaps, }
     conn id: 3, flow_id: Onboard VPN:3, sibling_flags 80000046, crypto map: VPN-BO
     sa timing: remaining key lifetime (k/sec): (4591136/3534)
     IV size: 8 bytes
     replay detection support: Y
     Status: ACTIVE

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
   spi: 0xFF66086F(4284876911)
     transform: esp-3des esp-md5-hmac ,
     in use settings ={Tunnel UDP-Encaps, }
     conn id: 4, flow_id: Onboard VPN:4, sibling_flags 80000046, crypto map: VPN-BO
     sa timing: remaining key lifetime (k/sec): (4591136/3534)
     IV size: 8 bytes
     replay detection support: Y
     Status: ACTIVE
```

Elaboración Propia

Nota. La Figura nos muestra el IPSec SA creada entre los pares de la sede remota Taraco y la sede principal, la lista de acceso, crypto map creado VPN-BO y el estado de la conexión que se muestra como activa, donde el número de paquetes descifrados, verificados y desencapsulados son iguales a los paquetes cifrados, paquetes adjuntos y encapsulados con éxito con un encabezado de túnel IPSec, también el modo de encapsulación túnel.

Figura 54: IPSec SA creada en router de cabecera sucursal Yunguyo.

```
protected vrf: (none)
local  ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.14.0/255.255.255.0/0/0)
current_peer 181.64.241.247 port 18694
  PERMIT, flags={}
 #pkts encaps: 113, #pkts encrypt: 113, #pkts digest: 113
 #pkts decaps: 110, #pkts decrypt: 110, #pkts verify: 110
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 0, #recv errors 0

  local crypto endpt.: 181.176.156.172, remote crypto endpt.: 181.64.241.247
  path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0
  current outbound spi: 0x863949BC(2251901372)
  PFS (Y/N): N, DH group: none

  inbound esp sas:
   spi: 0xC579D25B(3313095259)
     transform: esp-3des esp-md5-hmac ,
     in use settings ={Tunnel UDP-Encaps, }
     conn id: 1, flow_id: Onboard VPN:1, sibling_flags 80000046, crypto map: VPN-BO
     sa timing: remaining key lifetime (k/sec): (4541865/2943)
     IV size: 8 bytes
     replay detection support: Y
     Status: ACTIVE

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
   spi: 0x863949BC(2251901372)
     transform: esp-3des esp-md5-hmac ,
     in use settings ={Tunnel UDP-Encaps, }
     conn id: 2, flow_id: Onboard VPN:2, sibling_flags 80000046, crypto map: VPN-BO
     sa timing: remaining key lifetime (k/sec): (4541864/2943)
     IV size: 8 bytes
     replay detection support: Y
     Status: ACTIVE
```

Elaboración Propia

Nota. La Figura nos muestra el IPSec SA creada entre los pares de la sede remota Yunguyo y la sede principal, la lista de acceso, crypto map creado VPN-BO y el estado de la conexión que se muestra como activa, donde el número de paquetes descifrados, verificados y desencapsulados no son iguales a los paquetes cifrados, paquetes adjuntos y encapsulados con éxito con un encabezado de túnel IPSec, también el modo de encapsulación túnel.

4.4. RESULTADOS DEL INSTRUMENTO DE INVESTIGACIÓN

La tabla muestra los costos promedio y total que se efectuarían si el servicio de red privada virtual es contrato a un proveedor o implementado por la misma entidad, así como la diferencia a favor de la entidad.

Tabla 12: Costo promedio de instalación y servicio.

	Entidad	Proveedor	Diferencia
Costo de Instalación Promedio	S/2,101.00	S/800.00	-S/1,301.00
Costo Mensual promedio	S/122.48	S/1,089.70	S/967.22
Costo Total 36 Meses	S/17,636.76	S/156,916.80	S/139,280.04

Elaboración Propia

Nota: La Tabla muestra los promedios de los costos obtenidos por el proveedor y la entidad al instalar el servicio de red privada virtual.

4.5. CONTRASTE DE LA HIPÓTESIS

4.5.1. Contraste de Hipótesis Tiempo

Ho: La implementación de una Red Privada Virtual IPSec con IP Dinámica con routers Cisco no disminuye el tiempo de instalación del servicio.

Ho: $\mu Po \leq \mu P\, r$

Ha = La Red Privada Virtual IPSec con IP Dinámica con routers Cisco disminuye el tiempo de instalación del servicio.

Ho: $\mu Po > \mu P\, r$

Donde:

Ho = Hipotesis Nula

Ha = Hipotesis Alternativa

μPo = Media de la Post Prueba

$\mu P\, r$ = Media de la Pre Prueba

$\alpha = 0.05$; nivel de significancia

Tabla 13: Tiempo proveedor y entidad de instalación.

Descripción	Indicador	Pre	Post
Sucursal Acora	Tiempo días	67	17
Sucursal Coata	Tiempo días	56	17
Sucursal Taraco	Tiempo días	56	17
Sucursal Yunguyo	Tiempo días	61	26

Elaboración Propia

Nota. Tabla contiene las muestras tomadas de los tiempos de instalación en la muestra de la población seleccionada, es decir el pre y post de los tiempos medidos en días.

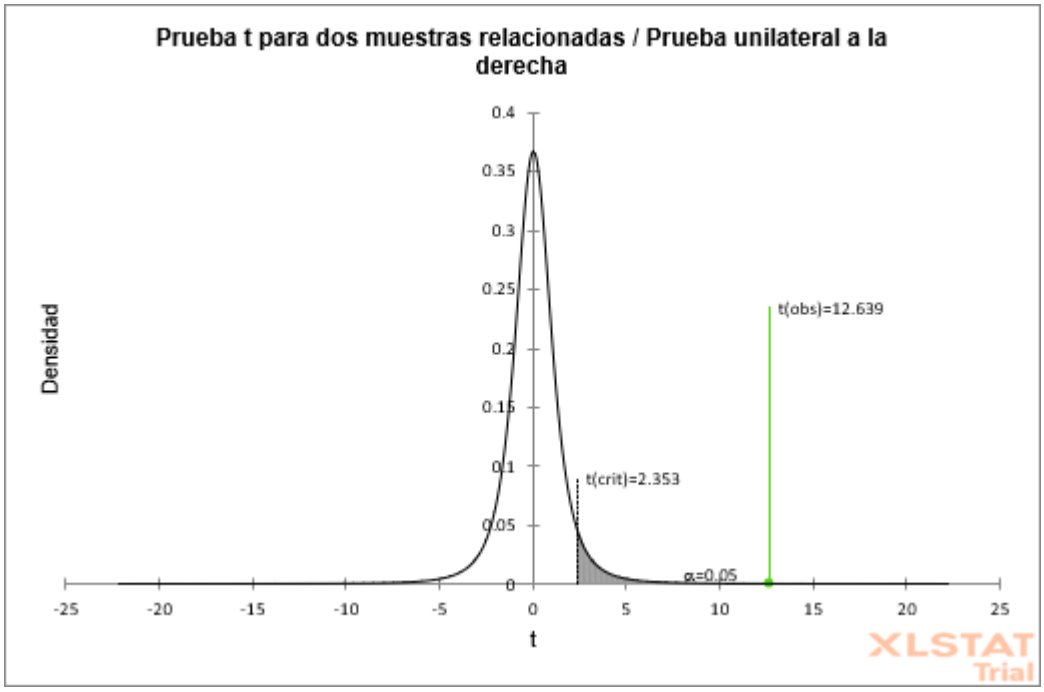
Tabla 14: Prueba t para tiempo de instalacion.

	Pre	***Post***
Media	60	19.25
Varianza	27.3333333	20.25
Observaciones	4	4
Coeficiente de correlación de Pearson	0.12751534	
Diferencia hipotética de las medias	0	
Grados de libertad	3	
Estadístico t	12.64	
P(T<=t) una cola	0.00053413	
Valor crítico de t (una cola)	2.35	
P(T<=t) dos colas	0.00106825	
Valor crítico de t (dos colas)	3.18244631	

Elaboración Propia

Nota. La Tabla, muestra el resultado de la prueba t realizado a los tiempos de instalación pre y post.

Figura 55: Distribución T-student tiempo de instalación.



Elaboración propia

Nota. La Figura muestra la distribución t – student, y que contiene el t crítico y el valor t estadístico calculado.

La interpretación para los resultados obtenidos en el contraste de la hipótesis especifica respecto a las muestras tomadas a los tiempos pre y post, se obtuvo que: µPo > µP r, el valor 60 es mayor que 19.25, además se tiene que t estadístico calculado es 12.639 y t critico 2.353, por lo cual t calculado se encuentra en la zona de rechazo, por lo cual se rechaza Ho, y aceptamos la hipótesis alternativa Ha que afirma que La Red Privada Virtual IPSec con IP Dinámica con routers Cisco disminuye el tiempo de instalación del servicio.

4.5.2. Contraste de Hipótesis Costo

Ho: La implementación de una Red Privada Virtual IPSec con IP Dinámica con routers Cisco no disminuye el costo de instalación y servicio total.

Ho: µPo $\leq$ µP r

Ha = La Red Privada Virtual IPSec con IP Dinámica con routers Cisco disminuye el costo de instalación y de servicio total.

Ho: μPo $>$ μP r

Donde:

Ho = Hipotesis Nula

Ha = Hipotesis Alternativa

μPo = Media de la Post Prueba

μ P r = Media de la Pre Prueba

$\alpha = 0.05$; nivel de significancia

Tabla 15: Costo proveedor y entidad de instalación.

Descripción	Pre	Post
Sucursal Acora	S/1,208.60	S/100.00
Sucursal Coata	S/970.80	S/100.00
Sucursal Taraco	S/1,208.60	S/100.00
Sucursal Yunguyo	S/970.80	S/189.91

Elaboración Propia

Nota. Tabla contiene los costos de instalación en las sucursales seleccionadas, pre igual a costo proveedor y Post igual a costo de proyecto.

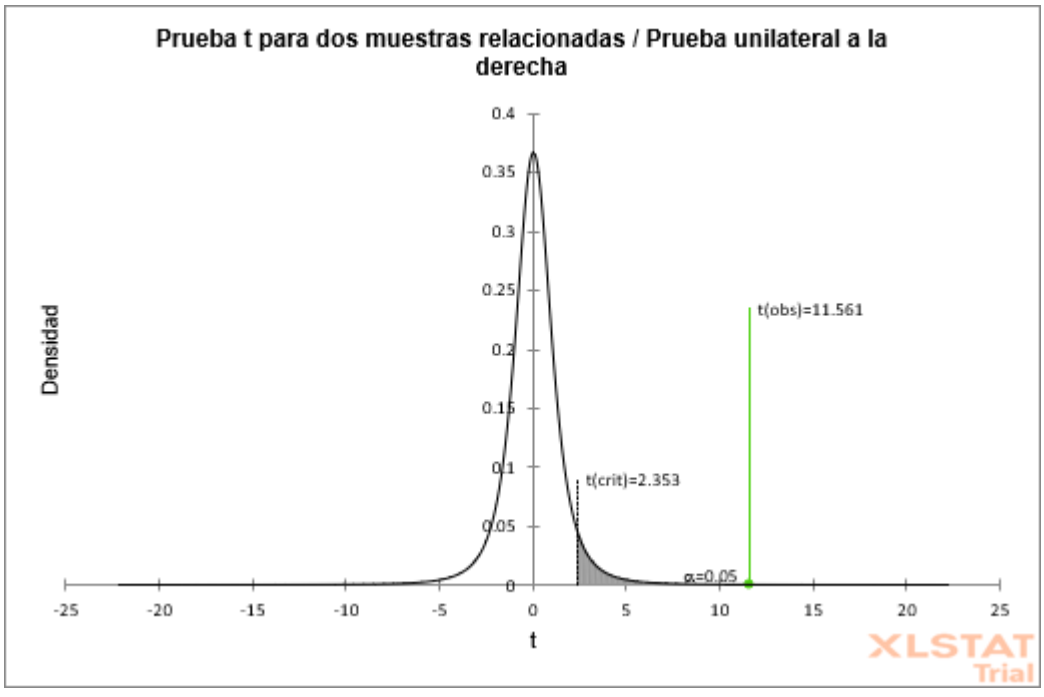
Tabla 16: Prueba t para costos de instalación.

Prueba t para medias de dos muestras emparejadas		
	Pre	*Post*
Media	1089.7	122.4775
Varianza	18849.61333	2020.952025
Observaciones	4	4
Coeficiente de correlación de Pearson	-0.577350269	
Diferencia hipotética de las medias	0	
Grados de libertad	3	
Estadístico t	11.56105034	
P(T<=t) una cola	0.000694822	
Valor crítico de t (una cola)	2.353363435	
P(T<=t) dos colas	0.001389643	
Valor crítico de t (dos colas)	3.182446305	

Elaboración Propia

Nota. La tabla, muestra el resultado de la prueba t realizado a los costos de instalación y servicio pre y post.

Figura 56: Distribución T-student costos de servicio.



Elaboración propia

Nota. La Figura muestra la distribución t – student, y que contiene el t crítico y el valor t estadístico calculado.

La interpretación para los resultados obtenidos en el contraste de la hipótesis especifica respecto a las muestras tomadas de los costos pre y post, μPo $>$ μP r, el valor 1089.7 es mayor que 122.47, además se tiene que t calculado es 11.561 y t critico 2.353, es decir t calculado se encuentra fuera de la zona de aceptación, por consiguiente se rechaza la hipótesis nula Ho, y aceptamos la hipótesis alternativa Ha, que afirma que La Red Privada Virtual IPSec con IP Dinámica con routers Cisco disminuye el costo de servicio.

4.6. DISCUSIÓN

A partir de los resultados obtenidos rechazamos la hipótesis nula y aceptamos la hipótesis alternativa que nos indica que los tiempos y los costos aplicando lo presentado en el presente proyecto se reducen a comparación de los obtenidos por el proveedor externo del servicio de red privada virtual contratado por la entidad, lo cual representa el éxito del proyecto en la implementación de una red privada virtual utilizando las funcionalidades y herramientas utilizadas.

Durante la implementación de la VPN IPSec se utilizó sus características que garantizan su seguridad para se tiene en cuanta lo obtenido por (Atencio Mendoza & Mamani Figueroa, 2017) donde verifica que la utilización de VPN IPSec garantiza la autenticación, integridad y confidencialidad en la transmisión de datos.

Para la medición de la conectividad se realizó la verificación de los tiempos obteniendo un 75 % de las sucursales que cumplen con el tiempo aceptable, así como (Zapata Rodríguez, 2016) nos indica en su tesis que la implementación de una VPN IPSec garantiza la disponibilidad y escalabilidad de la red, se logró verificar la conectividad entre las sucursales y la sucursal principal.

V. CONCLUSIONES

PRIMERO. Del análisis de la situación actual se obtuvo que el tiempo, el costo de instalación y mantenimiento del servicio de Red Privada Virtual contratado por la entidad son bastante elevados, porque las actividades que se realizaron durante la instalación demandaron un promedio de 2 meses por cada sucursal, con un costo único de instalación, y un costo promedio mensual de mantenimiento del servicio que supera los mil soles.

SEGUNDO. Durante el inicio del proyecto, se diseñó una topología física y lógica de una Red Privada Virtual IPSec con IP Dinámica que requieren un tiempo reducido en las actividades a realizar para su implementación, y el costo de mantenimiento del servicio también se reduce considerablemente, sin embargo, el costo de instalación es superior a lo cobrado por el proveedor contratado, porque se requiere de la adquisición de equipos como routers, módems y chips de Internet móvil para ejecutar el proyecto.

TERCERO: Se implementó la Red Privada Virtual con IP Dinámica con Routers Cisco y verificó la conectividad de las sucursales de la Caja Rural de Ahorro y crédito los Andes SA, para la implementación se cumplió con las actividades del diseño y el resultado obtenido en las pruebas de conectividad fue de un 75 % de las sucursales como aceptables respecto a la conectividad, y el 25% de las sucursales obtuvieron una calificación no aceptable, porque la cobertura de internet móvil del operador utilizado en esta sucursal fue defectuosa, para mejorar la conectividad en esta sucursal se puede optar por utilizar otro proveedor de internet móvil.

CUARTO: Durante la evaluación de la disminución de tiempo y costo de instalación de servicio luego de la implementación del proyecto, se obtuvo que existe una disminución promedio de cuarenta días, que representa el 68% del tiempo que demora el proveedor para la instalación del servicio por cada sucursal, también los resultados obtenidos respecto al costo de instalación y mantenimiento del servicio se reducen en un 88.8% que equivale a más de cien mil soles ahorrados, para un periodo de 36 meses de contrato.

VI. RECOMENDACIONES

PRIMERO: Para contratar un proveedor del servicio de Red Privada Virtual, se recomienda realizar un amplio análisis de los alcances como tiempo, costo, cobertura y SLAs, para no tener inconvenientes a la hora de solicitar la instalación en las sucursales que pueden estar ubicadas en distintas zonas del país.

SEGUNDO: El diseño de la Red Privada Virtual que fue implementada está enfocada exclusivamente a la transferencia de una LAN que contiene transacciones de la entidad Caja Rural de Ahorro y Crédito los Andes SA, por ello se recomienda continuar con la implementación para agregar las transferencias como la Voz y Video agregando QoS para este tipo de servicios.

TERCERO: La implementación puede ser adecuada para trabajar en paralelo al servicio de Red Privada Virtual ofrecido por otro proveedor, convirtiendo la conexión de las sucursales en una red de comunicación tolerante a fallos, ya que la implementación propuesta puede ser mejorada instalando internet más confiable utilizando medios como la fibra óptica o antena microondas.

CUARTO: La implementación de la red privada virtual con IPSec desarrollado en el presente proyecto, puede ser optimizado en tiempo y costo si se realiza la gestión de los equipos con anticipación, con lo cual la entidad puede disponer con el servicio para realizar sus transacciones cuando lo requiera sin depender de un proveedor.

VII. REFERENCIAS BIBLIOGRAFICAS

Hernández Sampieri , C. R., Fernández Collado, C. , & Baptista Lucio , P. (2014). *METODOLOGÍA DELA INVESTIGACIÓN* (sexta edición ed.). Mexico D.F: McGRAW-HILL/Interamericana Editores, S. A.

Alva Maldonado, E. (2013). *Desarrollo e Implementación de una Herramienta Gráfica para la Configuración Remota de una VPN con Routers Cisco.* Tesis, Pontificia Universidad Católica del Perú, Facultad de Ciencias e Ingeniería, Lima.

Atencio Mendoza, A. I., & Mamani Figueroa, E. J. (2017). *Diseño e Implementación de un Prototipo de Red Privada Virtual en Capa 3 Utilizando Cisco IOS para la Universidad Nacional del Altiplano.* Universidad Nacional del Altiplano, Escuela Profesional de Ingenieria Electronica, Puno.

Cisco. (2021). *¿Qué es una VPN? - Red privada virtual*. Obtenido de Cisco: https://www.cisco.com/c/es_mx/products/security/vpn-endpoint-security-clients/what-is-vpn.html

Cisco Networking Academy. (2016). *CCNA Security v1.1*. Cisco.

Cisco Networking Academy. (2017). *CCNA R&S v6.* Cisco.

Cosio Dueñas, H. (10 de Septiembre de 2016). *Población y Muestra.* Obtenido de slideshare: https://es.slideshare.net/HerbertCosioDueas/7-poblacin-y-muestra

Digital Guide IONOS. (02 de Marzo de 2020). *¿Qué es una red de área amplia (WAN)?* Obtenido de Digital Guide IONOS: https://www.ionos.es/digitalguide/servidores/know-how/wan/

Editorial Etecé. (5 de Agosto de 2021). *Red LAN*. Obtenido de Concepto: https://concepto.de/red-lan/

Fernandez, Y. (5 de Diciembre de 2019). *Tarjeta SIM: cómo funciona y cómo saber de qué tipo es la tuya*. Obtenido de Xataka Basics:

https://www.xataka.com/basics/tarjeta-sim-como-funciona-como-saber-que-tipo-tuya

Gillis, A. S. (Agosto de 2021). *Red privada virtual o VPN*. Obtenido de ComputerWeekly.es: https://www.computerweekly.com/es/definicion/Red-privada-virtual-o-VPN

google maps. (2022). *Ubicacion de Sedes Caja los Andes.* Obtenido de [imagen]: https://www.google.com/maps/@-15.7444418,-69.8434381,10z/data=!3m1!4b1!4m2!11m1!3e4?hl=es-419

Grupo de Sistemas Operativos DATSI FI UPM. (2022). *Protocolo IPsec*. Obtenido de Grupo de Sistemas Operativos DATSI FI UPM: https://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec#:~:text=IPsec%20(abreviatura%20de%20Internet%20Protocol,establecimiento%20de%20claves%20de%20cifrado.

Huarcaya Ramos, F. A., & Muñoz Apaza, A. K. (2022). Diseño de la red de área local aplicando la metodología del ciclo de vida de red de cisco para mejorar la calidad de los servicios, el índice de transferencia de datos y la estabilidad de los sistemas de información de la Municipalidad de Santa Rosa. *[Tesis de Grado]*. UNA PUNO, PUNO.

Hwang, D. (Abril de 2021). *Red de área local o LAN*. Obtenido de ComputerWeekly.es: https://www.computerweekly.com/es/definicion/Red-de-area-local-o-LAN

Intercompras Comercio Electrónico SA de CV. (13 de Mayo de 2022). *Router Cisco 881 Ethernet Security Router - 4x10/100Base-TX LAN - 1x10/100Base-TX WAN*. Obtenido de intercompras su compra por internet: https://intercompras.com/p/router-cisco-ethernet-security-router-4x10100base-tx-lan-1x10100base-tx-53029

KillMyBill. (13 de Marzo de 2017). *¿Cómo funciona un módem USB 3G o 4G?* Obtenido de KillMyBill Reductor de Facturas: https://www.killmybill.es/modem-usb-3g-4g/

Lima Rocha, L. E. (2017). *Implementación de una Red Privada Virtual Dinámica Multipunto DMVPN con Protocolos IPSEC, MGRE Y NHRP*. Proyecto de Grado, Universidad Mayor de San Andrés, Facultad de Ciencias Puras y Naturales Carrera de Informática, La Paz.

Lozada, J. (2014). Investigación Aplicada: Definición, Propiedad Intelectual e Industria. *Divulgación científica de la Universidad Tecnológica Indoamérica, III*, 47-50.

Mar Segundo, J. (2016). Propuesta de implementación de una intranet vía VPN para mejorar la confidencialidad del intercambio de información entre las sedes Lima - Cusco INEI. *[Tesis de Grado]*. UNIVERSIDAD ANDINA DEL CUSCO, Cusco.

Monter Martínez, L. F., Rios Casañas, D. I., Curiel Anaya, A., & Pozas Cárdenas, M. (s.f.). *Modelo OSI vs TCP/IP*. Obtenido de Comunicaciones en Redes: http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro27/1_introduccin.html

Nolle, T., & Gillis, A. (2022). *Topología de red de malla (red de malla)*. Obtenido de ComputerWeekly.es: https://www.computerweekly.com/es/definicion/Topologia-de-red-de-malla-red-de-malla

odalysicas. (1 de Diciembre de 2014). *Instalación y Configuración de Aplicaciones y Servicios - TIPOS DE CONEXIONES DISPONIBLES*. Obtenido de odalysicas: http://odalysicas.blogspot.com/

OSTEC Seguridad Digital de Resultados. (23 de Febrero de 2016). *Principales protocolos de comunicación VPN*. Obtenido de OSTEC: https://ostec.blog/es/acceso-remoto/protocolos-comunicacion-vpn/

Ramirez, T. (2010). Como Hacer un Proyecto de Investigación. PANAPO.

Romero López, J. P., & Romero López, C. E. (2016). Fronteras de seguridad en redes privadas virtuales (VPN). *[Proyecto de Grado]*. UNIVERSIDAD TECNOLÓGICA DE PEREIRA, Pereira.

Rouse, M. (Diciembre de 2016). *Red de área extensa (WAN)*. Obtenido de ComputerWeekly.es: https://www.computerweekly.com/es/definicion/Red-de-area-extensa-WAN

SmartyDNS. (16 de Mayo de 2019). *Beneficios y desventajas de VPN (todo lo que necesita saber)*. Obtenido de SmartyDNS: https://www.smartydns.com/es/base-de-conocimientos/beneficios-y-desventajas-de-vpn/

Tp-Link. (2022). *Router TP-LINK3420*. Obtenido de [Imagen]: https://www.tp-link.com/latam/home-networking/3g-4g-router/tl-mr3420/

WIKIPEDIA. (9 de Marzo de 2021). *Cable de conexión*. Obtenido de Wikipedia la enciclopedia libre: https://es.wikipedia.org/wiki/Cable_de_conexi%C3%B3n

Zapata Rodríguez, M. A. (2016). Evaluación de parámetros de calidad de servicio (QOS) para el diseño de una red VPN con MPLS. *[Tesis de Maestria]*. PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR, Quito. Obtenido de http://repositorio.puce.edu.ec/

ANEXOS

ANEXO A.

CONFIGURACION DE ROUTER CISCO SEDE ACORA

```
!
!
hostname R-ACORA
!
vlan 10
!
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key $$VPNIPsec#CRAC119$$ address 181.176.156.172
crypto isakmp keepalive 60 30 periodic
!
!
crypto ipsec transform-set TS esp-3des esp-md5-hmac
 mode tunnel
!
!
!
crypto map vpn-hq 10 ipsec-isakmp
```

```
 set peer 181.176.156.172
 set transform-set TS
 match address VPN-TRAFFIC
!
!
!
!
interface FastEthernet0
 switchport access vlan 10
 no ip address
!
interface FastEthernet1
 switchport access vlan 10
 no ip address
!
interface FastEthernet2
 switchport access vlan 10
 no ip address
!
interface FastEthernet3
 switchport access vlan 10
 no ip address
!
interface FastEthernet4
 ip address 192.168.67.2 255.255.255.0
```

```
 duplex auto
 speed auto
 crypto map vpn-hq
!
interface Vlan10
 ip address 192.168.10.1 255.255.255.0
!
!
ip route 0.0.0.0 0.0.0.0 192.168.67.1
!
ip access-list extended VPN-TRAFFIC
 permit ip 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255
!
```

CONFIGURACION DE ROUTER CISCO SEDE COATA

```
!
hostname R-COATA
!
!
!
vlan 11
!
!
!
crypto isakmp policy 1
```

```
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key $$VPNIPsec#CRAC119$$ address 181.176.156.172
crypto isakmp keepalive 60 30 periodic
!
!
crypto ipsec transform-set TS esp-3des esp-md5-hmac
 mode tunnel
!
!
!
crypto map vpn-hq 11 ipsec-isakmp
 set peer 181.176.156.172
 set transform-set TS
 match address VPN-TRAFFIC
!
!
!
!
!
interface FastEthernet0
 switchport access vlan 11
 no ip address
```

```
!
interface FastEthernet1
 switchport access vlan 11
 no ip address
!
interface FastEthernet2
 switchport access vlan 11
 no ip address
!
interface FastEthernet3
 switchport access vlan 11
 no ip address
!
interface FastEthernet4
 ip address 192.168.234.2 255.255.255.0
 ip mtu 1400
 ip tcp adjust-mss 1300
 duplex auto
 speed auto
 crypto map vpn-hq
!
interface Vlan11
 ip address 192.168.11.1 255.255.255.0
!
!
```

```
ip route 0.0.0.0 0.0.0.0 192.168.234.1
!
ip access-list extended VPN-TRAFFIC
 permit ip 192.168.11.0 0.0.0.255 192.168.100.0 0.0.0.255
!
```

CONFIGURACION DE ROUTER CISCO SEDE TARACO

```
!
hostname R-TARACO
!
!
!
vlan 13
!
!
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key $$VPNIPsec#CRAC119$$ address 181.176.156.172
crypto isakmp keepalive 60 30 periodic
!
!
```

```
crypto ipsec transform-set TS esp-3des esp-md5-hmac
 mode tunnel
!
!
!
crypto map vpn-hq 13 ipsec-isakmp
 set peer 181.176.156.172
 set transform-set TS
 match address VPN-TRAFFIC
!
!
!
!
!
!
interface FastEthernet0
 switchport access vlan 13
 no ip address
!
interface FastEthernet1
 switchport access vlan 13
 no ip address
!
interface FastEthernet2
 switchport access vlan 13
```

```
 no ip address
!
interface FastEthernet3
 switchport access vlan 13
 no ip address
!
interface FastEthernet4
 ip address 192.168.232.2 255.255.255.0
 ip mtu 1400
 ip tcp adjust-mss 1300
 duplex auto
 speed auto
 crypto map vpn-hq
!
interface Vlan13
 ip address 192.168.13.1 255.255.255.0
!
!
ip route 0.0.0.0 0.0.0.0 192.168.232.1
!
ip access-list extended VPN-TRAFFIC
 permit ip 192.168.13.0 0.0.0.255 192.168.100.0 0.0.0.255
!
!
```

CONFIGURACION DE ROUTER CISCO SEDE YUNGUYO

```
!
hostname R-YUNGUYO
!
!
!
vlan 14
!
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key $$VPNIPsec#CRAC119$$ address 181.176.156.172
crypto isakmp keepalive 60 30 periodic
!
!
crypto ipsec transform-set TS esp-3des esp-md5-hmac
 mode tunnel
!
!
!
crypto map vpn-hq 14 ipsec-isakmp
 set peer 181.176.156.172
```

```
 set transform-set TS
 match address VPN-TRAFFIC
!
!
!
!
!
interface FastEthernet0
 switchport access vlan 14
 no ip address
!
interface FastEthernet1
 switchport access vlan 14
 no ip address
!
interface FastEthernet2
 switchport access vlan 14
 no ip address
!
interface FastEthernet3
 switchport access vlan 14
 no ip address
!
!
interface FastEthernet4
```

```
 ip address 192.168.9.2 255.255.255.0
 ip mtu 1400
 ip tcp adjust-mss 1300
 duplex auto
 speed auto
 crypto map vpn-hq
!
!
interface Vlan14
 ip address 192.168.14.1 255.255.255.0
!
!
ip route 0.0.0.0 0.0.0.0 192.168.9.1
!
ip access-list extended VPN-TRAFFIC
 permit ip 192.168.14.0 0.0.0.255 192.168.100.0 0.0.0.255
!
```

CONFIGURACION DE ROUTER CISCO SEDE CABECERA

```
!
hostname R-CABECERA
!
!
vlan 100
```

```
!
!
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key $$VPNIPsec#CRAC119$$ address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 60 30 periodic
!
!
crypto ipsec transform-set TS esp-3des esp-md5-hmac
 mode tunnel
!
crypto dynamic-map hq-vpn 10
 set security-association lifetime seconds 86400
 set transform-set TS
 match address ACORA
crypto dynamic-map hq-vpn 11
 set security-association lifetime seconds 86400
 set transform-set TS
 match address COATA
crypto dynamic-map hq-vpn 13
 set security-association lifetime seconds 86400
```

```
 set transform-set TS
 match address TARACO
crypto dynamic-map hq-vpn 14
 set security-association lifetime seconds 86400
 set transform-set TS
 match address YUNGUYO
!
!
crypto map VPN-BO 1 ipsec-isakmp dynamic hq-vpn
!
!
interface FastEthernet0
 switchport access vlan 100
 no ip address
!
interface FastEthernet1
 switchport access vlan 100
 no ip address
!
interface FastEthernet2
 switchport access vlan 100
 no ip address
!
interface FastEthernet3
 switchport access vlan 100
```

```
 no ip address
!
interface FastEthernet4
 ip address 181.176.156.172 255.255.255.248
 ip mtu 1400
 ip tcp adjust-mss 1300
 duplex auto
 speed auto
 crypto map VPN-BO
!
!
interface Vlan100
 ip address 192.168.100.1 255.255.255.0
 !
!
ip route 0.0.0.0 0.0.0.0 181.176.156.169
!
ip access-list extended ACORA
 permit ip 192.168.100.0 0.0.0.255 192.168.10.0 0.0.0.255
ip access-list extended COATA
 permit ip 192.168.100.0 0.0.0.255 192.168.11.0 0.0.0.255
ip access-list extended TARACO
 permit ip 192.168.100.0 0.0.0.255 192.168.13.0 0.0.0.255
ip access-list extended YUNGUYO
```

permit ip 192.168.100.0 0.0.0.255 192.168.14.0 0.0.0.255

!

ANEXO B.

R-CABECERA#show crypto ipsec sa

interface: GigabitEthernet0

Crypto map tag: VPN-BO, local addr 181.176.156.172

protected vrf: (none)

local ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)

current_peer 201.230.37.79 port 45097

PERMIT, flags={}

#pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3

#pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 181.176.156.172, remote crypto endpt.: 201.230.37.79

path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0

current outbound spi: 0x4A284E6(77759718)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x5153D35C(1364448092)

transform: esp-3des esp-md5-hmac ,

in use settings ={Tunnel UDP-Encaps, }

conn id: 5, flow_id: Onboard VPN:5, sibling_flags 80000046, crypto map: VPN-BO

sa timing: remaining key lifetime (k/sec): (4558637/2570)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x4A284E6(77759718)

transform: esp-3des esp-md5-hmac ,

in use settings ={Tunnel UDP-Encaps, }

conn id: 6, flow_id: Onboard VPN:6, sibling_flags 80000046, crypto map: VPN-BO

sa timing: remaining key lifetime (k/sec): (4558637/2570)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

outbound ah sas:

outbound pcp sas:

protected vrf: (none)

local ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (192.168.11.0/255.255.255.0/0/0)

current_peer 179.6.82.21 port 34245

PERMIT, flags={}

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4

#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 181.176.156.172, remote crypto endpt.: 179.6.82.21

path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0

current outbound spi: 0xB3AB3FD3(3014344659)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x6CCD8666(1825408614)

transform: esp-3des esp-md5-hmac ,

in use settings ={Tunnel UDP-Encaps, }

conn id: 7, flow_id: Onboard VPN:7, sibling_flags 80000046, crypto map: VPN-BO

sa timing: remaining key lifetime (k/sec): (4496526/3525)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0xB3AB3FD3(3014344659)

transform: esp-3des esp-md5-hmac ,

in use settings ={Tunnel UDP-Encaps, }

conn id: 8, flow_id: Onboard VPN:8, sibling_flags 80000046, crypto map: VPN-BO

sa timing: remaining key lifetime (k/sec): (4496526/3525)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

outbound ah sas:

outbound pcp sas:

protected vrf: (none)

local ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (192.168.13.0/255.255.255.0/0/0)

current_peer 181.176.117.197 port 2270

PERMIT, flags={}

#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 7

#pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 7

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 181.176.156.172, remote crypto endpt.: 181.176.117.197

path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0

current outbound spi: 0xFF66086F(4284876911)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0xF5CD0376(4123853686)

transform: esp-3des esp-md5-hmac ,

in use settings ={Tunnel UDP-Encaps, }

conn id: 3, flow_id: Onboard VPN:3, sibling_flags 80000046, crypto map: VPN-BO

sa timing: remaining key lifetime (k/sec): (4591136/2541)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0xFF66086F(4284876911)

transform: esp-3des esp-md5-hmac ,

in use settings ={Tunnel UDP-Encaps, }

conn id: 4, flow_id: Onboard VPN:4, sibling_flags 80000046, crypto map: VPN-BO

sa timing: remaining key lifetime (k/sec): (4591136/2541)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

outbound ah sas:

outbound pcp sas:

protected vrf: (none)

local ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (192.168.14.0/255.255.255.0/0/0)

current_peer 181.64.241.247 port 18694

PERMIT, flags={}

#pkts encaps: 115, #pkts encrypt: 115, #pkts digest: 115

#pkts decaps: 112, #pkts decrypt: 112, #pkts verify: 112

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 181.176.156.172, remote crypto endpt.: 181.64.241.247

path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0

current outbound spi: 0x863949BC(2251901372)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0xC579D25B(3313095259)

transform: esp-3des esp-md5-hmac ,

in use settings ={Tunnel UDP-Encaps, }

conn id: 1, flow_id: Onboard VPN:1, sibling_flags 80000046, crypto map: VPN-BO

sa timing: remaining key lifetime (k/sec): (4541864/1950)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x863949BC(2251901372)

transform: esp-3des esp-md5-hmac ,

in use settings ={Tunnel UDP-Encaps, }

conn id: 2, flow_id: Onboard VPN:2, sibling_flags 80000046, crypto map: VPN-BO

sa timing: remaining key lifetime (k/sec): (4541864/1950)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

outbound ah sas:

outbound pcp sas:

R-CABECERA#

ANEXO C.

Campos de salida interpretación: sh crypto isakmp sa

Nombre	Descripción
Errores de paquetes entrantes (globales)	Las estadísticas de error de los paquetes entrantes globales, de la siguiente manera:
	SPI no válido: la cantidad de paquetes recibidos con un SPI no válido (que no se resuelve en ninguna SA conocida).
	Interfaz no válida: la cantidad de paquetes recibidos con un SPI que es válido en una interfaz diferente a aquella en la que se recibió
Interfaz	La interfaz para la que se muestra la siguiente información de SA.
	Si la lista criptográfica activada en la interfaz también está activada en otras interfaces, estas interfaces también se enumeran aquí.
	Las interfaces en estado 'inactivo' se designan como tales.
ID de lista criptográfica	El ID de la lista criptográfica que contiene las SA que se muestran
Dirección local	La dirección local configurada para la lista criptográfica, utilizada para el extremo del túnel local de todo el tráfico protegido por las SA pertenecientes a la lista criptográfica. La dirección local es un nombre de interfaz o una dirección IP, según la configuración.
Regla	El ID de la regla de la lista criptográfica que contiene las SA que se muestran
Mapa criptográfico	El ID del mapa criptográfico al que apunta la regla, incluida su descripción definida por el usuario
Dirección local	La dirección IP del extremo del tráfico del túnel local protegido por esta SA.
	Si se utiliza NAT transversal, se adjunta el número de puerto de encapsulación UDP.
dirección remota	La dirección IP y, opcionalmente, el nombre de host del interlocutor remoto. Se muestra un nombre de host si el par fue configurado por su FQDN.
	Si se utiliza NAT transversal, se adjunta el número de puerto de encapsulación UDP.
identidad local	La subred local protegida por esta SA, tal como se configuró en la regla de lista criptográfica. La subred se expresa como < *dirección* >/< *comodín* >.
identidad remota	La subred remota protegida por esta SA, tal como se configuró en la regla de lista criptográfica. La subred se expresa como <dirección>/<comodín>.

hombre del camino	La MTU de ruta guardada para esta SA, tal como se recibió de la red mediante mensajes de error de detección de MTU de ruta. Esto no incluye la sobrecarga de encapsulación de IPSec.
persona de los medios	La MTU de medios guardada para esta SA, según lo aprendido de la interfaz subyacente. Esto no incluye la sobrecarga de encapsulación de IPSec.
Spi de salida actual	El valor del SPI de salida actualmente activo, expresado en codificación hexadecimal. Si no existe ninguno,0x0se visualiza.
Paquetes entrantes	Las estadísticas de paquetes entrantes para la regla de lista criptográfica:
	Total: el número total de paquetes entrantes recibidos
	Total OK: el número total de paquetes entrantes recibidos y no descartados
	Descifrar: el número total de paquetes descifrados con éxito
	Verificar: el número total de paquetes verificados con éxito por HMAC
	Decaps: la cantidad total de paquetes desencapsulados con éxito del encabezado del túnel IPSec
	Descomprimido: el número total de paquetes descomprimidos con éxito por el proceso de compresión de carga IP (IPPCP)
	Incompresible: el número total de paquetes sin comprimir recibidos con éxito, cuando IPPCP está habilitado
	Descartes totales: el número total de paquetes descartados debido a algún error. Este número es un agregado de los números más específicos a continuación.
	Longitud no válida: la cantidad de paquetes descartados después de recibirse a través de este túnel, porque la longitud no está alineada con el bloque de cifrado.
	Reproducción fallida: la cantidad de paquetes descartados después de recibirse a través de este túnel, debido a una falla de verificación anti-reproducción
	Sa expirado: la cantidad de paquetes descartados después de recibirse a través de este túnel, porque la vida útil de SA KB es menor que la longitud total del paquete IP externo
	Error de autenticación: la cantidad de paquetes descartados después de recibirse a través de este túnel, debido a una falla de verificación de HMAC
Paquetes entrantes	Relleno incorrecto: la cantidad de paquetes descartados después de ser recibidos a través de este túnel, debido a

	una falla en la recepción del formato del tráiler de ESP incorrecto
	Identidad no válida: la cantidad de paquetes descartados después de recibirse a través de este túnel debido a una identidad no válida. Es decir, la dirección de encabezado de IP interna (original) no coincide con la subred de IP configurada en la regla de lista criptográfica contenedora.
	Desprotegido: la cantidad de paquetes descartados después de recibirlos sin protección (sin protección), aunque se esperaba que llegaran protegidos por este túnel (es decir, paquetes desprotegidos con IP de origen y de destino que coinciden con la subred de IP configurada en la regla de lista criptográfica contenedora).)
	Otros descartes: la cantidad de paquetes descartados debido a otras razones que no fueron cubiertas por los contadores anteriores
	Relación de descompresión general: una medida de la eficiencia de compresión total en el par remoto. Esta es la relación entre el número de octetos resultantes después de la descompresión y el número de octetos recibidos antes de la descompresión, para todos los paquetes, incluidos los paquetes incompresibles.
	Relación de descompresión: una medida de la eficiencia del motor de compresión en el par remoto. Esta es la relación entre el número de octetos resultantes después de la descompresión y el número de octetos recibidos antes de la descompresión, solo para paquetes comprimibles.
	Bytes descomprimidos: el número total de bytes después de la descompresión, incluidos los paquetes incompresibles.
	Comp bytes — el número total de bytes recibidos comprimidos
	Bytes incomprimidos: el número total de bytes incompresibles recibidos, es decir, que se recibieron sin comprimir
Paquetes salientes	Las estadísticas de paquetes salientes para la regla de lista criptográfica:
	Total: el número total de paquetes salientes enviados
	Total OK: el número total de paquetes salientes enviados y no descartados
	Cifrar: el número total de paquetes cifrados con éxito.
	Resumen: el número total de paquetes adjuntos con éxito con un HMAC

	Encaps: el número total de paquetes encapsulados con éxito con un encabezado de túnel IPSec
Paquetes salientes	Comprimido: el número total de paquetes comprimidos con éxito
	Incompresible: el número total de paquetes incompresibles cuando IPPCP está habilitado
	Comp bypass: la cantidad de paquetes incompresibles debido a que el paquete es demasiado corto para comprimirlo
	Comp abort: la cantidad de paquetes incompresibles debido a que el resultado de la compresión es más largo que el paquete original
	Descartes totales: el número total de paquetes descartados debido a algún error
	No sa: la cantidad de paquetes descartados antes de transmitirse a través de este túnel debido a que no existía IPSec SA cuando llegó el paquete.
	Seq rollover: la cantidad de paquetes descartados antes de ser transmitidos a través de este túnel, debido a la transferencia del número de secuencia: el número de secuencia de IPSec SA alcanzó su capacidad.
	Sa caducado: la cantidad de paquetes descartados antes de transmitirse a través de este túnel debido a que SA caducó: la vida útil de KB de SA es menor que la longitud total del paquete IP externo
	Otros descartes: la cantidad de paquetes descartados debido a otras razones no cubiertas por ninguno de los contadores anteriores
	Relación de compresión general: una medida de la eficiencia de compresión total. Esta es la relación entre el número de octetos antes de la compresión y el número de octetos resultantes después de la compresión, para todos los paquetes, incluidos los paquetes incompresibles.
	Relación de compresión: una medida de la eficiencia del motor de compresión. Esta es la relación entre el número de octetos antes de la compresión y el número de octetos resultantes después de la compresión, solo para paquetes comprimibles.
	Bytes descomprimidos: la cantidad de bytes que se presentaron al motor de compresión, incluidos los paquetes incompresibles
	Comp bytes: la cantidad de bytes comprimidos que resultaron del motor de compresión (solo paquetes comprimibles)
	Bytes incomp: el número de bytes de paquetes incompresibles

Tipo SA	El tipo de SA: ESP Entrante o ESP Saliente
SPI	El SPI de la SA en codificación hexadecimal
Transformar	Enumera todas las transformaciones que utiliza la SA. Cada transformación se enumera en una fila separada.
SLP	Muestra información sobre el uso de Perfect Forward Secrecy (PFS), cuando IKE Phase-2 negocia SA. Los valores posibles son:
	No, no se utiliza PFS
	#<N>: PFS se usa con el grupo N de Diffie-Hellman
Quedan segundos	El número de segundos restantes para la expiración de este SA
Quedan KB	El número de kilobytes restantes para el vencimiento de esta SA
Modo	El modo de encapsulación: túnel o transporte

ANEXO D.

ACUERDO PARA LA PRESTACIÓN DEL SERVICIO PÚBLICO DE ARRENDAMIENTO DE CIRCUITOS BAJO LA MODALIDAD DE ABONADO – RED PRIVADA VIRTUAL 3 CLASES DE SERVICIO

DATOS DEL CLIENTE:

RAZON SOCIAL / NOMBRE Y APELLIDOS *	R.U.C./D.N.I./C.E./PASAPORTE*
CAJA RURAL DE AHORRO Y CREDITO LOS ANDES SA	20322445564

NOMBRE DE SUCURSAL 43		SEDE ACORA				
DIRECCIÓN (Av./Calle/Jr.)		CARRE PANAMERICA 320			DEPARTAMENTO	PUNO
DISTRITO	ACORA	URBANIZACIÓN				
PLAN	ANCHO DE BANDA	CLASES DE SERVICIO			PAGO ÚNICO	CARGO FIJO
		CoS1	CoS2	CoS3		
RPV FULL MESH	8 Mbps	1.5 Mbps	2 Mbps	4.5 Mbps	-	US$ 292.64

NOMBRE DE SUCURSAL 8		SEDE COATA				
DIRECCIÓN (Av./Calle/Jr.)		PLAZA DE ARMAS S-N			DEPARTAMENTO	PUNO
DISTRITO	COATA	URBANIZACIÓN				
PLAN	ANCHO DE BANDA	CLASES DE SERVICIO			PAGO ÚNICO	CARGO FIJO
		CoS1	CoS2	CoS3		
RPV FULL MESH	6 Mbps	1 Mbps	1.5 Mbps	3.5 Mbps	-	US$ 235.06

NOMBRE DE SUCURSAL 52		SEDE TARACO				
DIRECCIÓN (Av./Calle/Jr.)		JR 28 DE JULIO S/N			DEPARTAMENTO	PUNO
DISTRITO	TARACO	URBANIZACIÓN				
PLAN	ANCHO DE BANDA	CLASES DE SERVICIO			PAGO ÚNICO	CARGO FIJO
		CoS1	CoS2	CoS3		
RPV FULL MESH	8 Mbps	1.5 Mbps	2 Mbps	4.5 Mbps	-	US$ 292.64

NOMBRE DE SUCURSAL 17		SEDE YUNGUYO				
DIRECCIÓN (Av./Calle/Jr.)		JR CUSCO 330			DEPARTAMENTO	PUNO
DISTRITO	YUNGUYO	URBANIZACIÓN				
PLAN	ANCHO DE BANDA	CLASES DE SERVICIO			PAGO ÚNICO	CARGO FIJO
		CoS1	CoS2	CoS3		
RPV FULL MESH	6 Mbps	1 Mbps	1.5 Mbps	3.5 Mbps	-	US$ 235.06

Los costos de la propuesta no incluyen IGV.

El tipo de cambio que se considera es de 3.5, para la conversión de Dólares a Soles.

ANEXO E.

CAJA LOS ANDES
BANCA DE INCLUSIÓN SOCIAL

ACTA DE CIERRE DE PROYECTO

DATOS

Empresa / Organización	Caja Rural De Ahorro Y Crédito Los Andes SA
Proyecto	Diseño e Implementación de VPN IPSec
Fecha	2019-2020
Encargado	Wilmer Alvaro Mamani Quispe

SUPERVISOR / ENCARGADO

Nombre	Cargo	Gerencia
Jose Eduardo Coasaca Curaca	JEFE USIC	Tecnología de Información
Wilmer Alvaro Mamani Quispe	Analista de Infraestructura	Tecnología de Información

RAZON DE CIERRE

Por medio de la presente, se da cierre formal al proyecto "Diseño e Implementación de VPN IPSec", por las razones especificadas en la siguiente ficha.

Entrega de proyecto en funcionamiento con conformidad del supervisor	X

ACEPTACION APROBADOR

Supervisor	Fecha	Firma
Eduardo Coasaca	2020	

Jr. Junin # 129 - Puno ☎ 051-368808 FAX: 051 - 369224
E-mail: craclosandes@cajarurallosandes.com ✉ 305