MEJORAS EN EL SISTEMA DE TRANSMISIÓN DE INFORMACIÓN BIOMÉTRICA ADQUIRIDA A PARTIR DE LAS TERMINALES MÓVILES DEL FONDO NACIONAL DEL AHORRO (FNA) MEDIANTE VPN

ANDREACAMILA FORERO ORTIZ

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA ELECTRÓNICA
BOGOTA
2014

MEJORAS EN EL SISTEMA DE TRANSMISIÓN DE INFORMACIÓN BIOMÉTRICA ADQUIRIDA A PARTIR DE LAS TERMINALES MÓVILES DEL FONDO NACIONAL DEL AHORRO (FNA) MEDIANTE VPN

ANDREACAMILA FORERO ORTIZ
2127714

Monografía para optar al Título de Ingeniera Electrónica

Asesor:
Ing. Angélica Salazar Madrigal
Docente Facultad de Ingeniería Electrónica.

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA ELECTRÓNICA
BOGOTA
2014

RECTOR GENERAL
Padre Carlos Mario Álzate Montes, O.P

VICERRECTOR ADMINISTRATIVO Y FINANCIERO GENERAL
Padre Diego Orlando Serna Salazar O.P.

VICERRECTOR ACADÉMICO GENERAL
Padre Eduardo González Gil, O.P.

SECRETARIO
Doctor Héctor Fabio Jaramillo Santamaría

DECANO DIVISIÓN DE INGENIERÍAS
Padre Pedro José Díaz Camacho, O.P.

SECRETARIA DE DIVISIÓN
Ec. Myriam Gómez Colmenares

DECANA FACULTAD DE INGENIERÍA ELECTRÓNICA
Ingeniera Adriana Páez Pino.

Nota de Aceptación

_____
_____
_____
_____
_____
_____
_____

_____

Tutor Monografía

_____

Jurado

_____

Jurado

Bogotá, Octubre de 2014

La Universidad Santo Tomás no se hace responsable de las opiniones y conceptos expresados por los autores en el trabajo de grado, solo velará porque no se publique nada contrario al dogma ni a la moral católica y porque el trabajo no tenga ataques personales y únicamente se vea el anhelo de buscar la verdad científica.

Capítulo III –Art. 46 del Reglamento de la Universidad Santo Tomás.

TABLA DE CONTENIDO

LISTA DE FIGURAS 8
INTRODUCCIÓN 9
CAPITULO I. DESCRIPCIÓN DEL PROYECTO 12
1. PLANTEAMIENTO DEL PROBLEMA 13
2. JUSTIFICACIÓN 16
3. OBJETIVOS 17
4. METODOLOGÍA 18
5. DELIMITACIÓN DEL PROYECTO 19
CAPITULO II. DE LA EMPRESA 20
5.1 RESEÑA DE ORANGE BUSINESS SERVICES 21
5.2 ACTIVIDADES DE LA EMPRESA 22
6. PRÁCTICA EN ORANGE BUSINESS SERVICES 23
CAPITULO III. DE LA TEMÁTICA 24
7. VIRTUAL PRIVATE NETWORK (VPN) 25
7.1 DEFINICIÓN 25
7.2 CLASIFICACIÓN 26
7.3 PARÁMETROS IMPORTANTES A TENER EN CUENTA PARA CONFIGURAR UNA VPN 29
7.4 OTROS CONCEPTOS ÚTILES A TENER EN CUENTA: 32
CAPITULO IV. DEL PROYECTO 33
8. DESARROLLO DEL PROYECTO 34
8.1 CONTEXTO 34
8.2 VALIDACIÓN BIOMÉTRICA Y ENROLAMIENTO 35
8.3 CONFIGURACIÓN DE LA VPN 37
8.4 VERIFICANDO LA CONEXIÓN A LA VPN 42
9. FUNDAMENTACIÓN HUMANÍSTICA 44
CAPITULO V. CONCLUSIONES 47
CAPITULO VI. VALOR AGREGADO Y TRABAJOS FUTUROS 49

REFERENCIAS BIBLIOGRÁFICAS 51

LISTA DE FIGURAS

Fig. 1. Esquema de desarrollo del proyecto 14
Fig. 2. Diagrama de flujo del Proceso de Enrolamiento. 15
Fig. 3. Diagrama estructural de las principales áreas de la empresa Orange. 23
Fig. 4. Actividades de los pasantes en la empresa. 23
Fig. 5 Esquema general de una VPN. 26
Fig. 6. Escenario de los elementos físicos en una VPN de Acceso Remoto. 27
Fig. 7. Escenario de los elementos físicos en una VPN Site-to-Site 28
Fig. 8. Configuración de IPsec 30
Fig. 9. Configuración L2TP/IPsec- 31
Fig. 10. Esquema de la Plataforma tecnológica que soporta los servicios de biometría para el intercambio de información entre los asesores remotos y la sede principal del FNA. 35
Fig. 11. Estación Biométrica Móvil 36
Fig. 12. Información biográfica y Biométrica del cliente desde la plataforma de gestión. 36
Fig. 13. Configuración estándar de la red en Cisco. 37
Fig. 14. Interfaz gráfica de acceso a escritorio. 43
Fig. 15. Información de acceso a la VPN 43
Fig. 16. Verificación de conexión a la VPN 44

INTRODUCCIÓN

Los sistemas de comunicaciones a través del tiempo han permitido a los seres humanos optimizar la gran mayoría de sus proyectos; parte de las soluciones que se implementaron han logrado con su ejecución realizar corrección de errores en tiempo real, la respuesta inmediata a los procesos que se llevan a cabo, el control de estos, la creación de canales que permitan asegurar la información que viaja por ellos, llegar a puntos remotos comunicando territorios, lo cual ha convertido a las comunicaciones en un motor de la transmisión de la información.

Tomando como base el incremento que han tenido las diferentes soluciones en el campo de las comunicaciones cada vez es mayor la evolución de diferentes tecnologías que de la mano con las telecomunicaciones y con equipos especializados que están a la vanguardia del avance de las tecnologías de la información y las comunicaciones (TIC), estructuran y apoyan los procesos que se llevan a cabo, con el fin de asegurar el óptimo funcionamiento y así mismo garantizar a los usuarios la seguridad en todos los procesos.

En este orden de ideas, es evidente que las grandes empresas buscan soluciones que les permitan mantener a salvo el punto más frágil de cualquier organización: su información. Factor que estimula a la vez la búsqueda de nuevas alternativas para soportar este tipo de sucesos con equipos y dispositivos capaces de unificar variedad de servicios y asegurar el óptimo funcionamiento de estos y de la misma forma, garantizar a los usuarios la seguridad en el manejo de la información más susceptible.

En este documento se presenta la solución planteada para el Fondo Nacional del Ahorro (FNA) en la cual se buscó mejorar el sistema de la transmisión de Información biométrica obtenida a partir de las terminales móviles del FNA a partir del uso de una Red Privada Virtual (VPN). Se encuentra dividido en 5 capítulos en los cuales se describe el desarrollo del proyecto, el primer apartado corresponde al planteamiento de la problemática a tratar, el objeto de la solución y la delimitación de la misma, una parte que contiene la información de la empresa Orange Business Services y las actividades que el pasante realizó en la pasantía empresarial; un capítulo que presenta la descripción, clasificación e importancia de las VPN (Redes privadas virtuales) en el desarrollo del proyecto, seguido del capítulo en el que se expone el proceso de la solución al problema planteado en los capítulos iniciales y se resalta la importancia de la labor realizada por el Ingeniero Electrónico tomasino, partiendo del análisis del impacto de la solución realizada y evaluando de forma ética, responsable, crítica y creativa las

consecuencias de las acciones y determinaciones del estudiante, que darán solución a las necesidades del FNA (Fondo Nacional del Ahorro) en cuanto a la transmisión de la información biométrica.

CAPITULO I. DESCRIPCIÓN DEL PROYECTO

En el Capítulo I, se describe el planteamiento de la problemática del Fondo Nacional del Ahorro, que representa el punto de partida en el proceso para dar solución al problema, también se presentan los objetivos y la delimitación y alcances de este proyecto.

1. PLANTEAMIENTO DEL PROBLEMA

La dificultad que presenta actualmente el FNA (Fondo Nacional del Ahorro) Entidad Financiera del Estado, radica en la carencia de una solución que permita transmitir la información de verificación en el menor tiempo posible; ya que por aspectos como el tamaño de la información obtenida para identificar al usuario, como las imágenes adquiridas a partir de todos los equipos de biometría y la forma en la que el asesor del FNA debe sincronizar la información obtenida con el aplicativo COBIS con la base de datos general en el servidor, situación representa un tiempo adicional en el proceso que podría utilizarse de una mejor manera, se ha recurrido a utilizar equipos que operan con resoluciones más bajas, de los cuales se obtienen imágenes de menor tamaño que se transmiten en menor tiempo factor que en muchos casos impide la correcta identificación del cliente, ya que no se tiene una imagen de buena calidad del rostro del afiliado.

El propósito de este trabajo consiste en el desarrollo de una solución a la problemática planteada, que permita abarcar las necesidades e intereses del FNA mejorando la forma de administrar la información biométrica, llevando a cabo la transmisión sin comprometer la información, es decir, evitando su posible pérdida e interceptación, garantizando la reducción de tiempos del sistema de transmisión y validación de la información, proporcionando una solución que beneficie al asesor, en la cual él logre acceder a la red corporativa en el menor tiempo posible para sincronizar los registros con la base de datos. Esta solución beneficiará a los clientes del FNA, ya que garantiza la seguridad y la integridad de la información.

A continuación se presenta el esquema implementado para el desarrollo del proyecto, en el cual se describe el proceso llevado a cabo para obtener la solución al problema planteado, la cual requiere garantizar seguridad, confiabilidad y confidencialidad a través de una herramienta que permita al asesor del FNA acceder remotamente a la información tanto de los clientes antiguos como de los

nuevos, conectándose a la red corporativa del FNA a partir de una VPN (Red virtual privada).

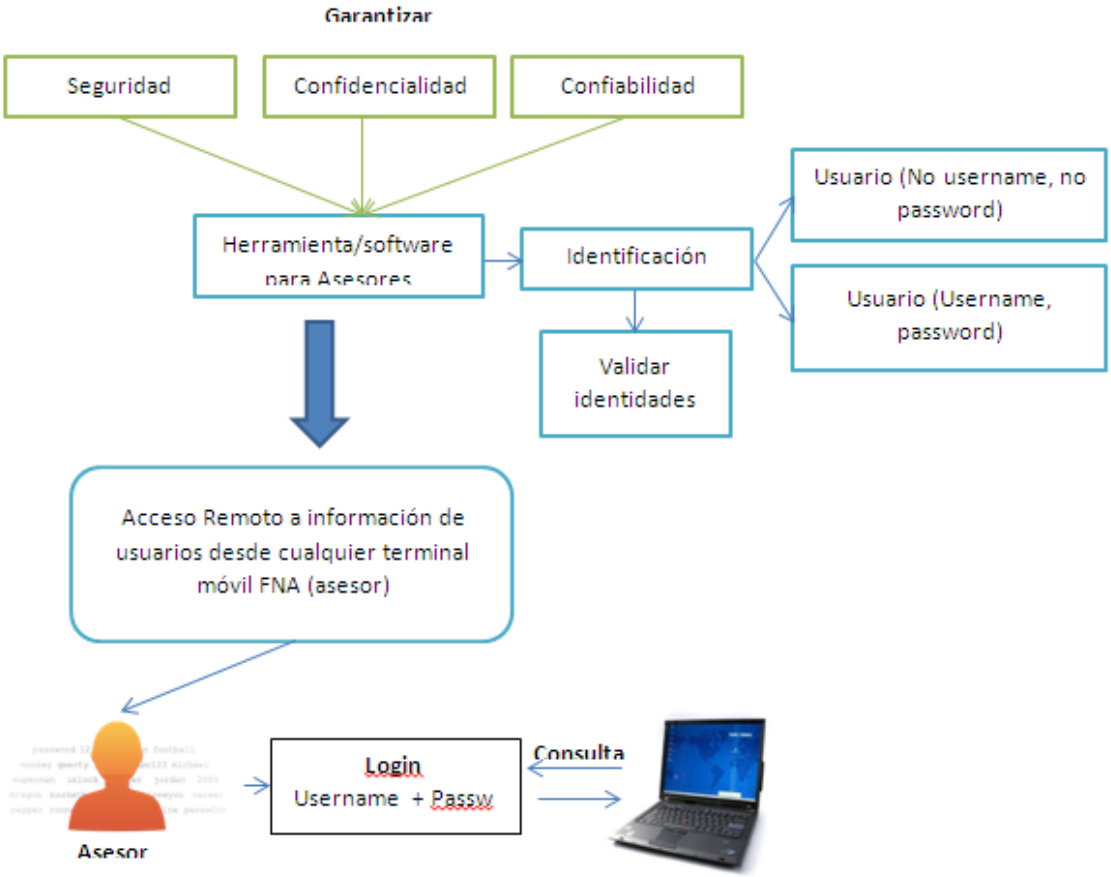

Fig. 1. Esquema de desarrollo del proyecto

Teniendo en cuenta que el proceso de Enrolamiento (Adición de nuevos clientes a la base de datos) incluye el proceso de Autenticación de los clientes, la solución hará énfasis en identificar el tipo de actividad que se llevará a cabo con cada cliente, dependiendo si se trata de un registro nuevo, un registro existente o un registro sospechoso, caso en el cual, al actualizar la información del cliente se presenten inconsistencias en la información biométrica, y consultando finalmente dicha información en las bases de datos de los diferentes servidores como se aprecia en la Fig. 2.

Proceso de enrolamiento de clientes dependiendo del tipo de cliente.

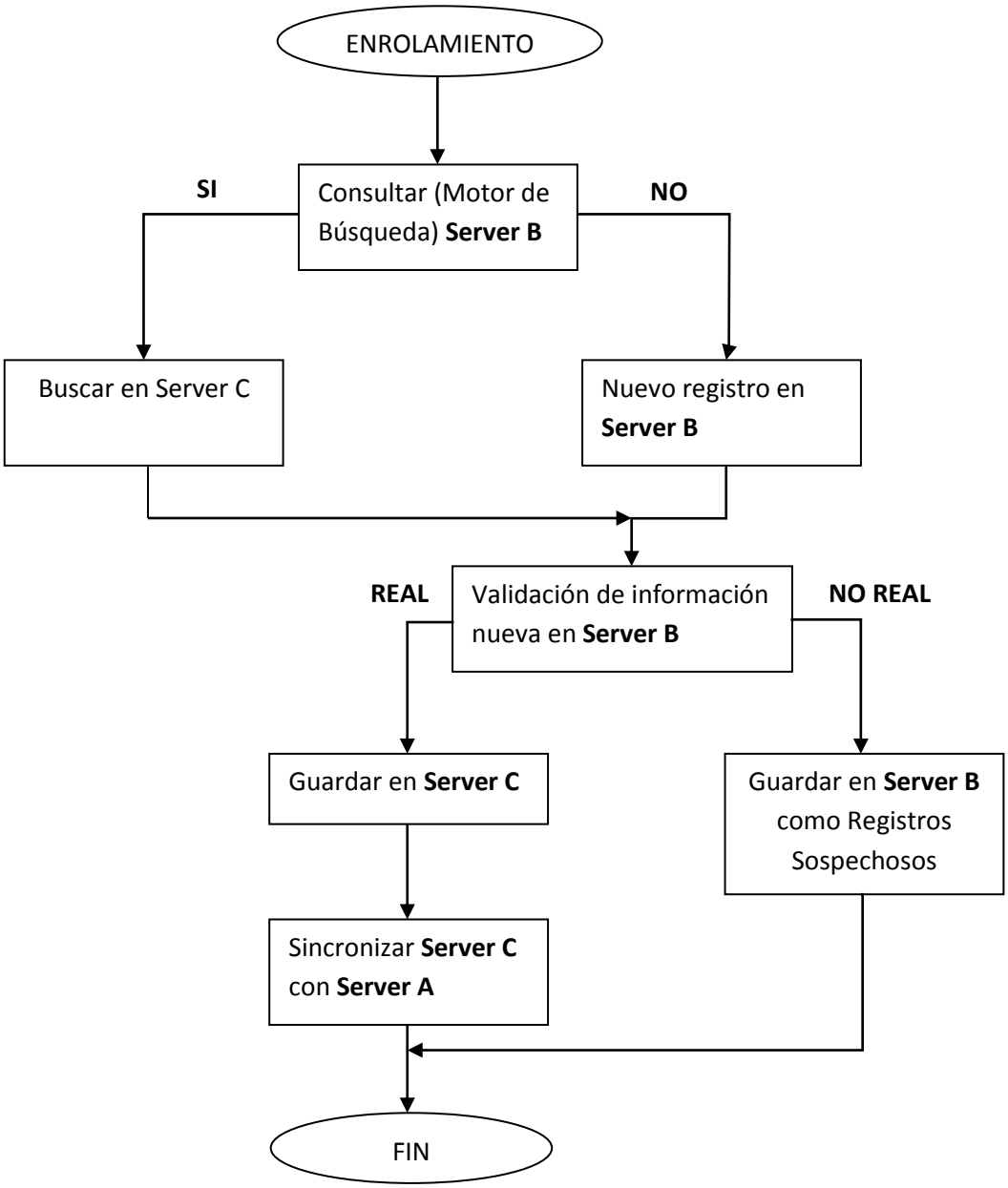

Fig. 2. Diagrama de flujo del Proceso de Enrolamiento.

2. JUSTIFICACIÓN

Los beneficios que aporta la realización de este proyecto se ven reflejados en la mejora de las condiciones tanto para el FNA como para sus clientes, quienes se benefician con la solución que responde a las necesidades de la empresa, ya que no es necesario que estos se acerquen a una sede del FNA para registrar su información personal porque el asesor se dirige a su domicilio, gestiona solicitudes y proporciona la información que el cliente necesite saber. En cuanto al FNA, la solución representa un alto beneficio, ya que se enfoca en reducir los tiempos en el proceso de la transmisión de la información biométrica de los clientes, y en mejorar el tiempo que transcurre en la actualización de la información de registro de los clientes en las bases de datos remotamente, suprimiendo tiempos de desplazamiento que resultan ser innecesarios y poco productivos, en los cuales, gracias a la solución, el asesor puede registrar mayor cantidad de información de clientes para su posterior estudio.

Por otra parte, la solución garantiza la seguridad del tráfico de la información enviada, protegiendo los recursos compartidos de la red interna de la empresa, a partir de las políticas que permiten y/o limitan el acceso a determinada información de la compañía, evitando personas ajenas a los procesos del FNA tengan acceso a la información de los clientes.

El proyecto que se presenta en este documento tiene como finalidad proporcionar una solución a un problema real que gira en torno a la susceptibilidad de la información que administra el FNA de sus clientes en cuanto a su seguridad, haciendo referencia a una solución que se realizó para dar solución al problema de la transmisión de la información biométrica desde las terminales móviles del FNA, con las herramientas proporcionadas por la empresa ***Orange Business Services*** y obtenidas a partir de la investigación y documentación de la tecnología utilizada para dar solución al punto vulnerable identificado: la seguridad de la información. En efecto resulta importante para el FNA, garantizar a sus clientes la tranquilidad y confianza respecto al tratamiento transparente de su información de identidad, la cual representa un aspecto muy sensible en estos días, en los que se presentan hurtos por suplantación de identidades y clonación de documentos de identidad en transacciones.
La solución a la problemática planteada que responde a la necesidad del cliente de la Empresa Orange, el Fondo Nacional del Ahorro, es fruto de la indagación e investigación y se da a conocer en este documento, en el cual se dejan las puertas

abiertas para acciones de mejora, ya que se trata de un modelo escalable y flexible en cuanto a las mejoras en el proceso de encriptación de la información.

3. OBJETIVOS

OBJETIVO GENERAL

Desarrollar una solución que permita optimizar el proceso de transmisión y recepción de información obtenida a partir de equipos biométricos con el fin de mejorar y afianzar la seguridad en los procesos de identificación de usuarios en el Fondo Nacional del Ahorro (FNA).

OBJETIVOS ESPECÍFICOS

- Optimizar la solución a la cual se llegue en el proceso de investigación, para reducir en el proceso factores como tiempo de transmisión y recepción de la información y dinero, teniendo en cuenta que lo ideal es buscar una opción que se ajuste tanto al presupuesto del cliente como a la disponibilidad de la empresa.

- Diseñar una solución confiable que permita la identificación de clientes y usuarios en el Fondo Nacional del Ahorro al momento de realizar transacciones, o diferentes tipos de situaciones en las cuales se requiera la validación plena del usuario.

- Salvaguardar los intereses tanto de clientes como del Fondo Nacional del Ahorro a partir de una herramienta que permita el acceso remoto a la información del usuario desde cualquier terminal móvil del FNA, garantizando un proceso transparente y seguro con el manejo de dicha información confidencial.

4. METODOLOGÍA

La solución se construyó a partir de la indagación primaria del proceso real que se lleva a cabo para la adquisición y el manejo de la información. Esta se obtuvo a través de los ingenieros de la empresa ***Orange Business Services*** que se encontraban en su momento asignados en la administración del proyecto, tanto en el área de Logística como en el área de Operaciones, quienes dieron a conocer en términos generales el proceso que lleva a cabo el FNA en cuanto a la administración de la información de sus clientes y algunos procesos que se realizan con los mismos y la información acerca de los equipos utilizados en el proyecto de Biometría de la empresa Orange con su cliente el FNA.

Cabe resaltar, como se mencionó anteriormente, que la información tanto técnica como comercial del funcionamiento del proyecto de Biometría, fue muy general y limitada, ya que se obtuvo conforme a las políticas de privacidad de la información tanto de la empresa ***Orange Business Services*** como del cliente Fondo Nacional del Ahorro, por tratarse de información sensible y susceptible a interceptaciones.

En cuanto al FNA, fue necesario conocer el proceso que realiza la entidad para reclutar nuevos clientes y guardar su información en una base de datos que debe sincronizarse dependiendo del tipo de cliente, actividad conocida como enrolamiento y la estructura del sistema vigente que cuenta con bases de datos que almacenan la información del proceso de enrolamiento. En lo que respecta a la empresa Orange, la plataforma que soporta los servicios del proyecto de Biometría cuenta con un servidor que cumple la función de ser el buscador para identificar en las bases de datos la información que se requiere encontrar, otro servidor que sirve de back-up y opera en tiempo real y los equipos utilizados para adquirir la información biométrica del cliente: lector de huella biométrico, lector bidimensional, cámara, scanner y dispositivos para digitalizar la firma del cliente.

Posteriormente, se indagó acerca del funcionamiento de las redes privadas virtuales (VPN), la importancia de su uso y las diferentes configuraciones de este tipo de red, eligiendo la que mejor se adaptaba al escenario propuesto en la Fig. 1.

5. DELIMITACIÓN DEL PROYECTO

El desarrollo de este proyecto se enfocó en el diseño de una solución en la red que permitiera optimizar el sistema de operación existente utilizado por el Fondo Nacional del ahorro para la administración de la información de los clientes teniendo en cuenta que el proceso vigente descrito en el planteamiento del problema, no incluye tecnología alguna que relacione una solución en comunicaciones. La solución proporcionada surge de la investigación académica y teórica del uso de una red VPN para garantizar la seguridad del tráfico de la información de contacto de los clientes, no es una solución comercializada e implementada actualmente por la empresa Orange Business Services a su cliente el Fondo Nacional de Ahorro.

El propósito de este proyecto es el planteamiento de una solución que cambia el tipo de transmisión y administración de la información de enrolamiento de los clientes del FNA, a partir de este proyecto se pueden llegar a obtener mejores ideas para dar solución a los problemas que traiga consigo el tiempo que tarda el FNA en almacenar y administrar la información de nuevos clientes.

La solución brindada no modifica ninguno de los procesos internos del tratamiento y dirección de información de la empresa Orange, como por ejemplo la asignación de servidores principales o la topología general de la red, sólo se limita a garantizar el tráfico seguro de la información y el cambio de procesos básicos de recolección de información de los clientes.

CAPITULO II.
DE LA EMPRESA

En el Capítulo II, se describe la actividad económica de la Empresa Orange Business Services, que incursiona en el campo de las telecomunicaciones, se presenta una reseña histórica de la evolución de la empresa y la labor de los pasantes en las diferentes áreas de la empresa.

6. ORANGE BUSINESS SERVICES

En la actualidad, Orange Business Services es una empresa que incursiona fuertemente en el campo de las telecomunicaciones brindando un amplio portafolio de servicios en soluciones tanto técnicas como logísticas de comunicaciones.

6.1 RESEÑA DE ORANGE BUSINESS SERVICES[1]

Inicialmente Orange se posesionaba en el mercado inglés como una marca de telefonía móvil, convirtiéndose con el tiempo en una de las principales marcas a nivel mundial de banda ancha, contenidos y servicios asociados destinados tanto a particulares como a empresas.

Posteriormente, en una alianza con France Telecom, se creó el Grupo Orange France Telecom, el cual, representa uno de los operadores de telecomunicaciones líderes en el mundo; ofreciendo comunicación móvil y de Internet fijo a 226 millones de clientes en 32 países. Es un líder mundial en servicios de comunicaciones para empresas de todos los tamaños en Francia y multinacionales con Orange Business Services[2]

La empresa Equant Colombia S.A. siendo una empresa Orange Business Services ha estado en Colombia desde el año de 1994, presente en 8 de las principales ciudades del país; ofreciendo el conjunto de datos e IP más completo, la integración de sistemas y soluciones de infraestructura y de gestión, ofreciendo servicios de adquisición, instalación, configuración y mantenimiento como solución integral para los clientes, mejorando la calidad de vida del personal y clientes.

Teniendo en cuenta que el desarrollo de las nuevas tecnologías de la información y las comunicaciones (TIC) es más rápido que el dominio de su uso, Orange permanece en un constante y auténtico desafío, para permitir que todo el mundo pueda beneficiarse del progreso de la tecnología, a partir del desarrollo de sus

[1]ORANGE BUSINESS SERVICES. [Sitio en Internet] Disponible en: http://www.orange-business.com/fr/entreprise/
[2]ORANGE BUSINESS SERVICES.Enterprise [Sitio en Internet] Disponible en: http://www.orange-business.com/fr/entreprise/a-propos-de/nous-connaitre/index.jsp

medios de acceso y a los servicios útiles para la vida cotidiana. Orange trabaja con tecnología de punta, brindando soluciones óptimas, líderes, y eficientes respaldadas por los productos y la experiencia que ofrece la asociación con Cisco Systems entre otras compañías líderes en las tecnologías de comunicación.

Entre sus principales clientes se encuentran ETB, Superintendencia de Notariado y Registro, Carvajal, Banco de Crédito y el Fondo Nacional del Ahorro. También apoyan a las grandes empresas multinacionales como Glaxo, Bimbo, Adidas, y la mayor parte del tráfico de aerolíneas; ofreciendo productos y soporte en seguridad, mercados emergentes, cloud-computing y movilidad.[3]

6.2 ACTIVIDADES DE ORANGE BUSSINES SERVICES

6.2.1 Productos y Soluciones:

Orange se encuentra en la capacidad como empresa, de comercializar equipos de redes, garantizando a sus clientes la adquisición de equipos directamente de fábrica, brindando también soporte en la instalación de dichos equipos, según sea la necesidad del cliente.

El cliente puede también adquirir soluciones en comunicaciones, telefonía IP y virtualización. Los ingenieros de esta área dependiendo de las necesidades de los clientes, diseñan proyectos para dar solución a la solicitud realizada, incluyendo el diseño de la red, los equipos a utilizar, la configuración de estos y los servicios requeridos. También se cuenta con un área de soporte técnico de los equipos como garantía de los proyectos, en la cual, ingenieros especializados se encargan de verificar los problemas que puedan presentar los equipos a nivel de software y hardware.

6.2.2 Área de Soporte:

El área de soporte se encarga de brindar tanto asesoría técnica de los equipos instalados de los diferentes proyectos como del monitoreo de muchos de los enlaces de los clientes principales como el FNA, ETB, Claro entre otros clientes.

[3]ORANGE BUSINESS SERVICES Colombia.[Sitio en Internet] Disponible en: http://www.orange-business.com/en/mnc2/footer/local/office_colombia/colombia/

7. PRÁCTICA EN ORANGE BUSINESS SERVICES

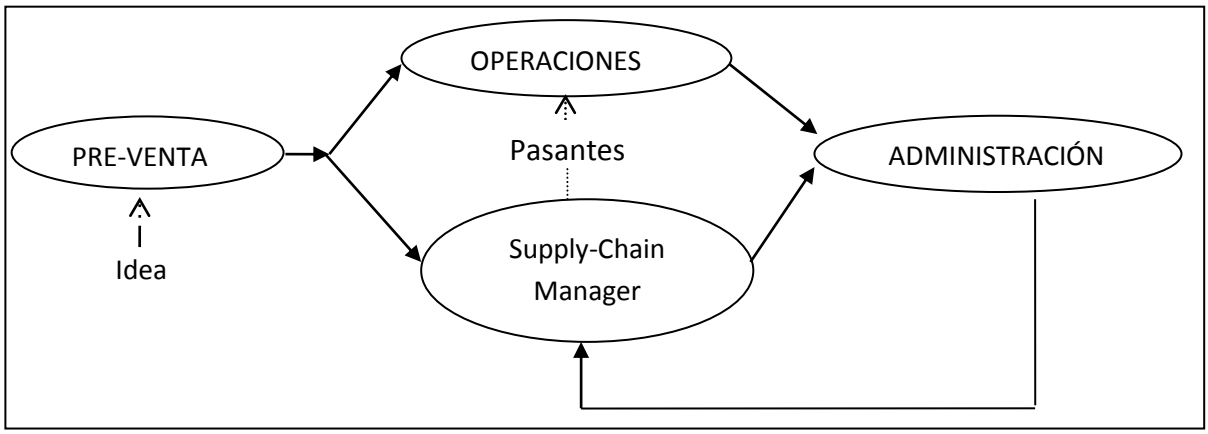

Fig. 3. Diagrama estructural de las principales áreas de la empresa Orange.

En la Fig. 3. se observa la ubicación de los pasantes en la Empresa Orange en el diagrama estructural. Los pasantes hacen parte del área de Operaciones y del área de "Supply-Chain Manager" o el área de Logística.

Las actividades realizadas en la empresa Orange se relacionan en la Figura 4, los pasantes desempeñaban las actividades laborales que incluían el Ingreso y Salida de equipos de telecomunicaciones, administración de los equipos y la realización de un proyecto basado en la necesidad de un cliente.

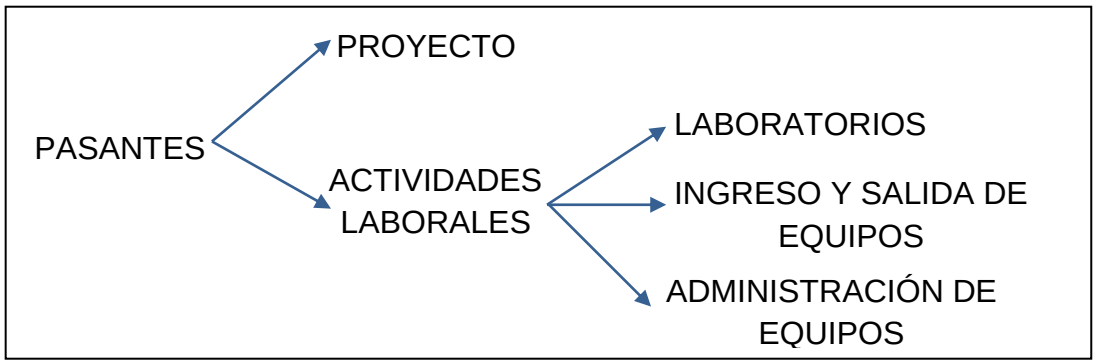

Fig. 4. Actividades de los pasantes en la empresa.

CAPITULO III. DE LA TEMÁTICA

El Capítulo III, contiene toda la información correspondiente a la definición, características, clases, ventajas, protocolos y configuración de las redes privadas virtuales VPN.

8. VIRTUAL PRIVATE NETWORK (VPN)

La solución realizada requirió la creación de una red privada virtual, que soporta el tráfico de la información de los clientes del FNA.

7.1 DEFINICIÓN

Una VPN es un tipo de red virtual que a partir de una red pública permite conectar remotamente usuarios o sitios por medio de conexiones "virtuales" enrutadas a través de internet desde la red privada de la compañía hasta el sitio remoto. La VPN debe garantizar seguridad, confiabilidad y rapidez haciendo uso de protocolos de seguridad y encriptación de datos, asegurando la confidencialidad y autenticidad de los mismos. El esquema de funcionamiento general de una VPN se observa en la Fig. 5, en la cual una persona puede acceder a una red corporativa desde cualquier lugar a través de una VPN.

Características:

- Garantiza la confidencialidad de la información que viaja por la red.
- Debe cumplir con proporcionar a los usuarios la seguridad, confiabilidad y rapidez de la red.
- Confidencialidad de los datos: Los datos son encriptados de tal forma que, codificando la información que viaja en la red pública, estos llegan a su destino, donde la información es descifrada.
- Virtual: No es una red real directa que conecta entre sí dos o más sitios; es sólo una conexión virtual proporcionada por un software, normalmente sobre redes públicas como Internet
- Privada: Sólo a los miembros de la compañía conectados a través del software VPN les es permitido tener acceso a la información que ha sido transferida[4]

[4]Beginning Open VPN 2. 0. 9: Build and Integrate Virtual Private Networks Using OpenVPN. Markus Feilner. Packt Publishing Ltd.2009

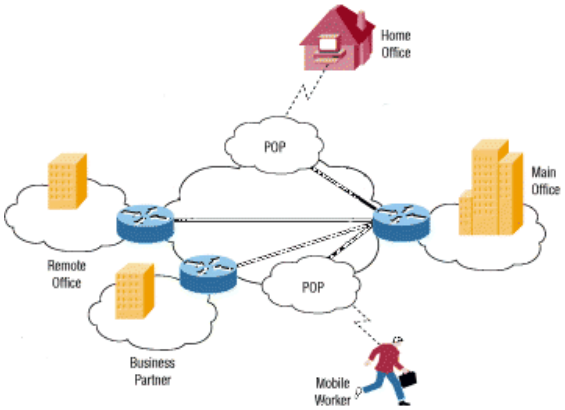

Fig. 5 Esquema general de una VPN[5]

Ventajas de una VPN:

- La escalabilidad es una de las mayores ventajas de las VPN sobre las líneas dedicadas, ya que la distancia geográfica no influye en los costos de la VPN.
- Como una VPN funciona a partir de Internet, permite conectar redes físicamente separadas, no depende del uso de un canal dedicado.

Cuando se hace uso de una VPN, el administrador de la red asegura que sólo aquellos usuarios que estén identificados y posean los permisos de ingreso (configurados en las políticas de privacidad) tengan acceso a los recursos protegidos de la empresa; todas las comunicaciones a través de la VPN pueden encriptarse para efectos de confidencialidad de datos.[6]

7.2 CLASIFICACIÓN

Según la Arquitectura de Conexión, las VPN se clasifican en dos tipos: REMOTE ACCESS (De Acceso Remoto) y SITE-TO-SITE (Punto a Punto).[7]

---

[5] CISCO SYSTEMS, IPSec Negotiation/IKE Protocols, How Virtual Private Networks Work. [Sitio en Internet] Disponible en: http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html

[6] MICROSOFT WINDOWS NT SERVER, Red Privada Virtual: Una descripción general. Microsoft Corporation.

[7] REDES PRIVADAS VIRTUALES (VPN) Tipos de VPN [Sitio de Internet] Disponible en: http://it.aut.uah.es/enrique/docencia/ii/seguridad/documentos/t9-0506.pdf

7.3 REMOTE ACCESS VPN

Las redes VPN de tipo Remote-Access permiten conexiones seguras y encriptadas entre la red privada de una empresa y los usuarios remotos a través de un proveedor de servicios. Cada una de las sedes remotas establecerá un túnel seguro utilizando la conexión a Internet para acceder a la VPN. El esquema de conexión general de este tipo de VPN se aprecia en la Figura 6.

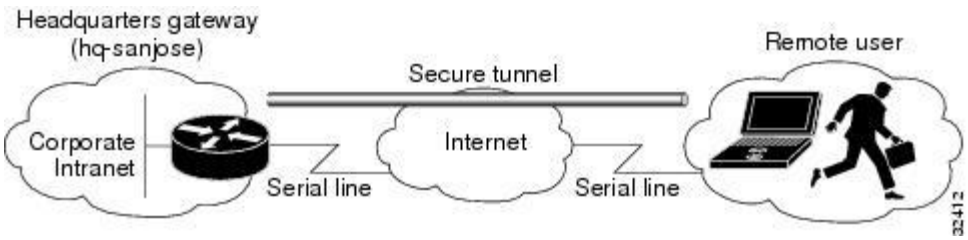

Fig. 6. Escenario de los elementos físicos en una VPN de Acceso Remoto[8]

En una configuración de Acceso Remoto, un usuario remoto se encuentra interconectado con una sede principal a través de Internet, por medio de una conexión segura a través de un túnel, sobre Internet. El usuario remoto tiene la capacidad de acceder a la información que le sea permitida, este acceso es configurado desde el Core (sede principal), que a partir de las políticas, establece los permisos y restricciones de acceso para dicho usuario a la red corporativa El core utiliza una puerta de enlace VPN de Cisco y el usuario remoto se conecta a la VPN a través de un software de cliente VPN desde un PC.

7.3.1 Tecnologías y Protocolos

Entre los protocolos que permiten una configuración de Acceso Remoto se encuentran:[9]

- PPTP
- L2tpv2

[8]CISCO SYSTEMS Remote Access VPN Business Scenarios.[Sitio en Internet] Disponible en: http://www.cisco.com/c/en/us/td/docs/security/vpn_modules/6342/vpn_cg/6342vpn4.html

[9] COMPARING, DESIGNING, AND DEPLOYING VPNS. By Mark Lewis (CCIE.) [Sitio en Internet] Disponible en: http://books.google.com.co/books?id=PMRmPPjTkVsC&pg=PA408&dq=vpn+site+to+site&hl=es-419&sa=X&ei=MTPHU7WhI4fhsATA9YDQDg&ved=0CBkQ6AEwAA#v=onepage&q=vpn%20site%20to%20site&f=false

- IPsec
- SSL

7.4 SITE –TO-SITE VPN

Una VPN tipo Site-to-Site es usualmente implementada en la conexión de una o varias oficinas o sedes a la sede principal de una organización. En la sede principal (Core) se establece el túnel VPN que permite la conexión vía Internet proveniente de los sitios que están conectándose a esta, como se observa en la Figura 7.

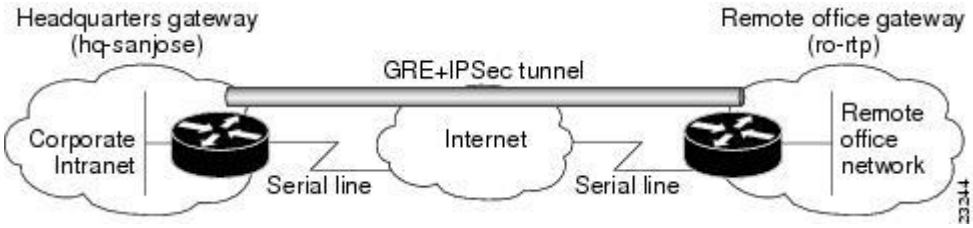

Fig. 7. Escenario de los elementos físicos en una VPN Site-to-Site[10]

Este tipo de configuración ha resultado favorable para las empresas, ya que ha sustituido la configuración antigua que permitía la conexión segura entre sedes sólo a partir de canales dedicados, solución que representa un alto incremento en el costo comparado con la implementación de una VPN, que proporciona una conexión rápida y segura.

7.4.1 Tecnologías y Protocolos

Entre los protocolos que permiten una configuración de Acceso Remoto se encuentran:[11]

- IPsec
- GRE
- Draft Martini
- L2TPv3
- MPLS

[10]CISCO SYSTEMS Site-to-Site and Extranet VPN Business Scenarios [Sitio en Internet] Disponible en: http://www.cisco.com/c/en/us/td/docs/security/vpn_modules/6342/vpn_cg/6342site3.html#wp1035810
[11]COMPARING, DESIGNING, AND DEPLOYING VPNS. By Mark Lewis (CCIE.) [Sitio en Internet] Disponible en: http://books.google.com.co/books?id=PMRmPPjTkVsC&pg=PA408&dq=vpn+site+to+site&hl=es-419&sa=X&ei=MTPHU7WhI4fhsATA9YDQDg&ved=0CBkQ6AEwAA#v=onepage&q=vpn%20site%20to%20site&f=false

7.5 PARÁMETROS IMPORTANTES A TENER EN CUENTA PARA CONFIGURAR UNA VPN

A continuación se mencionan los Protocolos de Encriptación y otros conceptos útiles para tener en cuenta en la configuración de una VPN.

7.5.1 IPSEC

IPsec es un protocolo diseñado con el fin de proteger el tráfico IP en su tránsito por una red intermedia. Proporciona servicios de autenticación además de la confidencialidad de los servicios. [12] Permite que las cargas útiles IP sean encriptadas y posteriormente se encapsulen en un encabezado IP para enviarse a través de una red corporativa IP o una red pública como Internet. IPSec define funciones que aseguran la confidencialidad: encriptación e integridad de los datos.

IPSec emplea mecanismos criptográficos en la capa de red[13]:

- Autentificación de cada paquete IP.
- Verificación de la integridad de los datos.
- Confidencialidad de los paquetes con carga útil.

Este protocolo proporciona un mecanismo para la transmisión segura de los datos asegurando confidencialidad, integridad y autenticidad. En el caso de las redes VPN de configuración Site-to-Site, IPSec construye túneles entre los sitios de la organización que se encuentran conectados a esta, una vez se estabilizan dichos túneles, permiten el transporte de tráfico transparente y seguro. En el caso de las redes VPN de configuración de Acceso Remoto IPSec túnel es construido entre el escritorio de los usuarios y el security Gateway del sitio corporativo[14].

La configuración de túnel en el protocolo IPSec utiliza el método de seguridad negociada con el fin de encapsular y encriptar paquetes completos de IP para transferencia segura a través de internet IP público o privado. El paquete encriptado se encapsula de nuevo con un indicador IP de texto sencillo y se envía entre-redes para entregarse al servidor de túnel. Cuando el datagrama lo recibe,

[12] Ibíd.
[13] ISCW Implementign Secure Corverged Wide Area Networks, Versión 1.0, version 0.1-21.06, Cisco Systems.
[14] Troubleshooting Virtual Private Networks. Mark Lewis. Cisco Press. 2004

el servidor de túnel procesa y descarta el iniciador IP de texto sencillo y desencripta sus contenidos para retirar el paquete original IP de carga de pago. El paquete IP de carga de pago se procesa normalmente y se encamina a su red objetiva.[15]

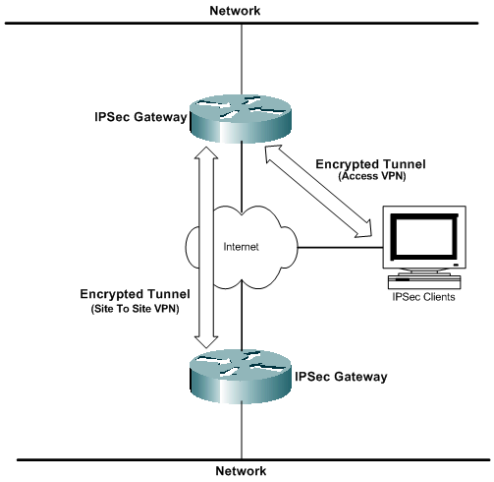

Fig. 8. Configuración de IPsec[16]

7.5.2 PPTP/MPPE (POINT TO POINT)

- **PPTP/MPPE (POINT TO POINT)**

PPTP es un protocolo de red que permite la transferencia segura de datos desde un cliente remoto a un servidor de la empresa privada mediante la creación de una VPN a través de redes basadas en TCP / IP de datos. PPTP apoya a la carta, multiprotocolo, red privada virtual a través de redes públicas, como Internet.[17]Éste protocolo permite que el tráfico sea encriptado y posteriormente se encapsule en un encabezado IP, para enviarse a través de una red.

MPPE es una tecnología de codificación desarrollado por Microsoft para cifrar los enlaces punto a punto. Estas conexiones PPP pueden ser a través de una línea de

[15] Microsoft Windows 2000 Server, Seguridad de red privada virtual de Microsoft.
[16] CISCO SYSTEMS IPSec Negotiation/IKE Protocols, Which VPN Solution is Right for You? [Sitio en Internet] Disponible en http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14147-which-vpn.html
[17]CISCO SYSTEMS Remote Access VPN Business Scenarios[Sitio en Internet] Disponible en http://www.cisco.com/c/en/us/td/docs/security/vpn_modules/6342/vpn_cg/6342vpn4.html

acceso telefónico o a través de un túnel VPN. MPPE trabaja como sub-función de Microsoft Point-to-Point Compresión (MPPC).

MPPE utiliza el algoritmo RC4, ya sea con 40 - o claves de 128 bits. Todas las claves se derivan de la contraseña de autenticación en texto plano del usuario. RC4 es cifrado de flujo, por lo tanto, los tamaños de los marcos cifrados y descifrados son del mismo tamaño que la trama original. La implementación de Cisco de MPPE es totalmente interoperable con la de Microsoft y utiliza todas las opciones disponibles, incluyendo el modo sin historia, donde se puede aumentar el rendimiento en entornos de altas pérdidas, tales como VPNs.

Encapsula paquetes PPP en datagramas IP para su transmisión bajo redes basadas en TCP/IP. [18]
Suele involucrar tres actores:

- Un cliente PPTP
- Un servidor de acceso de red (NAS)
- Un servidor PPTP

- **L2TP/IPsec-**

Para VPN site-to-site, el protocolo de encapsulamiento es usualmente IPsec o Generic-Routing-Encapsulation (GRE). GRE incluye información de que tipo de paquete se está encapsulando e información acerca de la conexión entre el servidor y el cliente. En la figura 9 se observa la configuración para el protocolo L2TP/IPsec.

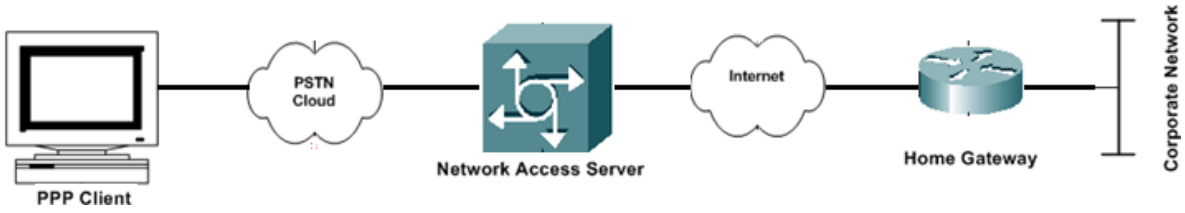

Fig. 9. Configuración L2TP/IPsec-

[18] Redes Privadas Virtuales (VPN) [Sitio en Internet] Disponible en http://it.aut.uah.es/enrique/docencia/ii/seguridad/documentos/t9-0506.pdf

L2TP es una extensión del protocolo punto a punto (PPP) y con frecuencia es un bloque de construcción fundamental para VPNs. L2TP combina las mejores características de los otros dos protocolos de túnel: Layer 2 Forwarding (L2F) de Cisco Systems y PPTP de Microsoft. L2TP es un Grupo de Tareas de Ingeniería de Internet (IETF) estándar emergente.

7.6 OTROS CONCEPTOS ÚTILES A TENER EN CUENTA PARA CONFIGURAR UNA VPN:

- SPLIT TUNNELING
- CRYPTO MAPS
- AAA(AuthenticationAuthorizationAccounting)
- ISAKMP (gestiona la negociación de conexiones y define sus
- propiedades mediante asociaciones de seguridad (SA))
- ESP (Encapsulating Security Payload)
- AH (AuthenticationHeader)
- PROTOCOLOS IKE (Negociación de parámetros y claves)

Finalmente, una VPN requiere abarcar los siguientes aspectos para garantizar una conexión y un flujo seguro de la información: [19]

- Confidencialidad de los datos
- Integridad de la información
- Origen de los datos de autenticación
- Anti Replay

[19] CISCO SYSTEMS IPSec Negotiation/IKE Protocols How Virtual Private Networks Work [Sitio en Internet] Disponible en: http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html

CAPITULO IV. DEL PROYECTO

El Capítulo IV presenta el desarrollo del proyecto, partiendo de contextualizar al lector de la situación y los procesos que actualmente lleva a cabo el FNA para el tratamiento y administración de la información biométrica, la descripción detallada de la solución que se realizó para dar solución al problema de la transmisión de la información biométrica, se describe el proceso de enrolamiento del FNA, los equipos utilizados para este fin y finalmente se describe el proceso de la configuración de la VPN para permitir a un asesor conectarse a la red corporativa de la empresa de forma remota.

9. DESARROLLO DEL PROYECTO

9.1 CONTEXTO

El proceso que actualmente se realiza para actualizar dicha información biométrica y biográfica y cargarla en las bases de datos se lleva a cabo una vez el asesor recorre cierto sector geográfico. Cuando éste finaliza la atención a los clientes, se dirige a una de las sedes principales del FNA, se conecta a la Intranet y a través de la Plataforma de Gestión sincroniza toda la información adquirida previamente, tales como los registros de nuevos clientes y la actualización de datos de los clientes existentes. Este proceso es algo inoficioso si el asesor debe dirigirse cada vez a una sede principal para sincronizar la información. Implica pérdidas de tiempo por desplazamiento, aumento de costos y exposición de la seguridad del asesor así como de los equipos de la estación biométrica móvil y por supuesto de la información sensible de los clientes consultados y enrolados.

Adicional a esto, también existe el caso en el que cada formulario que debe ser diligenciado por los clientes, cuando no se cuenta con una estación móvil cercana posteriormente debe ser digitalizado. Esta acción no garantiza al 100% la adquisición de la información correcta, por errores en el mal diligenciamiento de los formularios o en su defecto en el momento de digitar la información.

El recurso que se planteó para dar solución a estas situaciones, fue la creación de una red privada virtual VPN entre la sede principal y el Asesor del FNA, da tal forma que, una vez éste logre conectarse a Internet, pueda acceder a la red corporativa del FNA y sincronizar la información adquirida de los clientes directamente, evitando el desplazamiento hacia las sedes principales para tal fin.

Como inicialmente se manifestó, la solución realizada garantiza al FNA y beneficia a sus clientes en cuanto a la seguridad del flujo de información. La solución que se planteó para el problema de la optimización de los procesos en el proyecto de biometría, se observa en el esquema de la figura 10.

Fig. 10. Esquema de la Plataforma tecnológica que soporta los servicios de biometría para el intercambio de información entre los asesores remotos y la sede principal del FNA.

9.2 VALIDACIÓN BIOMÉTRICA Y ENROLAMIENTO

Cuando un asesor del FNA se encuentra presentando el portafolio de servicios a los clientes desde cualquier punto del país, a partir de la plataforma de identidad, puede realizar las siguientes acciones: Enrolamiento, Autenticación y Consulta, con las que se identifica al cliente, quien se vería beneficiado al adquirir cualquier producto del FNA, sin necesidad de presentarse a una oficina del FNA para registrar su información de contacto.

Para realizar dicho registro, proceso conocido como enrolamiento, el asesor hace uso de una terminal biométrica para registrar toda la información que permitirá identificar el tipo de cliente y el estado financiero de este.

El asesor cuenta con una plataforma de gestión de identidad que le permite registrar la información biográfica y biométrica de los afiliados, con el fin de permitir procesos de verificación e identificación automática de identidad por medio de la información de las huellas dactilares. La plataforma COBIS posee componentes que son almacenados en los diferentes servidores según sea el caso, para la utilización de las funciones de enrolamiento, autenticación y consulta de imágenes. Una Estación Biométrica Móvil se compone de los siguientes equipos, que permiten al asesor registrar la información del cliente a enrolar como se muestra en la siguiente Figura:

Fig. 11. Estación Biométrica Móvil

Fig. 12. Información biográfica y Biométrica del cliente desde la plataforma de gestión.

Tabla 1. Equipos de la Estación Móvil Biométrica.

Equipo	Características
Cámara Web	Resolución de imagen de hasta 1.3 Megapíxeles
Lector de huella	Reconocimiento automático de calidad de huella
Panel de firma	Resolución de imagen de hasta 800 x 400
Lector de Código 2D	Compatible con el estándar PDF-471
Scanner	Resolución de imagen de hasta 600 dpi
Impresora	Velocidad de impresión de hasta 17 ppm
PC Portátil	HP, Proc. Intel Core Duo T2050, Disco 120 GB, Mem. 1GB, DVD+/-R/RW/RAM y CD-RW

9.3 CONFIGURACIÓN DE LA VPN

La solución realizada, hace uso de una VPN de tipo Acceso Remoto (Remote Access) como se observa en la Figura 13, para conectar a los asesores remotos con la sede principal del FNA y de esta forma actualizar en tiempo real la información de los clientes en la plataforma de gestión.

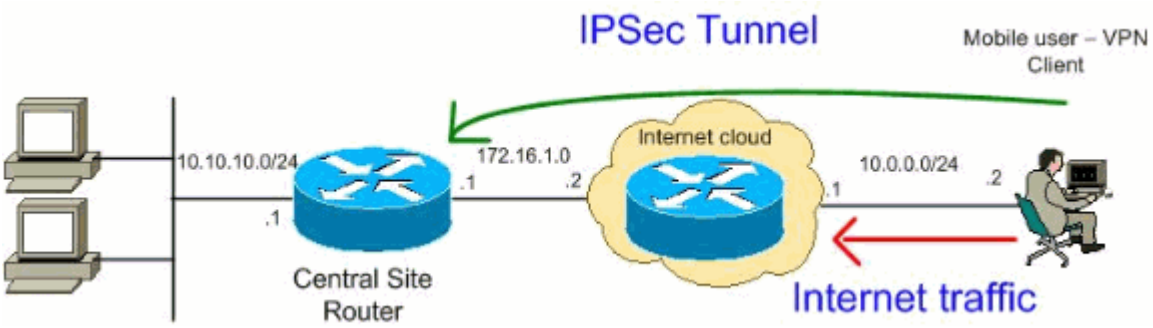

Fig. 13. Configuración estándar de la red en Cisco.[20]

[20] CISCO SYSTEMS Router Allows VPN Clients to Connect IPsec and Internet Using Split Tunneling Configuration Example [Sitio en Internet] Disponible en http://www.cisco.com/c/en/us/support/docs/routers/3600-series-multiservice-platforms/91193-rtr-ipsec-internet-connect.html#config

El diseño de la red se llevó a cabo en el software Cisco PacketTracer V.6.0.1, por lo tanto los equipos utilizados son marca Cisco. Aspecto que beneficia económicamente a la Empresa Orange Business Services con su marca Equant, por ser una empresa Partner de Cisco, ya que la adquisición de los equipos se hace directamente con la empresa.

Para configurar la VPN con equipos Cisco fueron necesarios:

- Router Cisco 2811 y 2620 with Cisco IOS Software
- Cisco VPN Client 4.8 (Software utilizado por el asesor remoto para conectarse a Internet de forma segura a través de la VPN del FNA)

Los asesores remotos establecen una conexión segura con el software de cliente VPN instalado en sus PC. El Cliente VPN inicia una conexión a un dispositivo de sitio central configurado para aceptar estas solicitudes. En este caso, el equipo central es un Router de Cisco que utiliza mapas criptográficos dinámicos.

Se utilizó el Protocolo IPsec con la configuración de Split Tunneling para configurar la VPN, inicialmente se llama a la configuración AAA (autenticación, autorización y contabilidad), se define la lista de control de acceso ACL, se define el rango de direcciones entre los cuales debe estar la dirección IP del asesor que esté intentando conectarse a la red, teniendo en cuenta que por defecto cada usuario por el equipo desde el que se conecte posee una dirección IP, al crearse la VPN, dicho equipo recibe otra dirección IP, la cual se encuentra dentro del rango de las direcciones definidas en IP pool, se definen las políticas de privacidad y finalmente a partir de crypto mapas dinámicos, se asocian todos los parámetros de configuración con la VPN.

La configuración que se muestra a continuación hace referencia a la conexión para un solo usuario, el usuario **user** con password **cisco** se habilita para tener acceso a la red del FNA por medio de una VPN. Se pueden definir dos fases en la configuración, en una primera fase, se configura la red con el protocolo **isakmp**, posteriormente, pasamos a una segunda fase en la cual se configura con **transform set** la forma en la que se cifran los datos.

Configuración de **Router 3, (R_Office)**

hostnameR_Office

%Estableciendo la configuración de los parámetros AAA, se crea un nuevo modelo, será un usuario local perteneciente a un grupo de usuarios%
aaa new-model
aaa authentication login userauthen local
aaa authorization network groupauthor local
!
%Se define el usuario y a contraseña de acceso%
usernameuserpassword 0 cisco
!
cryptoisakmp policy 3
encr 3des%Prioridad 3DES, (Data Encriptaton Standard)
authentication pre-share %Config. Por defecto, llaves precargadas
group 2%Define Algoritmo DiffieHellman, algoritmo que permite intercambiar llaves de forma segura.
!
%Configuración de la lista de control de acceso ACL
Se definen los permisos de acceso que tienen los asesores remotos que se conectan a la red%
cryptoisakmp client configuration group **vpnclient**%grupo
key cisco123%key
poolippool%Rango de direcciones en las que debe estar la dirección de la persona que intente conectarse a la red, key cisco 123 es la clave de acceso para poder conectarse.
!
cryptoipsectransform-setmyset esp-3des esp-md5-hmac%Transform Set define cuáles políticas de seguridad se aplican al tráfico de entrada y salida, Myset es el nombre que le estoy asignando a esa transformación, esp-3des esp-md5-hmac son los algoritmos de cifrado que voy a utilizar y la función hash utilizada, la cual valida que la información que se recibe es la correcta, sin alteraciones.
!
%Reverse route, enruta la información hacia el túnel de la VPN.
crypto dynamic-map dynmap 10 set transform-set myset
reverse-route
!
crypto map clientmap client authentication list userauthen
crypto map clientmapisakmp authorization list groupauthor
crypto map clientmap client configuration address respond
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
!
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
duplex auto

speed auto
!
interface FastEthernet0/1
ip address 172.16.1.1 255.255.255.248
duplex auto
speed auto
crypto map clientmap
!
interface FastEthernet0/2/0
switchport mode access
shutdown
!
interface FastEthernet0/2/1
switchport mode access
shutdown
!
interface FastEthernet0/2/2
switchport mode access
shutdown
!
interface FastEthernet0/2/3
switchport mode access
shutdown
!
interface Serial0/3/0
noip address
shutdown
!
interface Serial0/3/1
noip address
shutdown
!
interface Vlan1
noip address
shutdown
!
ip local pool ippool 192.168.1.5 192.168.1.10**%se define el rango de direcciones que se asigna a los clientes de la VPN**
ipclassless
iproute 0.0.0.0 0.0.0.0 172.16.1.2
!

access-list 101 permitip 10.10.10.0 **0.0.0.255** 192.168.1.**0 0.0.0.255** **%permite las IP's con su wildcard (en la máscara de la ip, se intercambian 1 por 0 y 0 por 1)**
!
line con 0
line aux 0
linevty 0 4
!
End

Configuración de lado del Asesor Remoto:

Cabe resaltar, que la configuración de la VPN, se realizó desde el Router R_Office. La configuración en el Router 2, vista desde el cliente, es la siguiente:

hostnameR_Cliente
!
interface FastEthernet0/0
ip address 10.10.10.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/0
noip address
shutdown
!
interface Serial0/1
noip address
shutdown
!
interface Ethernet1/0
ip address 172.16.1.2 255.255.255.248
duplex auto
speed auto
!
interface Ethernet1/1
noip address
duplex auto
speed auto
shutdown
!
interface Ethernet1/2

```
noip address
duplex auto
speed auto
shutdown
!
interface Ethernet1/3
noip address
duplex auto
speed auto
shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
line con 0
!
line aux 0
!
linevty 0 4
login
!
End
```

9.4 VERIFICANDO LA CONEXIÓN A LA VPN

En un entorno real, el usuario debe hacer uso de una herramienta adicional conocida como VPN Client para introducir la información que le permitirá autenticarse como usuario con acceso a la red.
Teniendo en cuenta que la red creada se encuentra simulada en el software Cisco Packet Tracer, hay una opción para verificar que la configuración realizada es la correcta, que se logró crear la VPN y que el o los usuarios configurados para acceder a esta pueden conectarse.

Accediendo desde el equipo del asesor remoto, Packet Tracer nos proporciona una interfaz gráfica como se observa en la Figura 14, en la cual, entre otras opciones, podemos conectarnos a la red VPN, desde la opción VPN Configuration, que se encuentra señalada en rojo.

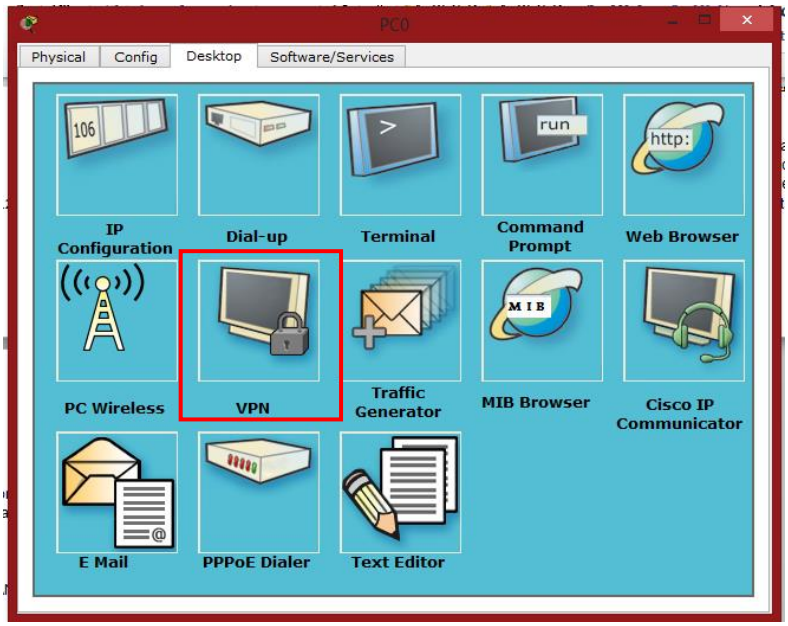

Fig. 14. Interfaz gráfica de acceso a escritorio.

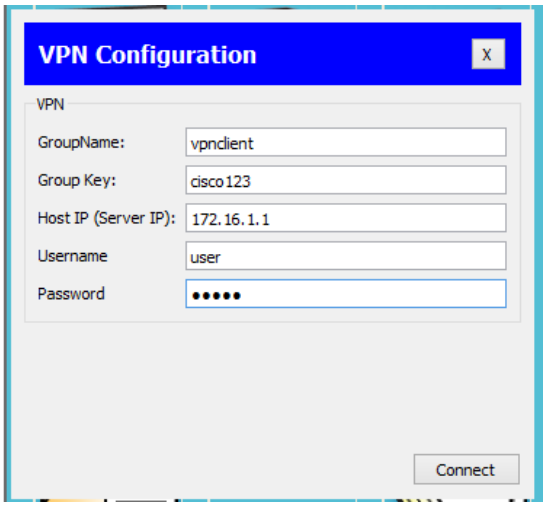

Fig. 15. Información de acceso a la VPN

Se valida que la información que esté proporcionando el usuario sea la correcta y finalmente, informa al usuario que ya se encuentra conectado a la VPN, como se observa a continuación:

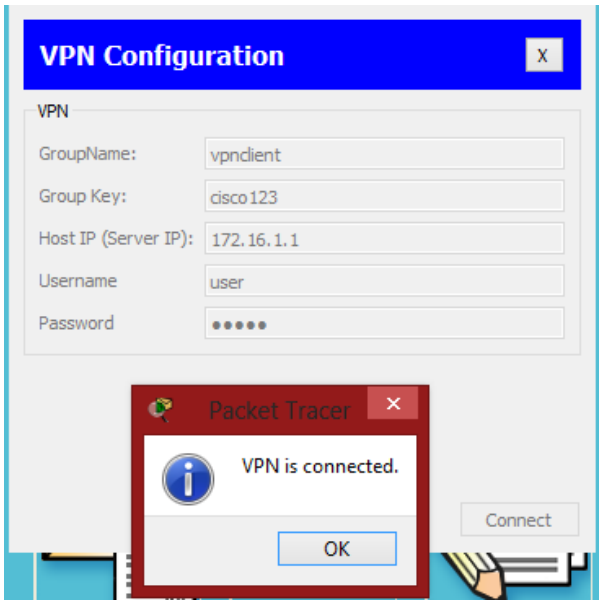

Fig. 16. Verificación de conexión a la VPN

10. FUNDAMENTACIÓN HUMANÍSTICA

El hombre en el transcurso de la historia ha buscado a través del estudio, la indagación y la experiencia, incrementar su conocimiento y explorar las barreras del pensamiento para llegar cada vez más lejos, explorando los límites de su imaginación, buscando lograr lo inalcanzable y realizar lo impensable.

Actualmente, nos encontramos en una era tecnológica naciente, que promueve la innovación y el desarrollo, lo cual le implica a la sociedad, tener más recursos a su alcance, simplificar tareas y optimizar procesos, conforme a las necesidades sociales, políticas, económicas y éticas.

Las Telecomunicaciones en la actualidad presentan al mundo avances tecnológicos visibles, rompiendo las barreras de la distancia y el tiempo, posibilitando un mundo con mayor conectividad, y procurando mayor acceso a la información de forma inmediata y segura.

Es así como, las redes privadas virtuales (VPN) son de gran ayuda para las empresas que buscan salvaguardar los intereses de la compañía y la información de muchos procesos internos que son de interés exclusivo de las mismas. Estas brindan seguridad y confianza en que representan una solución transparente a las necesidades de seguridad de la información de las empresas. Sin embargo no dejan de ser vulnerables ante el ataque de personas que quieran infiltrarse y hacer uso de dicha información con otros propósitos. El reto de este trabajo es plantear una posible solución que garantice un flujo información de una manera rápida y segura en el FNA, asegurando la transparencia de los procesos, manejo adecuado de la información, siendo esto un aspecto sensible y de riesgo para las empresas, en caso de no llevarse a cabo

De esta manera, el papel que desempeña el profesional tomasino conforme al progreso del ser humano en este campo, en la era tecnológica surgente, representa un proceso de alta responsabilidad y un compromiso ético con sí mismo y con la sociedad, ya que, no sólo como seres humanos, sino también como ingenieros, tenemos la responsabilidad en nuestras manos de proporcionar a una sociedad ansiosa de avances e innovación tecnológica, las soluciones que beneficien y suplan las necesidades del día a día, teniendo en cuenta que el ser humano, como ser racional, es responsable de sus acciones, aspecto que lo convierte en un ser consciente que debe asumir las implicaciones de su responsabilidad. En su desempeño profesional, el ingeniero electrónico, debe

estar en capacidad de proporcionar soluciones constructivas, innovadoras y creativas que respondan a las necesidades sociales de forma ética, integral y crítica.

Conscientes de esta alta responsabilidad, es necesario no pasar por alto que, el avance de la tecnología no puede ser la involución de la humanidad, que la tecnología nunca puede afectar su integridad. Ante esta era de progreso y desarrollo tecnológico los Tomasinos debemos actuar de forma ética, crítica y creativa, de acuerdo a nuestros principios y a la formación humanística infundida en el proceso de educativo.

CAPITULO V. CONCLUSIONES

Se realizó un proyecto diseñando una solución real y factible acorde a la necesidad presentada por uno de los clientes más importantes de la empresa Orange Business Service, el Fondo Nacional del Ahorro FNA, para optimizar el proceso de transmisión de la información biométrica desde las terminales móviles, salvaguardando los intereses del FNA y de sus clientes, con el fin de mejorar los procesos actuales en el manejo de la información.

- La solución se realizó conforme a los intereses de la empresa Orange y del cliente el FNA, haciendo uso de la ventaja que representa la implementación de soluciones Cisco y la frecuente adquisición de equipos de tecnología en telecomunicaciones. La solución tecnológica a la que se llegó a partir del estudio del caso, representa una opción de mejora en el proceso, ya que se incrementa la velocidad de transmisión de la información mediante el uso de protocolos nuevos, que garantizan la seguridad en el tráfico de la información.

- Se presentó un modelo inicial, flexible a mejoras y escalable, que permite en cuanto al diseño de la red adicionar más equipos que futuramente puedan involucrarse en el proceso de la transmisión de la información y nuevos protocolos de encriptación que mejoren las condiciones de seguridad de la información en su tráfico por la VPN a través de una red pública.

- A partir de la realización del proyecto se concluye que una VPN es una herramienta bastante útil y necesaria en las empresas ya que, genera tranquilidad y confianza en que la información susceptible de la empresa, y en el caso puntual del proyecto, puede transitar de forma segura y el acceso y uso de esta información está limitado a personas de la empresa en específico, siendo responsables del uso de la información. Una empresa que utiliza una VPN para asegurar que el tráfico de la información privada, balances financieros o información contable se encuentre disponible sólo para las personas que tienen el dominio exclusivo de esta, está menos expuesta a infiltraciones, robos de información financiera, que una empresa que no presta importancia a la protección de su información susceptible, de la cual hace uso en redes públicas como el Internet que no garantizan la seguridad de los datos y están propensos a ser infiltrados y suplantados.

CAPITULO VI. VALOR AGREGADO Y TRABAJOS FUTUROS

El proyecto presentado es resultado de una propuesta para mejorar los procesos actuales que se realizan en el proyecto de Biometría con el FNA, la misma está sujeta a modificaciones, acciones y desarrollos futuros que permitan incrementar el nivel de seguridad del tráfico de la información, detectando amenazas de infiltración a la red. La configuración de las políticas de seguridad pueden ir variando de acuerdo a las necesidades y solicitudes del cliente (FNA).

En cuanto a la estación móvil del FNA, pueden adquirirse equipos que integren los elementos de verificación de información biométrica, representando una ventaja que beneficia tanto a la empresa Orange por la adquisición de menor número de equipos biométricos como al personal del FNA que hace uso de los mismos, exponiendo menos la seguridad del funcionario que trabaja diariamente con estos equipos que son muy visibles.

En cuanto al aplicativo que permite administrar la información biográfica y biométrica pueden desarrollarse mejoras, en las que, por ejemplo, sólo se pueda tener acceso a él para consultar y/o ingresar información, pero no extraerla, dependiendo del tipo de asesor que tenga acceso a la información y el nivel de seguridad del entorno empresarial.

REFERENCIAS BIBLIOGRÁFICAS

1. ORANGE BUSINESS SERVICES Colombia. [Sitio en Internet] Disponible en: http://www.orange-business.com/en/mnc2/footer/local/office_colombia/colombia/

2. ORANGE BUSINESS SERVICES. [Sitio en Internet] Disponible en: http://www.orange-business.com/fr/entreprise/

3. ORANGE BUSINESS SERVICES.Enterprise [Sitio en Internet] Disponible en: http://www.orange-business.com/fr/entreprise/a-propos-de/nous-connaitre/index.jsp

4. ORANGE BUSINESS SERVICES Colombia. [Sitio en Internet] Disponible en: http://www.orange-business.com/en/mnc2/footer/local/office_colombia/colombia

5. Beginning Open VPN 2. 0. 9: Build and Integrate Virtual Private Networks Using OpenVPN. Markus Feilner. Packt Publishing Ltd.2009

6. CISCO SYSTEMS, IPSec Negotiation/IKE Protocols, How Virtual Private Networks Work. [Sitio en Internet] Disponible en: http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html

7. MICROSOFT WINDOWS NT SERVER, Red Privada Virtual: Una descripción general. Microsoft Corporation.

8. REDES PRIVADAS VIRTUALES (VPN) Tipos de VPN [Sitio de Internet] Disponible en: http://it.aut.uah.es/enrique/docencia/ii/seguridad/documentos/t9-0506.pdf

9. CISCO SYSTEMS Remote Access VPN Business Scenarios.[Sitio en Internet] Disponible en: http://www.cisco.com/c/en/us/td/docs/security/vpn_modules/6342/vpn_cg/6342vpn4.html

10. COMPARING, DESIGNING, AND DEPLOYING VPNS. By Mark Lewis (CCIE.) [Sitio en Internet] Disponible en: http://books.google.com.co/books?id=PMRmPPjTkVsC&pg=PA408&dq=vpn+site+to+site&hl=es-

419&sa=X&ei=MTPHU7WhI4fhsATA9YDQDg&ved=0CBkQ6AEwAA#v=onepage&q=vpn%20site%20to%20site&f=false

11. CISCO SYSTEMS Site-to-Site and Extranet VPN Business Scenarios [Sitio en Internet] Disponible en: http://www.cisco.com/c/en/us/td/docs/security/vpn_modules/6342/vpn_cg/6342site3.html#wp1035810

12. COMPARING, DESIGNING, AND DEPLOYING VPNS. By Mark Lewis (CCIE.) [Sitio en Internet] Disponible en: http://books.google.com.co/books?id=PMRmPPjTkVsC&pg=PA408&dq=vpn+site+to+site&hl=es-419&sa=X&ei=MTPHU7WhI4fhsATA9YDQDg&ved=0CBkQ6AEwAA#v=onepage&q=vpn%20site%20to%20site&f=false

13. Ibíd.

14. ISCW Implementign Secure Corverged Wide Area Networks, Versión 1.0, version 0.1-21.06, Cisco Systems.

15. Troubleshooting Virtual Private Networks. Mark Lewis. Cisco Press. 2004.

16. Microsoft Windows 2000 Server, Seguridad de red privada virtual de Microsoft.

17. CISCO SYSTEMS IPSec Negotiation/IKE Protocols, Which VPN Solution is Right for You? [Sitio en Internet] Disponible en http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14147-which-vpn.html

18. CISCO SYSTEMS Remote Access VPN Business Scenarios[Sitio en Internet] Disponible en http://www.cisco.com/c/en/us/td/docs/security/vpn_modules/6342/vpn_cg/6342vpn4.html

19. Redes Privadas Virtuales (VPN) [Sitio en Internet] Disponible en http://it.aut.uah.es/enrique/docencia/ii/seguridad/documentos/t9-0506.pdf

20. CISCO SYSTEMS IPSec Negotiation/IKE Protocols How Virtual Private Networks Work [Sitio en Internet] Disponible en: http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html

21. CISCO SYSTEMS Router Allows VPN Clients to Connect IPsec and Internet Using Split Tunneling Configuration Example [Sitio en Internet] Disponible en http://www.cisco.com/c/en/us/support/docs/routers/3600-series-multiservice-platforms/91193-rtr-ipsec-internet-connect.html#config