

RAE

1. **TIPO DE DOCUMENTO:** Trabajo de grado para optar por el título de INGENIERO DE TELECOMUNICACIONES
2. **TÍTULO:** DISEÑO Y PLANEACIÓN DE UN PROYECTO PILOTO DE TELETRABAJO PARA EL SECTOR BANCARIO A PARTIR DE MODELOS TECNOLÓGICOS DE TT Y LA APROPIACIÓN DE LAS TIC
3. **AUTOR:** Fabian Esteban Santacruz Guataquirá
4. **LUGAR:** Bogotá, D.C
5. **FECHA:** Mayo de 2015
6. **PALABRAS CLAVE:** Teletrabajo, Sector Bancario, Modelos tecnológicos, TIC, VPN, IPSEC, BYOD.
7. **DESCRIPCIÓN DEL TRABAJO:** El objetivo principal de este proyecto es diseñar y planificar un proyecto piloto de teletrabajo que se ajuste a las necesidades del sector bancario y financiero, cumpliendo las políticas de seguridad y acceso a la red necesarias; por medio del diseño de un modelo tecnológico para el apropiamiento y adaptación de las TIC. Se identificaron las necesidades, recursos e infraestructura tecnológica indispensables, así como las posibles fallas de seguridad o riesgos que puede traer la implementación del teletrabajo, para determinar la tecnología de VPN, métodos de cifrado y de seguridad que brinden un acceso remoto seguro y garanticen la confiabilidad, integridad, disponibilidad de la información.
8. **LÍNEAS DE INVESTIGACION:** Línea de Investigación propia: Diseño de modelo tecnológico para el teletrabajo en el sector bancario, y análisis de protocolos y algoritmos de cifrado de información.
9. **METODOLOGÍA:** Es de tipo tecnológica abarcando gran contenido de procedimientos, estudios y pruebas técnicas para la apropiación de un modelo de teletrabajo efectivo para el sector bancario, demostrando su efectividad a partir del diseño de una prueba piloto que garantice la seguridad para el acceso remoto a la información.
10. **CONCLUSIONES:** La implementación de un modelo de teletrabajo en una organización debe contemplar las necesidades, riesgos, y nivel de seguridad para el acceso a la información. Cualquier descuido u omisión puede afectar seriamente la continuidad de negocio y tener resultados negativos para la producción y disponibilidad de servicio. A partir de las pruebas simuladas y el análisis de costos y beneficios se demostró que el modelo de teletrabajo propuesto para el sector bancario, es rentable y seguro, siempre y cuando se cumpla con las recomendaciones ISO 27001/2, su ciclo de mejora continua, las políticas de seguridad y manejo de contraseñas propuestas en esta investigación. Las pruebas de descubrimiento de vulnerabilidades y ataques a la red de teletrabajo, se realizaron bajo simulación en un ambiente de red público como Internet; sus resultados están limitados al uso de tecnología comercial, no se contemplan ataques con computadoras o tecnologías cuánticas. La prueba piloto para la implementación de teletrabajo está limitada por la infraestructura tecnológica disponible; La capacidad de los canales de internet contratados por la empresa es el mayor limitante a la hora de definir la cantidad de trabajadores remotos. La infraestructura tecnológica es determinante para el alcance de la prueba piloto y el modelo tecnológico que va a ser adoptado. La cantidad de teletrabajadores, los anchos de banda disponibles, las licencias VPN pueden incrementar los costos del piloto.



DISEÑO Y PLANEACIÓN DE UN PROYECTO PILOTO DE TELETRABAJO PARA EL SECTOR BANCARIO A PARTIR DE MODELOS TECNOLÓGICOS DE TT Y LA APROPIACIÓN DE LAS TIC



ESTEBAN SANTACRUZ
GUATAQUIRA

UNIVERSIDAD DE SAN BUENAVENTURA
INGENIERIA DE TELECOMUNICACIONES

2014

**DISEÑO Y PLANEACIÓN DE UN PROYECTO PILOTO DE TELETRABAJO
PARA EL SECTOR BANCARIO A PARTIR DE MODELOS TECNOLÓGICOS
DE TT Y LA APROPIACIÓN DE LAS TIC**

FABIAN ESTEBAN SANTACRUZ GUATAQUIRA

**Trabajo presentado como requisito parcial para optar por el título de profesional en
Ingeniería de Telecomunicaciones**

**Asesor: Ingeniero
Félix Gutiérrez**

**UNIVERSIDAD DE SAN BUENAVENTURA
FACULTAD DE INGENIERÍA
INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ, D.C. – 2015**

DEDICATORIA

Este trabajo es fruto del esfuerzo de mi familia. Mi éxito y superación es gracias a la dedicación de mi Mamá Rosa Victoria Guataqira, mi Abuela Erminda Santana, y mi hermana Marcela Santacruz; a ustedes dedico mi carrera y futuro, que no serían posibles sin todo su apoyo.

AGRADECIMIENTOS

Quiero agradecer a toda mi familia por su dedicación, al Banco Davivienda y su apoyo con el cual fue posible culminar mi carrera profesional; al Ingeniero Nelson Rosas gracias por su ayuda y comprensión como Director de Ingeniería de Telecomunicaciones, y a todos mis compañeros y amigos que encontré durante mi paso por la Universidad de San Buenaventura.

RESUMEN

Este trabajo de grado busca demostrar las ventajas de la aplicación de las TIC¹ al sector laboral financiero, específicamente en la modalidad de teletrabajo, bajo los estándares de seguridad y de acceso a la red necesarios para su implementación de forma segura, garantizando la disponibilidad, confidencialidad y continuidad de negocio.

En este trabajo de grado se analiza desde la criptografía, técnicas de encriptación y cifrado, hasta la aplicación de protocolos, técnicas de tunelización y VPN², que hacen posible la adopción de un modelo de trabajo a distancia, materializado en reducción de costos y aumento de beneficios para la organización y sus trabajadores con ayuda de las TIC¹.

²TIC, Acrónimo de Tecnologías de la Información y las Telecomunicaciones

¹VPN, Acrónimo de Virtual Private Network en español Red Privada Virtual

1 TABLA DE CONTENIDO

INTRODUCCIÓN	12
OBJETIVOS	13
OBJETIVO GENERAL	13
OBJETIVOS ESPECÍFICOS	13
PROBLEMA	14
JUSTIFICACIÓN	14
ALCANCES	15
LIMITACIONES	15
METODOLOGÍA	16
CAPITULO 1	17
ANTECEDENTES Y MARCO LEGAL	17
1. ANTECEDENTES	18
1.1. Antecedentes tesis	18
1.2. Antecedentes en el mundo	19
1.3 ESTÁNDAR ISO/IEC 27001 Y MARCO LEGAL	23
CAPITULO 2	25
MARCO TEÓRICO	25
2 MARCO TEÓRICO	26
2.1.1 Teletrabajo	26
Ventajas	26
Desventajas	27
2.1.2 Criptografía	28
2.1.3 Métodos criptográficos antiguos	29
El Escítalo	29
El cifrado César	29

<i>Máquina Enigma</i>	30
<i>Código Navajo</i>	31
<i>2.1.4 Criptografía Moderna</i>	31
<i>2.1.4 Métodos de Creación de Texto cifrado</i>	33
CAPITULO 3	34
3 ACCESO REMOTO DE DATOS	35
3.2 VPN Red Privada Virtual	35
3.2.1 Tipos de VPN	36
3.3 IPsec	37
CAPITULO 4	38
MODELOS DE TELETRABAJO, PRUEBA PILOTO, DISEÑO Y SIMULACIÓN DE RED	38
4.1 MODELOS DE TT	39
4.1.1 Modelo propuesto por la Fundación Universitaria Konrad Lorenz	39
4.1.2 Modelo propuesto por la Junta de Andalucía. Publicado en el 2010.	40
4.1.3 Modelo propuesto por la Agencia de Administración de Servicios de Estados Unidos.	40
4.1.4 Modelo propuesto por la Oficina de patentes y Marcas de Estados Unidos.	41
4.2 ESTRUCTURAS ORGANIZACIONALES BANCARIAS	43
4.2.1 DEFINICIÓN DE LOS PERFILES DE LOS TELETRABAJADORES	45
4.3 DETERMINACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA NECESARIA PARA LA IMPLEMENTACIÓN DEL TELETRABAJO	48
4.4 ANÁLISIS DE PROTOCOLOS Y TÉCNICAS DE CIFRADO PARA LA CONFIDENCIALIDAD, INTEGRIDAD Y ACCESO LA INFORMACIÓN	52
4.4.1 Funciones de resumen o hash	53
4.4.2 Algoritmos de Encriptación	56
4.4.2.6 Criptoanálisis Y Comparación de sistemas criptográficos	59
4.4.2.7 Intercambio de llaves Diffie-Hellman	60
4.4.2.7.1 Funcionamiento de DH	60

4.5 DEFINICIÓN DE LA PRUEBA PILOTO, DISEÑO Y SIMULACIÓN DE RED...	61
4.5.1 Definición de prueba piloto	61
4.5.1.1 Marco Jurídico para la adopción del Teletrabajo	62
4.5.1.2 Modelo de Teletrabajo que se va a implementar en la organización.....	64
4.5.1.2.1 Definición Organizacional.....	65
4.5.1.2.2 Disponibilidad Tecnológica	65
4.5.1.2.3 Alta Disponibilidad y BYOD	66
4.5.1.3 Definición de la cantidad de Teletrabajadores	67
4.6 DISEÑO Y SIMULACIÓN DE RED.....	68
4.6.1 Simulación de red	73
4.6.2 Componentes	74
4.6.3 Desarrollo	76
4.6.4 Alistamiento de Componentes	76
4.6.5 Configuración	79
4.6.5.1 Pruebas de conexión y negociación VPN	87
4.6.6 PRUEBAS	89
4.7 PRUEBAS DE VULNERABILIDAD Y ACCESO NO AUTORIZADO A LA INFORMACIÓN BAJO EL AMBIENTE SIMULADO.	92
4.7.1 Descubrimiento de puertos e infraestructura con Nmap	92
4.7.2 Criptoanálisis de contraseñas y tráfico cifrado con Cain y calculadoras MD5 de Internet	94
4.7.3 Ataques de fuerza bruta y de diccionarios con la herramienta Hydra.....	94
4.7.4 Ataques de denegación de servicio por medio de ICMP.	96
CAPITULO 5	97
ANÁLISIS DE RIESGOS, COSTOS Y BENEFICIOS DE LA IMPLEMENTACIÓN DEL TELETRABAJO.....	97
5. ANÁLISIS DE RIESGOS, COSTOS Y BENEFICIOS DE LA IMPLEMENTACIÓN DEL TELETRABAJO.	98
5.1.1 Análisis de riesgos.....	98

5.1.2 Costos.....	100
3.1.2 Beneficios	102
3.1.2.1 Beneficios para la empresa.....	102
3.1.2.2 Beneficios para el Teletrabajador	104
CONCLUSIONES.....	106
PERSPECTIVAS FUTURAS.....	108
Referencias.....	109

TABLA DE ILUSTRACIONES

<i>Ilustración 1: Estado del Teletrabajo en el mundo.</i>	20
<i>Ilustración 2: Trabajo flexible en Europa.</i>	21
<i>Ilustración 3: Proyección Teletrabajo.</i>	22
<i>Ilustración 4: Escítalo</i>	29
<i>Ilustración 5: Cifrado César</i>	30
<i>Ilustración 6: Código Vigenère</i>	30
<i>Ilustración 7: Máquina Enigma</i>	31
<i>Ilustración 8: Tipos de VPN</i>	36
<i>Ilustración 9: IPSec Framework</i>	37
<i>Ilustración 10: Modelo Konrad Lorenz</i>	39
<i>Ilustración 11: Modelo Junta de Andalucía</i>	40
<i>Ilustración 13: Modelo de La Oficina de Patentes y Marcas</i>	41
<i>Ilustración 14: Modelo DDABI de Implementación de TT. Fuente: Autor</i>	42
<i>Ilustración 15: Esquema organizacional de primer nivel.</i>	44
<i>Ilustración 16: Esquema organizacional de segundo nivel.</i>	45
<i>Ilustración 16: Teletrabajo.</i>	46
<i>Ilustración 17: Infraestructura Tecnológica TT. SOHO (Small Office Home Office).</i>	49
<i>Ilustración 18: Infraestructura Tecnológica Empresarial TT.</i>	50
<i>Ilustración 19: Infraestructura Tecnológica Trabajador Remoto.</i>	51
<i>Ilustración 20: Función de Hash</i>	54
<i>Ilustración 20: HMAC.</i>	54
<i>Ilustración 21: Métodos criptográficos.</i>	55
<i>Ilustración 22: 3DES.</i>	56
<i>Ilustración 23: Algoritmo DH.</i>	60
<i>Ilustración 24: Módulos de teletrabajo Fuente: Autor</i>	64
<i>Ilustración 25: Comportamiento de retardo y jitter túnel IPSec.</i>	70
<i>Ilustración 25: Comportamiento de retardo y jitter túnel IPSec.</i>	71
<i>Ilustración 25: Diseño de red Teletrabajo.</i>	73
<i>Ilustración 25: Simulación Red Teletrabajo.</i>	76

<i>Ilustración 26: Ubuntu VM</i>	77
<i>Ilustración 27: Creación de interfaces de bucle invertido</i>	78
<i>Ilustración 28 : Reglas Firewall de Windows.</i>	78
<i>Ilustración 29: Topología GNS3.</i>	79
<i>Ilustración 30: Instalación de SDM en router.</i>	80
<i>Ilustración 30: Acceso por SDM al router.</i>	81
<i>Ilustración 31: Router con gestión gráfica.</i>	81
<i>Ilustración 32: Gestión módem ZTE 4g de UNE.</i>	82
<i>Ilustración 33: Configuración de DNS dinámico.</i>	82
<i>Ilustración 34: Pruebas desde el router a dominios de Internet.</i>	83
<i>Ilustración 34: Pruebas desde Internet al dominio del router.</i>	83
<i>Ilustración 34: Servidor VPN SDM.</i>	85
<i>Ilustración 35: Elección de interfaz VPN.</i>	85
<i>Ilustración 36: Configuración de políticas IKE.</i>	86
<i>Ilustración 37: Configuración de transformada IPSec.</i>	86
<i>Ilustración 38: Configuración de grupo de autorización.</i>	87
<i>Ilustración 39: Prueba de Servidor VPN de SDM.</i>	88
<i>Ilustración 40: Prueba de Servidor VPN de SDM.</i>	88
<i>Ilustración 41: Captura intentos de conexión Cliente VPN.</i>	89
<i>Ilustración 42: Configuración de servicio VPN en NAT de Windows.</i>	89
<i>Ilustración 42: Servicio VPN en NAT de Windows.</i>	90
<i>Ilustración 43: Fallas de negociación VPN.</i>	90
<i>Ilustración 43: Captura fallas de NAT Transversal.</i>	91
<i>Ilustración 42: Comparación gráfica de las transformadas criptográficas configuradas.</i>	92
<i>Ilustración 43: Resultados Nmap.</i>	93
<i>Ilustración 44: Captura de tráfico cifrado con Wireshark.</i>	94
<i>Ilustración 45: Hydra 8.0 Ubuntu.</i>	95
<i>Ilustración 46: Ataque Hydra 8.0 a red de Teletrabajo.</i>	95
<i>Ilustración 47: Ping de la muerte a red de Teletrabajo.</i>	96
<i>Ilustración 47: Análisis gráfico de Factores de riesgo.</i>	99
<i>Ilustración 48: Beneficios del Teletrabajo.</i>	102

TABLAS

<i>Tabla 1. Algoritmos, protocolos y funciones de Hash criptografía.</i>	53
<i>Tabla 2: Expectativa vs longitud de llaves.</i>	55
<i>Tabla 3. Comparación y criptoanálisis de los sistemas criptográficos. Fuente: Autor, Criptoanálisis (NIST, 2012).</i>	59
<i>Tabla 4. Cálculo de teletrabajadores. Fuente: Autor</i>	68
<i>Tabla 5. Niveles de retardo. Diseño de red. Fuente: Autor</i>	69
<i>Tabla 13. Costos Mensuales por consumo de agua. Fuente: Autor</i>	103
<i>Tabla 14. Costos Mensuales por consumo de agua. Fuente: Autor</i>	103
<i>Tabla 15. Costos Mensuales totales. Fuente: Autor</i>	104
<i>Tabla 16. Ahorro mensual empresa. Fuente: Autor</i>	104

<i>Tabla 17. Ahorro Tiempo Teletrabajador. Fuente: Autor</i>	104
<i>Tabla 18. Ahorro Transporte Teletrabajador. Fuente: Autor</i>	105
<i>Tabla 19. Ahorro Gasolina Teletrabajador. Fuente: Autor</i>	105
<i>Tabla 20. Ahorro Anual Teletrabajador. Fuente: Autor</i>	105

INTRODUCCIÓN

El gran avance en cobertura de telecomunicaciones del país brinda la posibilidad de implementar modelos de teletrabajo, combinando el cumplimiento de objetivos dentro de las organizaciones, con los recursos tecnológicos necesarios para conseguirlos en una relación gana-gana entre empresa y sociedad, reduciendo costos y aprovechando mejor el tiempo e infraestructura tanto privada como pública. El teletrabajo más que una tendencia mundial de múltiples beneficios, es una necesidad a la cual le están apostando las grandes ciudades y la virtualización de las redes y Cloud Computing³.

Este proyecto tiene como fin el estudio y desarrollo de un modelo de teletrabajo específicamente para el sector financiero, definiendo los perfiles o cargos compatibles y tecnologías de seguridad que garanticen el buen manejo de información y el acceso a los recursos necesarios para trabajar eficientemente.

El contenido de este trabajo de grado se desarrollará de la siguiente manera:

Capítulo 1 Antecedentes nacionales e internacionales del teletrabajo

Capítulo 2 conceptos de criptografía, técnicas y protocolos de cifrado, tipos de VPN, definición de TT⁴, regulación y estatutos jurídicos del teletrabajo en Colombia.

Capítulo 3 Acceso remoto de datos

Capítulo 4: Modelos de teletrabajo, prueba piloto, diseño y simulación de red

Desarrollo técnico y de ingeniería del proyecto

Ítem 1: Análisis de modelos de teletrabajo, estructuras organizacionales bancarias y definición de los perfiles de los teletrabajadores.

Ítem 2: Determinación de la infraestructura tecnológica necesaria para la implementación del teletrabajo y definición de prueba piloto

Ítem 3: Análisis de protocolos y técnicas de cifrado para la confidencialidad, integridad y acceso a la información.

Ítem 4: Pruebas de vulnerabilidad y acceso no autorizado a la información bajo el ambiente simulado

³ En español Computación en la nube. Es el almacenamiento y acceso a información corporativa o individual en Internet

⁴ TT Abreviación de Teletrabajo

Capítulo 5 Análisis de riesgos, costos y beneficios de la implementación del teletrabajo.

ABSTRACT

The breakthrough in the country's telecommunications coverage provides the ability to implement telecommuting models, joining the fulfillment of objectives within the organizations, with the technological resources needed to get them in a win win relationship between business and society. Reducing costs and better use of time and both private and public infrastructure, telecommuting more than a global trend of multiple benefits, is a necessity to which we are betting big cities and virtualization of networks and Cloud Computing.

This project aims to study and develop a telecommuting model specifically for the financial sector, defining compatible profiles or charges and security technologies to ensure the proper handling of information and access to the resources needed to work efficiently.

OBJETIVOS

OBJETIVO GENERAL

Diseñar y planificar un proyecto piloto de teletrabajo que se ajuste a las necesidades del sector bancario y financiero, cumpliendo las políticas de seguridad y acceso a la red necesarias; siguiendo lineamientos propios de modelos tecnológicos para el apropiamiento y adaptación de las TIC

OBJETIVOS ESPECÍFICOS

Identificar las necesidades, recursos e infraestructura tecnológica indispensables para una red bancaria; así como las posibles fallas de seguridad o riesgos que puede traer la implementación del teletrabajo, para determinar la tecnología de VPN, métodos de cifrado y de seguridad AAA⁵ que brinden un acceso remoto seguro y garanticen la confiabilidad, integridad, disponibilidad de la información y reserva bancaria.

Realizar un entorno simulado sobre infraestructura de seguridad y comunicaciones Cisco con software de simulación de red libre como GNS3, packet tracer, VM, y soluciones de seguridad basadas en host de acceso libre o licenciado.

Realizar pruebas de vulnerabilidad necesarias para el descubrimiento y mitigación de riesgos con herramientas y software dedicado al rompimiento de claves y escaneo de puertos y dispositivos de red.

PROBLEMA

A nivel mundial ningún país suramericano muestra desarrollo significativo para la modalidad de teletrabajo (Haber Kern, 2009), a pesar del gran avance de las tecnologías de la información y las comunicaciones e interconexión, además de los beneficios sociales y productivos que trae su implementación y casos de éxito comprobados de grandes organizaciones en Europa y Estados Unidos que han demostrado su efectividad; de allí la necesidad de demostrar un modelo eficiente de teletrabajo que incentive sectores económicos tan sensibles como el sector bancario y financiero, garantizando la seguridad de la información y el acceso a recursos por medio de las TIC y la planificación de un proyecto piloto.

JUSTIFICACIÓN

En Colombia a pesar del gran avance en materia de telecomunicaciones y tecnologías de la información, aún se maneja un alto nivel de “tabú tecnológico” o prejuicio a nivel empresarial y organizacional al hablar o considerar el teletrabajo como una opción de vinculación laboral seria, que puede lograr mayor productividad, reducción de costos fijos, mejoramiento de la calidad de vida, e inclusión de comunidades discapacitadas o población vulnerable. Este proyecto busca mostrar el teletrabajo como una modalidad laboral por medio del diseño de un proyecto piloto para el sector bancario y financiero, analizando sus necesidades, recursos tecnológicos, riesgos y costos necesarios para la implementación y adaptación de las TIC a la organización y sus empleados, con ayuda de modelos tecnológicos definidos, aplicados al diseño y puesta en marcha del proyecto piloto. Esta investigación tiene gran sentido e interés social dados los beneficios comprobados del teletrabajo aprovechando su regulación y reconocimiento a nivel jurídico para el Estado Colombiano.

⁵AAA Acrónimo de seguridad AAA (Authentication/Authorizatin/Accounting)

ALCANCES

- Se realizarán pruebas simuladas bajo infraestructura de comunicaciones y seguridad de Cisco Systems.
- Planificación del proyecto piloto y el modelo tecnológico para su implementación en el sector bancario.
- Determinación de los perfiles laborales aptos para tele-trabajar.
- Este proyecto se realizará bajo la regulación y estatutos jurídicos del teletrabajo en Colombia.
- Se analizarán los costos y beneficios al implementar el modelo de teletrabajo.

LIMITACIONES

- Las pruebas del proyecto piloto sólo podrán ser de tipo simulado dado el alcance de la infraestructura.
- La información sobre seguridad e infraestructura bancaria está limitada o generalizada de acuerdo a los servicios financieros básicos.
- Se realizarán pruebas de descubrimiento de vulnerabilidades con la limitación de su funcionamiento simulado.

METODOLOGÍA

La investigación para el desarrollo de este proyecto es de tipo tecnológica abarcando gran contenido de procedimientos, estudios y pruebas técnicas para la apropiación de un modelo de teletrabajo efectivo para el sector bancario, demostrando su efectividad a partir del diseño de una prueba piloto que garantice la seguridad para el acceso remoto a la información.

Como primer paso se recopilarán y analizarán, los antecedentes nacionales e internacionales de esta nueva modalidad laboral, las tecnologías de acceso remoto, de seguridad IT⁶, y el marco legislativo; todos fundamentales en los modelos exitosos de TT.

Los datos analizados para la elección o diseño del modelo de teletrabajo, se recolectaron y estudiaron en base al sector financiero Colombiano; pero son igualmente válidos para cualquier sector empresarial del país. Las fuentes de esta investigación hacen parte de información del MinTic, bibliografía, cursos, manuales especializados, contenidos de la NSA⁷ y de reconocidos fabricantes de tecnologías de telecomunicaciones, en formatos digitales y físicos.

Para el desarrollo del segundo paso se estudiará la información organizacional bancaria general, para luego definir los cargos y perfiles compatibles para el trabajo remoto. Se analizarán los modelos de teletrabajo y en base a sus características se escogerá o diseñará un modelo propio para satisfacer las necesidades del sector financiero.

Luego se definirá la prueba piloto en base al análisis de la infraestructura tecnológica necesaria. Calculando el porcentaje de teletrabajadores respecto a los limitantes tecnológicos, de presupuesto y las distintas tecnologías de VPN, algoritmos, y protocolos criptográficos disponibles.

Posteriormente se realizará la simulación de red utilizando software y hardware especializado donde se realizarán pruebas a una escala moderada de acuerdo a las limitaciones del diseño piloto antes mencionadas.

Finalmente se realizará el descubrimiento de vulnerabilidades de tipo experimental con software especializado, y el análisis de resultados de las pruebas de diseño y modelo empleado. A partir de los resultados obtenidos se realizarán correcciones al diseño o al modelo, y se realizará un análisis de riesgos de tipo matriz y mapa de calor, y el cálculo de costos y beneficios de acuerdo al tamaño del piloto.

⁶ IT, Acrónimo de Information Technologies en español Tecnologías de la Información.

⁷ NSA, Acrónimo de National Security Agency, Agencia Nacional de Seguridad de Estados Unidos

CAPITULO 1

ANTECEDENTES Y MARCO LEGAL

1. ANTECEDENTES

1.1. Antecedentes tesis

Universidad

Fundación universitaria Konrad Lorenz

Autor

Marllely Catañeda Espindola

Tesis

1.1.1 MÉTODOS DE GESTIÓN PARA UNA ARQUITECTURA DE TELETRABAJO

Resumen

“La evolución de las tecnologías de la Información y las Telecomunicaciones (TIC), han facilitado el desarrollo de actividades remuneradas o prestación de servicios a terceros, sin requerir la presencia física en un sitio de trabajo (teletrabajo), con lo cual se generan muchas ventajas para las empresas y los empleados. En este documento se analiza la gestión de una arquitectura de teletrabajo”. (Castañeda, 2009)

Por Diana Marllely Castañeda Espindol - Egresada Ingeniería de Sistemas Konrad Lorenz.

Universidad

Universidad EAN

Autores

Mauricio Ríos Hurtado

José Julián Flórez Pineda

Luis Andrés Rodríguez

Tesis

1.1.2 Proyecto de implementación en modalidad de teletrabajo para personas con discapacidad motora “Teledisc@”

Resumen

“Colombia es un país en el cual los fenómenos de violencia y de desigualdad han dado lugar a tener unos altos índices de población con discapacidad (6,4%, 2,632.255, según Censo del Dane del 2005) esta población habita en zonas con bajos ingresos económicos, dificultades de accesibilidad de transporte y equipamientos urbanos, sumado a esto, está el poco acceso a oportunidades laborales que les permita tener una calidad de vida digna y

que les permita desarrollarse a cabalidad como ciudadanos que construyan país.” (Mauricio Ríos Hurtado, 2008)

1.2. Antecedentes en el mundo

La primera referencia de teletrabajo se da en 1957 donde la industria británica del software empleaba mujeres que desde sus casas (Solano, 2012). Sin embargo su la propuesta formal se dio durante la crisis petrolera de 1973 donde el mayor inconveniente era el abastecimiento de combustible a nivel mundial. Los constantes problemas de transporte o movilidad llevaron al norteamericano Jack Nilles de la Universidad del Sur California a proponer la idea, de gran acogida, de “llevar el trabajo al trabajador en lugar del trabajador al trabajo” (Gallusser, 2005); esto parecía solucionar el problema de la escasez de combustible o crisis energética, los congestionamientos de tráfico y la pérdida de tiempo o tiempos muertos en la actividad de “ir al trabajo”. De aquí surge su nombre en inglés “telecommuting” (Padilla, 2007). La concepción norteamericana enfatiza en el hecho de evitar desplazamientos, y fue en un principio adoptada por IBM quien permitía que los altos ejecutivos realizaran labores a distancia desde sus hogares y hoteles, logrando con esta medida reducir costos y aprovechar el tiempo libre (Padilla, 2007).

Para los años 80s el teletrabajo se acentuó como forma de autoempleo para muchas personas que empezaron a trabajar desde su hogar en negocios independientes o que simplemente por sus responsabilidades familiares o personales no podían salir de su vivienda.

Han sido muchos los casos de éxito y empresas que han acogido de manera total o parcial el modelo, aprovechando la evolución tecnológica y la depreciación de costos en materia de telecomunicaciones. A pesar de esta situación se habla que el teletrabajo no ha tenido el impacto esperado a nivel mundial ya que su evolución no ha sido homogénea y se ha desarrollado de una forma amplia en Europa y aún mayor en Estados Unidos.

El Reporte Europeo de Estado del Teletrabajo muestra la mayor cantidad de teletrabajadores para EEUU, con el 22,9% de la población traducido en más de 15 millones de personas que utilizan esta modalidad de trabajo. El factor determinante para este resultado, es el incremento de la inversión realizada en países como EEUU y Japón y que incide directamente, en la penetración de internet en la sociedad.

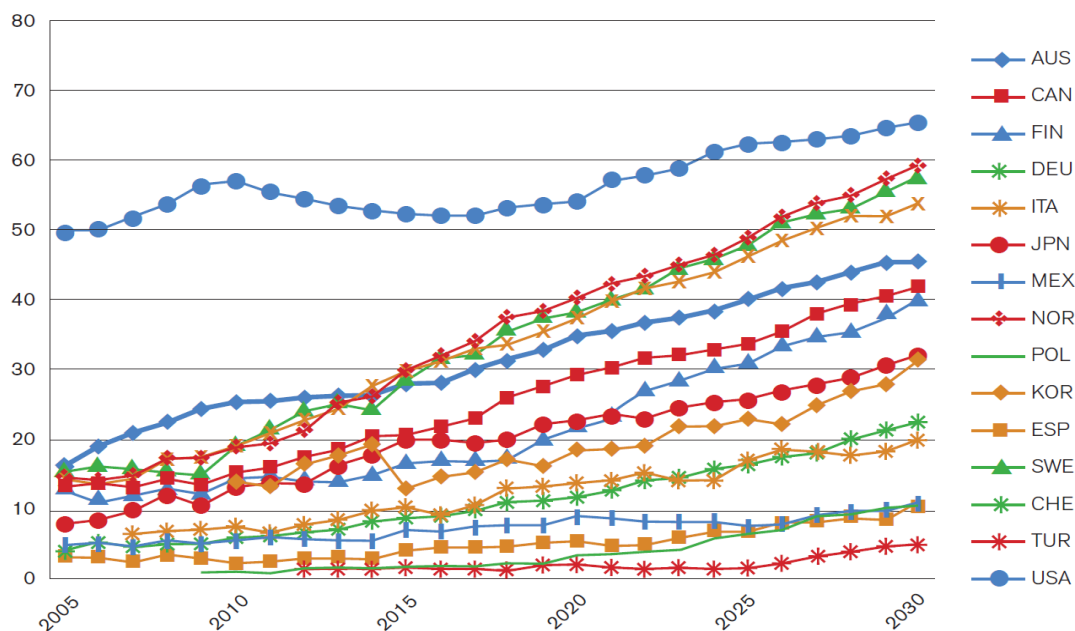


Ilustración 1: Estado del Teletrabajo en el mundo. Fuente: (Haber Kern, 2009). **Based on World Value Survey.**

Razones para el desarrollo de TT en Estados Unidos (Anis, 1992) :

- Descentralización de las empresas dada la amplitud del territorio
- Recorte de gastos
- Agilización de sus servicios.
- Búsqueda de un mayor radio de acción de las empresas con sus empleados dispersos por una gran área geográfica.

Sin embargo son varios los factores de índole económico y organizacional de un país o una compañía los que facilitan el avance en materia de teletrabajo:

- Costo económico de acceso a Internet
- El incremento de los costos de combustible
- La tendencia de las empresas a proporcionar soluciones de equilibrio de vida laboral, personal y familiar.
- La tendencia al uso y acceso de las nuevas tecnologías de la información y las comunicaciones según los distintos países.

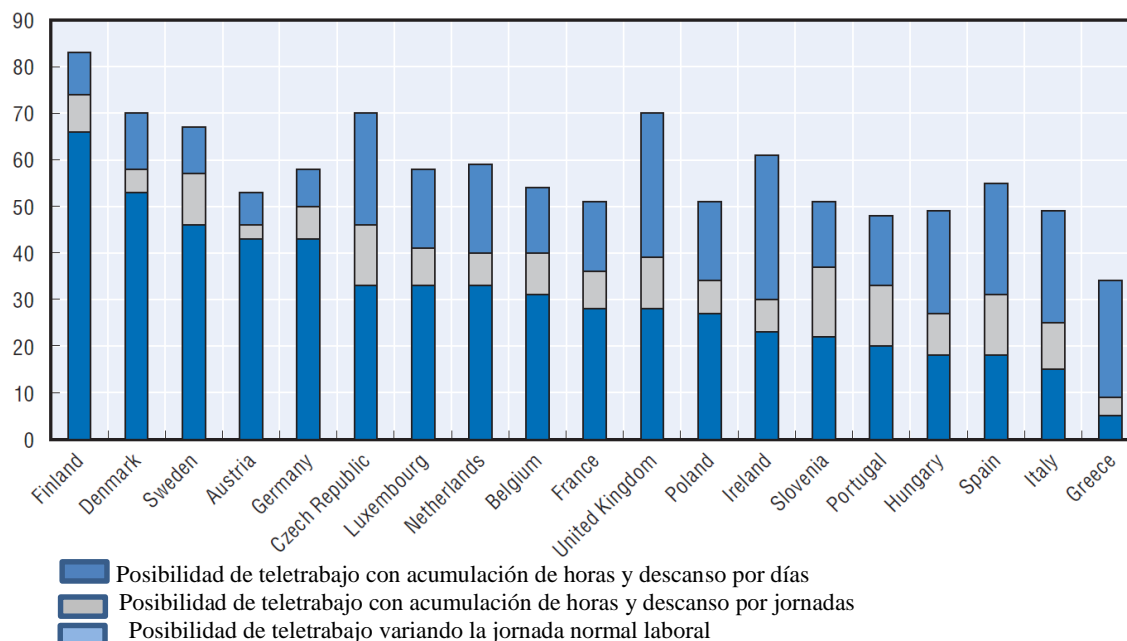


Ilustración 2: Trabajo flexible en Europa. Fuente: Doing Better for families: (OECD, 2011)

Razones para el desarrollo de TT en Europa (MONTIEL, 2003):

- Desarrollo de economía local de regiones aisladas, disminución de costos y fomento del empleo (Reino Unido).
- Desarrollo regional y fomento de la competitividad (Francia).
- Reducción de costes (Italia).
- Desarrollo regional y organización del mercado laboral (Alemania).
- Fomento de la competitividad (España).

Algunos ejemplos de éxito con el modelo de teletrabajo son (Videgain Muro, 1995):

- IBM quienes acogieron el concepto de teletrabajo desde su origen, y desde entonces cuentan con cerca del 30% de teletrabajadores luego del desarrollo con proyectos piloto exitosos en España, Austria, Alemania. Y Estados Unidos.
- SIEMENS, organización Alemana que cuenta con cerca del 24% de teletrabajadores luego del éxito en la adopción del modelo de TT. En Colombia Siemens otorga un día de trabajo desde el hogar para todos los trabajadores quienes no desempeñan labores operativas.
- CISCO Empresa líder en desarrollo de telecomunicaciones, tiene modalidades de teletrabajo total o semipresencial para el 100% de sus empleados, Además

incentiva esta modalidad de trabajo en todos los países donde hace presencia, formando alianzas con los gobiernos para educar y brindar ayuda a las empresas que se deseen vincular al TT.

Son muchos los casos de éxito en la adopción y apropiación del teletrabajo en varias organizaciones a nivel mundial, no obstante para nuestro país los niveles de empresas nacionales que han acogido proyectos piloto son muy pocas a pesar del apoyo y asesoría del Estado y el MinTic. La gran mayoría de empresas que tienen esta opción son consideradas multinacionales. Para el sector financiero, Bancolombia desarrolló una prueba piloto con buenos resultados, que ha llevado a tener cerca de un 8% de trabajadores móviles o suplementarios.

Según el congreso iberoamericano de teletrabajo la proyección del modelo a nivel mundial estaría marcada así:

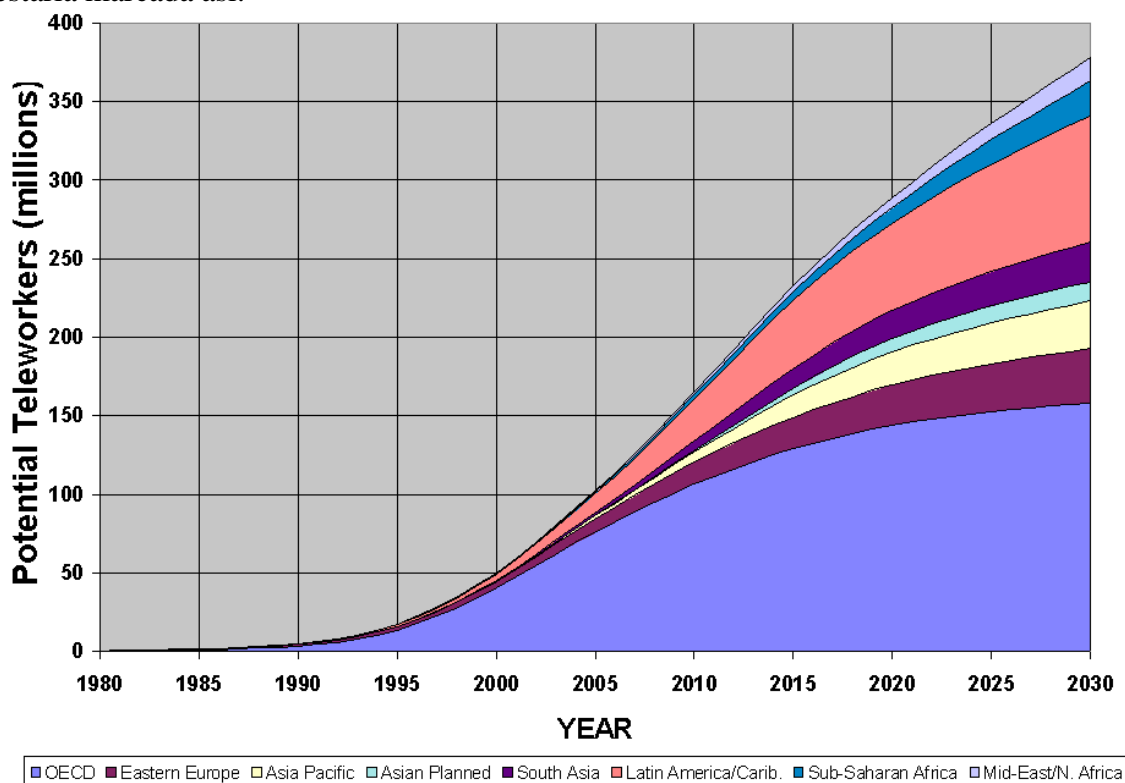


Ilustración 3: Proyección Teletrabajo. Fuente (OIT, 2008) Segundo congreso Iberoamericano de teletrabajo

Según la proyección se puede observar el atraso en la apropiación del teletrabajo, el cual muestra un crecimiento exponencial desde 1993 en todo el mundo, dos décadas después de

su formulación. Este comportamiento fue producto de factores estructurales, coyunturales, y de la evolución tecnológica, según (Chaparro, 1996).

Sin embargo no se ha cumplido la meta de teletrabajadores proyectada para el 2015 por varios motivos como escepticismo y pruebas piloto fallidas donde se ha demostrado que no todas las personas pueden teletrabajar.

1.3 ESTÁNDAR ISO/IEC 27001 Y MARCO LEGAL

“La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización. Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de riesgos a los que está sometida la información de la organización”*. (ISO, 2005)

ISO/IEC 27000 es un conjunto de estándares desarrollados – o en fase de desarrollo –, por ISO – International Organization for Standardization – e IEC – International Electrotechnical Commission –, que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

La norma estándar internacional ISO/IEC 27002, se compone por quince capítulos, cuyo alcance está orientado a: información, disponibilidad, confidencialidad, e integridad de la información. La norma busca minimizar los riesgos de seguridad en el manejo y acceso a la información de una empresa bajo un marco de recomendaciones buenas prácticas y gestión de la seguridad en una organización.

Esta norma en su aparte 11.7.2 teletrabajo establece:

(ISO, 2005)“La compañía únicamente debe autorizar actividades de teletrabajo si se encuentra satisfecha con los mecanismos y controles de seguridad implantados en cumplimiento con la(s) Política(s) de Seguridad. Los sitios de teletrabajo deben estar protegidos contra robo, divulgación no autorizada de información, acceso remoto no autorizado a los sistemas de la compañía o uso inadecuado de los recursos.

Se deben considerar los siguientes aspectos:

- La existencia de seguridad física en los sitios de teletrabajo

- La propuesta de ambiente físico para teletrabajo
- Los requerimientos de seguridad en las comunicaciones teniendo en cuenta la necesidad de acceso remoto a los sistemas de la compañía, la sensibilidad de la información que será accedida y la sensibilidad de los sistemas internos
- La amenaza de acceso no autorizado de otras personas que utilicen los equipos, el uso de redes domésticas
- Los requerimientos o restricciones para el uso de redes inalámbricas,
- Las políticas y procedimientos para proteger los derechos de propiedad intelectual
- La posibilidad de que la legislación prohíba el acceso a equipos de propiedad de las personas, los acuerdos de licencia de software
- La protección antivirus y los requerimientos del firewall. “

En 2008, Colombia reguló el Teletrabajo a partir de la Ley 1221 de 2008. Esta Ley busca:

Promover y regular la figura del Teletrabajo como instrumento de generación de empleo y autoempleo mediante la utilización de tecnologías de la información y las telecomunicaciones TIC.

La Ley 1221 estableció los tipos de modalidades laborales: el suplementario, autónomo y móvil. Además reglamenta el teletrabajo en los siguientes aspectos:

- Mujeres en estado de Lactancia
- Sector público y privado
- Avala los Derechos y garantías laborales

En 2012 el decreto 0884 estableció las condiciones laborales y contractuales entre empleador y empleadores del sector público y privado otorgando todos los beneficios de ley estipulados para trabajadores en Colombia

Para el cumplimiento del objeto de la presente ley el Gobierno Nacional, a través del Ministerio de la Protección Social, formulará, previo estudio Conpes, una Política Pública de Fomento al teletrabajo. Esta Política tendrá en cuenta los siguientes componentes:

- Infraestructura de telecomunicaciones.
- Acceso a equipos de computación.
- Aplicaciones y contenidos.
- Divulgación y mercadeo.
- Capacitación.
- Incentivos.
- Evaluación permanente y formulación de correctivos cuando su desarrollo lo requiera.

CAPITULO 2

MARCO TEÓRICO

2 MARCO TEÓRICO

2.1.1 Teletrabajo

La evolución tecnológica y de la economía global, ha transformado la forma tradicional de muchas actividades y servicios, entre ellos la necesidad de trabajar de forma dinámica y móvil, descentralizando la idea de empresa, otorgando al trabajador la posibilidad de desarrollar sus actividades laborales remotamente a su oficina.

El teletrabajo es un cambio organizacional a las empresas que surge como solución ecológica y móvil a las ciudades saturadas, donde por medio de las TIC es posible aprovechar de mejor forma el tiempo e infraestructura de trabajadores y empleadores. Se puede decir que es una respuesta evolutiva de nuestras conductas al progreso y adaptación de las telecomunicaciones donde la flexibilidad da la posibilidad de incluir a la sociedad en condición de discapacidad, y apoyar de gran manera a los programas de madres lactantes.

Esta modalidad de trabajo puede tener muchas ventajas pero también desventajas. Hay que tener en cuenta que no todas las personas son útiles como trabajadores remotos, El hecho de implementar el teletrabajo implica riesgos y una buena gestión de la seguridad para evitar el acceso no autorizado y pérdidas de información (Di Martino, n^a 4)

Ventajas

- Adaptación a las demandas del trabajo
- Aumento de la concentración
- Control de horas, flexibilidad, desempeño y productividad
- Calidad de vida
- Satisfacción personal
- Disminución del estrés
- Autonomía
- Ahorro de espacio
- Incremento de productividad
- Relaciones más horizontales
- Descentralización
- Oportunidad de empleo a discapacitados, personas de la tercera edad, enfermos y mujeres con hijos menores

- Reducción de costos: transporte, alimentación, vestuario, entre otros.

Desventajas

- Complejidad para administrar la comunicación y las relaciones sociales.
- Necesidad de automotivación
- Capacitación en comunicación electrónica
- Crear y mantener intercambios con compañeros
- Delimitar horarios de trabajo
- Delimitar el entorno
- Distribuir tiempos y recursos
- Enfrentar toma de decisiones
- No es adecuado para todos
- No trabajar en equipo
- Demanda de autocontrol
- Aislamiento del trabajador
- Distractores

El Teletrabajo también se puede definir como un marco de tecnologías de comunicaciones y de seguridad, para desempeñar funciones o tareas remotamente, utilizando infraestructura pública, como Internet, o privada con el uso de canales dedicados, donde la disponibilidad y acceso a la información está determinado por la infraestructura de telecomunicaciones de la organización (Carrasco Gutiérrez, 1997).

Se puede pensar que la clave del teletrabajo radica en el éxito de las tecnologías de transmisión y conexión a internet, sin embargo actualmente el núcleo de toda organización está en la confiabilidad, integridad y disponibilidad de su información, que aseguran la continuidad del negocio y minimizan los riesgos internos y externos que pueden afectar seriamente la producción y reputación de una compañía.

Actualmente, la necesidad de cifrar la información, se ha convertido en uno de los grandes pilares de todos los negocios. Casos como la extracción de cuentas de la infraestructura de Sony, que terminó en pérdidas millonarias y casi la quiebra de Sony networks, así como los números de tarjetas de crédito del instituto de estudios de seguridad estadounidense Stratfor, el robo de cuentas PayPal en ebay, y miles de ejemplos a más bajo nivel, de robos de información personal o privada.

El concepto de teletrabajo es tan sensible para cualquier empresa, por los riesgos inherentes de una mala implementación o cualquier deficiencia en su planificación, aún más cuando se trata de una red bancaria o financiera, donde el corazón de su información es la transferencia electrónica de capital. Esta modalidad laboral gira en torno a las tecnologías de seguridad de red y de las comunicaciones, y son las que realmente hacen posible su implementación en cualquier organización sin poner en riesgo su productividad o confiabilidad. Las últimas tendencias en comunicaciones móviles y fijas de alta velocidad para acceso a Internet, facilitan la implementación de modelos de teletrabajo, no sólo por brindar un acceso rápido desde cualquier lugar, sino porque hacen posible cifrar y descifrar la información de manera casi imperceptible para los usuarios remotos, utilizando métodos y protocolos criptográficos que utilizan grandes longitudes de llaves para el cifrado de información en tiempo real.

Hay tres partes fundamentales en la seguridad de una red de telecomunicaciones:

- Criptografía o cifrado de datos (Protocolos, técnicas y algoritmos)
- Tecnologías VPN
- Pruebas de vulnerabilidad: Ethical Hacking⁸.

Como base de todo el desarrollo de seguridad de la información está la criptografía y su evolución que abrió el camino a toda una ciencia y desarrollo de protocolos, nuevas tecnologías y dispositivos dedicados a proteger la información que facilitaron el gran avance de las telecomunicaciones a nivel mundial. Para el desarrollo de este proyecto es importante conocer los conceptos, tecnologías y dispositivos que en materia de seguridad son necesarios para implementar TT en una organización.

2.1.2 Criptografía

La criptografía es la práctica y el estudio de ocultar información (Academmy, 2008). Los servicios criptográficos son la base de muchas implementaciones de seguridad y se utilizan para garantizar la protección de los datos cuando pueden estar expuestos o vulnerables. Los principios de la criptografía se pueden utilizar para explicar cómo los protocolos y algoritmos que hoy en día se utilizan para proteger las comunicaciones. Data desde los círculos diplomáticos miles de años atrás. Los mensajeros de la corte de un rey tomaron

⁸ En español Hackeo Etico. Conjunto de técnicas, software y hardware para el descubrimiento consentido de vulnerabilidades de seguridad

mensajes cifrados de otras cortes. Ocasionalmente descubrieron sin querer, información clara, que podía ser robada, así como otras transcripciones que eran difíciles de entender, ya fuese por su idioma o escritura. No mucho tiempo después, los comandantes militares comenzaron a utilizar el cifrado para el envío de mensajes seguros (Galende Díaz, 1995). Dada la necesidad de proteger la información, fue implementada como estrategia militar por los espartanos en el año 600 A.C y Julio César en el imperio romano; que le otorgó gran éxito como emperador, ante la imposibilidad del enemigo para entender los mensajes cifrados interceptados. Conocido como cifrado Cesar evolucionó hasta hoy día en protocolos con el mismo principio pero mucho más sofisticados. Varios métodos de cifrado, dispositivos físicos, y demás se han utilizado para cifrar y descifrar texto desde la antigüedad (Díaz, 2005).

2.1.3 Métodos criptográficos antiguos

El Escítalo

Uno de los primeros métodos pudo haber sido el Escítalo de la antigua Grecia, una varilla presuntamente utilizada por los espartanos como herramienta para un cifrado de transposición. El emisor y el receptor tenían varillas idénticas en la cual se enrollaban los papiros para descifrar el mensaje.



Scytale - (700 BC)

Ilustración 4: Escítalo Fuente: Fuente (Academmy, 2008),INS Cisco networking Academy. Guía oficial INS Security Course Booklet Version 1.1 2nd Edition Cap. 7

El cifrado César

Es un cifrado de sustitución simple que fue utilizado por Julio César en el campo de batalla para cifrar rápidamente un mensaje, que luego podía ser fácilmente descifrado por sus comandantes. El método para cifrar consiste en dos alfabetos, moviendo uno respecto al otro, desplazándose de a una posición. La cantidad de desplazamiento está dada por una clave única que ambas partes conocen para cifrar y descifrar.

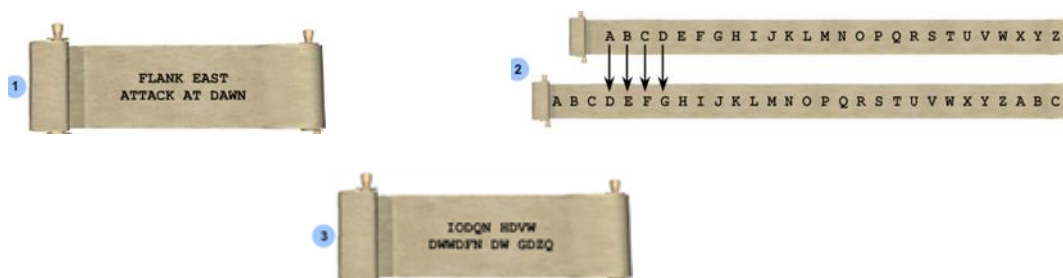


Ilustración 5: Cifrado César Fuente:INS Cisco networking Academy. Guía oficial INS Security Course Booklet Version 1.1 2nd Edition Cap. 7

El cifrado Vigenère

Fue inventado por el francés Blaise de Vigenère en el siglo XVI con un sistema polialfabético de cifrado. Basado en el sistema de cifrado César, donde el texto plano es codificado mediante una clave de múltiples letras.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Ilustración 6: Código Vigenère Fuente:INS Cisco networking Academy. Guía oficial INS Security Course Booklet Version 1.1 2nd Edition Cap. 7

Máquina Enigma

Arthur Scherbius inventó un dispositivo de codificación electro-mecánico llamado Enigma en 1918 que vendió a Alemania. Sirvió como modelo para las máquinas que todos los

principales participantes en la Segunda Guerra Mundial utilizaron. Se ha estimado que si 1.000 criptoanalistas probaran cuatro teclas por minuto, todo el día, todos los días, se necesitarían 1,8 mil millones años para probar todas las combinaciones⁹.



Ilustración 7: Máquina Enigma Fuente: INS Cisco networking Academy. Guía oficial INS Security Course Booklet Version 1.1 2nd Edition Cap. 7 pág, 167

Código Navajo

Durante la Segunda Guerra Mundial, Japón pudo descifrar todos los códigos de los estadounidenses, estos necesitaron de un nuevo código de cifrado para proteger sus comunicaciones, y la solución fueron los traductores de código navajos. No había palabras en el idioma navajo para términos militares; el idioma fue escrito y muy pocas personas fuera de las reservas navajo podían hablarlo. Durante la guerra los japoneses no lograron descifrar el código.

2.1.4 Criptografía Moderna

Los sistemas de cifrado modernos son una serie de pasos bien definidos con básicos y complicados procesos matemáticos, que varían dependiendo de la fortaleza y complejidad del método. Dichos algoritmos han evolucionado paralelamente al desarrollo de las telecomunicaciones y tecnologías de transmisión de información. En un principio para fines militares y de protección de información clasificada, hasta convertirse en parte fundamental de las arquitecturas tecnológicas de grandes y pequeñas organizaciones públicas o privadas.

⁹ Criptoanálisis de Enigma estimado por la NSA

En 1976 luego de una convocatoria de la NBS¹⁰ en 1973 para presentar criptosistemas, para la transmisión y manejo de información, se escogió el sistema DES (Data Encryption Standard)¹¹ creado por IBM, el cual consiste en un cifrado por bloques que combina sustituciones y permutaciones¹²; utiliza clave simétrica de hasta 56 bits, es decir que utiliza la misma clave tanto para el proceso de cifrado como para descifrar. La elección del DES se realizó bajo la supervisión de la agencia más representativa a nivel mundial en los ámbitos de criptoanálisis, criptografía e interceptaciones, la NSA (Academy, 2009).

A causa de los problemas del manejo de clave o llaves compartidas se diseñó el sistema de clave asimétrica en 1976 por Martin Hellman y Whitfield Diffie. La clave asimétrica, utiliza una clave pública para cifrar y otra privada para descifrar. En mayo de 1998, la EFF¹² diseño el computador llamado COPACABANA con una inversión de 210.000 dólares, capaz de realizar criptoanálisis efectivo en un mensaje cifrado con sistema DES. Mediante el ataque diccionario logró probar todas las claves en nueve días (Academy, 2008).

DES dejó de ser el cifrado estándar en el año 2000, cuando el NIST¹³ declaró como nuevo estándar el sistema AES¹⁴, también conocido como Rijndael, por las iniciales de sus creadores, Rijmen y Daemen. AES trabaja con longitudes de llave variable entre 128 y 256 bits y es un sistema simétrico de cifrado del cual no se han comprobado métodos de crackeo o rompimiento exitosos (NSA, 2012).

Muchas de las aplicaciones y servicios modernos pueden garantizar la autenticación con protocolos como HMAC¹⁵. La integridad con el uso de MDA¹⁶, MD5¹⁷ o SHA-1¹⁸. Confidencialidad de los datos está a través de algoritmos de cifrado simétrico, como DES, 3DES¹⁹, RC²⁰, AES, o algoritmos asimétricos, como RSA y la infraestructura de clave pública (PKI).

Cada uno de los métodos de encriptación utiliza un algoritmo específico, denominado cifrado, para encriptar y descifrar mensajes. Con la tecnología moderna, y algoritmos mejorados, el descifrado exitoso requiere conocimiento de las claves criptográficas apropiadas. Esto significa que la seguridad del cifrado moderno se encuentra en el secreto de las claves, no del algoritmo.

¹⁰ NBS, Acrónimo de National Bureau of Standards

¹¹ DES, Tiene como base el criptosistema Lucifer, diseñado por Horst Feistel

¹² EFF, Acrónimo de Electronic Frontier Foundation.

¹³ NIST, Acrónimo de National Institute of Standards and Technology

¹⁴ AES, Acrónimo de Advanced Encryption Standard, también conocido como algoritmo Rijndael.

¹⁵ HMAC Acrónimo de Hash-based message authentication code

¹⁶ MDA, Acrónimo de Message-Digest Algorithm Algoritmo de reducción criptográfico diseñado por el profesor Ronald Rivest del MIT (Massachusetts Institute of Technology, Instituto Tecnológico de Massachusetts).

¹⁷ MD5, Acrónimo de Message Digest 5

¹⁸ SHA, Acrónimo de Secure Hash Algorithm: Un conjunto de funciones hash diseñado por la Agencia de Seguridad Nacional de los Estados Unidos. Consta de tres versiones, la última de ellas aún en desarrollo

¹⁹ 3DES, Acrónimo de Triple Data Encryption Standard

²⁰ RSA, Acrónimo de Rivest, Shamir y Adleman, sistema criptográfico de clave pública desarrollado en 1977

El organismo internacional que se ha encargado de patentar y realizar el criptoanálisis profundo de la mayor parte de métodos de cifrado modernos a nivel mundial es la NSA de Estados Unidos, además de varios científicos y profesores reconocidos como Whitfield Diffie, Martin Hellman, Ron Rivest, Joan Daemen y Vincent Rijmen. A nivel nacional no hay registro de desarrollo científico en esta ciencia, sólo se encuentran especializaciones y diplomados, por parte de universidades como la Universidad Nacional, U. Distrital, U. Externado, U Piloto; artículos descriptivos, informativos y jurídicos; en Investigación resalta el trabajo de Javier Fernando Castaño Forero con el Diseño e implementación de un prototipo criptoprocador de curvas elípticas, e implementaciones criptográficas en FPGA.

2.1.4 Métodos de Creación de Texto cifrado

- **Transposición:** Las letras o información solo se reorganiza con un patrón constante o clave. Algoritmos de cifrado modernos, como el DES y el 3DES, siguen utilizando transposición como parte del algoritmo.
- **Sustitución:** Sustituye letras o información de acuerdo a un patrón o clave. El cifrado César y el código Vigenère son ejemplos de este método.
- **Vernam:** Gilbert Vernam de AT&T Bell Labs. Ingeniero que, en 1917, inventó y patentó el cifrado de flujo y más tarde inventó el sistema de cifrado one-time pad. Propuso un sistema de cifrado de teletipo donde la llave se creaba de acuerdo a una longitud arbitraria, que no repite la secuencia de números y se guarda en una cinta de papel. Se combinaban entonces carácter por carácter con el mensaje de texto para producir el texto cifrado. Para descifrar el texto cifrado, la clave de cinta de papel se combinaba de nuevo carácter a carácter, produciendo el texto plano. Cada cinta se utiliza una sola vez. Mientras la cinta de clave no se repita o no se reutilice, este tipo de cifrado es inmune a los ataques de criptoanálisis porque el texto cifrado disponible no muestra el patrón de la clave. El ejemplo más claro de éste es el desarrollo de RC, algoritmo de cifrado de amplio uso en la Internet, SSL²¹ y WEP²² (Academmy, 2008).

²¹ SSL, Acrónimo de Secure Socket

²²WEP , Acrónimo de Wired Equivalent Privacy

CAPITULO 3

ACCESO REMOTO DE DATOS

3 ACCESO REMOTO DE DATOS

El acceso remoto a la red o a la información de una organización es tal vez la parte más importante y delicada para el éxito y funcionamiento de un modelo de teletrabajo; es donde se define qué información estará disponible y cómo será accedida, la tecnología, dispositivos y protocolos para lograr de manera efectiva y segura su uso. A nivel de infraestructura para la implementación existen dos posibilidades:

- Infraestructura propia. Consiste en una red extendida a la empresa. Es un modelo poco flexible y con movilidad limitada
- Por infraestructura de terceros. Consiste en la utilización de la red pública o Internet para establecer la comunicación entre la empresa y los trabajadores. Actualmente es la opción más común dados sus beneficios de movilidad y costos. El límite de usuarios está dado por el ancho de banda de salida a Internet y la infraestructura y licenciamiento a nivel de seguridad con el que cuente la empresa. Aunque es la mejor opción es la que conlleva el mayor riesgo, ya que la información viaja a través de Internet y puede estar expuesta a ser robada o alterada.

Para un acceso remoto a red o información desde internet es completamente necesaria la utilización de servicios y tecnologías de seguridad, que garanticen un modelo de AAA y contemplen y controlen los riesgos establecidos en las normas internacionales de gestión de seguridad. Para este fin las tecnologías de tunelización y VPN son la mejor opción, dada su funcionalidad y capacidad de asegurar, cifrar y transmitir información a través de la red pública mundial.

3.2 VPN Red Privada Virtual

Una red privada virtual es el establecimiento seguro y transparente de comunicación a través de la una red pública como Internet sin necesidad de enlaces dedicados. Una VPN crea una conexión de red privada punto a punto llamada túnel sobre una infraestructura pública o de terceros como las extranets o Internet. Un túnel acaba con la barrera de distancia en términos de conexión y permite a usuarios remotos acceder a la oficina central y a sus recursos de red.

Entre los beneficios de utilizar VPNs, está la reducción de costos, alto nivel de seguridad usando encriptación avanzada y autenticación, se consideran escalables y compatibles con tecnologías de Banda Ancha

Las VPNs pueden establecer conexiones de capa 2 o capa 3 a través de túneles:

- GRE (Encriptación genérica de Enrutamiento): Protocolo de tunelización de Cisco que puede encapsular distintos tipos de paquetes dentro de un túnel IP. Se utiliza para conexiones punto a punto
- MPLS: Utilizado ampliamente por proveedores de servicios de internet. Se utiliza para conexiones multipunto
- IPSEC: Protocolo y método de Seguridad IP que provee un conjunto de prácticas y protocolos para configurar una VPN segura. Se utiliza para conexiones punto a punto. Provee confidencialidad, integridad y autenticación de información.

3.2.1 Tipos de VPN

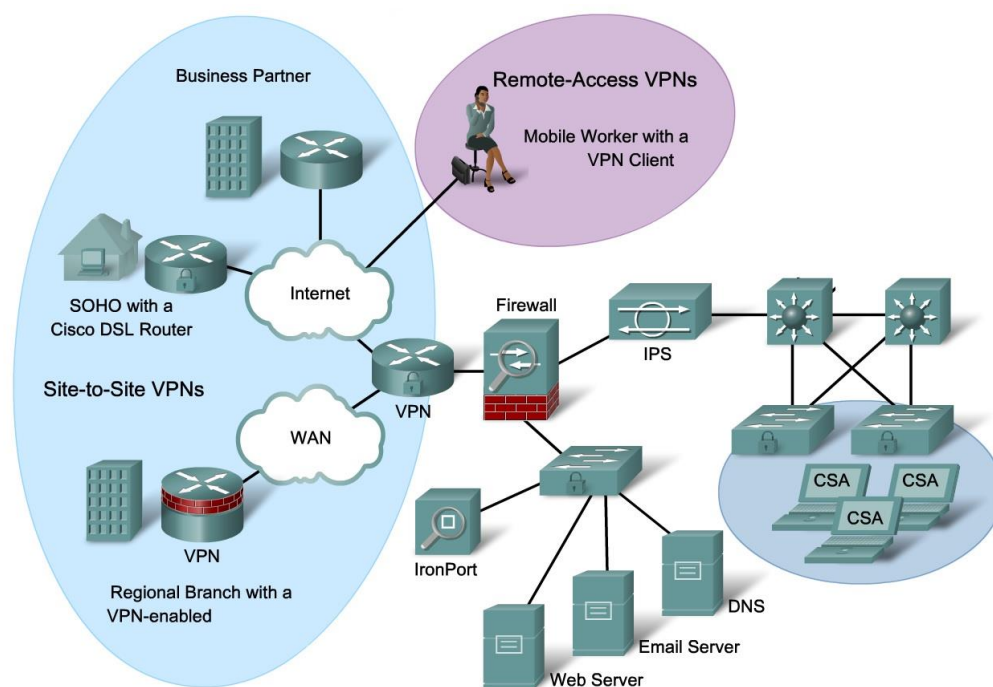


Ilustración 8: Tipos de VPN Fuente: (Academy, 2009) CCNS Route Cisco networking Academy. Guía oficial CCNS Course Booklet Version 2.0 1st Edition Cap. 11 pág.687

VPN punto a punto: Se considera una extensión de una red WAN. Creada con dispositivos VPN en ambos extremos de la conexión. Se consideran estáticas y los usuarios internos no conocen de su existencia. Son ejemplos de estos tipos de VPN:

- Frame Relay VPNs
- ATM VPNs
- GRE
- MPLS VPNs

VPN de Acceso Remoto: Se considera una evolución de las redes de conmutación de circuitos que soportan las necesidades de los teletrabajadores y los usuarios móviles dentro de una empresa. Son flexibles y dinámicas, y pueden ser habilitadas o deshabilitadas por los usuarios y soportan las arquitecturas cliente servidor. Los usuarios se conectan por medio de clientes VPN para encapsular y encriptar la información sin la necesidad de tener un dispositivo VPN disponible para la conexión.

3.3 IPSec

Es un conjunto de tecnologías y protocolos de seguridad de estándares abiertos que establecen las normas para las comunicaciones seguras, construido sobre algoritmos para implementar la encriptación, autenticación, e intercambio de llaves ofreciendo las funciones esenciales de seguridad como Integridad, confidencialidad, Autenticación, e intercambio de llaves IKE.

IPSec se constituye de cinco bloques de funcionalidades o algoritmos cada uno con un objetivo

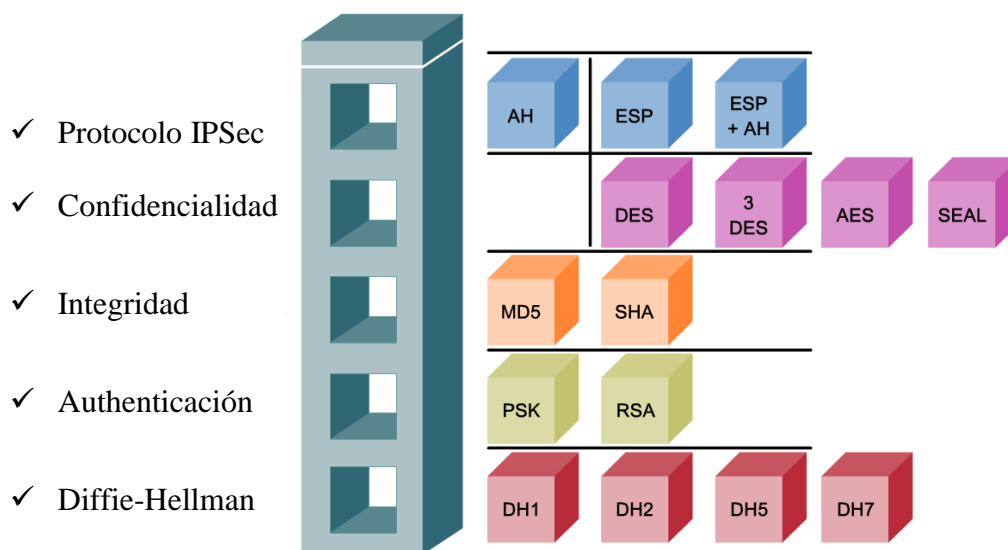


Ilustración 9: IPSec Framework Fuente: (Academmy, 2008) *INS Cisco networking Academy. Guía oficial INS Security Course Booklet Version 1.1 2nd Edition Cap. 7 pág, 985*

CAPITULO 4

MODELOS DE TELETRABAJO, PRUEBA PILOTO, DISEÑO Y SIMULACIÓN DE RED

4.1 MODELOS DE TT

Actualmente existen varios modelos de TT. Para esta investigación se analizarán varios para determinar el modelo a seguir o establecer un modelo propio que se ajuste a las necesidades.

4.1.1 Modelo propuesto por la Fundación Universitaria Konrad Lorenz



Ilustración 10: Modelo Konrad Lorenz Fuente: El Abc del teletrabajo MinTic.

La investigación “Métodos de gestión para una arquitectura de teletrabajo” (Castañeda, 2009), dio como resultado un modelo para la implementación de TT de la FU Konrad Lorenz que se basa en dos factores:

- La infraestructura Tecnológica de una organización: La inversión y madurez en infraestructura tecnológica es necesaria para la implementación de TT en una organización
- Formación para el Teletrabajo: Proceso educativo para el teletrabajador acorde al cumplimiento de objetivos, establecimiento de políticas, evaluación de conocimientos y cultura

4.1.2 Modelo propuesto por la Junta de Andalucía. Publicado en el 2010.

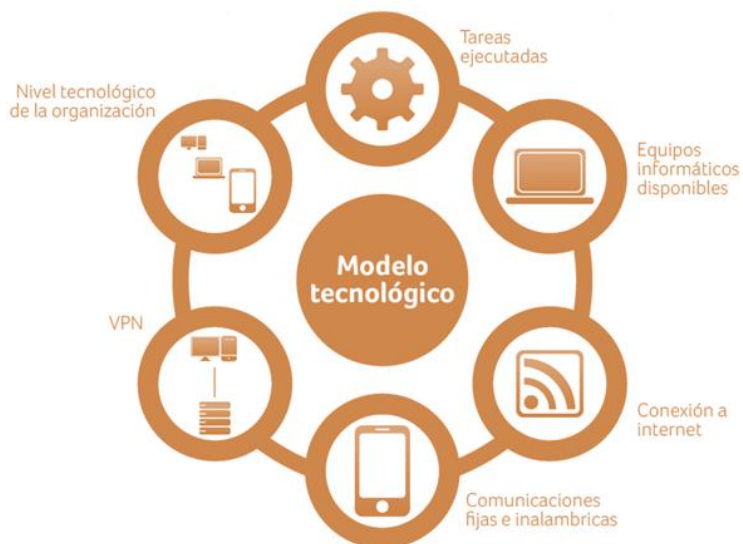


Ilustración 11: Modelo Junta de Andalucía Fuente: (MINTIC, Libro Blanco:El ABC del Teletrabajo, 2012).

Este modelo es más completo que el anterior al integrar las comunicaciones fijas o inalámbricas con el uso de VPN, contempla el nivel tecnológico y la definición de tareas en una organización.

4.1.3 Modelo propuesto por la Agencia de Administración de Servicios de Estados Unidos.

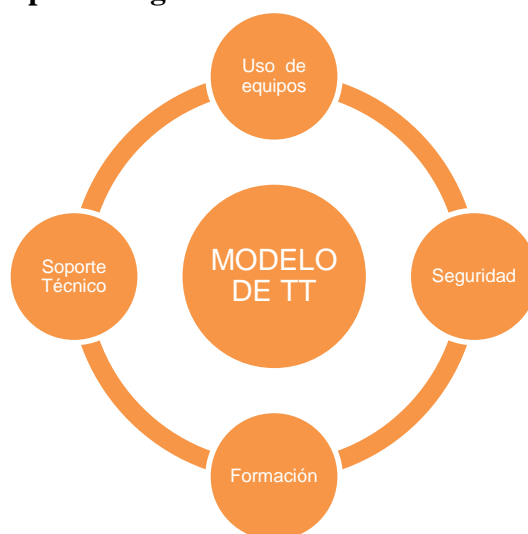


Ilustración 12: Modelo de GSA Fuente: (Office., 2008)

Este modelo presenta conceptos como el soporte técnico y un uso correcto de equipos de propiedad de la organización; Sin embargo queda un poco desactualizado con las nuevas tendencias de BYOD²³, y puede representar costos más altos para el establecimiento de TT en una empresa.

4.1.4 Modelo propuesto por la Oficina de patentes y Marcas de Estados Unidos.



Ilustración 13: Modelo de La Oficina de Patentes y Marcas Fuente: (MINTIC, Libro Blanco:El ABC del Teletrabajo, 2012).

Es un modelo simple aunque muy funcional, pues busca garantizar que la transición entre la oficina y el hogar sea casi imperceptible en el sentido de pasar de una LAN a una VPN. Esto es muy importante para un trabajador que no puede presentar lentitud o intermitencias con sus tareas, ya que esto puede afectar el cumplimiento de sus objetivos.

4.1.5 ELECCIÓN DEL MODELO

Todos los modelos anteriormente analizados tienen muy buenos conceptos respecto a la implementación de TT en una empresa; a pesar de esto ninguno es totalmente apropiado para la implementación de TT en el sector financiero dado que no son lo suficientemente claros y específicos para el fin de esta investigación.

²³ BYOD (Bring Your Own Device) o Trae tu propio dispositivo: Es una política empresarial que está marcando gran tendencia mundial respecto al uso y propiedad de los dispositivos.

Para tal objetivo se ha diseñado y propuesto el siguiente modelo siguiendo las recomendaciones del MinTic (Disponibilidad tecnológica-Seguridad-Rendimiento-Recursos) en cuanto a elección y adopción de modelos tecnológicos para la implementación de TT.

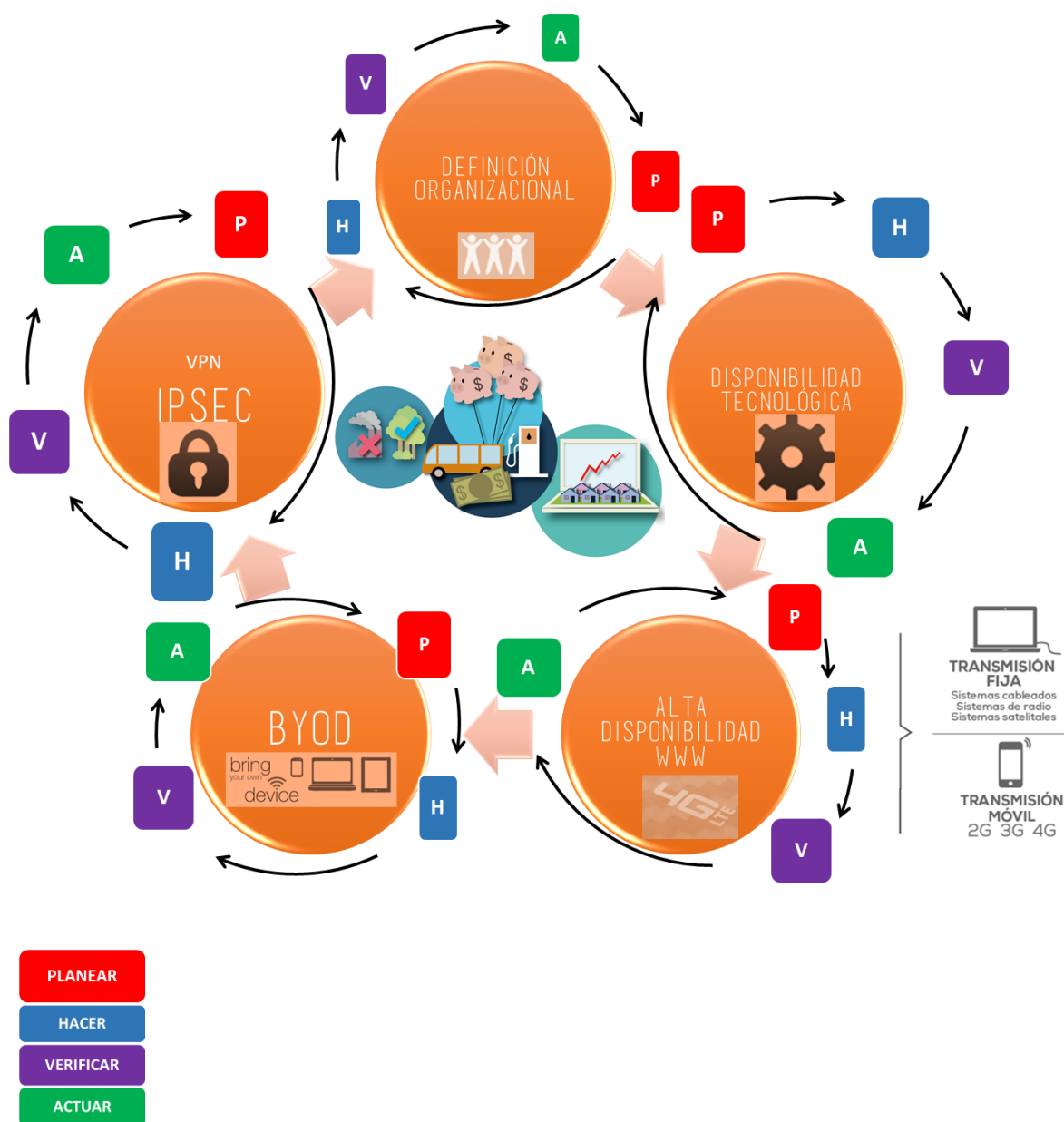


Ilustración 14: Modelo DDABI de Implementación de TT. Fuente: Autor

Este modelo busca facilitar e implementar el TT en una organización de forma completa, segura y con beneficios a nivel de costos. Para ello cuenta con módulos de BYOD, alta disponibilidad a nivel de comunicaciones entre el teletrabajador y la organización; seguridad construida bajo el marco IPSEC, Infraestructura, disponibilidad tecnológica necesaria, y una definición organizacional que adopte una modalidad jurídica de TT dentro del esquema jerárquico de la empresa. Cada módulo está rodeado por un ciclo de mejora continua y gestión de la seguridad recomendada por las normas internacionales ISO 27001 e ISO 27002.

Este modelo además de ser una propuesta para el sector financiero puede ser adoptado por cualquier organización que cuente con una infraestructura tecnológica madura y actualizada. Su éxito depende de la correcta planificación, ejecución, verificación, y evaluación de cada módulo propuesto.

4.2 ESTRUCTURAS ORGANIZACIONALES BANCARIAS

Las sociedades financieras cuentan con grandes y complejos esquemas organizacionales, donde se establecen jerarquías y rangos para miles de empleados. Ayudan al establecimiento de políticas de seguridad y segmentan la organización en varias vicepresidencias y departamentos que cumplen objetivos definidos y actúan de forma sistémica para el buen funcionamiento de la organización. Su principal objetivo es la continuidad de negocio, la respuesta oportuna y disponibilidad de servicios para millones de clientes.

De una buena organización depende el éxito de una empresa, por esto es muy importante analizar y encontrar el lugar del teletrabajo dentro de los perfiles y cargos definidos en su interior, considerando los puestos y tareas que pueden ser ejecutadas de manera remota.

El TT debería considerarse fundamental para todos los integrantes de una empresa, no solo por los beneficios y ahorros de costos, sino por el bienestar y satisfacción de los empleados. Las rutinas pueden llegar a considerarse como una de las principales causas, no solo, de ausentismo laboral sino también de retiros voluntarios por parte de los trabajadores lo cuales se pueden traducir en considerables sumas de capital en procesos de nuevas vinculaciones y liquidaciones a empleados

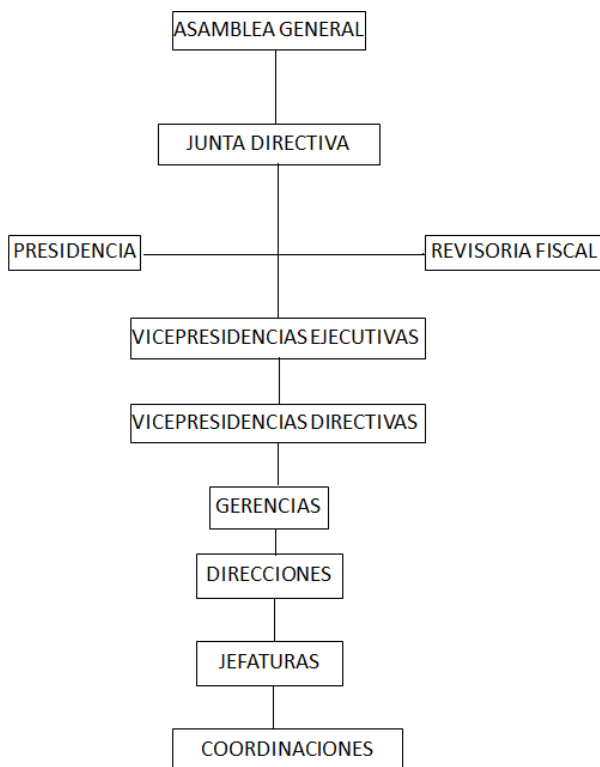


Ilustración 15: Esquema organizacional de primer nivel. Fuente Autor

En el anexo 1 se puede encontrar la estructura organizacional completa

En esta ilustración se puede observar la jerarquía de primer nivel, generalizada desde la Asamblea General y presidencia, hasta las jefaturas y coordinaciones. Cada Vicepresidencia puede contar con miles de empleados, varias gerencias y jefaturas. Estas últimas son las que cuentan con la mayor parte de personal con funciones y tareas definidas.

Los cargos descritos en la ilustración 15 son considerados capaces de teletrabajar, dados sus perfiles laborales y responsabilidades intrínsecas, así como las tareas administrativas que fácilmente pueden ser llevadas a cabo remotamente.

Cada departamento está conformado por una jefatura y una o varias coordinaciones; y sus empleados serían los más beneficiados con el establecimiento de trabajo remoto.

A continuación se puede ver el esquema organizacional de un departamento

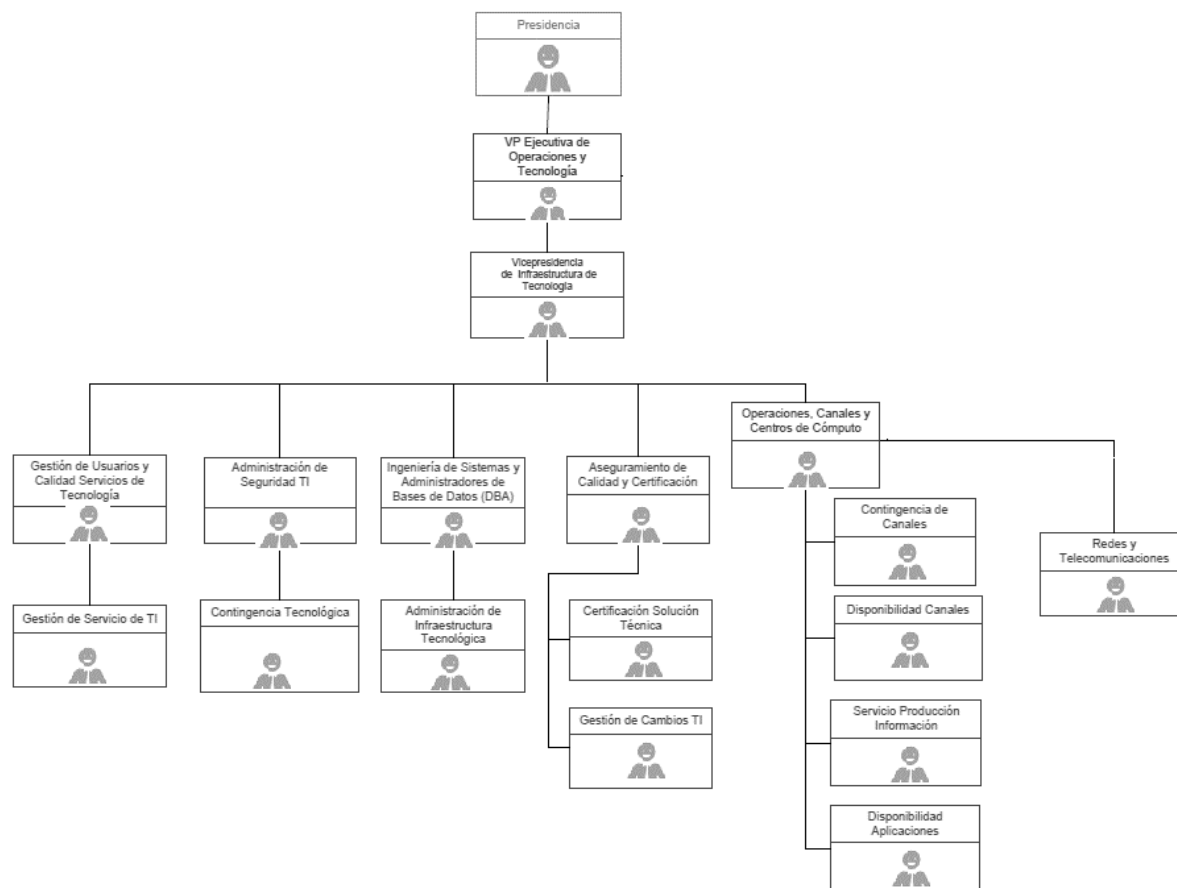


Ilustración 16: Esquema organizacional de segundo nivel. Fuente Autor

Este es un esquema organizacional generalizado a un departamento completo dentro de una organización financiera, con varias jefaturas y coordinaciones. Dentro de este diagrama se debe estipular un porcentaje de teletrabajadores limitado por la infraestructura tecnológica disponible en la organización.

4.2.1 DEFINICIÓN DE LOS PERFILES DE LOS TELETRABAJADORES

Aunque la oportunidad de teletrabajar debería ser para todos los empleados, está sujeta a la personalidad y responsabilidad de cada uno; la antigüedad también es importante al momento de definir la confianza de la empresa hacia su personal. Los trabajadores considerados adultos mayores o con algún tipo de discapacidad, y madres lactantes deben

tener prioridad al momento de la implementación de un proyecto piloto y adopción del TT en la organización.

También existe cierta dificultad para que los cargos parcial o completamente operativos adopten un modelo de TT, dadas las tareas efectuadas presencialmente. Para estos tipos de cargos se deben establecer oportunidades y tareas que puedan desarrollar remotamente en ciertas franjas horarias si sus cargos y actividades lo permiten.

Para definir los perfiles y tareas de un teletrabajador hay que tener en cuenta el concepto de teletrabajo, respetándolo y tratándolo seriamente como el trabajo presencial



Ilustración 16: Teletrabajo. Fuente Libro Blanco del TT MinTic pág. 13

Los teletrabajadores no se deben confundir como profesionales independientes, ni agentes de call center; tampoco desempeñan servicios de manufactura o servicios a domicilio para las empresas. Ellos hacen parte activa de una empresa y tienen cargos y perfiles con tareas y objetivos orientados al crecimiento y cumplimiento de metas dentro de una organización.

Para entender mejor el perfil laboral de un teletrabajador hay que tener en cuenta y abrir la mente hacia una nueva forma de trabajo, donde se cambian los horarios estrictos; la oficina central; el uso de dispositivos únicamente en la empresa; los encuentros y reuniones laborales presenciales, o el monitoreo y control físico a los trabajadores por parte de las jefaturas. Todo lo anterior se convierte en un modelo flexible de trabajo, donde el mayor problema es la mentalidad de las directivas y las jefaturas, que impiden dar mayor confianza e independencia a los trabajadores a cargo, y se rehúsan a creer en un crecimiento productivo y de beneficios para toda la organización.

“Las compañías deben confiar en sus trabajadores” (Nilles, 1970)

Un empleado apto para teletrabajar debe contar con cualidades como responsabilidad, disciplina, compromiso, etc., y un perfil que asegure su éxito como trabajador remoto, y

no el fracaso ante implementación y adopción del TT, que puede ser causado por falta de responsabilidad, desórdenes de atención y factores distractores en el hogar que puedan afectar la concentración y el cumplimiento de los objetivos propuestos.

El perfil de un trabajador a distancia debe contar con las siguientes cualidades además de las que cada empresa considere necesarias para sus empleados (Plus, 2013):

- **Debe ser disciplinado, autónomo y comprometido.** Es muy importante que el teletrabajador pueda organizar su tiempo y prioridades de manera correcta, y sepa mantener distancia a los factores distractores de su hogar, que pueden afectar seriamente su desempeño y cumplimiento de metas u objetivos
- **Confiable.** Para las empresas es tal vez lo más crítico, ya que su información puede ser utilizada de forma fraudulenta. Uno de los factores a tener en cuenta para la evaluación de esta cualidad es la antigüedad y hoja de vida del empleado. Personas con antecedentes y llamados de atención recientes deben tener un tiempo de reivindicación para poder ser tenidos en cuenta. Personal en riesgo financiero o con adicciones comprobadas, son de igual forma un riesgo potencial para el modelo.
- **Conocimiento general sobre uso de las TICs necesarias para trabajar a distancia.** El correcto uso de tecnologías de información y comunicación es totalmente obligatorio, pues es el núcleo de éxito para el desarrollo de tareas a distancia.
- **Competencias en uso frecuente las TICs para el desarrollo de funciones.** Es necesario una relación y adaptación con las TICs y dispositivos tecnológicos. Un trabajador debe ser capaz de sortear con situaciones asociadas a sus dispositivos de trabajo o de comunicaciones, sin la necesidad de ser un especialista o profesional en alguna de estas ramas.
- **Capacidad para tomar decisiones.**
- **Habilidades interpersonales y comunicación.** El TT no es sinónimo de trabajo solitario. El trabajo en equipo, aunque remoto, sigue siendo uno de los factores más importantes
- **Liderazgo a distancia.** Capacidad para dirigir equipos virtuales de trabajo con disciplina y buenos resultados productivos.

- **El teletrabajador debe contar con la infraestructura propia para trabajar a distancia.** Este es un requisito primordial para lograr el módulo BYOD del modelo de TT. El empleado debe tener disponible una conexión de banda ancha a Internet, así como un dispositivo de cómputo actualizado y con sistemas operativos, compatibles con el software y tecnologías de comunicación necesarias para el trabajo remoto. La empresa no brindará soporte técnico o mantenimientos preventivos o correctivos sobre los dispositivos del trabajador, de aquí la importancia en el manejo y uso correcto de las TICs.

4.3 DETERMINACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA NECESARIA PARA LA IMPLEMENTACIÓN DEL TELETRABAJO

La infraestructura tecnológica es un factor determinante para la implementación del TT en una organización, dada su criticidad en cuanto al correcto manejo de la información y la capacidad de establecer comunicaciones seguras a través de internet con los trabajadores remotos.

Las organizaciones financieras en su mayoría cuentan con una infraestructura madura y actualizada que facilita la adopción de modelos de teletrabajo, pues tienen dispositivos de comunicaciones robustos, compatibles con tecnologías de VPN, prevención de intrusos, detección y control de amenazas internas y externas, además de canales redundantes de Internet con capacidades entre 50 y 80 Mbps.

Para adoptar un modelo de TT la infraestructura tecnológica debe contar con varios dispositivos y tecnologías de comunicaciones. Esta se puede dividir en dos partes que conforman la comunicación punto a punto o punto multipunto, entre la oficina central y sus trabajadores:

- Infraestructura tecnológica de la empresa.
- Infraestructura tecnológica del trabajador.

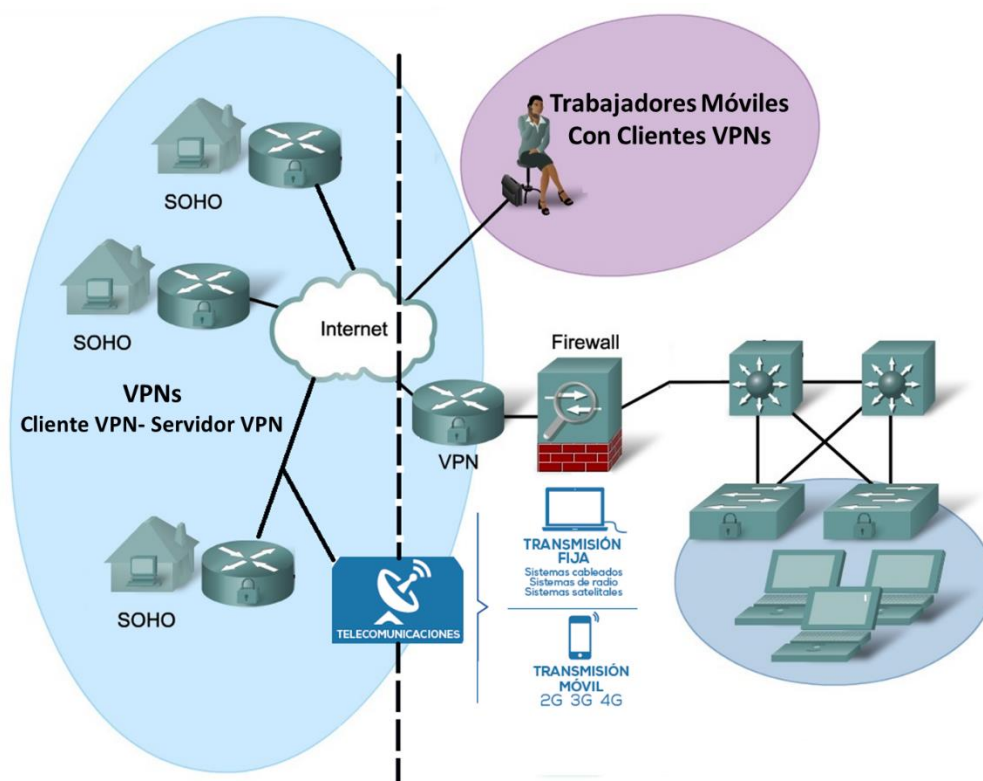


Ilustración 17: Infraestructura Tecnológica TT. SOHO (Small Office Home Office). Fuente Autor

La ilustración 17 muestra ambos tipos de infraestructura, empresarial y del teletrabajador. Se pueden observar algunos de los requisitos mínimos a tener en cuenta antes de adoptar un modelo de teletrabajo.

Estos dos tipos de infraestructura son importantes en la misma magnitud, y no puede haber una funcionalidad completa si alguna de las dos presenta fallas o deficiencias en su operación y definición. Ambas deben coexistir y compartir parámetros de configuración y de tecnologías de comunicación; es necesario definirlos paralelamente junto con las tecnologías, costos asociados a la implementación de algún modelo de TT, y a la cantidad de teletrabajadores que se desee dentro de la estructura organizacional.

4.3.1 INFRESTRUCTURA TECNOLÓGICA DE LA EMPRESA

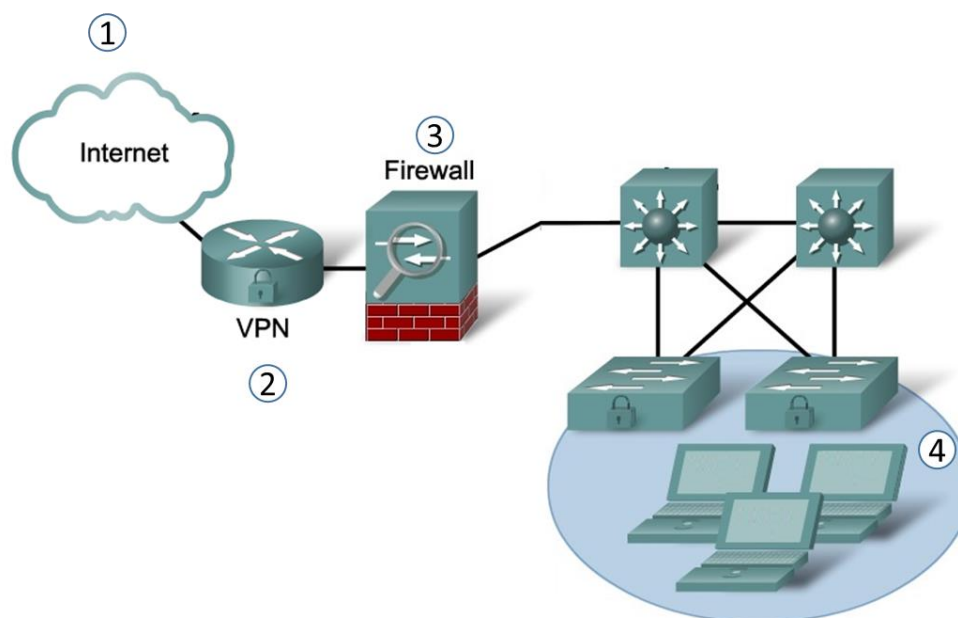


Ilustración 18: Infraestructura Tecnológica Empresarial TT. Fuente Autor

- 1) Conexión redundante por fibra óptica a Internet
- 2) Concentrador o servidor de VPNs compatible con IPSEC o certificados RSA
- 3) Firewall de inspección de estado o de Aplicación. Los firewall de inspección de paquetes se consideran obsoletos e inseguros.
- 4) Escritorios físicos o virtuales con autenticación en directorios activos, dominios de red o sistemas de control de acceso a la red. Los trabajadores remotos deben autenticarse con usuarios propios en los dominios o la red de la empresa.

Cada compañía puede definir su infraestructura para el TT, la Ilustración 18 muestra lo esencial y recomendado para adoptar un modelo tecnológico de trabajo remoto. La capacidad de los enlaces a Internet, los fabricantes o marcas de los equipos propuestos, y la manera en que los usuarios acceden a los recursos de red dependen del presupuesto y

necesidades de cada empresa. Sin embargo es recomendable que toda infraestructura sea escalable y cuente con calidad y el respaldo necesario. También se aconseja que los enlaces a Internet sean conexiones a redes de fibra óptica como medio de transmisión, con distintos proveedores de servicios para asegurar contingencia y alta disponibilidad al contratar ultimas millas diferentes. El ancho de banda dedicado al TT es proporcional a la cantidad de trabajadores remotos deseados, con consumos desde 0.25 Mbps en adelante; donde se debe asegurar comunicación sin saturación o intermitencias, con tiempos de retardo y jitter, recomendados más adelante en esta investigación, para los servicios utilizados remotamente.

4.3.2 INFRESTRUCTURA TECNOLÓGICA DEL TRABAJADOR REMOTO

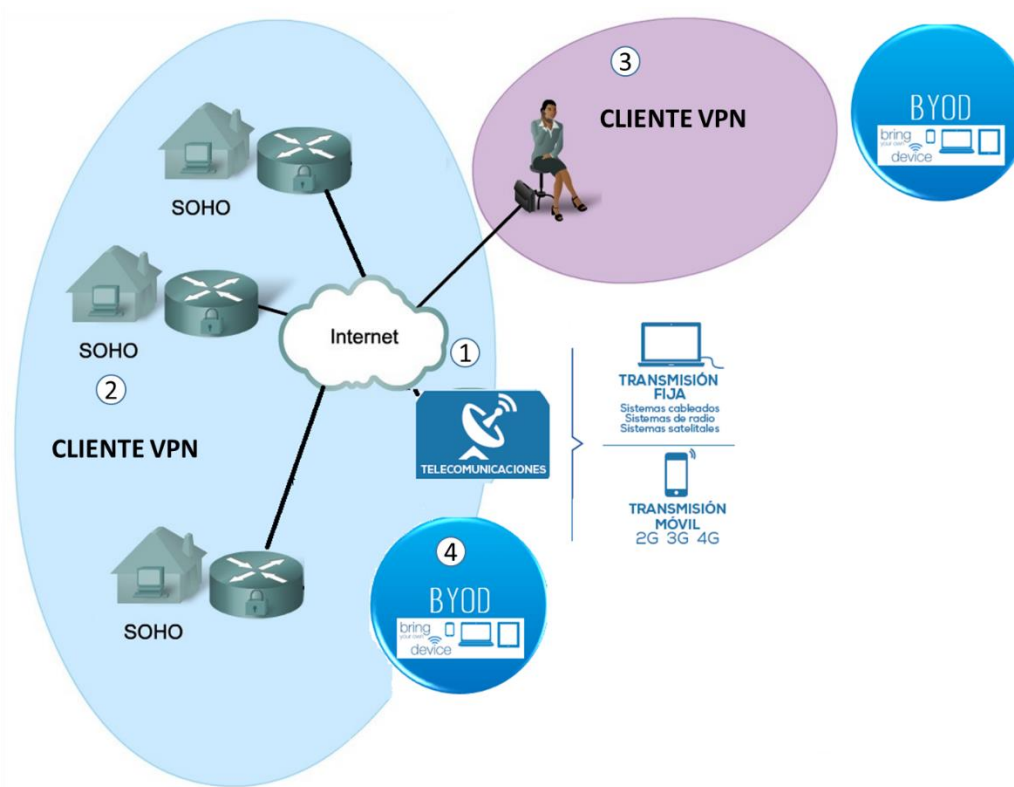


Ilustración 19: Infraestructura Tecnológica Trabajador Remoto. Fuente Autor

- 1) Conexión redundante a Internet con medios de transmisión fijos (Fibra óptica, Cobre, Radio, etc.), y móviles con tecnologías 3G o 4G.
- 2) Dispositivos de cómputo actualizados, con sistemas operativos licenciados y antivirus de libre distribución instalados con definiciones de Malware y virus al día.
- 3) Software de libre distribución para clientes VPN.
- 4) BYOD (Bring Your Own Device). El trabajador Remoto debe estar dispuesto a trabajar con sus dispositivos, y a acoplarlos a las políticas de seguridad y recomendaciones de la empresa.

La conexión a Internet debe ser banda ancha con una velocidad mayor o igual a 2Mbps para soportar los servicios prestados remotamente a la empresa, y el consumo propio del hogar y la familia (MINTIC, Libro Blanco:El ABC del Teletrabajo, 2012). Esta estimación es muy importante para el cumplimiento de objetivos y el correcto funcionamiento de los servicios y trabajo a través de la VPN. Las conexiones fijas deben tener prelación sobre las móviles para los enlaces de SOHO, para estos las tecnologías móviles son la contingencia ante los fallos de los enlaces principales y sus costos si deberían ser asumidos por la compañía.

El teletrabajador debe contar con su equipo de cómputo o dispositivos móviles, con las características suficientes para desempeñar sus labores con éxito. Dichas especificaciones deben ser estipuladas y puestas en conocimiento por parte de la compañía al momento de seleccionar a los trabajadores a distancia. El cliente VPN es una aplicación que puede ser o no licenciada, la elección, instalación y configuración de este software en los dispositivos de teletrabajador es responsabilidad de la empresa así como sus costos o mantenimiento asociados.

4.4 ANÁLISIS DE PROTOCOLOS Y TÉCNICAS DE CIFRADO PARA LA CONFIDENCIALIDAD, INTEGRIDAD Y ACCESO LA INFORMACIÓN.

“Las tecnologías de la encriptación constituyen el avance tecnológico más importante de los últimos mil años. Ningún otro descubrimiento tecnológico - desde las armas nucleares (espero) hasta Internet- tendrá un impacto más significativo en la vida social y política de la humanidad. La criptografía va a cambiar absolutamente todo”.

Lawrence Lessig

La criptografía moderna consta de tres partes que tienen como finalidad la Integridad, la autenticación y la confidencialidad:

- Hashes o funciones picadillo, de digestión o de resumen
- Protocolos
- Algoritmos

INTEGRIDAD	AUTENTICACIÓN	CONFIDENCIALIDAD
MD5	HMAC-MD5	DES
SHA	HMAC-SHA-1	3DES
	RSA Y DSA	AES

Tabla 1. Algoritmos, protocolos y funciones de Hash criptografía.

La tabla 1 clasifica algoritmos, protocolos y hashes con su funcionalidad específica dentro de los objetivos de seguridad. Cada uno fue desarrollado para proteger distintos vértices y campos dentro de la protección del acceso y gestión de la información. Para esta investigación es necesario analizarlos y entender sus ventajas, desventajas, y conveniencia al momento de utilizarlos para garantizar un acceso seguro a la información.

4.4.1 Funciones de resumen o hash

MD5 y SHA son consideradas las funciones de hash más importantes para asegurar la integridad y autenticación dentro de las negociaciones de llaves privadas o públicas. Las funciones de hash toman un mensaje, lo procesan y producen una representación condensada llamada mensaje digerido. Son consideradas funciones de un solo sentido, es decir que una vez aplicadas no hay forma o método de encontrar el mensaje original dentro del mensaje final. Estas funciones son usadas para:

- Proveer autenticación cuando se utilizan llaves simétricas, proceso que realiza IPSec y protocolos de enrutamiento.
- Provee Integridad en los certificados de llave pública PKI y firmas digitales.

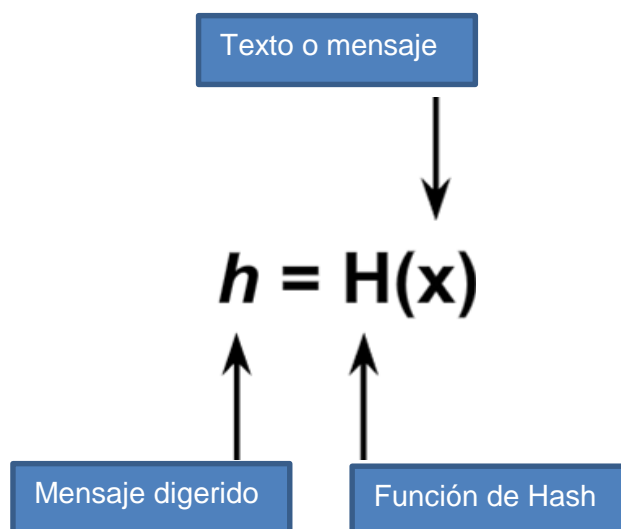


Ilustración 20: Función de Hash. Fuente Autor

MD5 utiliza 128 bits y 64 procesos para digerir mensajes mientras que SHA utiliza 10 bits y 80 procesos para el mismo fin. Actualmente se considera SHA más seguro que MD5 (Shirley Radack, 2008) y existen cuatro funciones de SHA adicionales publicadas por el NIST con mayores longitudes, conocidas como SHA-2:

- SHA-224 (224 bit)
- SHA-256 (256 bit)
- SHA-384 (384 bit)
- SHA-512 (512 bit)

El código de autenticación de mensajes HMAC o KMAC (keyed-hash message authentication code) se basa en las funciones MD5 o SHA usando una llave simétrica adicional en la entrada del mensaje a digerir. Este método es utilizado por todos los fabricantes de tecnologías de seguridad y participa de forma activa en IPSec

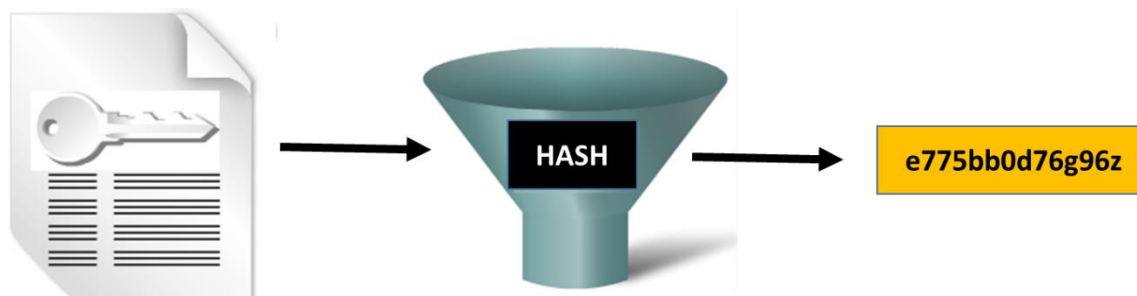


Ilustración 20: HMAC. Fuente Autor

La longitud de las claves o llaves y su combinación con números y letras mayúsculas define cuán seguro es el sistema.

El uso de dichas claves define dos métodos criptográficos, de dos tipos; simétricos y asimétricos. Los métodos simétricos como Cesar, DES, 3DES, AES, etc, se basan en el establecimiento o generación de una clave o llave compartida, es decir conocida tanto por el emisor como el receptor, para poder cifrar o descifrar de manera correcta el mensaje o información.

El cifrado asimétrico como el RSA, Elliptical Curve, Diffie Hellman, utilizan la criptografía de dos claves o llaves, una de ella pública, y la otra privada necesaria para cifrar o descifrar el mensaje, otorgando confidencialidad y confiabilidad, fundamento de las firmas digitales.

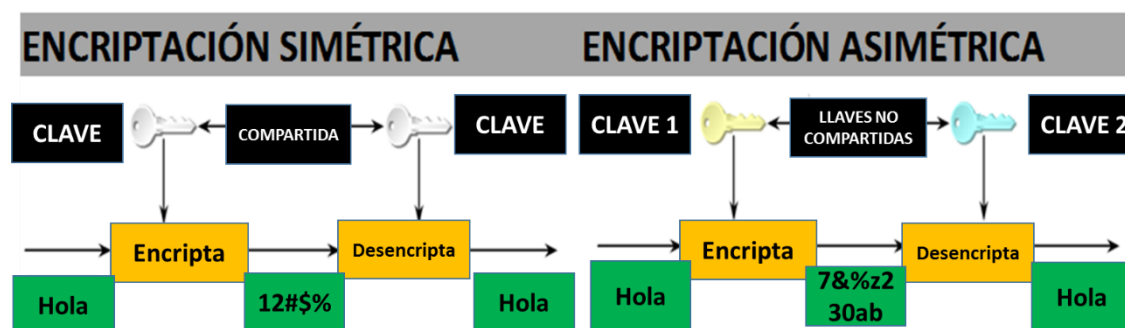


Ilustración 21: Métodos criptográficos. Fuente Autor

Según las estimaciones de la NSA se puede comparar el tiempo de protección ante un ataque diccionario con la longitud de las llaves así:

TIEMPO DE PROTECCIÓN	CLAVE SIMÉTRICA	CLAVE ASIMÉTRICA	CERTIFICADO DIGITAL	HASH
HASTA 3 AÑOS	80	1248	160	160
HASTA 10 AÑOS	96	1776	192	192
HASTA 20 AÑOS	112	2432	224	224
HASTA 30 AÑOS	128	3248	256	256
CONTRA COMPUTADORAS CUÁNTICAS	256	15424	512	512

Tabla 2: Expectativa vs longitud de llaves. Fuente Cisco networking Academy. Guía oficial CCNS Security Course Booklet Version 1.1 2nd Edition Cap. 7 pág, 185

4.4.2 Algoritmos de Encriptación

4.4.2.1 Data Encryption Standard (DES)

Es un algoritmo de cifrado simétrico que normalmente funciona en modo bloque. Se encriptan los datos en bloques de 64 bits. El algoritmo DES es esencialmente una secuencia de permutaciones y sustituciones de bits de datos en combinación con una clave de cifrado. El mismo algoritmo y la clave se utiliza para el cifrado y el descifrado.

DES tiene una longitud de clave fija. La clave es 64-bits de longitud, pero sólo 56 bits se utilizan para el cifrado. Los 8 bits restantes se utilizan para la paridad. El bit menos significativo de cada byte de la clave se utiliza para indicar la paridad impar.

Las claves DES son siempre de 56 bits de longitud por defecto. Cuando DES se utiliza con un cifrado más débil de una clave de 40-bits, la clave de cifrado es de 40 bits y 16 bits secretos conocidos, que hacen que la longitud de clave de 56 bits. En este caso, DES tiene una resistencia a la clave de 40 bits. Este algoritmo se considera completamente desactualizado e inseguro ya que fue descifrado por la súper computadora COPACABANA

4.4.2.2 3DES

Con los avances en la potencia procesamiento de los computadores comerciales, el DES original de 56-bit de clave no pudo resistir el ataque de las tecnologías de hacking. Así que 3DES aumentó la longitud efectiva de la clave DES, sin cambiar el algoritmo, utilizándolo con diferentes claves varias veces, exactamente tres veces.

La técnica de aplicar DES tres veces en una fila para un bloque de texto claro se llama 3DES.

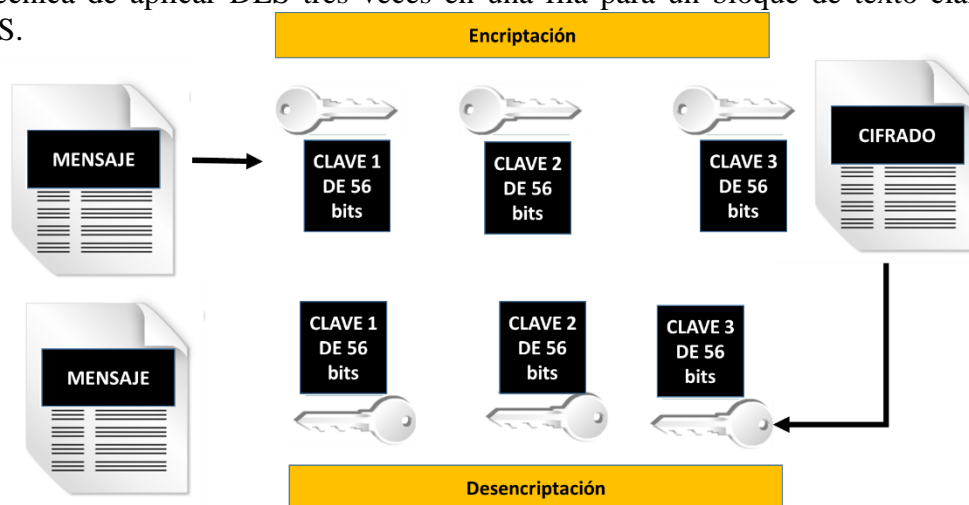


Ilustración 22: 3DES. Fuente Autor

4.4.2.3 Advanced Encryption System AES

En 1997, la implementación de AES fue anunciada, y se invitó al público a proponer esquemas de cifrado para reemplazar a DES. Después de un proceso de normalización de cinco años en el que compitieron 15 diseños que fueron presentados y evaluados, en EE.UU. por el Instituto Nacional de Estándares y Tecnología (NIST), se seleccionó el bloque de cifrado Rijndael como el algoritmo AES.

El algoritmo de cifrado Rijndael, desarrollado por Joan Daemen y Vincent Rijmen, tiene una longitud de bloque y clave variables. Rijndael es un cifrado de bloques iterado, lo que significa que el bloque de entrada inicial y clave de cifrado debe someterse a ciclos múltiples de transformación antes de producir la salida. El algoritmo puede operar sobre un bloque de longitud variable usando claves de longitud variable de 128 bits, 192 bits, o 256 bits. Se puede utilizar para cifrar bloques de datos que son de 128, 192, o 256 bits de longitud, y todas las nueve combinaciones de clave y la longitud de bloque son posibles.

La implementación de AES aceptada de Rijndael contiene sólo algunas de las capacidades del algoritmo Rijndael. El algoritmo se escribe de modo que la longitud de bloque o la longitud de la clave o de ambos pueden ser fácilmente extendidas en múltiplos de 32 bits, y el sistema está diseñado específicamente para una aplicación eficiente en hardware o software en una amplia gama de procesadores.

El algoritmo AES ha sido ampliamente analizado y ahora se utiliza en todo el mundo. Aunque no se ha comprobado en el uso del día a día en la medida en que tiene 3DES, AES con el cifrado Rijndael es el algoritmo más eficiente. Puede ser utilizado en entornos de alto rendimiento y baja latencia, especialmente cuando 3DES no puede manejar los requisitos de rendimiento o latencia.

4.4.2.4 Software-optimized Encryption Algorithm SEAL

Es un algoritmo alternativo al software basado en DES, 3DES y AES. Phillip Rogaway y Don Coppersmith diseñaron SEAL en 1993. Es un cifrado de flujo que utiliza una clave de cifrado de 160-bits. Debido a que es un cifrado de flujo, los datos a ser encriptados siempre se procesan más rápido que en algoritmos con cifrado por bloque. Sin embargo, tiene una fase de inicialización más larga durante la cual se crea un gran conjunto de tablas usando SHA.

4.4.2.5 Rivest Cipher RC

Los algoritmos fueron diseñados en parte por Ronald Rivest, quien también inventó MD5. Los algoritmos de RC son ampliamente utilizados en muchas aplicaciones de redes debido a su velocidad favorable y capacidades variables de longitud de claves.

Hay un número de algoritmos ampliamente utilizados RC:

- RC2: Algoritmo de tamaño de clave variable y cifrado de bloque que fue diseñado como un "drop-in"²² de reemplazo para DES.
- RC4: El más utilizado del mundo en cifrado de flujo. Este algoritmo de clave variable y cifrado de flujo Vernam, que se utiliza a menudo en los productos de cifrado de archivos y para las comunicaciones seguras, como SSL. No se considera de una sola vez, ya que su clave no es aleatoria. El cifrado corre muy rápidamente en el software y se considera seguro, aunque puede ser implementado de forma no segura, como en Wired Equivalent Privacy (WEP).
- RC5: Es un cifrado de bloques rápido que tiene un tamaño de bloque y clave variable. Puede ser utilizado como un reemplazo directo para DES si el tamaño de bloque se establece en 64-bits.
- RC6: Desarrollado en 1997, fue un finalista de AES. Diseñado por Rivest, Sidney, y Yin, basado en RC5. Su objetivo principal era el diseño para cumplir con el requisito de la convocatoria AES.

Todos los algoritmos de encriptación tienen ventajas y desventajas en cuanto a rendimiento y seguridad, llaves muy largas pueden provocar mayor gasto de recursos y tiempos elevados de procesamiento, aunque garantizan una seguridad elevada. Así mismo los métodos de cifrado asimétrico como RSA manejan altas longitudes de llave, como se pudo apreciar en la Tabla 2, esto puede generar tiempos más largos en el establecimiento y aseguramiento de los canales de comunicación, y algo de latencia dentro de las comunicaciones seguras.

El éxito de todos los algoritmos de encriptación está en la confidencialidad de las llaves, esta, se puede decir, que es el punto débil de todos ellos, y de su correcta gestión depende la seguridad y el buen uso de la información que día a día se convierte en el objetivo principal de cualquier ataque.

Para el diseño de red y la simulación se utilizarán llaves pre compartidas, teniendo en cuenta el elevado procesamiento de algoritmos asimétricos y el impacto que puede tener en el desempeño y tiempos de simulación de la VPN. El uso de RSA y certificados o firmas digitales, también representa costos más elevados por licencias en concentradores o servidores VPN.

² Drop-In Replacement, Término que hace referencia a una actualización, mejora y reemplazo de tecnología

4.4.2.6 Criptoanálisis Y Comparación de sistemas criptográficos

Algoritmo de encriptación simétrica	Longitud de la llave	Descripción	Tiempo de crackeo(Suponiendo 255 claves por segundo)	Velocidad	Consumo
DES	56	-Diseñado en IBM durante los años 1970 y adoptado como el estándar NIST hasta 1997. -Aunque se considera obsoleto, DES sigue siendo ampliamente utilizado. -DES fue diseñado para ser implementado sólo en el hardware, y es por lo tanto extremadamente lento en software.	(6,4 días por parte de la máquina COPACABANA. Un dispositivo de craqueo especializado)	Media	Medio
3DES	112 y168	-Basado en el uso de DES tres veces lo que significa que los datos de entrada se cifra tres veces y se considera por lo tanto mucho más fuerte que DES. -Sin embargo, es bastante lento en comparación con algunas nuevas cifras de bloque, como AES.	4,6 mil millones de años con la tecnología actual	Baja	Medio
AES	128, 192, y 256	-AES es rápido tanto en software y hardware, e fácil de implementar, requiere poca memoria. -Nuevo estándar de cifrado, que está siendo desplegado actualmente a gran escala.	149 billones de años	Alta	Bajo
Software Encryption Algorithm (SEAL)	160	SEAL es un algoritmo alternativo a DES, 3DES y AES. -Se utiliza una clave de encriptación de 160-bits y tiene un menor impacto en la CPU en comparación con otros algoritmos basados en software.	Desconocido, se considera muy seguro	Alta	Bajo
RC	RC2 (40 y 64) RC4 (1 a 256) RC5 (0 a 2040) RC6 (128, 192, a 256)	Conjunto de algoritmos de cifrado de clave simétrica inventado por Ron Rivest. -RC1 nunca fue publicado y RC3 se rompió incluso antes de que se utilizara. -RC4 sistema de cifrado más utilizado en el mundo. -RC6, tiene un bloque de cifrado 128-bit basado en gran medida en RC5, fue un finalista de AES desarrollado en 1997.	se considera seguro, aunque puede ser implementado de forma no segura, como en Wired Equivalent Privacy (WEP)	Alta	Bajo

Tabla 3. Comparación y criptoanálisis de los sistemas criptográficos. Fuente: Autor, Criptoanálisis (NIST, 2012)

4.4.2.7 Intercambio de llaves Diffie-Hellman

El algoritmo Diffie Hellman es la base de todos los métodos modernos de intercambio de llaves de forma automática. DH no es un método de encriptación y no es utilizado para encriptar datos. Es un método de aseguramiento de las claves compartidas que son utilizadas para cifrar la información. El Algoritmo Matemático DH logra que dos host generen una clave secreta idéntica sin necesidad de tener o haber establecido una comunicación con anterioridad; esta clave nunca es transmitida entre las partes pero ambos logran saber que tienen la misma gracias a DH.

Características de DH:

- DH se considera un algoritmo asimétrico con aplicación en la negociación de métodos simétricos de encriptación
- Puede generar llaves de 512, 1024 o 2048 bits
- Se considera muy seguro, pues no documenta pruebas de crackeo efectivas con la tecnología actual

4.4.2.7.1 Funcionamiento de DH

Como es un algoritmo Asimétrico DH cuenta con una clave o llave, pública o pre compartida, conocida por ambas partes o host que se van a comunicar. Esta clave tiene una parte denominada base o generador y otra llamada principal o módulo.

Si se toma como ejemplo la clave compartida “HOLA“= 5(base), 23(módulo) entonces el proceso de DH es el siguiente:

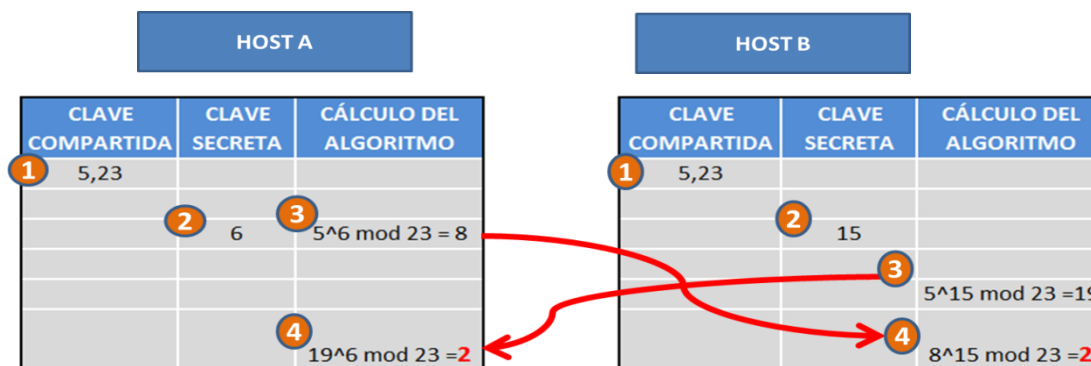


Ilustración 23: Algoritmo DH. Fuente Autor

1. Se establece la clave pre compartida “HOLA“= 5(base), 23(módulo) entre el Host A y el Host B
2. El Host A genera la clave secreta $SA=6$ y el Host B genera la clave secreta $SB=15$
3. El Host A aplica el algoritmo DH $b^{SA} \cdot SA \bmod = XA(5^6 \bmod 23) = 8$ (EC. 1)
4. El Host B aplica el algoritmo DH $b^{SB} \cdot SB \bmod = XB(5^{15} \bmod 23) = 19$ (EC. 2)
 XA y XB son intercambiadas entre los host
5. El host A ejecuta un nuevo algoritmo DH
 $XB^{SA} \cdot SA \bmod = XA(5^6 \bmod 23) = 2$ (EC. 3)
El host B ejecuta un nuevo algoritmo DH
 $XA^{SB} \cdot SB \bmod = Z(19^6 \bmod 23) = 2$ (EC. 4)

Como el resultado en ambas partes es 2, la negociación de claves o intercambio ha sido exitoso y la comunicación segura entre el Host B y el Host A puede empezar a transferir datos o información.

Los algoritmos asimétricos como DH son fundamentales para la negociación de claves manteniendo su integridad y confidencialidad.

Existen cuatro protocolos que utilizan algoritmos asimétricos de negociación de llaves:

- IKE Internet Key Exchange. Parte fundamental de IPSec
- SSL Secure Socket Layer
- SSH Secure Shell
- PGP Pretty Good Privacy

Todos los protocolos anteriores son parte fundamental de las comunicaciones modernas con aplicaciones desde el uso de exploradores de internet, hasta el aseguramiento de grandes infraestructuras de correo, de acceso y gestión remota de equipos de red.

4.5 DEFINICIÓN DE LA PRUEBA PILOTO, DISEÑO Y SIMULACIÓN DE RED.

4.5.1 Definición de prueba piloto

Hay tres aspectos a tener en cuenta:

- Marco Jurídico para la adopción del Teletrabajo

- Modelo de Teletrabajo que se va a implementar en la organización
- Definición de la cantidad de Teletrabajadores.

4.5.1.1 Marco Jurídico para la adopción del Teletrabajo

De acuerdo a las modalidades de teletrabajo estipuladas en la Ley 1221 de 2008 (MINTIC, Ministerio de Tecnologías de la Información y las Comunicaciones , 2008):

- Teletrabajo suplementario,
- Teletrabajo autónomo
- Teletrabajo móvil.

Para este proyecto será utilizada la modalidad de Teletrabajo Suplementario, definido por la Ley 1221 de 2008 como:

“Trabajadores con contrato laboral que alternan sus tareas en distintos días de la semana entre la empresa y un lugar fuera de ella, Usando las TIC para su cumplimiento”

Esta modalidad es la más conveniente para evolucionar de un modelo común de trabajo a un modelo de teletrabajo en una organización, ya que permite que los trabajadores continúen desempeñando sus labores en oficinas centrales, con la posibilidad y flexibilidad de realizar, en cuanto sea posible, su trabajo remotamente. El teletrabajo suplementario facilita la adopción de un modelo de trabajo remoto en una organización, ya que implica pocos cambios a niveles contractuales y organizacionales, ayuda a una rápida evaluación de resultados, y es más fácil de aceptar por parte de directivas y jefaturas quienes pueden realizar seguimientos semanales o periódicos a los objetivos y metas propuestas de manera presencial con los empleados.

Cualquier modificación a los contratos laborales debe estar amparada por el decreto 0884 de 2012, para garantizar los beneficios de ley para los trabajadores. Estas modificaciones deberán ser estudiadas y realizadas por los departamentos de recursos humanos o áreas especializadas en acuerdo con las directivas de la Organización. Uno de los apartes a tener en cuenta, si hay lugar dentro de los contratos existentes, es la modificación para cumplimiento de horarios, flexibilizándolos al trabajo remoto y el cumplimiento y seguimiento de tareas y objetivos.

Estas son las consideraciones legales para su cumplimiento:

- La voluntariedad: El teletrabajo no puede ser impuesto, así como los modelos de BYOD. Los empleados con contratos existentes son quienes se deben postular al modelo de trabajo remoto, y las condiciones deben ser de libre aceptación.
- Suministro de Equipos Informáticos: Según el Artículo 6 de la Ley 1221 de 2008, “los empleadores deberán proveer y garantizar el mantenimiento de los equipos de los teletrabajadores, conexiones, programas; así mismo el valor de la energía y los desplazamientos ordenados por él, necesarios para desempeñar sus funciones”. Sin embargo, El Artículo 57 del Código Sustantivo del Trabajo establece en el numeral 1º: “Son obligaciones especiales del patrono: 1. Poner a disposición de los trabajadores, salvo estipulación en contrario, los instrumentos adecuados y las materias primas necesarias para la realización de las labores”. Sin embargo, las partes pueden pactar que el empleado suministre el equipo informático; en ese caso, el empleador deberá acordar por contrato una prima extra en compensación por la utilización de las herramientas tecnológicas para fines laborales.
- Costos asociados a los servicios públicos: La empresa no puede trasladar los costos de funcionamiento a los trabajadores remotos, la Ley dispone el reconocimiento por parte del empleador, de costos asociados al servicio de energía o conexiones adicionales.
- Jornada laboral de los teletrabajadores: El Artículo 3º del Decreto 884 de 2012 establece que el contrato o vinculación que se genere a través del teletrabajo deberá indicar los días y los horarios en que el teletrabajador realizará sus actividades para efectos de delimitar la responsabilidad en caso de accidente de trabajo y evitar el desconocimiento de la jornada laboral.
- Derechos de los teletrabajadores: La ley 1221 de 2008 establece que la igualdad de trato entre teletrabajador y trabajador se deberá fomentar, particularmente en estos aspectos:
 - Derecho de constituir o afiliarse a las organizaciones que escojan.
 - Protección en materia de Seguridad Social
 - Remuneración.
 - Acceso a la formación.
 - Protección de la maternidad.
 - Respeto a la intimidad y privacidad del trabajador.
 - Edad mínima de admisión al empleo o al trabajo

El Artículo 4° del Decreto 884 de 2012, establece: “El empleador debe promover la igualdad de trato en cuanto a remuneración, capacitación, formación, acceso a mejores oportunidades laborales y demás derechos fundamentales laborales, entre teletrabajadores y demás trabajadores de la empresa privada o entidad pública”.

También es importante tener en cuenta que el trabajador tiene derecho a retractarse, según las condiciones pactadas en el contrato, a la modalidad laboral a distancia.

4.5.1.2 Modelo de Teletrabajo que se va a implementar en la organización

Se adoptó el modelo diseñado en la sección 2.1.4 de esta investigación, el cual corresponde a un diseño propio que se adapta a las necesidades del sector financiero. Dicho modelo consta de cinco módulos:

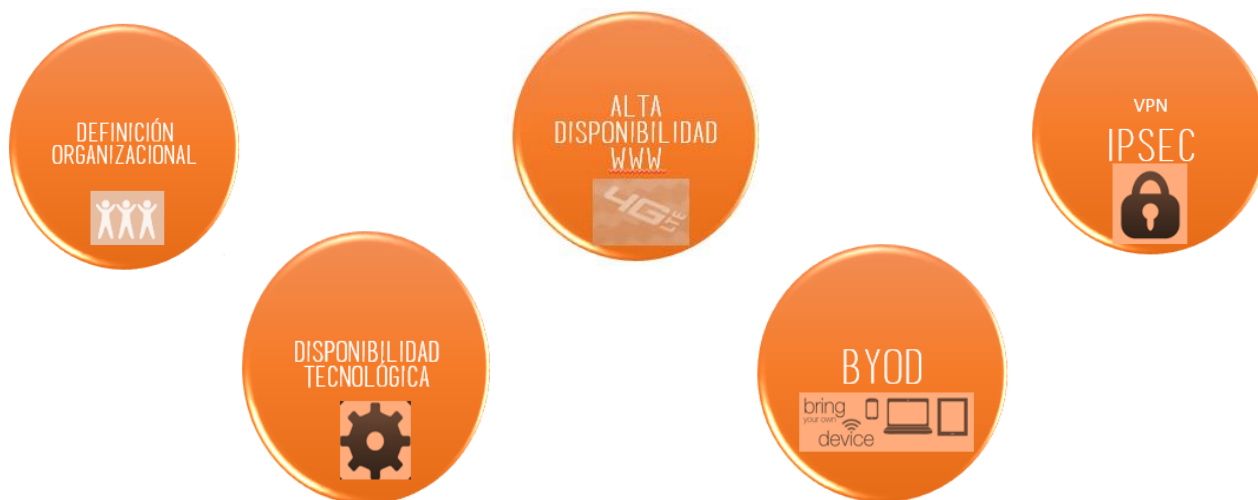


Ilustración 24: Módulos de teletrabajo Fuente: Autor

- Definición Organizacional
- Disponibilidad Tecnológica
- Alta disponibilidad
- BYOD
- VPN (IPSec)

4.5.1.2.1 Definición Organizacional

La modalidad de teletrabajo suplementario modifica en su mayoría las condiciones contractuales con los empleados, los esquemas organizacionales cambian, no con la creación de un departamento, sino con la inclusión de teletrabajadores en las dependencias donde los perfiles laborales se ajusten a las necesidades del trabajo remoto.

No habrá modificación de la jornada laboral de los empleados, es decir que se mantendrá el horario de oficina de las 8:30 a las 18:00 horas, de lunes a viernes.

El trabajador tendrá la posibilidad de realizar su trabajo de manera remota de 3 a 4 días hábiles por semana según sus actividades. Siendo mandatorio la asistencia presencial de al menos un día hábil a la semana, para desarrollar sus labores operativas y respectivos seguimientos por parte de sus jefes o coordinadores.

4.5.1.2.2 Disponibilidad Tecnológica

La cantidad de trabajadores remotos para una empresa está limitada por su infraestructura tecnológica. Dichos limitantes son:

- El ancho de banda o enlaces a Internet contratados por la empresa (50-80Mbps)
- Licenciamiento para usuarios VPN en los dispositivos de red como routers o firewalls.
- Aplicativos y servicios a utilizar de forma remota. De acuerdo a estos servicios los usuarios remotos se pueden clasificar en:
 - Usuarios básicos
 - Usuarios intermedios
 - Usuarios avanzados

Estos limitantes pueden generar costos adicionales. Sin embargo para la prueba piloto la cantidad de teletrabajadores no puede ser exagerada. Si se parte de la infraestructura tecnológica de una organización financiera, esta prueba puede llevarse a cabo sin necesidad de incurrir en gastos adicionales.

Para el piloto se tendrán en cuenta los siguientes datos:

- Un promedio de 4000 empleados para una compañía financiera del país. (García, 2014)

- Ancho de banda de 50 Mbps disponible para soportar trabajadores remotos (MINTIC, Libro Blanco:El ABC del Teletrabajo, 2012)
- Un total de 250 licencias de VPN. Este dato corresponde a la cantidad de usuarios VPN soportados por equipos de red de mediana capacidad que es aproximadamente 500 licencias (Cisco, 2012).
- Se debe asegurar un ancho de banda de (MINTIC, Libro Blanco:El ABC del Teletrabajo, 2012):
 - ✓ 0,25 Mbps para usuarios remotos básicos
 - ✓ 0,5 Mbps para usuarios Intermedios
 - ✓ 1.0 Mbps para usuarios avanzados

4.5.1.2.3 Alta Disponibilidad y BYOD

Para la prueba piloto se utilizarán los dispositivos de los empleados bajo la normativa expuesta en la sección 2.4.1.1.

La empresa instalará el cliente VPN, y brindará mantenimiento y soporte, presencial en la empresa o asesoría remota, para este software.

Para lograr la Alta Disponibilidad del modelo adoptado, La empresa tendrá:

- Una bolsa mensual destinada a la recarga de horas o días de planes 3G o 4G para los teletrabajadores. Esta bolsa será administrada por las jefaturas.
- En caso de daño o corte del plan de internet de los teletrabajadores, la jefatura correspondiente debe realizar la recarga restante a la jornada laboral, por ejemplo: si la falla del enlace de internet del hogar falla a las 10:00 de la mañana de un día laboral, se realizará una recarga de seis horas, medio día o en su defecto un día dependiendo los planes de los operadores de telefonía móvil de los empleados. Esto teniendo en cuenta que el trabajador cuente con un dispositivo móvil 3G o 4G con capacidad de compartir su conexión al PC o desempeñar sus funciones desde el celular o Tablet. Si el trabajador no cuenta con un equipo móvil apto, deberá acudir a las instalaciones físicas de la empresa para terminar su jornada laboral.
- Si el enlace fijo de internet, falla por más de un día, el trabajador remoto deberá presentarse a las instalaciones centrales para desempeñar sus funciones hasta que su respectivo proveedor solucione los inconvenientes.

- Si llegará a ocurrir alguna falla de tipo eléctrico, el trabajador remoto puede cambiar su sitio remoto de trabajo, o acudir a las instalaciones centrales para terminar su jornada laboral.

Para la compensación del uso de dispositivos de los empleados, se establecerán primas o bonos que justifiquen la depreciación de los equipos de cómputo de los trabajadores de acuerdo a la ley tributaria vigente, dependiendo del valor comercial del dispositivo. Este valor se calculará así

$$\text{Compesación} = \frac{\text{MOI} * \% \text{ de depreciación}}{12(1\text{Año})} \quad (\text{EC. 5})$$

MOI= Monto original de la inversión (Costo comercial del dispositivo)

% de depreciación= 30% Para equipos de cómputo

Así mismo se reconocerá el consumo de energía del hogar, provocado por el PC o computador portátil en la jornada laboral, dependiendo del estrato socioeconómico del empleado. El valor compensado se calculará en base a:

$$(\text{Consumo de PC o laptop Kwh}) * 8 \text{ horas} * \text{Costo 1 Kwh} * \text{días de teletrabajo al mes} \quad (\text{EC. 6})$$

4.5.1.3 Definición de la cantidad de Teletrabajadores

Al revisar los limitantes y los datos se puede concluir que la mayor restricción está dada por el ancho de banda disponible en la empresa

Para calcular el número total de empleados se propone la siguiente igualdad

$$(\mathbf{Nb} * \mathbf{Bw}) + (\mathbf{Ni} * \mathbf{Bw}) + (\mathbf{Na} * \mathbf{Bw}) = \mathbf{Bw}_{\text{Total}} \quad (\text{EC. 7})$$

Dónde:

Bw=Ancho de banda

Nb= Usuarios básicos

Ni= Usuarios intermedios

Na=Usuarios avanzados

Reemplazando con los anchos de banda según los tipos de usuarios en la Ecuación 7 tenemos:

$$(N_b * 0.25) + (N_i * 0.5) + (N_a * 1) = 50\text{Mbps}$$

Para el piloto se determinan los siguientes porcentajes del número total de teletrabajadores:

- El 50% serán usuarios básicos
- El 40% serán usuarios Intermedios
- El 10% restante usuarios avanzados

$$(50\% N_b * 0.25) + (40\% N_i * 0.5) + (10\% N_a * 1) = 50\text{Mbps}$$

Esto se traduce en:

Tipo de Usuario	BW Asegurado Mbps	Bw por usuario Mbps	Cantidad de usuarios
Básico	25	0,25	100
Intermedio	20	0,5	40
Avanzado	5	1	5
Total de Usuarios			145

Tabla 4. Cálculo de teletrabajadores. Fuente: Autor

25 Mbps asegurados para usuarios básicos = $25/0.25 = 100$ usuarios básicos
 20 Mbps asegurados para usuarios intermedios = $20/0.5 = 40$ usuarios intermedios
 5 Mbps asegurados para usuarios avanzados = $5/1 = 5$ usuarios avanzados

Como resultado se tiene un total de 145 teletrabajadores, los cuales representan el 3,62 % del total de empleados (4000).

De acuerdo a los resultados anteriores se decide que la prueba piloto contará con un 3,62% de teletrabajadores, los cuales serán repartidos en 5 departamentos de la organización financiera. Es decir 20 usuarios básicos, 8 usuarios intermedios, y 1 usuario avanzado por departamento.

4.6 DISEÑO Y SIMULACIÓN DE RED

La red de teletrabajo utilizará infraestructura y software de comunicaciones y VPN de Cisco, líder mundial de infraestructura y soluciones de telecomunicaciones. Las consideraciones de diseño basados en la prueba piloto son:

- ✓ Red VPN para 145 teletrabajadores
- ✓ Uso de IPSec como protocolo VPN por sus ventajas y rapidez de procesamiento.

- ✓ Servidor VPN
- ✓ VPN a través de Internet o red pública
- ✓ Cliente VPN para teletrabajadores
- ✓ Conexión redundante a Internet
- La red VPN será de tipo cliente-servidor. Como se trata de una extensión de 145 host a la LAN de la empresa se asignará una red tipo C privada 192.168.X.X/24 máscara 24 para que el piloto sea escalable hasta 253 host.
- La salida a Internet conectada o compartida al servidor VPN será de 50Mbps para asegurar la conexión de los 145 trabajadores remotos. Esta conexión debe ser:
 - Canales redundantes
 - Utilizará HSRP como protocolo de alta disponibilidad entre el servidor o router VPN y los ISPs contratados para asegurar la disponibilidad de información a los trabajadores.
 - El medio de transmisión de los canales de internet debe asegurar parámetros de retardo y jitter aceptables para el establecimiento, conexión sin intermitencias de la VPN, y tráfico encriptado. El uso de túneles IPSec o cualquier otro tipo de túneles aumenta los parámetros de jitter y retardo entre el servidor VPN y los usuarios remotos.

La siguiente tabla muestra una relación entre el valor del retardo y la calidad de los servicios de comunicaciones de acuerdo a experiencia propia para servicios de voz y datos

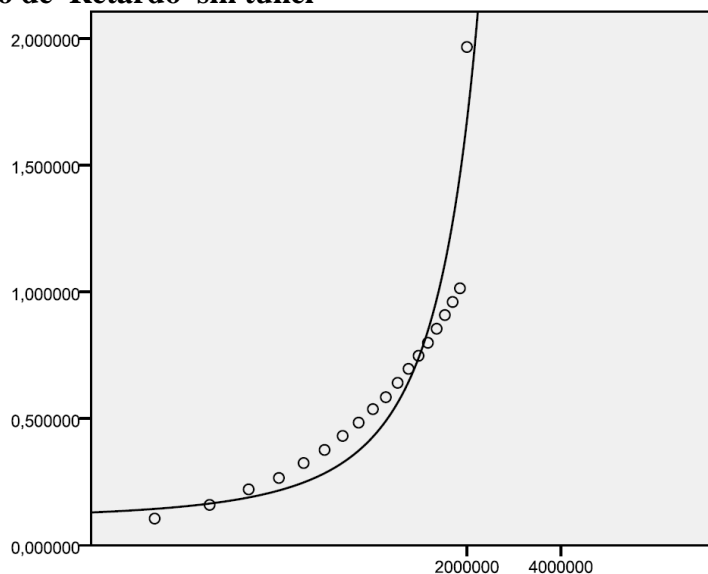
RETARDO ms	NIVEL DE SERVICIO
0-150	Aceptable para servicios de comunicaciones
151-400	Regular. Algunos servicios pueden funcionar deficientemente
>400	Inaceptable para diseño y planeación de red

Tabla 5. Niveles de retardo. Diseño de red. Fuente: Autor

El Jitter (variación en el retardo de transmisión) recomendado debe ser de menos de 20ms. Sobrepassar los tiempos de jitter y retardo recomendados producirían lentitud, pérdidas y retransmisiones de información, lo cual provocaría un comportamiento de red inestable para el teletrabajo

El tráfico IPsec aumenta exponencialmente el jitter y el retardo en una red. Por esto es importante en lo posible que la tecnología de transmisión en las conexiones a internet sean fibra óptica; esto con el fin de minimizar el impacto de la encriptación de la información, dado que el jitter aumenta de manera exponencial en relación al volumen de información que cursa a través de un túnel IPsec

Promedio de Retardo sin túnel



○ Observado
— Exponencial

Promedio de Retardo con túnel

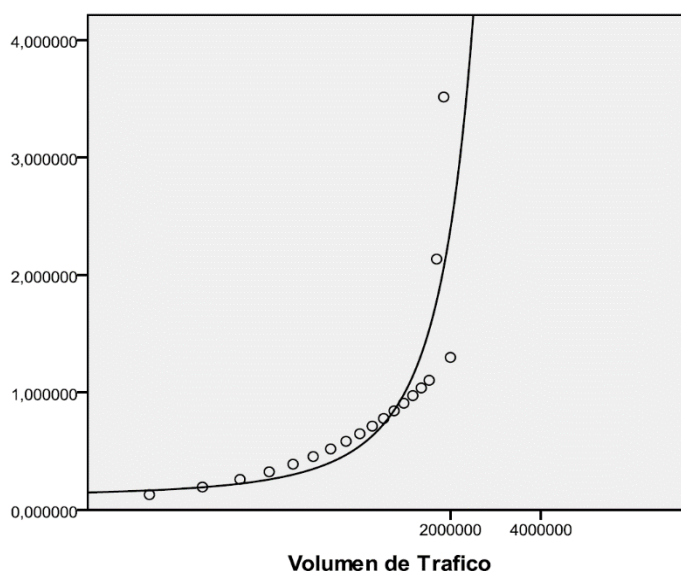
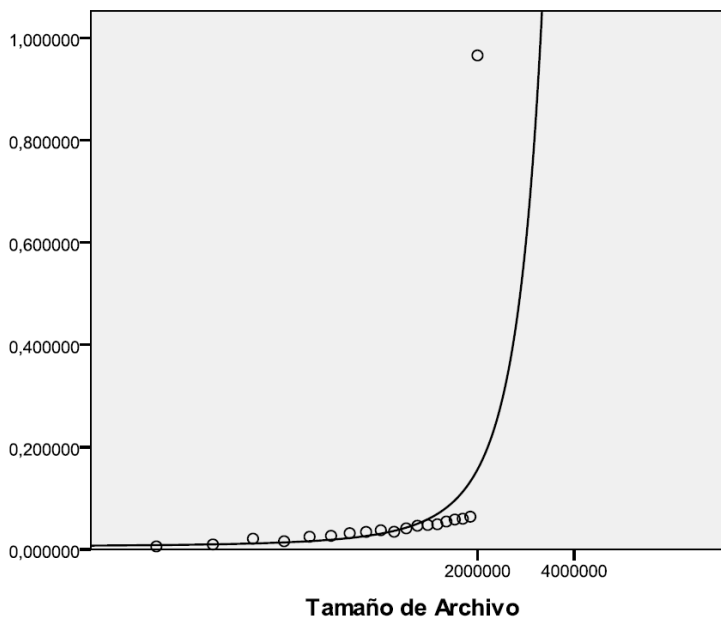
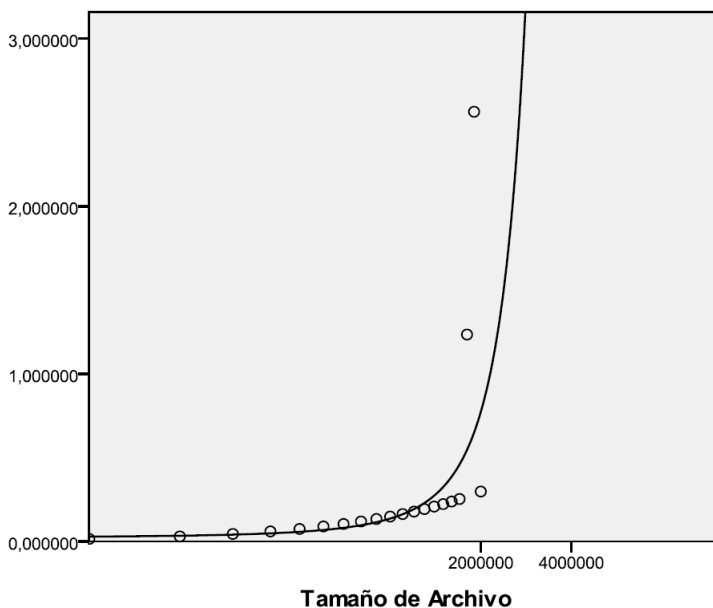


Ilustración 25: Comportamiento de retardo y jitter túnel IPsec. Fuente: Jacobs Gonzalez Universidad Dr. Rafael Bellosó Chacín, Venezuela

Promedio de Jitter sin túnel



Promedio de Jitter con túnel



○ Observado
— Exponencial

Ilustración 25: Comportamiento de retardo y jitter túnel IPSec. Fuente: INFLUENCIA DEL VOLUMEN DE TRÁFICO SOBRE JITTER EN TUNEL VPN IPSEC/UDP EN ENLACES WAN. Jacobs Gonzalez Universidad Dr. Rafael Beloso Chacín, Venezuela

- Los equipos de borde y servidor VPN solo deben aceptar conexiones internas por SSH para su gestión.
- Para la conexión de VPN, por tratarse de una conexión punto multipunto, se utilizará autenticación por grupo, con usuarios personalizados.
- Como política de seguridad para la generación de contraseñas
 - Se utilizarán claves de frase, es decir que las contraseñas asignadas a los usuarios remotos incluirán como mínimo 2 palabras separadas por espacios. La tecla espacio funciona como un carácter excepcional en los campos de contraseñas. Incluir un espacio en las claves puede dificultar de gran manera los ataques de diccionario o criptoanálisis a claves cifradas que puedan ser captadas por terceros través de Internet.
 - Como mínimo 10 caracteres alfanuméricos con letras mayúsculas. Por ejemplo:
“Un1v3rS1d4D D3 S4N 3uEnAv3nturA”
 - La renovación o cambio de claves será máximo cada mes o antes si el usuario lo requiere.
- Las llaves generadas en RSA, DH, AES, HMAC, y demás algoritmos o protocolos necesarios para IPsec y SSH tendrán una longitud de mínimo 1024 bits.
- Las contraseñas de gestión y modos privilegiados de configuración de dispositivos de red en la infraestructura de TT deben estar cifradas en MD5.
- Las redes inalámbricas WiFi de los empleados deben estar encriptadas con el protocolo WPA2, para evitar ataques o robo de información de tipo Man In the Middle. Los empleados deben asegurar esta condición con sus proveedores de servicios de internet.
- Se utilizará el Cliente VPN de Cisco para la negociación y establecimiento de VPNs entre los usuarios y la organización. Este Software es de libre distribución y debe ser instalado en los dispositivos de los usuarios remotos.

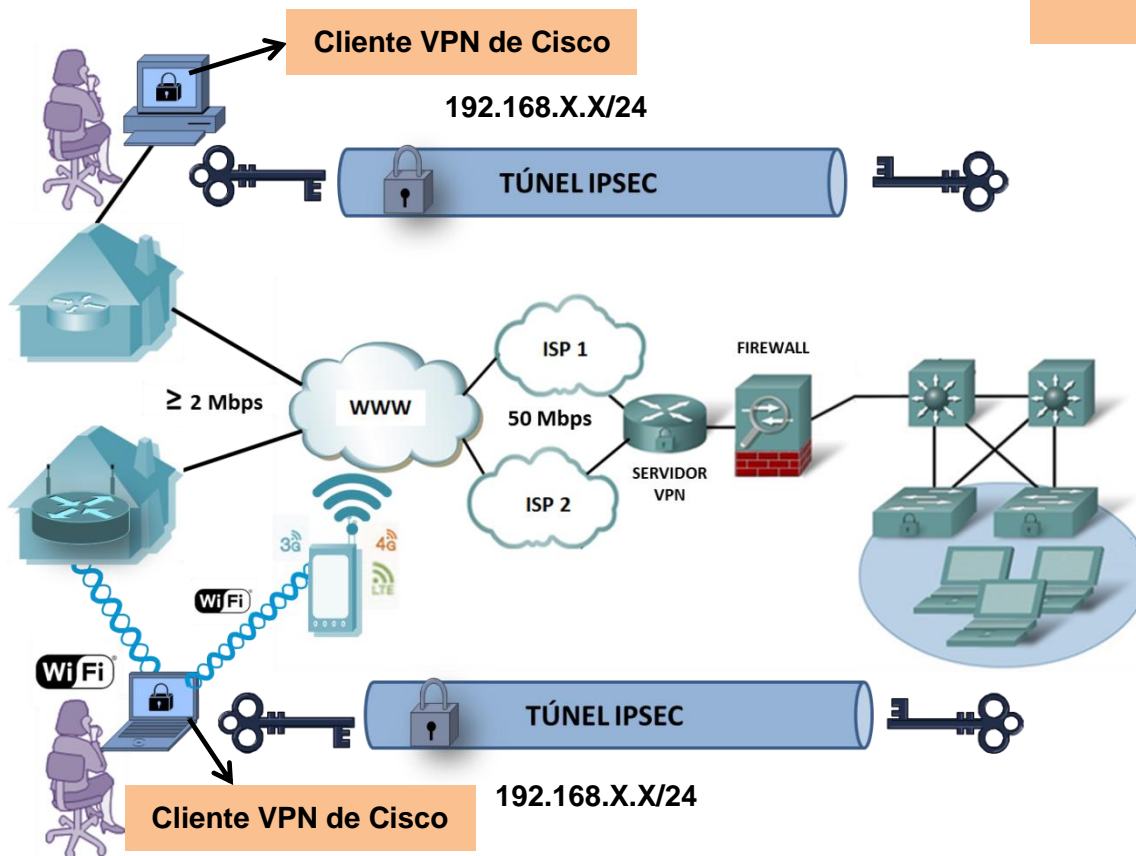


Ilustración 25: Diseño de red Teletrabajo. Fuente: Autor

La ilustración 25 muestra el diseño de la red de teletrabajo.

4.6.1 Simulación de red

El objetivo de la simulación es observar y evaluar el funcionamiento de una VPN IPsec a través de Internet de acuerdo al tiempo de establecimiento y el nivel de seguridad configurado. A partir de la simulación de la red se decidirá qué algoritmos y protocolos de seguridad serán configurados para el establecimiento del Túnel IPsec,

Para la simulación de la red de teletrabajo existen limitantes como:

- Ancho de Banda del servidor VPN: Está limitado a la capacidad de la salida a internet del lugar donde se realizarán las pruebas. Es decir anchos de banda de tipo residencial entre mayor o igual a 2Mbps.
- Se utilizarán IOS de seguridad de cisco y router Cisco 3745 de tipo simulado en la herramienta de software de libre distribución GNS3. La cantidad de memoria RAM

y procesamiento está limitada al computador que emule el router. Para esta simulación se utilizó un computador portátil con las siguientes especificaciones:

- ✓ Procesador Intel Core I5-2467M de 1.60 GHz
- ✓ Memoria RAM de 4 GB
- ✓ Espacio de más de 10 Gigas en disco duro.
- ✓ SO Windows 7 Enterprise

Estas especificaciones afectan el rendimiento de la simulación y los tiempos de respuesta del router y la VPN.

- Se utilizará el Firewall de Windows como dispositivo de aseguramiento e inspección de puertos, con conexión virtual al router 3745 emulado.
- El IOS utilizado limita el número de usuarios VPN a 10. Es decir que para esta simulación el máximo número de usuarios creados y admitidos por el servidor VPN es de 10 host. Sistemas operativos y dispositivos de mayor capacidad funcionan en hardware con cobros de licenciamiento por número de usuarios remotos.
- Se utilizará software de DNS dinámico de libre distribución para la conexión de los clientes VPN a través de Internet.
- Se instalará y configurará el Cliente VPN de Cisco en un computador portátil, diferente al que emulará el router central, que simulará el usuario o empleado remoto.
- El ancho de banda del servidor VPN no será redundante por la imposibilidad de configuración de HSRP, VRRP o GLBP en los PE de los proveedores con las conexiones a Internet residenciales o móviles. Para realizar esta prueba los router de los proveedores deberían ser Cisco o tener capacidades de VRRP o GLBP. Para esta simulación los ISP son Claro y UNE con routers o módems de última milla de marca ARRIS y ZTE los cuales no brindan la posibilidad de configurar protocolos de alta disponibilidad por lo tanto no es posible simular redundancia.

4.6.2 Componentes

Los componentes de la simulación se dividen en tres partes:

1. Componentes de Infraestructura Tecnológica para red teletrabajo Empresa:

- ✓ Computador portátil SO Windows 7 Enterprise de 32 bits
 - ✓ Firewall de Windows 7
 - ✓ Simulador GNS3 versión 0.8.3.1
 - ✓ DNS dinámico DonWeb versión 1.0.0.2
 - ✓ Conexión a Internet 4G UNE 2Mbps asimétricos
 - ✓ Módem 4G ZTE UNE MF93D
 - ✓ Software SDM (Security Device Management) de Cisco version 2.5
2. Componentes de Infraestructura Tecnológica para red teletrabajo Empleado remoto:
- ✓ Computador portátil SO Windows 8
 - ✓ Cliente VPN de Cisco versión 5.0.2
 - ✓ Conexión a Internet Banda ancha de 5 Mbps asimétricos proveedor Claro
3. Componentes Tecnológicos para descubrimiento de vulnerabilidades y Ethical Hacking red Teletrabajo
- ✓ Computador portátil SO Windows 8.1 de 64 bits con las siguientes características:
 - Procesador Intel Core x64 I5-3337U de 1.80 GHz
 - Memoria Ram de 4 GB
 - ✓ Cliente VPN de Cisco versión 5.0.2
 - ✓ Software de Ethical Hacking y descubrimiento de vulnerabilidades Nmap versión para Windows
 - ✓ Software de Ethical Hacking y descubrimiento de vulnerabilidades Cain versión 4.9.56 para Windows
 - ✓ Software de Máquina Virtual VMware versión 4.3.8
 - ✓ Sistema Operativo Ubuntu de 32 bits emulado en VMware con las siguientes características:
 - Procesador Intel Core I5 de 1.80 GHz
 - Memoria Ram de 1GB
 - Disco duro de 8 GB
 - ✓ Software de Ethical Hacking y descubrimiento de vulnerabilidades Hydra versión 8.0 para Ubuntu
 - ✓ Sniffer WireShark versión 1.6.8 para Windows
 - ✓ Conexión a Internet Banda ancha de 5 Mbps asimétricos proveedor Claro

4.6.3 Desarrollo

Según los componentes y limitantes, se plantea la siguiente topología para la red simulada:

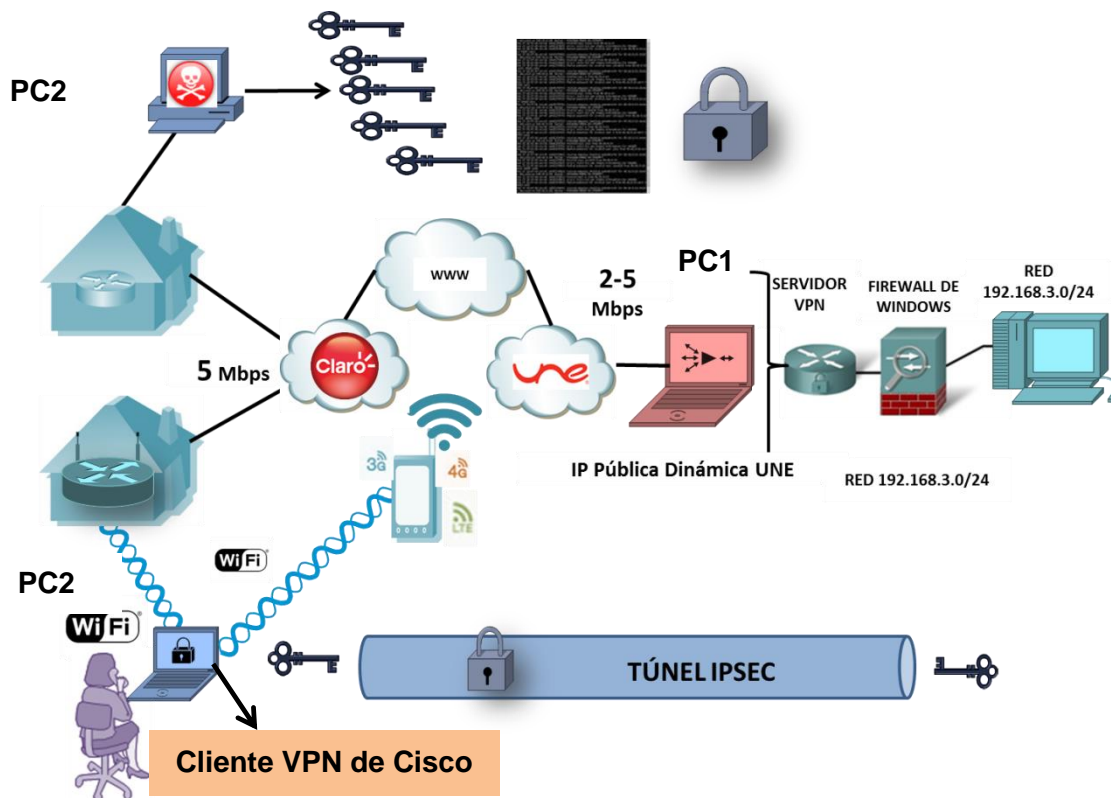


Ilustración 25: Simulación Red Teletrabajo. Fuente: Autor

4.6.4 Alistamiento de Componentes

- En el PC1 se instaló el siguiente software:
 - Simulador de red GNS3
 - SDM de Cisco
 - DNS dinámico Donweb
 - Sniffer Wireshark
 - Java versión 6 update 6
- En el PC 2 se instaló el siguiente software:
 - Cliente VPN

- VMware
 - Nmap
 - Cain
 - Sniffer Wireshark
- Para la máquina virtual se escogió el SO Ubuntu el cual fue instalado con la siguiente configuración

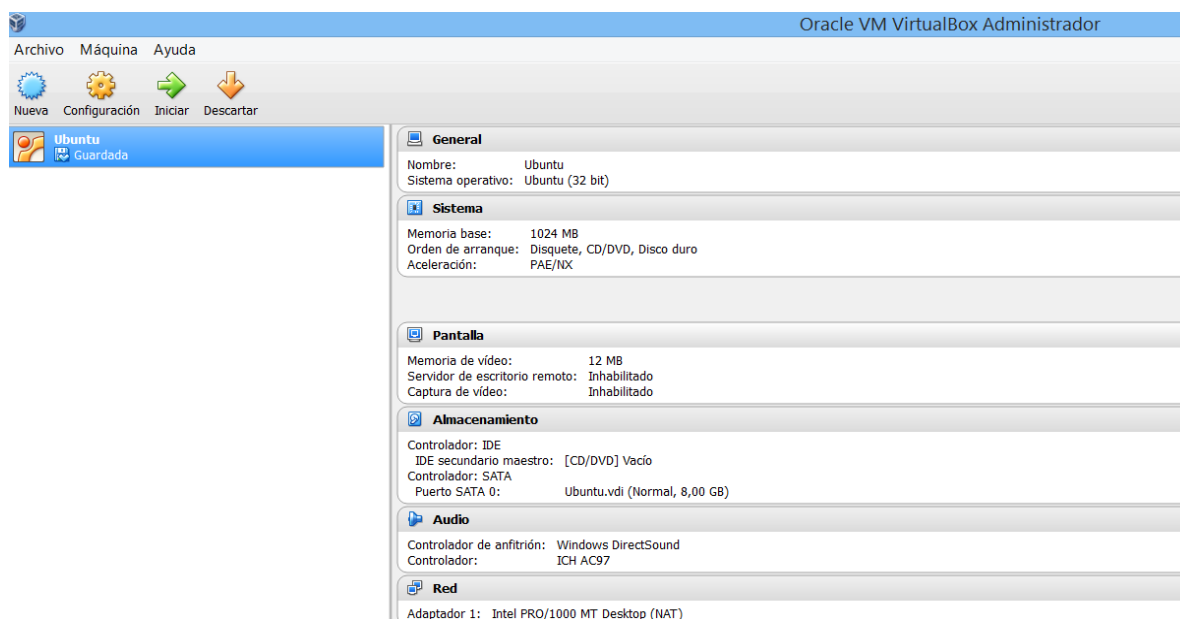


Ilustración 26: Ubuntu VM Fuente: Autor

- Dentro de la infraestructura de routers de GNS 3, fue elegido el router Cisco 3745 series. Para su funcionamiento se cargó, en el emulador, el IOS c3745-ADVENTERPRISEK9-M, Versión 12.4 (23), por sus capacidades de configuración de VPN, seguridad AAA y compatibilidad con SDM. Este router cuenta con
 - Procesador R7000 de 240MHz
 - Memoria de 128MBytes
 - Flash Compacta de 16 MBytes
- Para el funcionamiento de SDM en el PC1 se configuró la versión java 6u6 En el explorador de internet.
- Para las conexiones virtuales entre el router 3745, el SDM, el firewall de Windows y la interfaz de red inalámbrica del computador, se crearon 3 interfaces de loopback

o bucle invertido de Microsoft en el PC1,. Estas interfaces se crearon por medio del asistente de nuevo hardware de Windows Así:

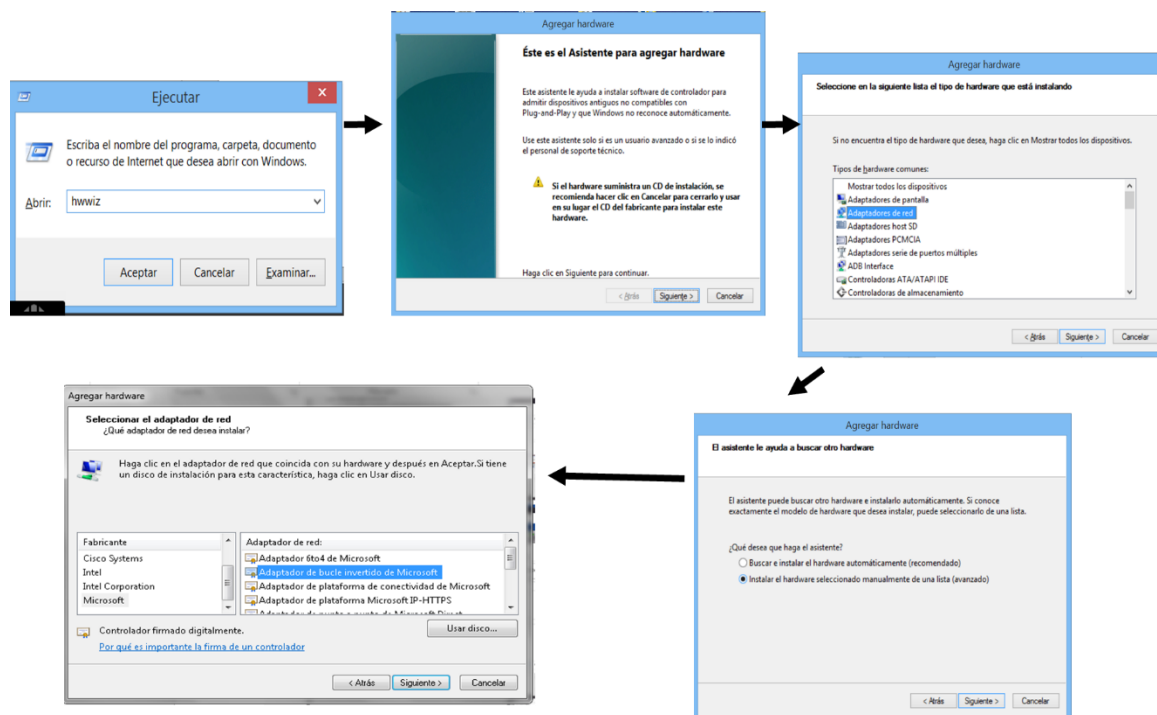


Ilustración 27: Creación de interfaces de bucle invertido Fuente: Autor

- En el Firewall de Windows se configuraron dos reglas avanzadas de entrada, llamadas **VPN_Cisco_SDM** y **VPN_CISCO_UDP**. Estas reglas habilitan el puerto 500 y 64500 de IPsec.

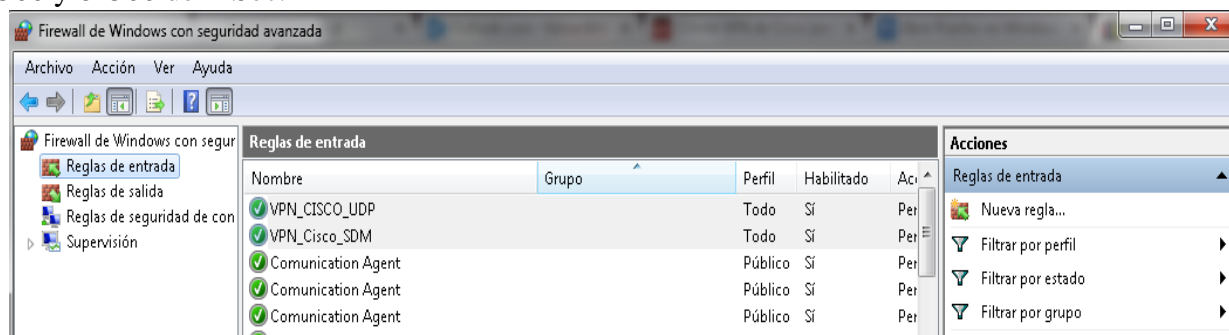


Ilustración 28: Reglas Firewall de Windows. Fuente: Autor

4.6.5 Configuración

1. En GNS3 se crea el router, y tres nubes de interconexión. A cada nube en su configuración se le asigna una de las interfaces de loopback creadas en Windows.
2. Cada nube es conectada a una de las interfaces FastEthernet del router con una conexión directa en el emulador. Como el cisco 3745 sólo cuenta con dos interfaces FastEthernet, fue necesario agregar un módulo NM-1FE-TX en el slot 1 del router, por medio de la configuración de dispositivo de GNS3. Dicho módulo agregó una interfaz FastEthernet al cisco 3745.
3. Cada elemento agregado al campo de topología de GNS3, fue editado con un nombre de host e íconos específicos. Dos de los íconos de nubes son cambiados por íconos de Host, y se editaron los nombres.

La topología resultante en GNS3 es la siguiente:

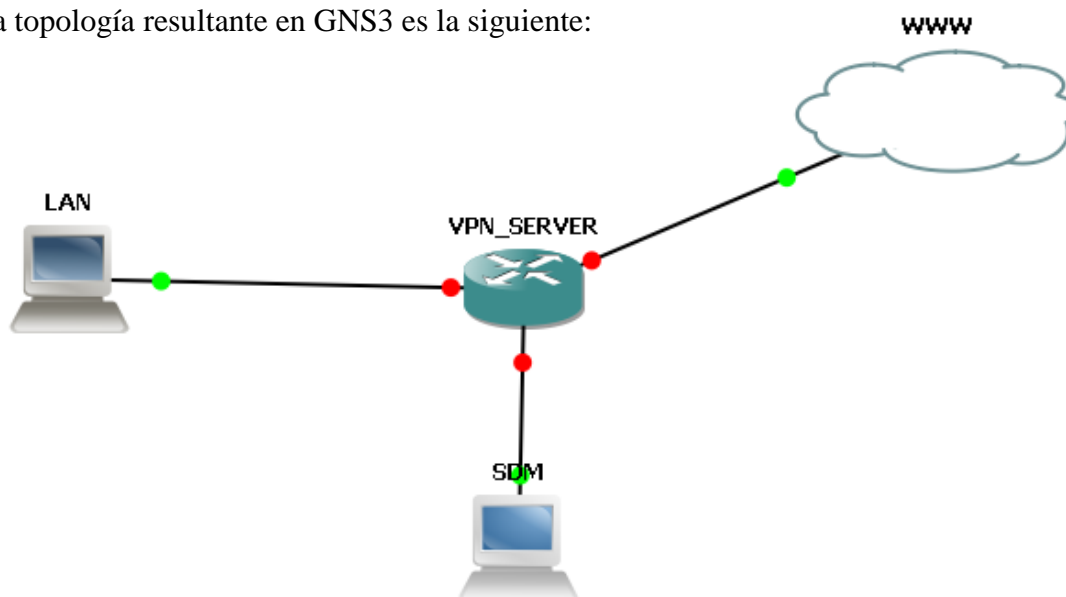


Ilustración 29: Topología GNS3. Fuente: Autor

4. Se configuraron tres segmentos de red en las interfaces del router así:
 - Interfaz SDM FastEthernet0/0 192.168.1.1/24
 - Interfaz WAN FastEthernet0/1 192.168.137.4
 - Interfaz LAN FastEthernet1/0 192.168.3.254

5. Se configuró nombre del host, nuevo modelo AAA, servidor https, dominio del router, y usuario de administración nivel 15 en MD5, todos necesarios para la administración por SDM. Se configuraron con los siguientes comandos IOS desde el modo de configuración global del router:
 - ip http server
 - ip http authentication local
 - ip http secure-server
 - username security privilege 15 secret 5Dm M4nAG3
 - aaa new-model
 - hostname VPN_SERVER

6. Se instaló el paquete SDM en el router ejecutando el instalador de SDM hacia la dirección IP 192.168.1.1.

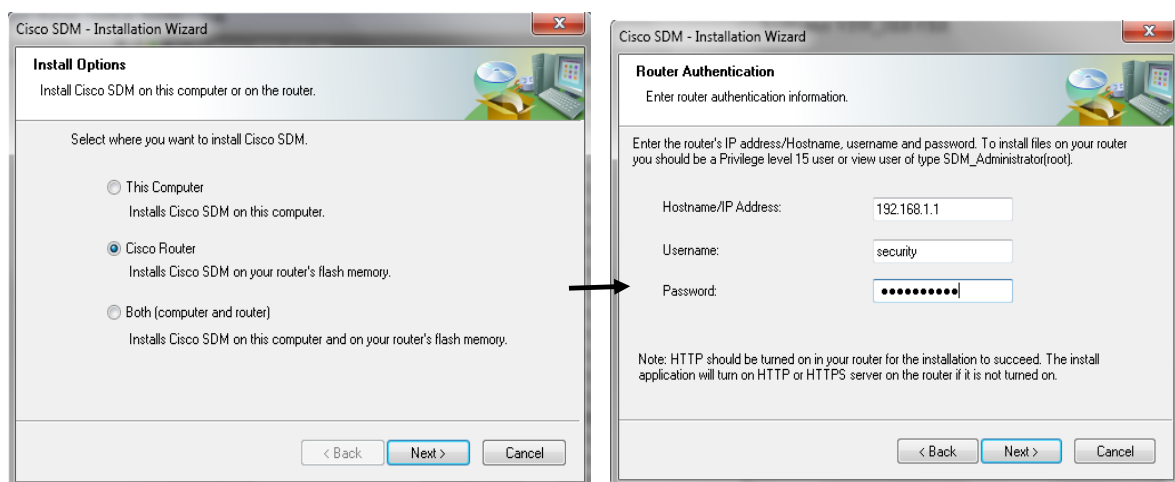


Ilustración 30: Instalación de SDM en router. Fuente: Autor

Nota: Todas las configuraciones son guardadas en la NVRAM del router para evitar pérdidas de configuración al apagar la simulación o reiniciar el dispositivo.

7. Se accede al router por medio de SDM desde internet explorer con las credenciales del nivel 15 anteriormente configuradas

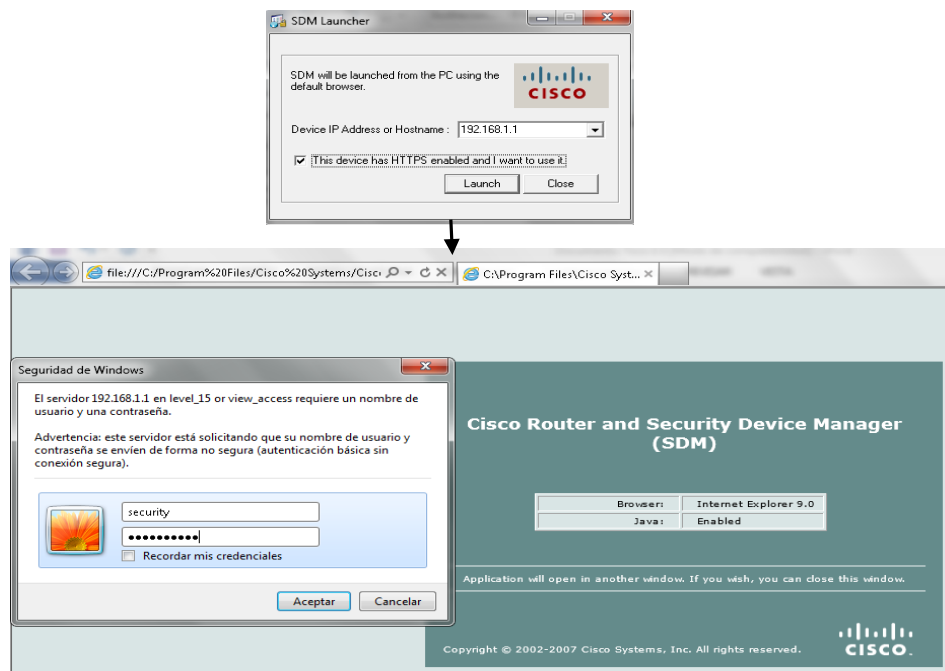


Ilustración 30: Acceso por SDM al router. Fuente: Autor
SDM carga la configuración del router y muestra el entorno gráfico de gestión y monitoreo del dispositivo

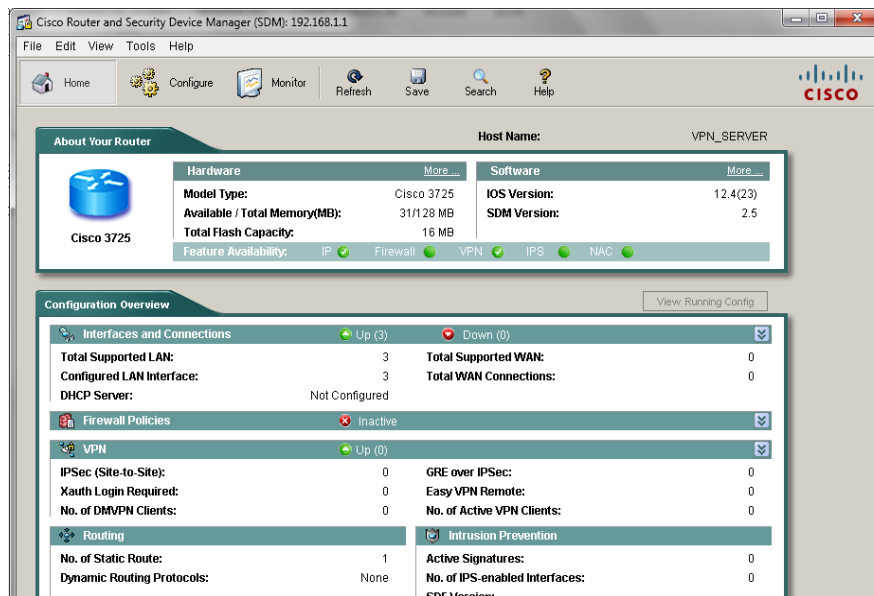


Ilustración 31: Router con gestión gráfica. Fuente: Autor

8. Para poder realizar las pruebas de conectividad y de DNS a la IP pública de UNE, fue necesario ingresar a l módem 4G ZTE y deshabilitar el filtrado de puertos del firewall



Ilustración 32: Gestión módem ZTE 4g de UNE. Fuente: Autor

9. Se configuró el DNS dinámico DonWeb con el dominio gratuito **teletrabajosanbu.donweb-homeip.net** configurado en el PC1 con la IP pública del módem 4G

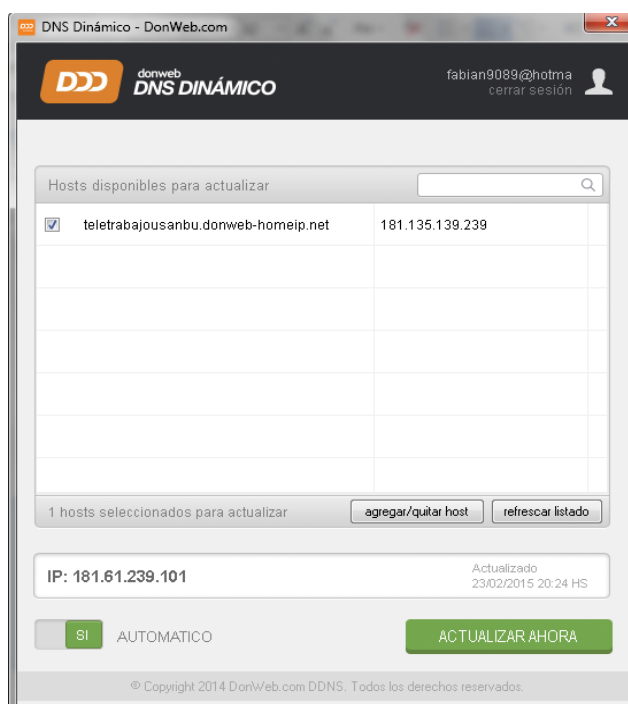


Ilustración 33: Configuración de DNS dinámico. Fuente: Autor

10. En el router fue necesario configurar el servidor de DNS **200.13.249.101** de la red de UNE con el siguiente comando IOS en modo de configuración global:

- ip name-server 200.13.249.101

También fue necesario compartir la conexión de red inalámbrica del PC1 con la interfaz de bucle invertido de microsoft configurada en la nube de internet de GNS3, desde las propiedades de conexión de red inalámbrica en Uso compartido.

Se realizaron pruebas de conectividad exitosas desde el router hacia Internet

```

VPN_SERVER
VPN_SERVER#ping www.google.com

Translating "www.google.com"...domain server (200.13.249.101) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 173.194.37.80, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/137/204 ms
VPN_SERVER#ping www.hotmail.com

Translating "www.hotmail.com"...domain server (200.13.249.101) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 65.55.77.28, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 140/156/200 ms
VPN_SERVER#ping www.facebook.com

Translating "www.facebook.com"...domain server (200.13.249.101) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 31.13.73.1, timeout is 2 seconds:
!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 200/218/232 ms
  
```

Ilustración 34: Pruebas desde el router a dominios de Internet. Fuente: Autor

También se realizaron pruebas de conectividad exitosas desde el Internet hacia el dominio del router

```

C:\WINDOWS\system32\cmd.exe
C:\Users\fabian>ping teletrabajousanbu.donweb-homeip.net -t

Haciendo ping a teletrabajousanbu.donweb-homeip.net [181.135.148.10] con 32 bytes de datos:
Respuesta desde 181.135.148.10: bytes=32 tiempo=489ms TTL=118
Respuesta desde 181.135.148.10: bytes=32 tiempo=89ms TTL=118
Respuesta desde 181.135.148.10: bytes=32 tiempo=299ms TTL=118
Respuesta desde 181.135.148.10: bytes=32 tiempo=97ms TTL=118
Respuesta desde 181.135.148.10: bytes=32 tiempo=314ms TTL=118
Respuesta desde 181.135.148.10: bytes=32 tiempo=220ms TTL=118
Respuesta desde 181.135.148.10: bytes=32 tiempo=212ms TTL=118
Respuesta desde 181.135.148.10: bytes=32 tiempo=205ms TTL=118
  
```

Ilustración 34: Pruebas desde Internet al dominio del router. Fuente: Autor

11. Se aseguró el router y sus interfaces de gestión con listas y métodos de autenticación AAA locales, así como la configuración de SSH y el bloqueo de ingreso por intentos de conexión inválidos consecutivos; esta última configuración es muy importante para evitar ataques de fuerza bruta o de diccionarios. Se aplicaron los siguientes comandos IOS desde línea de comando en modo de configuración global:

- aaa authentication login default local
- aaa authorization exec default local
- aaa session-id common
- login block-for 120 attempts 3 within 30
- Crypto key rsa generate. (Con longitud de 1024 bits)
- ip ssh time-out 30
- ip ssh authentication-retries 2
- ip ssh version 2
- access list 100 permit ip 192.168.1.0 0.0.0.255 any equal 22
- access list 100 deny any any
- line console 0
 - ✓ exec-timeout 0 0
 - ✓ privilege level 15
 - ✓ authorization commands 1 local
 - ✓ authorization commands 15 local
 - ✓ authorization exec local
 - ✓ logging synchronous
 - ✓ login authentication local
- Line vty 0 15
 - ✓ access-class 100 in
 - ✓ exec-timeout 9 0
 - ✓ authorization commands 1 local
 - ✓ authorization commands 15 local
 - ✓ authorization exec local
 - ✓ login authentication local
 - ✓ transport input ssh

12. Para configurar la VPN se eligió el modo **Easy VPN Server** de Cisco en SDM. Este modo es el necesario para la red de teletrabajo por tratarse de varios puntos remotos conectados desde un cliente a un servidor de VPN central. Se configuró desde SDM.

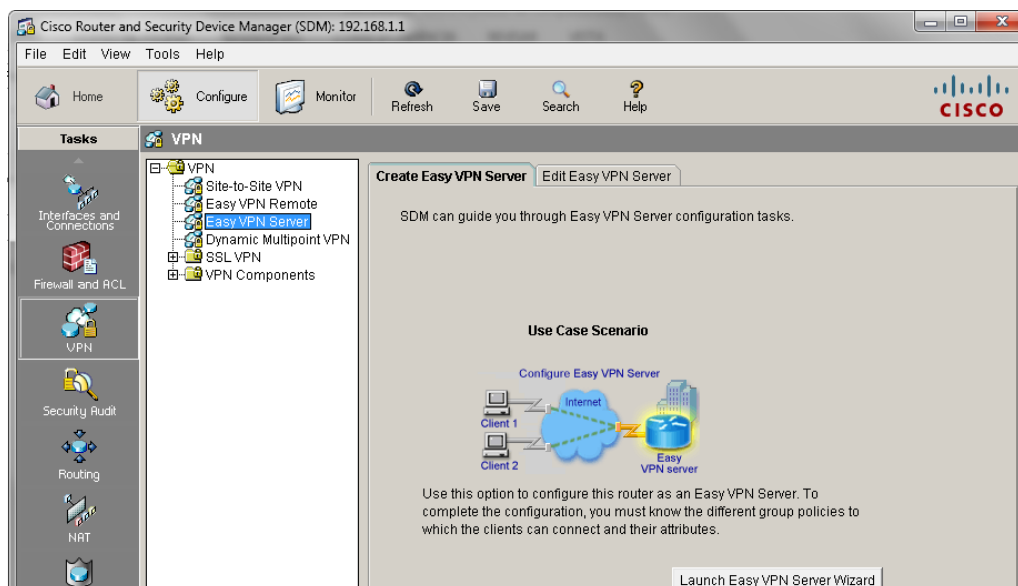


Ilustración 34: Servidor VPN SDM. Fuente: Autor

El proceso de configuración del servidor de VPN tuvo las siguientes etapas:

- i. Elección de la interfaz del router donde los clientes realizarán la conexión

Se configuró la interfaz WAN FastEthernet0/1 192.168.137.4 del router, porque es la interfaz que conecta a internet. También se especificó llaves compartidas como método de autenticación entre clientes y servidor.

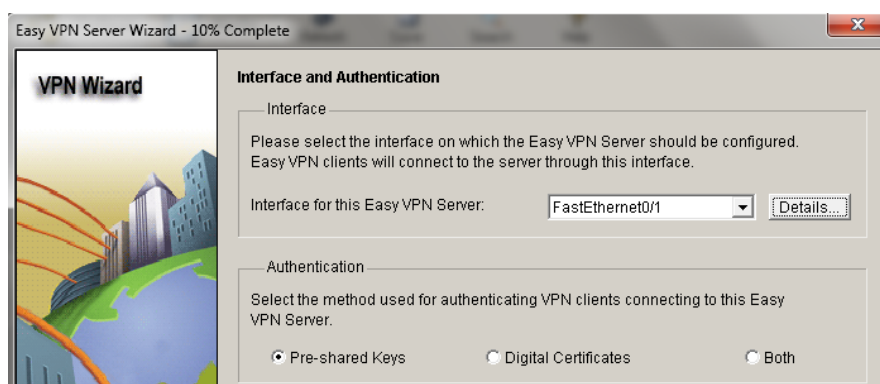


Ilustración 35: Elección de interfaz VPN. Fuente: Autor

ii. Configuración de políticas IKE

Para el intercambio seguro de llaves durante la negociación de la VPN se eligió

- ✓ AES de 256 bits para encriptar; teniendo en cuenta su rápido desempeño a comparación de 3DES
- ✓ SHA1 como función de resumen o Hash
- ✓ DH group 2 como método de intercambio de llaves

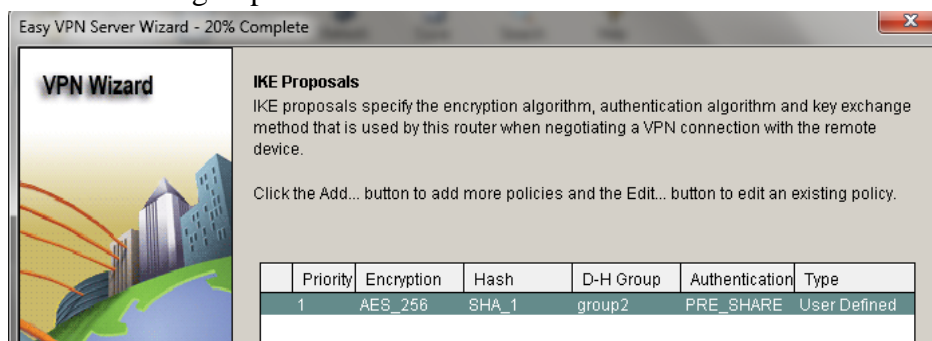


Ilustración 36: Configuración de políticas IKE. Fuente: Autor

iii. Configuración de la transformada de IPSec

Se creó la transformada Teletrabajo con los siguientes algoritmos

- ✓ ESP y AES de 256 bits para encriptar la información a través del túnel; teniendo en cuenta su rápido desempeño a comparación de ESP y 3DES
- ✓ ESP_SHA_HMAC para asegurar la integridad de la información que viajará entre el túnel IPSec.

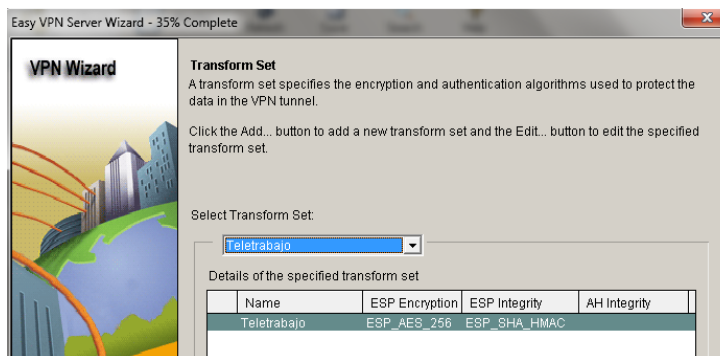


Ilustración 37: Configuración de transformada IPSec. Fuente: Autor

iv. Configuración del método para la política de conexión de grupo

Como método de conexión de grupo se eligió que fuera local.

v. Configuración de autenticación de usuarios

Como método de autenticación de los usuarios VPN se eligió que fuera local. Es decir que los clientes VPN se autenticarán con los usuarios configurados en el router o servidor VPN

vi. Configuración de políticas de grupo en el router local

Los clientes VPN se autorizarán con un grupo denominado Teletrabajadores con la clave de frase H0M3 w0rK U5b en el router o servidor VPN. Para este grupo se configuró un pool de 40 direcciones IP.192.168.3.1-192.168.3.40 que serán asignadas dinámicamente a los clientes VPN conectados al servidor.

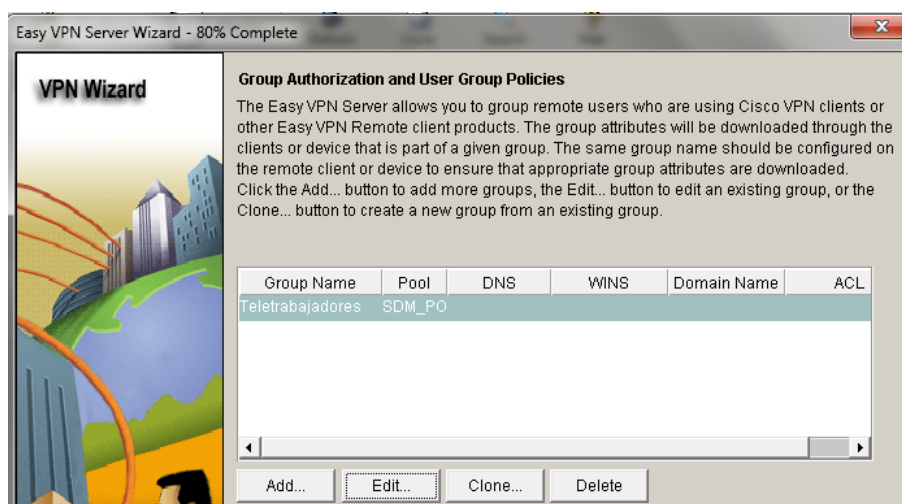


Ilustración 38: Configuración de grupo de autorización. Fuente: Autor

Por último se envía la configuración anterior desde SDM al router y se puede empezar a realizar pruebas de conexión a la VPN desde clientes VPN a través de Internet.

4.6.5.1 Pruebas de conexión y negociación VPN

Se realizó el test del servidor VPN desde SDM con los siguientes resultados:

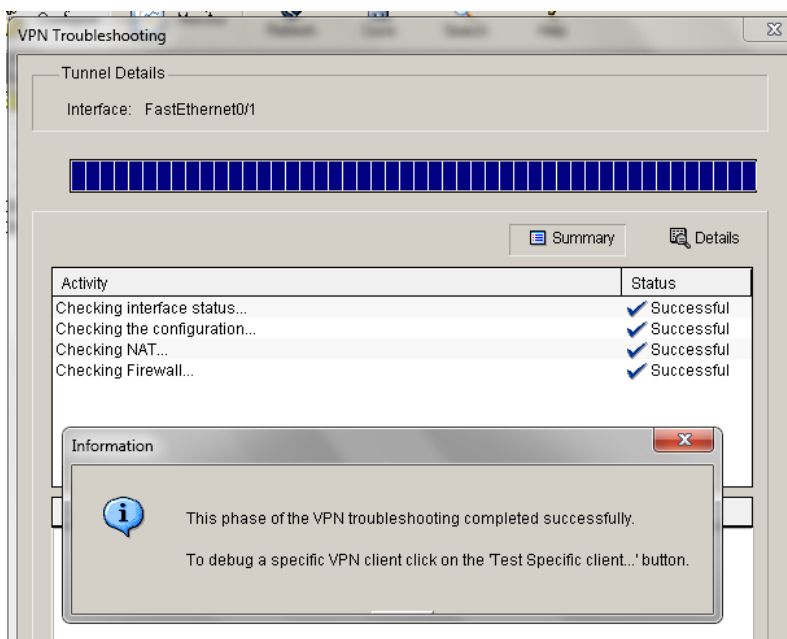


Ilustración 39: Prueba de Servidor VPN de SDM. Fuente: Autor

Con los resultados exitosos del lado del servidor de VPN se procede a realizar pruebas de conexión desde el PC2 con el cliente VPN de Cisco. Se configuró el cliente VPN del PC2 con el nombre y clave de grupo configurados en el servidor y el DNS creado para la red de teletrabajo.

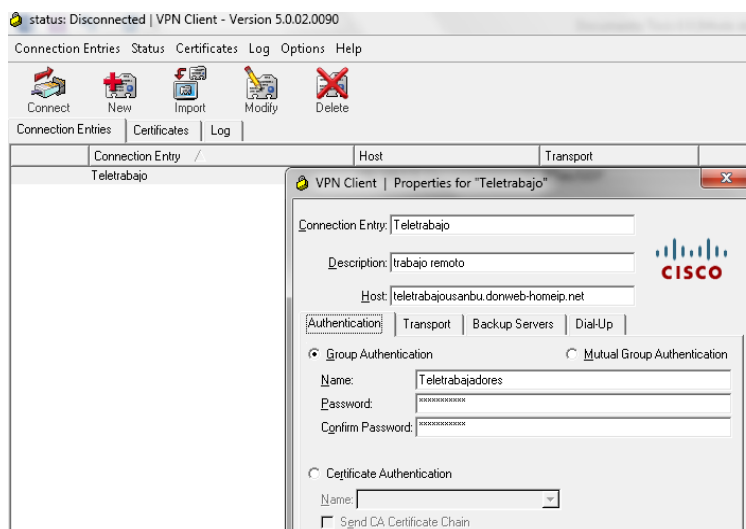
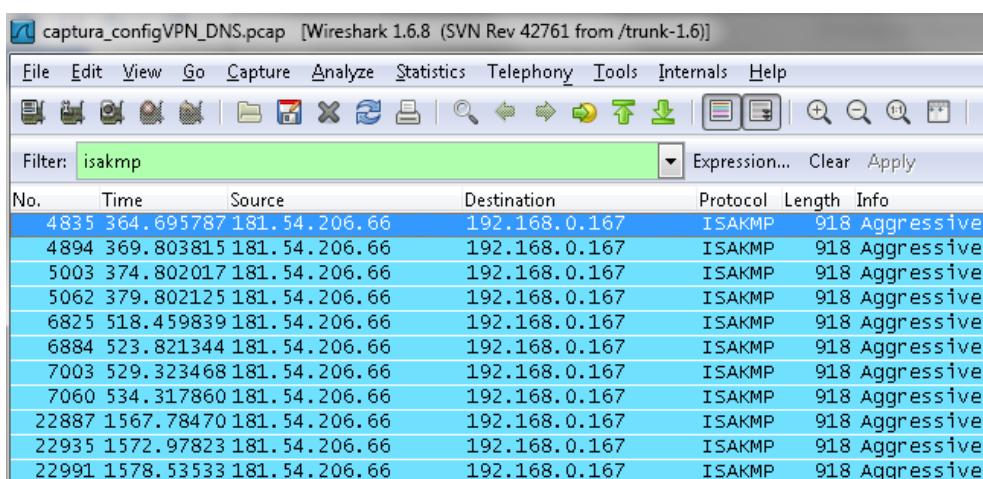


Ilustración 40: Prueba de Servidor VPN de SDM. Fuente: Autor

4.6.6 PRUEBAS

Al intentar conectar el cliente VPN al servidor, son rechazadas las peticiones de intercambio de llaves y negociación. Para diagnosticar la falla fue necesario activar el sniffer de Wireshark en el PC1, y activar las funciones debug de los procesos IPsec en el router 3745. Se activó el **debug crypto isakmp** en el router pero no se pudo observar ningún intento de negociación de llaves.

Se capturaron los siguientes paquetes en Wireshark



No.	Time	Source	Destination	Protocol	Length	Info
4835	364.695787	181.54.206.66	192.168.0.167	ISAKMP	918	Aggressive
4894	369.803815	181.54.206.66	192.168.0.167	ISAKMP	918	Aggressive
5003	374.802017	181.54.206.66	192.168.0.167	ISAKMP	918	Aggressive
5062	379.802125	181.54.206.66	192.168.0.167	ISAKMP	918	Aggressive
6825	518.459839	181.54.206.66	192.168.0.167	ISAKMP	918	Aggressive
6884	523.821344	181.54.206.66	192.168.0.167	ISAKMP	918	Aggressive
7003	529.323468	181.54.206.66	192.168.0.167	ISAKMP	918	Aggressive
7060	534.317860	181.54.206.66	192.168.0.167	ISAKMP	918	Aggressive
22887	1567.78470	181.54.206.66	192.168.0.167	ISAKMP	918	Aggressive
22935	1572.97823	181.54.206.66	192.168.0.167	ISAKMP	918	Aggressive
22991	1578.53533	181.54.206.66	192.168.0.167	ISAKMP	918	Aggressive

Ilustración 41: Captura intentos de conexión Cliente VPN. Fuente: Autor

Al revisar los paquetes capturados se encuentra que la negociación de VPN se está realizando entre el Cliente VPN del PC2 y el servicio VPN de Windows del PC1. Para resolver este problema se revisa el NAT de la tarjeta de red compartida en el PC1, y se crea un servicio llamado VPN.

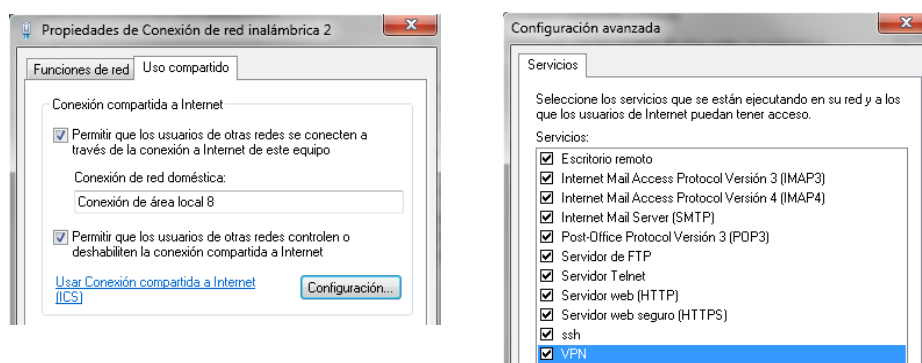


Ilustración 42: Configuración de servicio VPN en NAT de Windows. Fuente: Autor

Para el servicio VPN creado se configura la IP de la interfaz WAN del servidor VPN y los puertos UDP 500 de entrada y salida.

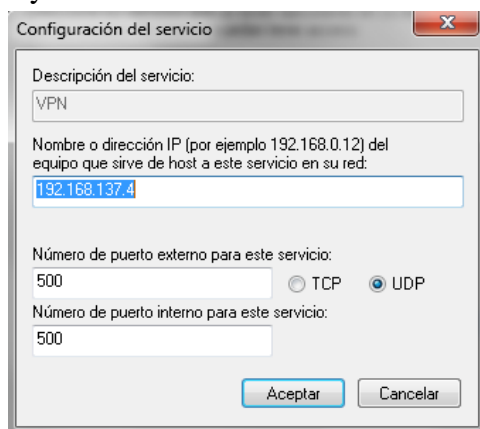


Ilustración 42: Servicio VPN en NAT de Windows. Fuente: Autor

Después de realizar estas correcciones se intenta conectar de nuevo el cliente VPN, sin éxito. Sin embargo el debug activado en el router y el sniffer empiezan a mostrar eventos de negociación ISAKMP. Como los resultados de los comandos debug por línea de comando pasan a gran velocidad, se exportaron a un archivo de texto plano para ser analizados, encontrando el siguiente problema

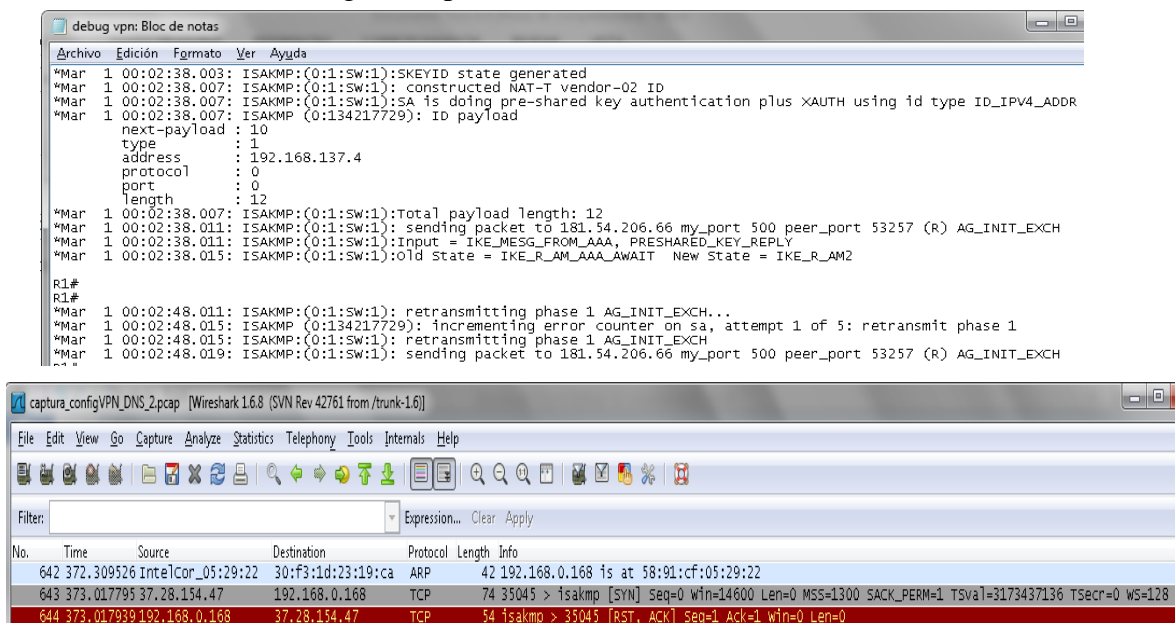


Ilustración 43: Fallas de negociación VPN. Fuente: Autor

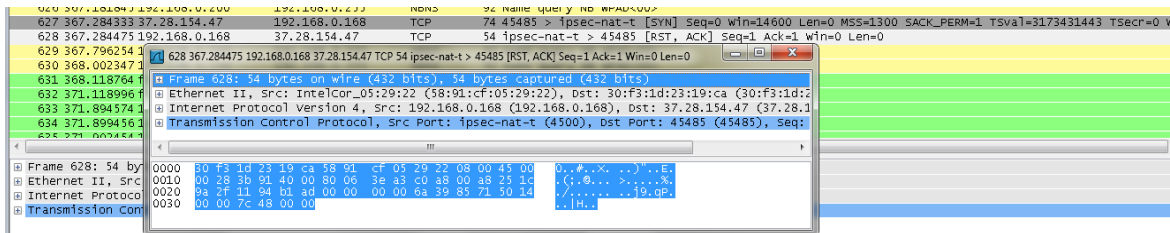


Ilustración 43: Captura fallas de NAT Transversal. Fuente: Autor

Con los resultados anteriores se concluye que la falla está en el encapsulamiento de paquetes crypto isakmp por medio de NAT-T.

Para solucionar el problema fue necesario desactivar el encapsulamiento de tipo NAT-T en el servidor VPN con el comando IOS **no crypto ipsec nat-transparency udp-encaps** en el modo de configuración global del router. Luego de realizar estos ajustes la conexión del Cliente VPN es un hecho, y la autenticación se realiza con los usuarios y contraseñas locales creadas el router. El PC2 toma una IP del pool VPN configurado y conecta a través de un túnel seguro IPsec al segmento 192.168.3.0/24.

Luego de las pruebas exitosas se crearon tres configuraciones de VPN con transformadas DES, 3DES Y AES 256. Se tomaron los tiempos de aseguramiento del canal en el Cliente VPN y se graficaron los resultados así:

Algoritmo de Encriptación	t (seg) Establecimiento túnel IPSEC
DES	50
3DES	35
AES	20

Tabla 6. Comparación tiempo de establecimiento IPsec de transformadas criptográficas configuradas

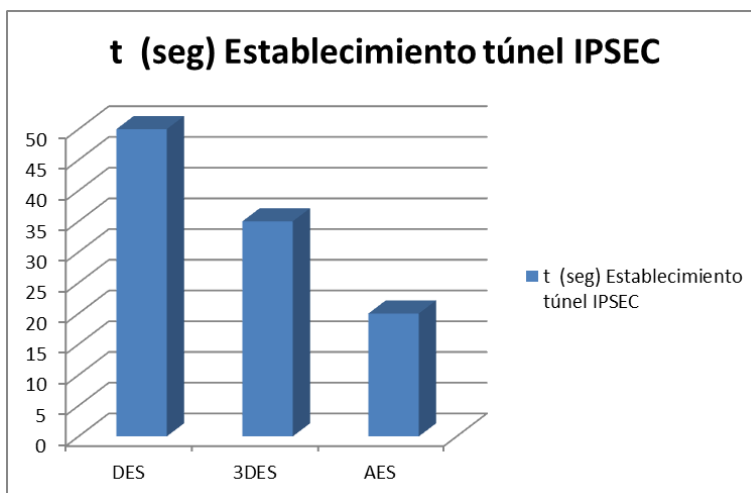


Ilustración 42: Comparación gráfica de las transformadas criptográficas configuradas. Fuente: Autor

En base a las pruebas anteriores y los tiempos de establecimiento de IPsec con los enlaces utilizados en la simulación, se decide utilizar la transformada de AES 256, que brinda mayor seguridad y menores tiempos de establecimiento y negociación IPsec.

4.7 PRUEBAS DE VULNERABILIDAD Y ACCESO NO AUTORIZADO A LA INFORMACIÓN BAJO EL AMBIENTE SIMULADO.

Se realizaron cuatro tipos de pruebas:

- Descubrimiento de puertos e infraestructura con Nmap,
- Criptoanálisis de contraseñas y tráfico cifrado con Cain y calculadoras MD5 de Internet
- Ataques de fuerza bruta y de diccionarios con la herramienta Hydra
- Ataques de denegación de servicio por medio de ICMP.

4.7.1 Descubrimiento de puertos e infraestructura con Nmap

Para el descubrimiento de puertos e infraestructura tecnológica con Nmap, se configuró como objetivo la IP pública de la red de Teletrabajo y se activó un escáner completo de puertos y servicios. El resultado de Nmap fue el siguiente:

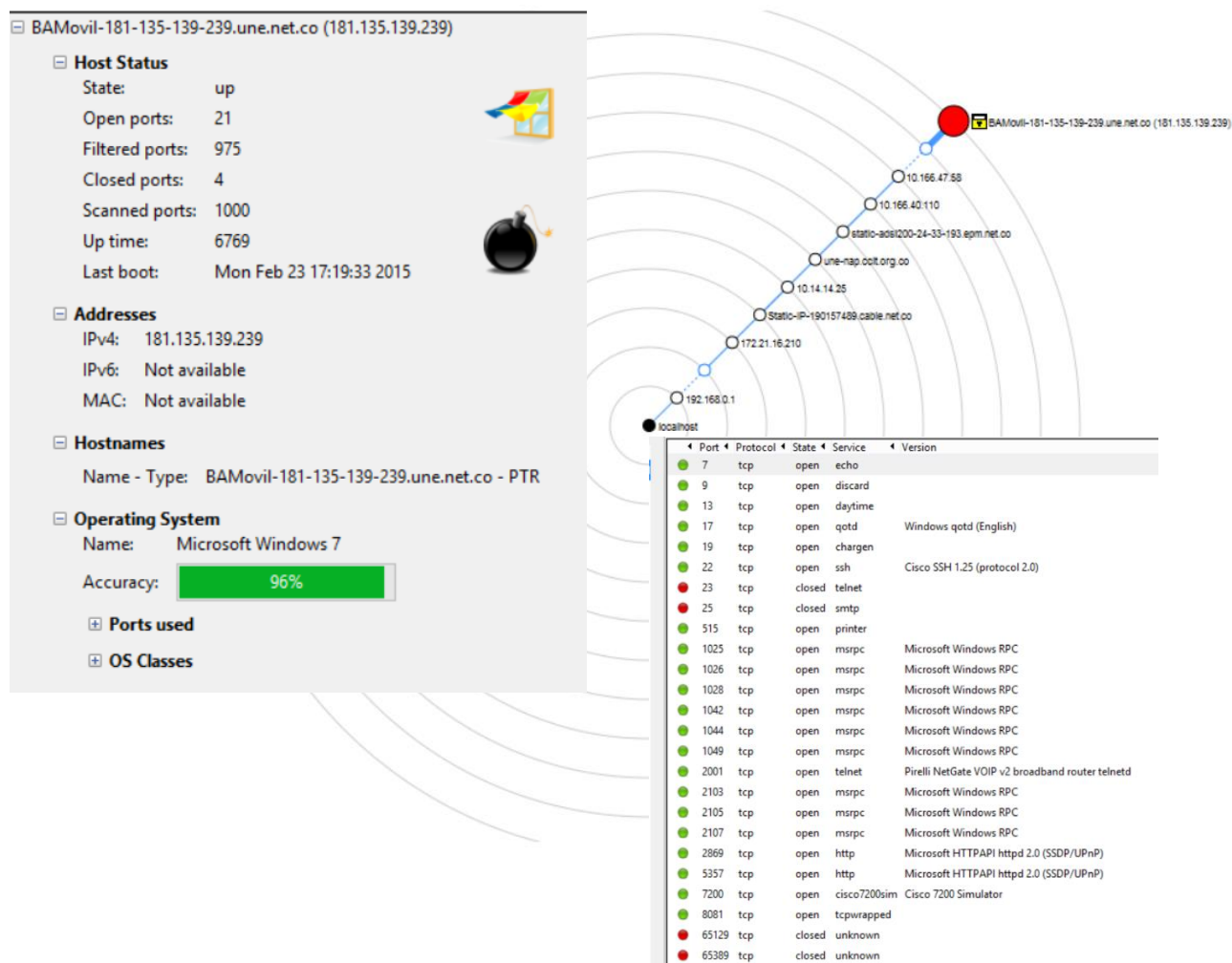


Ilustración 43: Resultados Nmap. Fuente: Autor

Según los resultados no es posible encontrar los segmentos de red privados de la red. Nmap tampoco pudo determinar el tipo de IOS ni modelo de router o servidor VPN. Los puertos encontrados corresponden a puertos seguros de Windows, no se descubrieron puertos inseguros como Telnet, FTP, SNMP, CDP etc. (Academy, 2009) En base a esto la red de teletrabajo soportó el descubrimiento de vulnerabilidades y no fue necesario tomar medidas correctivas para proteger la seguridad de la red.

4.7.2 Criptoanálisis de contraseñas y tráfico cifrado con Cain y calculadoras MD5 de Internet

Con el sniffer Wireshark se capturó información cifrada, para ser analizada con el programa Cain y calculadoras de MD5 desde el PC2. Sin embargo no fue posible descifrar ninguna contraseña, ni siquiera suponiendo que se conocía la longitud de las claves. Los tiempos de descifrado en Cain oscilaron entre los dos mil y 20 mil millones de años no hubo claves generadas en las calculadoras de MD5 de Internet

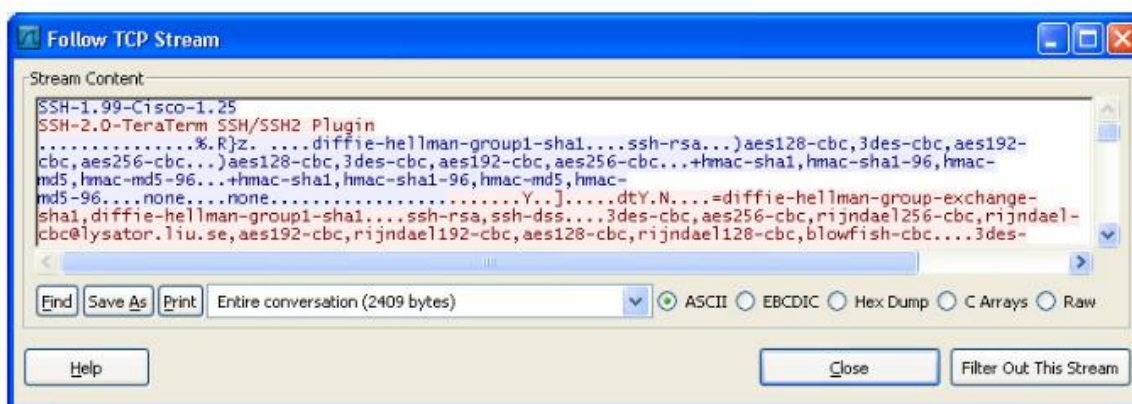


Ilustración 44: Captura de tráfico cifrado con Wireshark. Fuente: Autor

4.7.3 Ataques de fuerza bruta y de diccionarios con la herramienta Hydra

En la máquina virtual de Ubuntu del PC2 se descargaron e instalaron las siguientes librerías para el funcionamiento de Hydra:

```
libssl-dev libssh-dev libidn11-dev libpcre3-dev libgtk2.0-dev libmysqlclient-dev libpq-dev
libsvn-dev firebird2.1-dev libncp-dev libncurses5-dev
```

Luego se compiló y ejecutó la aplicación Hydra 8.0 en Ubuntu para las pruebas de seguridad y ataques de red, como se puede observar en la ilustración 45.

Para realizar los ataques de BFA y diccionario se descargaron cuatro bases de datos con diccionarios y miles de usuarios y contraseñas de Facebook, Hotmail, y demás servidores de internet, disponibles en sitios de entrenamiento y documentación de Hackers, Crackers y Ethical Hacking.

Desde Hydra se ejecutaron los ataques con cada base de datos o diccionario descargado, hacia la IP pública de la red de Teletrabajo. Sin embargo ninguna de las contraseñas de las bases de datos coincidía con las contraseñas de usuarios VPN o de gestión del router, incluso suponiendo que el atacante conocía uno de los usuarios.

```
santo@santo-VirtualBox: ~/Escritorio/hydra-8.0
Options:
-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
-p PASS or -P FILE try password PASS, or load several passwords from FILE
-C FILE colon separated "login:pass" format, instead of -L/-P options
-M FILE list of servers to attack, one entry per line, ':' to specify port
-t TASKS run TASKS number of connects in parallel (per host, default: 16)
-U service module usage details
-h more command line options (COMPLETE HELP)
server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
service the service to crack (see below for supported protocols)
OPT some service modules support additional input (-U for module help)

Supported services: asterisk cisco cisco-enable cvs ftp http-{head|get} http-{ge
t|post}-form http-proxy http-proxy-urlenum icq imap irc ldap2 ldap3[s] mssql mys
ql(v4) nntp pcan anywhere pcnfs pop3 redis rexec rlogin rsh s7-300 smb smtp smtp-en
um snmp socks5 teamspeak telnet vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs. Licensed under AGPL
v3.0. The newest version is always available at http://www.thc.org/thc-hydra
Don't use in military or secret service organizations, or for illegal purposes.

Example: hydra -l user -P passlist.txt ftp://192.168.0.1
santo@santo-VirtualBox:~/Escritorio/hydra-8.0$ d
```

Ilustración 45: Hydra 8.0 Ubuntu. Fuente: Autor

Las políticas configuradas para bloquear el acceso luego de 3 intentos fallidos, evitaron que el ataque fuera exitoso luego de los primeros tres usuarios o contraseñas inválidas en los puertos de SSH, Telnet, y FTP. Hydra no posee complementos para ejecutar ataques a IPSec.

```
santo@santo-VirtualBox: ~/Escritorio/hydra-8.0
v3.0. The newest version is always available at http://www.thc.org/thc-hydra
Don't use in military or secret service organizations, or for illegal purposes.

Example: hydra -l user -P passlist.txt ftp://192.168.0.1
santo@santo-VirtualBox:~/Escritorio/hydra-8.0$ hydra 181.135.139.239 telnet -l
security -P rockyou.txt -s 23 -t 4
Hydra v8.0 (c) 2014 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2015-02-23 19:09:13
[WARNING] telnet is by its nature unreliable to analyze, if possible better choo
se FTP, SSH, etc. if available

[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344398 login tries (l:1/p:14
344398), ~896525 tries per task
[DATA] attacking service telnet on port 23
[23][telnet] host: 181.135.139.239 login: security password: password
[23][telnet] host: 181.135.139.239 login: security password: 123456789
[23][telnet] host: 181.135.139.239 login: security password: iloveyou
[23][telnet] host: 181.135.139.239 login: security password: princess
1 of 1 target successfully completed, 4 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2015-02-23 19:09:37
santo@santo-VirtualBox:~/Escritorio/hydra-8.0$
santo@santo-VirtualBox:~/Escritorio/hydra-8.0$
```

Ilustración 46: Ataque Hydra 8.0 a red de Teletrabajo. Fuente: Autor

4.7.4 Ataques de denegación de servicio por medio de ICMP.

Para evitar un ataque de DoS en la red, se deshabilitó el tráfico de ICMP desde el servidor de VPNs, el módem ZTE de UNE y el PC1, para evitar la respuesta de la IP pública a paquetes de echo request desde Internet.

Al intentar lanzar un ping de la muerte desde el PC2 al PC1, no hubo respuesta ya que todas las solicitudes ICMP fueron bloqueadas. El ping de la muerte consiste en enviar solicitudes de echo request a la dirección pública de la red de teletrabajo, manteniéndolo y añadiéndole carga añadiendo `-t` y `-l` desde el `cmd` de Windows.

```
C:\Users\fabian>ping 181.135.139.239 -t -l 25000

Haciendo ping a 181.135.139.239 con 25000 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 181.135.139.239:
    Paquetes: enviados = 3, recibidos = 0, perdidos = 3
              (100% perdidos),
Control-C
^C
C:\Users\fabian>ping 181.135.139.239 -t -l 65000

Haciendo ping a 181.135.139.239 con 65000 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 181.135.139.239:
    Paquetes: enviados = 6, recibidos = 0, perdidos = 6
              (100% perdidos),
Control-C
^C
C:\Users\fabian>ping 181.135.139.239 -t -l 1500

Haciendo ping a 181.135.139.239 con 1500 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 181.135.139.239:
    Paquetes: enviados = 3, recibidos = 0, perdidos = 3
              (100% perdidos),
```

Ilustración 47: Ping de la muerte a red de Teletrabajo. Fuente: Autor

CAPITULO 5

ANÁLISIS DE RIESGOS, COSTOS Y BENEFICIOS DE LA IMPLEMENTACIÓN DEL TELETRABAJO.

5. ANÁLISIS DE RIESGOS, COSTOS Y BENEFICIOS DE LA IMPLEMENTACIÓN DEL TELETRABAJO.

5.1.1 Análisis de riesgos

Se diseñó una matriz de riesgos asociados al sector bancario, que incluye todas las vulnerabilidades asociadas a un mapa de calor dentro de la actividad y continuidad del negocio bancario el cual puede ser afectado por trabajadores fijos o remotos. Para esta matriz se cuantificaron dos factores de riesgo desde tres ambientes: Datos, Sistemas y Personal:

- Magnitud de daño: 1 = Insignificante
2 = Bajo
3 = Mediano
4 = Alto
- Probabilidad de Amenaza: 1 = Insignificante
2 = Baja
3 = Mediana
4 = Alta

Calculando los promedios de la magnitud de daño y la probabilidad de amenaza en la matriz de riesgos de Excel así:

=PROMEDIOA('Ambiente'!Probabilidad de amenaza:Magnitud de daño)

Los resultados del mapa de calor y la matriz de riesgo fueron los siguientes:

Análisis de Riesgo promedio

		Probabilidad de Amenaza		
		Criminalidad y Político	Sucesos de origen físico	Negligencia y Institucional
Magnitud de Daño	Datos e Información	6.5	6.5	8.3
	Sistemas e Infraestructura	5.9	5.9	7.5
	Personal	5.2	5.2	6.6

Tabla 7. Riesgo promedio. Fuente: Autor

Valoración	Escala	Valor_min	Valor_max	Lineas	Umbral Medio Riesgo	Umbral Alto Riesgo
Ninguna	1	1	3		7	10,5
Baja	2	4	6	x	y	y
Mediana	3	8	9	1,0	7,0	10,5
Alta	4	12	16	1,1	6,4	9,5
				1,2	5,8	8,8
				1,3	5,4	8,1
				1,4	5,0	7,5
				1,5	4,7	7,0
				1,6	4,4	6,6
				1,8	4,0	6,0
				1,8	3,9	5,8
				1,9	3,7	5,5
				2,0	3,5	5,3
				2,1	3,3	5,0
				2,2	3,2	4,8
				2,3	3,0	4,6
				2,4	2,9	4,4
				2,5	2,8	4,2
				2,6	2,7	4,0
				2,7	2,6	3,9
				2,8	2,5	3,8
				2,9	2,4	3,6
				3,0	2,3	3,5
				3,1	2,3	3,4
				3,2	2,2	3,3
				3,3	2,1	3,2
				3,4	2,1	3,1
				3,5	2,0	3,0
				3,6	1,9	2,9
				3,7	1,9	2,8
				3,8	1,8	2,8
				3,9	1,8	2,7
				4,0	1,8	2,6

Tabla 8. Umbrales de Riesgo. Fuente: Autor

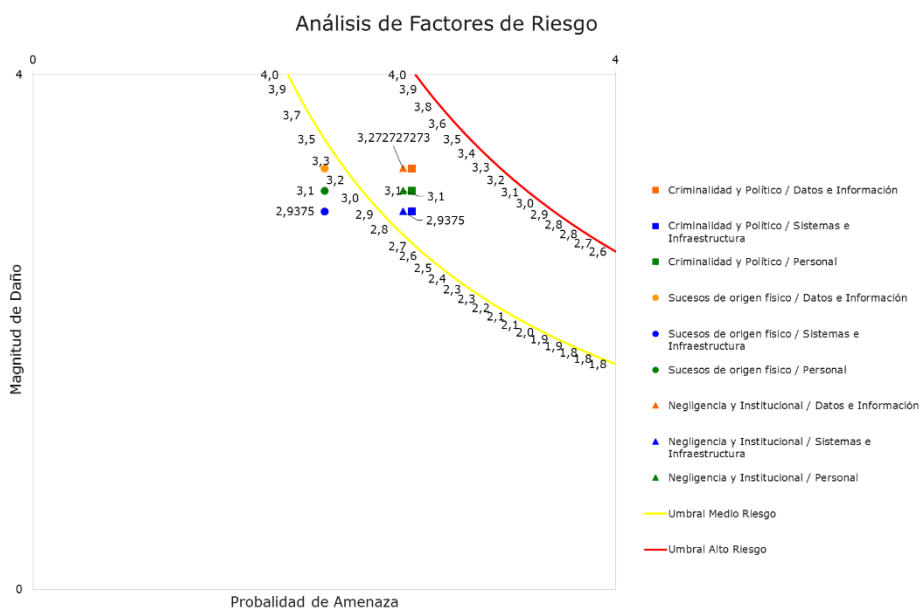


Ilustración 47: Análisis gráfico de Factores de riesgo. Fuente: Autor

La matriz de riesgos y el mapa de calor completos se pueden observar en el Anexo 2 de este trabajo.

Según los resultados el mayor riesgo para los datos e información, y los sistemas e infraestructura, están dados por la negligencia institucional. Algún descuido en el diseño de la red y el modelo de teletrabajo puede afectar seriamente la continuidad de servicio y reputación empresarial. Los umbrales resultantes tienen un máximo de 4.0 en magnitud Media y Alta, esto quiere decir que cualquier factor de riesgo que alcance una probabilidad o concurrencia mayor puede ser catastrófico para la organización.

5.1.2 Costos

Los costos asociados al modelo de teletrabajo fueron calculados en base a las fórmulas de la sección 2.4.1.2.3 para la compensación del uso de dispositivos y el uso de servicio eléctrico de los empleados

$$\text{Compesación} = \frac{\text{MOI} * \% \text{ de depreciación}}{12(1\text{Año})}$$

MOI= Monto original de la inversión (Costo comercial del dispositivo)

% de depreciación= 30% Para equipos de cómputo

El Monto original de la inversión reconocido por la empresa será para equipos con un valor comercial de \$1'000.000 hasta un máximo de \$2'000.000 M/C

Tomando como referencia el valor máximo del MOI para los 145 trabajadores del piloto se obtienen los siguientes costos mensuales por compensación de BYOD

Teletrabajadores Prueba Piloto	MOI	Porcentaje de Depreciación	t (meses)
145	2000000	30	12
		Costo mensual Total	\$7.250.000,000
		Compensación BYOD máx. por trabajador	\$50.000,000

Tabla 9. Costos Mensuales por compensación BYOD. Fuente: Autor

La compensación por BYOD para la prueba piloto puede variar entre \$3'625.000 y \$7'250.000 mensuales, o entre \$25.000 y \$50.000 mensuales por teletrabajador.

El valor compensado por el uso de energía eléctrica del trabajador remoto fue calculado según el costo de Kwh y el consumo aproximado de un PC o un computador portátil en la Ciudad de Bogotá. (Codensa SA., 2015)

$$(\text{Consumo de PC o laptop Kwh}) * 8 \text{ horas} * \text{Costo 1 Kwh} \\ * \text{días de teletrabajo al mes}$$

Computador portátil:

ESTRATO	Costo KWh	Consumo KWh	Consumo diario KWh	Días de trabajo remoto al mes	Total compensación mensual
1	\$142,22	0,1	0,8	16	\$1.820,38
2	\$177,78	0,1	0,8	16	\$2.275,61
3	\$302,22	0,1	0,8	16	\$3.868,38
4	\$355,56	0,1	0,8	16	\$4.551,22
5 y 6	\$496,69	0,1	0,8	16	\$6.357,67

Tabla 10. Costos Mensuales por compensación de consumo eléctrico LAPTOP. Fuente: Autor

PC:

ESTRATO	Costo KWh	Consumo KWh	Consumo diario KWh	Días de trabajo remoto al mes	Total compensación mensual
1	\$142,22	0,6	4,8	16	\$10.922,27
2	\$177,78	0,6	4,8	16	\$13.653,66
3	\$302,22	0,6	4,8	16	\$23.210,27
4	\$355,56	0,6	4,8	16	\$27.307,32
5 y 6	\$496,69	0,6	4,8	16	\$38.146,02

Tabla 11. Costos Mensuales por compensación de consumo eléctrico PC. Fuente: Autor

Si se estima que los tipos de computadores en la población de la prueba piloto es 50% 50% entonces el costo promedio por compensación eléctrica mensual será igual a \$1'906.198,69 pesos.

Los costos totales mensuales de esta prueba piloto pueden estar entre \$5.531.198,69 y \$9.156.198,69 pesos para 145 trabajadores remotos.

3.1.2 Beneficios

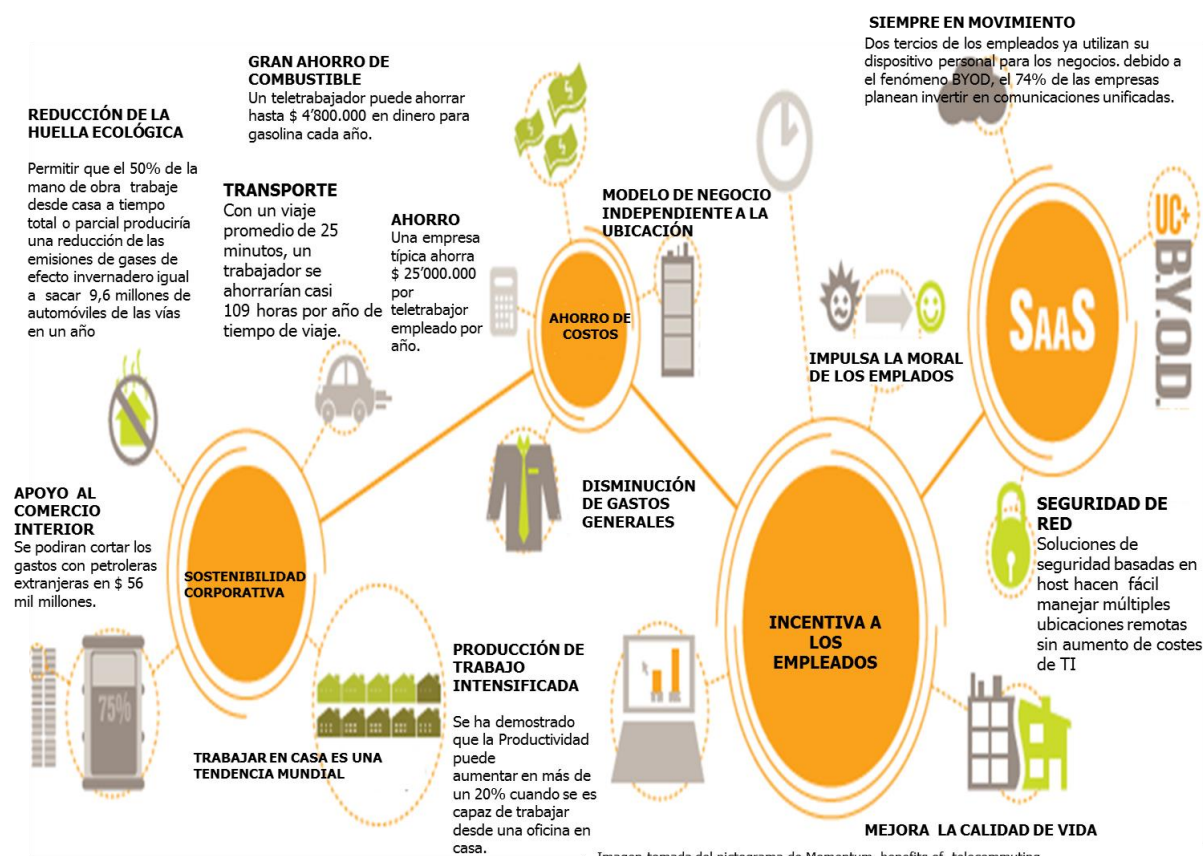


Ilustración 48: Beneficios del Teletrabajo. Fuente: Momentum benefits of telecommuting

Los beneficios de esta prueba piloto se pueden dividir así:

- Beneficios para la empresa
- Beneficios para el Teletrabajador

3.1.2.1 Beneficios para la empresa

Los empleados remotos representan ahorro de costos por consumo de agua, energía y mantenimiento de la infraestructura de la empresa. Estos costos pueden ser calculados de acuerdo a las tarifas comerciales de servicios públicos para el sector comercial (Codensa EAAB, 2015).

Consumo de energía eléctrica de 145 trabajadores fijos utilizando PCs, impresoras, iluminación, etc.

# de Teletrabajadores	Costo KWh	Consumo KWh	Consumo diario KWh	Días laborales al mes	Total costo mensual
1	\$417,44	0,9	7,2	20	\$60.110,64
145	\$417,44	0,6	7,2	20	\$8.716.042,80
			COSTO MENSUAL DE CONSUMO		\$8.716.042,80

Tabla 12. Costos Mensuales por consumo eléctrico PC. Fuente: Autor

Consumo de Agua de 145 trabajadores fijos m³:

La dotación de agua para consumo humano se calcula a razón de 80 litros por operario o empleado, por cada turno de 8 horas o fracción. Si se tiene en cuenta que cada m³ tiene 1000 litros se pueden calcular los siguientes costos

# de Teletrabajadores	Costo m3	Consumo personal de Agua	Consumo diario en m3	Días laborales al mes	Total costo mensual
1	\$2.381,24	80	0,08	20	\$3.809,98
145	\$2.381,24	80	0,08	20	\$552.447,68
			COSTO MENSUAL DE CONSUMO		\$552.447,68

Tabla 13. Costos Mensuales por consumo de agua. Fuente: Autor

Los costos por mantenimiento de infraestructura, incluyen servicios de limpieza, mantenimiento, elementos de aseo y cafetería

Costo personal de Mantenimiento	Costo personal de aseo y cafetería	Elementos de aseo diarios	Elementos de cafetería diarios	Días laborales al mes	Total compensación mensual
\$644.336,00	\$1.288.672,00	\$100.000	\$100.000	20	\$5.933.008,00
			COSTO MENSUAL DE CONSUMO		\$5.933.008,00

Tabla 14. Costos Mensuales por consumo de agua. Fuente: Autor

CONSUMO ELÉCTRICO	\$8.716.042,80
CONSUMO DE AGUA	\$552.447,68
COSTOS DE MANTENIMIENTO	\$5.933.008,00
COSTOS TOTALES MENSUALES	\$15.201.498,48

Tabla 15. Costos Mensuales totales. Fuente: Autor

Costos Prueba Piloto	Costos Prueba Piloto	Costos Mensuales Empresa	Total Ahorro mensual
Costo mínimo	\$5.531.198,69	\$15.201.498,48	\$9.670.299,79
Costo máximo	\$9.156.198,69	\$15.201.498,48	\$6.045.299,79

Tabla 16. Ahorro mensual empresa. Fuente: Autor

El ahorro de costos mensuales de la empresa puede estar entre \$6.045.299,79 y \$9.670.299,79 pesos mensuales según los costos analizados anteriormente para la prueba piloto.

Las tarifas de servicios públicos pueden ser observadas en el Anexo 3 de este trabajo.

3.1.2.2 Beneficios para el Teletrabajador

Los empleados remotos tienen múltiples beneficios de capital y de calidad de vida. Un teletrabajador puede ahorrar en transporte público, gasolina, vestuario y tiempo.

Un teletrabajador ahorraría:

- 2 horas diarias de desplazamientos. Esto se puede traducir en 384 horas al año para cada teletrabajador de esta prueba piloto.

Horas ahorradas diarias	Días de teletrabajo a la semana	Cantidad de ahorro de horas mensuales	Total Ahorro de tiempo anual
2	4	32	384

Tabla 17. Ahorro Tiempo Teletrabajador. Fuente: Autor

- Se ahorra \$ 691200 pesos anualmente en base al costo por trayecto en el transporte público más utilizado de Bogotá.

Ahorro Diario de Transporte	Ahorro Semanal de Transporte	Ahorro Mensual de Transporte	Ahorro Anual de Transporte
\$3.600,00	\$14.400,00	\$57.600,00	\$691.200,00

Tabla 18. Ahorro Transporte Teletrabajador. Fuente: Autor

- Puede ahorrar \$ 1'920.000 pesos en gasolina. Tomando como referencia un consumo diario de \$ 10.000 pesos en combustible para 16 días de teletrabajo al mes.

Ahorro Diario de Gasolina	Ahorro Semanal de Gasolina	Ahorro Mensual de Transporte	Ahorro Anual de Transporte
\$10.000,00	\$40.000,00	\$160.000,00	\$1.920.000,00

Tabla 19. Ahorro Gasolina Teletrabajador. Fuente: Autor

- Se ahorraría un 80% de gastos generales y de vestuario, al reducir el desgaste y consumo diario de los mismos.

$$\frac{5 \text{ días de trabajo a la semana}}{4 \text{ días de teletrabajo semanales}} = \frac{100\%}{X}$$

$$X = 80\%$$

Teletrabajar 4 días a la semana significa un 80% menos de gastos generales y de vestuario,

Total Ahorro de tiempo anual	\$384,00
Ahorro Anual de Transporte	\$691.200,00
Ahorro Anual de Gasolina	\$1.920.000,00
Ahorro Total Anual	\$2.611.584,00

Tabla 20. Ahorro Anual Teletrabajador. Fuente: Autor

El ahorro anual calculado para un teletrabajador es de \$2.611.584, más el ahorro del 80% en gastos generales al trabajar remotamente 16 días al mes.

CONCLUSIONES

- La implementación de un modelo de teletrabajo en una organización debe contemplar las necesidades, riesgos, y nivel de seguridad para el acceso a la información. Cualquier descuido u omisión puede afectar seriamente la continuidad de negocio y tener resultados negativos para la producción y disponibilidad de servicio.
- A partir de las pruebas simuladas y el análisis de costos y beneficios se demostró que el modelo de teletrabajo propuesto para el sector bancario, es rentable y seguro, siempre y cuando se cumpla con las recomendaciones ISO 27001/2, su ciclo de mejora continua, las políticas de seguridad y manejo de contraseñas propuestas en esta investigación.
- Las pruebas de descubrimiento de vulnerabilidades y ataques a la red de teletrabajo, se realizaron bajo simulación en un ambiente de red público como Internet; sus resultados están limitados al uso de tecnología comercial, no se contemplan ataques con computadoras o tecnologías cuánticas.
- La configuración de seguridad utilizada no fue soportada por packet tracer. El uso de GNS3 brinda todo el potencial disponible en el IOS de los dispositivos emulados.
- El uso de contraseñas de tipo frase brinda protección contra ataques diccionario y de fuerza bruta; ninguno de los diccionarios utilizados en los ataques con Hydra utilizaba el espacio como parte de las contraseñas.
- La prueba piloto para la implementación de teletrabajo está limitada por la infraestructura tecnológica disponible; La capacidad de los canales de internet contratados por la empresa es el mayor limitante a la hora de definir la cantidad de trabajadores remotos
- La infraestructura tecnológica es determinante para el alcance de la prueba piloto y el modelo tecnológico que va a ser adoptado. La cantidad de teletrabajadores, los

anchos de banda disponibles, las licencias VPN pueden incrementar los costos del piloto dependiendo de la cantidad de trabajadores remotos.

- La simulación se limitó a 10 usuarios por el licenciamiento del IOS utilizado para el servidor VPN. Un mayor número de usuarios VPN implica costos por licencia.
- El ancho de banda utilizado por los usuarios remotos en la simulación fue compartido. No se aplican políticas de calidad de servicio o anchos de banda dedicados por usuario. Esto no significó efectos negativos para la simulación o el diseño de la red al no sobrepasar el límite de 50 Mbps con el total de trabajadores de la prueba piloto

PERSPECTIVAS FUTURAS

Con el adelanto de esta investigación y el diseño del modelo de teletrabajo, se deberían idear mecanismos de masificación, capacitación e incentivos para organizaciones que adopten cualquier modalidad de trabajo a distancia, para lograr posicionar al país dentro de las estadísticas y proyecciones de teletrabajo a nivel mundial.

Este trabajo se basó en tecnologías VPN bajo el marco IPSec con protocolos y algoritmos simétricos. Para futuras investigaciones se deberían tener en cuenta protocolos y técnicas asimétricas de encriptación más avanzadas, con la posibilidad de mitigar ataques con computadoras cuánticas, y reducir los tiempos de negociación y retardo por el aseguramiento de la información.

El apoyo para futuras investigaciones en el campo de la seguridad de la información debe mejorar en cuanto a la infraestructura disponible en Universidades y entidades públicas o privadas, facilitando el acceso a nuevas tecnologías de protección y acceso seguro a la información, que son en esencia la base de funcionamiento y éxito en la adopción de modelos de teletrabajo al interior de cualquier organización.

REFERENCIAS

- Academmy, C. N. (2008). *INS v1.1 (Implementation of network Security). CCNA Security Course Booklet Version 1.1 2nd Edition* . Pearson VUE.
- Academy, C. N. (2009). *CCNS v1.1 (Cisco Certified Network Security Professional). CCNS Security Course Booklet Version 1.1 2nd Edition* . . Peason VUE.
- Anis, J. C. (1992). *Guide to PC Telecommunications* . Osborne/McGraw-Hill.
- Carrasco Gutiérrez, J. (1997). EL TELETRABAJO COMO NUEVA OPCIÓN. *Revista de Trabajo y Seguridad Social* nº 177.
- Carrasco, F. (17 de Marzo de 2013). *CLARO CHILE INICIA MARCHA BLANCA DE SU RED 4G LTE EN SANTIAGO CON PRIMERA LLAMADA DE VOZ*. Obtenido de <http://www.cioal.com/2013/03/08/claro-chile-inicia-marcha-blanca-de-su-red-4g-lteen-santiago-con-primera-llamada-de-voz-y-friendly-users/>
- Castañeda, D. M. (2009). *Métodos de gestión para un arquitectura de teletrabajo*. Bogotá: Fundación universitaria Konrad Lorenz.
- Chaparro, F. O. (1996). *El teletrabajo: una nueva sociedad laboral en la era de la tecnología*. Madrid: Mc. Graw-Hill.
- Cisco, S. (2012). *Dispositivos adaptables de seguridad de la serie Cisco ASA 5500*. Obtenido de <https://www.cisco.com/web/ES/publicaciones/07-08-cisco-dispositivos-serie-ASA5500.pdf>
- Codensa EAAB. (2015). *Tarifario 2015*. Bogotá.
- Codensa SA. (25 de Febrero de 2015). *Simulador de consumo Codensa*. Obtenido de <http://simulador.micodensa.com/>
- Di Martino, V. y. (nº 4). TELETRABAJO; UN NUEVO MODO DE TRABAJO Y DE VIDA. *Revista Internacional del Teletrabajo*, vol. 109 nº 4.
- Díaz, C. y. (2005). *La Criptografía: Una guerra de Piratas y Corsarios*. Editorial Complutense.: Editorial Complutense.
- Galende Díaz, J. C. (1995). *Criptografía. Historia de la escritura cifrada*.

- Gallusser, P. (23 de Octubre de 2005). *Creciente avance del teletrabajo como modalidad laboral* *La Trama de la Comunicación*. Obtenido de <http://www.redalyc.org/articulo.oa?id=323927060015>
- García, C. A. (27 de 06 de 2014). *Diario El Tiempo*. Obtenido de EITiempo: <http://www.eltiempo.com/economia/finanzas-personales/trabajadores-del-sector-bancario-colombiano/14177018>
- Haberkern, K. (2009). based on World Value Survey.
- ISO, I. (2005). *NORMA NTC-ISO/IEC 27001*. Reino Unido: ISO.
- ITU, A. A. (s.f.). Obtenido de http://departamento.pucp.edu.pe/ingenieria/images/documentos/seccion_telecomunicaciones/Capitulo%205%20Modelos%20de%20Trafico.pdf
- Mauricio Ríos Hurtado, J. J. (2008). *Proyecto de implementación en modalidad de teletrabajo para personas con discapacidad motora "Teledisc@"*. Bogotá: Unniversidad EAN.
- MINTIC. (2008). *Ministerio de Tecnologías de la Información y las Comunicaciones*. Obtenido de <http://www.mintic.gov.co/portal/604/w3-article-3703.html>
- MINTIC. (2012). *Libro Blanco: El ABC del Teletrabajo*. Obtenido de Colombia Digital: http://www.medellindigital.gov.co/Mediateca/repositorio%20de%20recursos/ColombiaDigital_ABCTeletrabajo.pdf
- MONTIEL. (2003). *Municipio y teletrabajo*. Cuadernos L Primer Semestre.
- Nilles, J. (1970). *Teletrabajo*. Estados Unidos.
- NIST. (2012). *National Institute of Standards and Technology*. Obtenido de <http://www.itl.nist.gov/lab/bulletns>
- NSA. (Noviembre de 2012). *Center of cryptologic history [en línea]: Savage Road Fort Meade, 2012*. Obtenido de <http://www.nsa.gov/>
- OECD. (2011). *Doing Better for families*:. Francia: Organisation for Economic Co-operation and Development . Obtenido de Organisation for Economic Co-operation and Development .

- Office., U. S. (2008). *Excellence in Telework IT. Telework Exchange Case Study. Junioe Networks.*
- OIT. (2008). *Segundo Congreso Iberoamericano de Teletrabajo.* Madrid.
- Padilla, A. (Mayo de 2007). *Caminando Utopias org: Cronología del Teletrabajo.* Obtenido de <http://www.caminandoutopias.org.ar/tesis/tesina/cap2.pdf>
- Plus, C. T. (16 de 10 de 2013). *Teletrabajo Integral.* Obtenido de <http://teletrabajoip.co/blog/perfil-del-teletrabajador/>
- Shirley Radack, N. (2008). *NEW CRIPTOGRAPHIC HASH ALGORITHM FAMILY: NIST HOLDS A PUBLIC COMPETITION TO FIND NEW ALGORITHMS.* Gaithersburgo, Maryland: Information Tecnology Laboratory.
- Solano, J. (Octubre de 2012). *Javier Solano blog: Las Tic En El Desarrollo Social Colombiano: El Teletrabajo .* Obtenido de <http://javersolanopolitecnico.blogspot.com/2012/10/el-teletrabajo-en-cifras.html>
- Videgain Muro, J. I. (1995). *UNA EXPERIENCIA EUROPEA DE TELETRABAJO. Revista Alta Dirección, nº 184.*