



UNA UNIVERSIDAD CON ALMA DE GUERRERO

# ANÁLISIS COMPARATIVO DE ALGORITMOS CRIPTOGRÁFICOS PARA REDES PRIVADAS VIRTUALES

Tesis para optar por el Título de Ingeniero  
de Sistemas, que presenta el bachiller.

AUTOR

**DENYS IVAN CAPUÑAY PUICAN**

ASESOR

**ING. JUAN ELÍAS VILLEGAS CUBAS**

CHICLAYO - PERÚ 2016



# ANÁLISIS COMPARATIVO DE ALGORITMOS CRIPTOGRÁFICOS PARA REDES PRIVADAS VIRTUALES

Aprobación de Tesis

---

Mg. Guerrero Millones Ana María

**Asesor Metodólogo**

---

Ing. Villegas Cubas Juan Elías

**Asesor Especialista**

---

Ing. Tuesta Monteza Víctor Alexci

**Presidente del Jurado de Tesis**

---

Ing. Carrión Barco Gilberto

**Secretario del Jurado de Tesis**

---

Ing. Villegas Cubas Juan Elías

**Vocal del Jurado de Tesis**

## DEDICATORIA

El presente está dedicado a Dios por llevarme de su mano por el camino correcto enseñándome a encarar adversidades y no desmayar en momentos de dificultades; gracias mi Dios por el amor que nos brindas y darme la placidez de ver realizada una meta más.

A mis padres Capuñay Zarpan Marcelino y Puican Chancafe Elva, por ser mi motor y motivo, mi ayuda idónea; por la confianza recibida por ustedes y por haber confiado en mí, gracias por brindarme su apoyo incondicional, su orientación, sus consejos para tener una mejor formación profesional y personal.

## AGRADECIMIENTO

Agradecer a mis padres por ser mi guía, darme el apoyo incondicional, y por darme la fortaleza para seguir luchando por mis objetivos trazados, a Cinthia Chancafe LLontop por su apoyo incondicional en el transcurso de mi formación profesional, por compartir momentos de alegría, tristeza y demostrarme que siempre podré contar con ella.

Es muy cordial agradecer a mi asesor metodólogo de proyecto de tesis Ing. Miguel Vidaurre Flores, a mi asesor metodólogo de desarrollo de tesis Mg. Ana María Guerrero Millones y de manera especial a mi asesor especialista Ing. Juan Villegas Cubas por compartirme sus experiencias, nuevos conocimientos, nuevas ideas.

A todos ustedes gracias haberme exigido día a día, a superarme más y ser mejor.

**RESUMEN:**

La necesidad de manipular la información de una manera más segura y confiable, es a través de las llamadas redes privadas virtuales (VPN), que nos permite vincularnos y tener un enlace privado, el cual se va acoplado sobre una red pública que garantiza la integridad y confidencialidad de la información gracias a los diversos procesos de autenticación, encriptación y codificación, obteniendo un enlace que garantiza la privacidad.

Es en este sentido, que la presente tesis trata de hacer un análisis comparativo de los algoritmos criptográficos usados para redes privadas virtuales, ya que el problema principal radica en asegurar la integridad y seguridad que tiene la información al conectarnos a otro equipo de forma remota. Esto se logró seleccionando todos los algoritmos existentes para redes privadas virtuales (VPN), e implementándolos en una red donde se hizo los estudios y captura de tráfico para observar y analizar cual nos ofrece una mejor integridad y seguridad de la información.

Para el desarrollo de esta investigación se utilizó la metodología experimental, que permitió manipular las variables en función de que permita la recolección de datos, conociéndose así la encriptación que ofreció cada algoritmo.

Después que se evaluó cada algoritmo en la red implementada, se logró determinar que algoritmos es mejor en tiempos, tamaño de los paquetes, el nivel de encriptación y desencriptación, grado de encapsulación, etc. Obteniendo que el algoritmo AES divide los datos en un mayor número de paquetes y necesita menor tiempo para enviarlos en comparación con los demás algoritmos. Sobre los paquetes encriptados algoritmo AES presenta igual número de paquetes encriptados que el algoritmo DES, pero algoritmo AES desencripta mas paquetes



que el algoritmo DES utilizando menos recursos.

Entre las conclusiones se obtuvo que el algoritmo AES es el mejor protocolo en tiempo de envío, en número de paquetes de encriptación y en número de paquetes de desencriptación.

**PALABRAS CLAVE:** ANÁLISIS, CRIPTOGRAFÍA, ALGORITMOS, REDES PRIVADAS VIRTUALES, INTEGRIDAD, SEGURIDAD.

**ABSTRACT:**

The need to manipulate information in a more secure and reliable way is through so-called virtual private networks (VPN), which allows us to link up and have a private link, which is coupled to a public network that ensures the integrity and confidentiality of the information through the various processes of authentication, encryption and encoding, getting a link that ensures privacy.

It is in this context that this thesis is a comparative analysis of cryptographic algorithms used for virtual private networks, because the main problem in ensuring the integrity and security is our information to connect to another computer remotely. This was achieved by selecting all existing algorithms for virtual private networks (VPN), and implementing them in a network where traffic capture studies and was to observe and analyze which offers better integrity and security of our information. For the development of this experimental research methodology was used, as this allowed us to manipulate the variables in terms of enabling data collection, and knowing the encryption offered each algorithm.

After evaluating each algorithm implemented in the network, it was determined that algorithms is better at times, packet size, the level of encryption and decryption, degree of encapsulation, etc. Obtaining the AES algorithm divides the data into a larger number of packets and requires less time to send as compared to the other algorithms. About AES encrypted packet has the same number of encrypted the DES algorithm, but decrypting AES algorithm more packets DES algorithm using fewer resources packages.



Among the findings it was obtained that the AES algorithm is the best time protocol sent in number of encryption packages and the number of packages decryption.

**KEYWORDS:** ANALYSIS, CRYPTOGRAPHY, ALGORITHMS, VIRTUAL PRIVATE NETWORKS, INTEGRITY, SECURITY.



## INTRODUCCIÓN:

La presente investigación se refiere al tema de seguridad informática, la cual analicé comparativamente algoritmos criptográficos para redes privadas virtuales.

Las redes privadas virtuales o VPN son aquellas conexiones punto a punto a través de una red privada o pública, como el internet.

La descripción de la presente tesis cuenta con seis capítulos distribuidos de la siguiente manera: En el primer capítulo se hizo la presentación de la investigación, la tecnología que se utilizó durante el desarrollo del mismo y la problemática identificada, en el segundo capítulo se efectúa un recorrido teórico sobre el cual se fundamenta el proyecto, el uso de la redes privadas virtuales, el protocolo IPSec, los algoritmos de encriptación que se utilizaron y las herramientas para la ejecución de proyecto, en el tercer capítulo se detalla el análisis de estudio de la población, el método, técnicas e instrumentos usados para la recolección de datos, en el cuarto capítulo se realizó el análisis e interpretación de los resultados, en el quinto capítulo se realizó la propuesta de investigación, implementación de la VPN, configuración de IPSec en los routers y la captura de tráfico que se hizo con los diferentes algoritmos utilizados.

Al final del documento el lector podrá encontrar las conclusiones, recomendaciones y detalles sobre la experiencia generada en el desarrollo de la presente tesis. Es así como está la investigación se enfocó en la seguridad y privacidad utilizando los estándares más utilizados para redes privadas. A tal efecto, se investigaron VPNs, el protocolo IPSEC, y los algoritmos AES, DES y 3DES, desde un punto de vista teórico y experimental, identificando y demostrando el alcance de vulnerabilidades en las mismas y explorando el impacto que tiene en la seguridad de la información.



## ÍNDICE

1.	El Problema de Investigación .....	21
1.1.	Situación problemática .....	21
1.2.	Formulación del problema .....	22
1.3.	Delimitación de la Investigación .....	23
1.4.	Justificación e importancia .....	23
1.5.	Limitaciones de la Investigación .....	24
1.6.	Objetivos de la Investigación .....	24
1.6.1.	Objetivo general .....	24
1.6.2.	Objetivos específicos .....	24
2.	Marco Teórico .....	26
2.1.	A Nivel Internacional.....	26
2.2.	Estado del Arte .....	30
2.3.	Bases teórico científicas .....	33
2.3.1.	Algoritmo .....	33
2.3.2.	Algoritmo Data Encryption Stándar (DES) .....	34
2.3.3.	Algoritmo Advanced Encryption Standard (AES) .....	35
2.3.4.	Criptografía .....	37
2.3.5.	Redes Privadas Virtuales .....	37
2.3.6.	Internet Protocol Security (IPSec) .....	40
2.3.7.	IKE (Intercambio de claves de Internet): .....	47
2.3.8.	ISAKMP .....	48



2.3.9.	PuTTY.....	54
2.3.10.	Wireshark .....	55
2.3.11.	Tcpextract .....	56
2.3.12.	Acrylic WIFI .....	57
2.3.13.	Método Descriptivo .....	58
2.3.14.	Método Analítico .....	58
2.3.15.	Método Deductivo .....	59
2.3.16.	Método inductivo – deductivo.....	59
2.3.17.	Observación- Encuesta.....	60
2.3.18.	Observación - Entrevista Estructurada.....	61
2.4.	Definición de Terminología.....	61
2.4.1.	Encriptado .....	61
2.4.2.	Clave Privada:.....	62
2.4.3.	IPsec (Internet Protocol Security):.....	62
2.4.4.	Hash.....	62
2.4.5.	MD5 (Message-Digest Algorithm 5) .....	62
2.4.6.	Algoritmo de hash seguro (SHA).....	62
2.4.7.	Encabezado de autenticación (AH).....	63
2.4.8.	Contenido de seguridad encapsulado (ESP) .....	63
2.4.9.	ISAKMP.....	63
2.4.10.	Advanced Encryption Standard (AES): .....	64



2.4.11.	Data Encryption Standard (DES) .....	64
2.4.12.	HTML (HyperText Markup Language):.....	64
2.4.13.	Internet.....	64
3.	Marco metodológico .....	66
3.1.	Tipo y diseño de la investigación.....	66
3.1.1.	Tipo de Investigación .....	66
3.1.2.	Diseño de la investigación.....	66
3.2.	Población y muestra .....	67
3.2.1.	Población: .....	67
3.2.2.	Muestra: .....	67
3.3.	Hipótesis.....	68
3.4.	Operacionalización: .....	68
3.5.	Métodos, técnicas e instrumentos de recolección de datos .....	69
3.5.1.	Métodos de Investigación.....	69
3.5.2.	Técnicas de recolección de datos .....	69
3.5.3.	Instrumentos de recolección de datos.....	69
3.6.	Procedimiento para la recolección de datos.....	70
3.7.	Análisis Estadístico e interpretación de los Datos .....	70
3.8.	Criterios Éticos .....	72
3.9.	Criterios de rigor Científico .....	72
4.	Análisis e Interpretación de los Resultados.....	75
4.1.	Resultados en Tablas.....	75



4.1.1.	Selección de algoritmos .....	75
4.1.2.	Evaluación Cuantitativa de los Algoritmos .....	85
4.1.3.	Resume de evaluación cuantitativa de los algoritmos.....	92
5.	Propuesta de Investigación .....	95
5.1.	VPN Implementada. ....	95
5.1.1.	Modelo de VPN implementada.....	95
5.1.2.	Equipos para la Implementación de VPN.....	95
5.2.	Configuración de Router Cisco.....	98
5.2.1.	Configuración de Router 1 .....	98
5.2.2.	Configuración de Router 2 .....	99
5.2.3.	Configuración de Router 3 .....	100
5.2.4.	Comprobación de Conectividad entre HOST .....	101
5.3.	Configuración de IPSec en Router. ....	103
5.3.1.	Configuración de IPSec – 3DES .....	105
5.3.2.	Configuración de IPSec – AES .....	106
5.3.3.	Configuración de IPSec – DES .....	107
5.4.	Captura de Tráfico en VPN .....	108
5.4.1.	Captura de tráfico de datos con IPSec y 3DES.....	108
5.4.2.	Captura de tráfico de datos con IPSec y AES.....	113
5.4.3.	Captura de tráfico de datos con IPSec y DES.....	118
5.4.4.	Captura tráfico de voz y Video con IPSec y 3DES.....	123



5.4.5.	Captura tráfico de voz y Video con IPSec y AES .....	127
5.4.6.	Captura tráfico de voz y Video con IPSec y DES.....	128
6.	Conclusiones y Recomendaciones .....	130
6.1.	Conclusiones.....	130
6.2.	Recomendaciones.....	131
	REFERENCIAS BIBLIOGRÁFICAS: .....	132
	ANEXOS .....	135

## ÍNDICE DE TABLAS

<b>Tabla 1</b> - Diseño de la Investigación .....	66
<b>Tabla 2</b> - Operacionalización de las variables en estudio .....	68
<b>Tabla 3</b> - Algoritmo de DES.....	75
<b>Tabla 4</b> - Algoritmo de 3DES.....	78
<b>Tabla 5</b> - Algoritmo de AES.....	80
<b>Tabla 6:</b> Estudio comparativo entre DES, 3DES y AES.....	84
<b>Tabla 7</b> - Evaluación por el tamaño de archivo .....	85
<b>Tabla 8</b> - Evaluación por el número de paquetes.....	85
<b>Tabla 9</b> - Evaluación por el tiempo de envío. ....	86
<b>Tabla 10</b> - Evaluación por el # de paquetes encapsulados .....	86
<b>Tabla 11</b> - Evaluación por el # de paquetes desencapsulados .....	86
<b>Tabla 12</b> - Evaluación por el # de paquetes encriptados .....	87
<b>Tabla 13</b> - Evaluación por el # de paquetes descriptados.....	88
<b>Tabla 14</b> - Evaluación por el tamaño de archivo .....	88
<b>Tabla 15:</b> Por el número de paquetes.....	89
<b>Tabla 16:</b> Por el número de paquetes encapsulados.....	90
<b>Tabla 17:</b> Por el número de paquetes desencapsulados .....	90
<b>Tabla 18:</b> Por el número de paquetes encriptados .....	91
<b>Tabla 19:</b> Por el número de paquetes descriptados.....	91
<b>Tabla 20</b> - Tabla resumen de evaluación de algoritmos para Datos .....	92
<b>Tabla 21:</b> Tabla resumen de evaluación de algoritmos para voz y video.....	93



## ÍNDICE DE FIGURAS

<b>Figura 1</b> - Esquema general del algoritmo DES.....	34
<b>Figura 2</b> - Esquema del algoritmo de AES.....	35
<b>Figura 3</b> - Red Privada Virtual.....	38
<b>Figura 4</b> - Red Privada Virtual –Conexión desde internet.....	39
<b>Figura 5</b> - Entorno de Seguridad IP .....	42
<b>Figura 6</b> – Marco de IPSEC .....	43
<b>Figura 7</b> - Marco de IPsec.....	44
<b>Figura 8</b> - Estructura de AH .....	52
<b>Figura 9</b> - Estructura de ESP .....	53
<b>Figura 10</b> - Estructura de NAT- T.....	54
<b>Figura 11</b> - Proceso de Recolección de Datos.....	70
<b>Figura 12</b> - Esquema de Algoritmo DES.....	76
<b>Figura 13</b> - Formula de 3 DES .....	78
<b>Figura 14</b> - Esquema de Algoritmo 3 DES.....	79
<b>Figura 15</b> - Algoritmo de Rijndael - AES .....	81
<b>Figura 16</b> - Cifrado y Descifrado de AES.....	82
<b>Figura 17</b> - Evaluación por el número de paquetes .....	85
<b>Figura 18</b> - Evaluación por el # de paquetes encapsulados .....	86
<b>Figura 19</b> - Evaluación por el # de paquetes desencapsulados.....	87
<b>Figura 20</b> - Evaluación por el # de paquetes encriptados.....	87
<b>Figura 21</b> - Evaluación por el # de paquetes descriptados .....	88
<b>Figura 22:</b> Tiempo de Video Presencia.....	89
<b>Figura 23:</b> Número de Paquetes Generados .....	89
<b>Figura 24:</b> Por el número de paquetes encapsulados .....	90





<b>Figura 25:</b> Por el número de paquetes desencapsulados .....	90
<b>Figura 26:</b> Por el número de paquetes encriptados.....	91
<b>Figura 27:</b> Por el número de paquetes desenscriptados .....	91
<b>Figura 28 -</b> Red VPN .....	95
<b>Figura 29 -</b> Router Cisco 1900.....	95
<b>Figura 30 -</b> Switch Cisco 24 puertos .....	96
<b>Figura 31 -</b> Cable Consola.....	96
<b>Figura 32 -</b> Cable Serial.....	97
<b>Figura 33 -</b> Cable Directo.....	97
<b>Figura 34 -</b> Configuración de Acceso a R1 .....	98
<b>Figura 35 -</b> Configuración de Interfaces de R1 .....	98
<b>Figura 36 -</b> Enrutamiento con EIGRP en R1 .....	98
<b>Figura 37 -</b> Configuración de Acceso a R2 .....	99
<b>Figura 38 -</b> Configuración de Interfaces de R2 .....	99
<b>Figura 39 -</b> Enrutamiento con EIGRP en R2.....	99
<b>Figura 40 –</b> Configuración de Acceso a R3 .....	100
<b>Figura 41 -</b> Configuración de Interfaces en R3 .....	100
<b>Figura 42 -</b> Enrutamiento con EIGRP en R3.....	100
<b>Figura 43 -</b> Conectar dos PC a la RED.....	101
<b>Figura 44 -</b> Configurar las IP en las PC .....	101
<b>Figura 45 -</b> Comprobar las IP Asignadas.....	102
<b>Figura 46 -</b> Conectividad de PC-A y PC-C.....	102
<b>Figura 47 -</b> Conectividad de PC-C y PC-A.....	102
<b>Figura 48 -</b> Configuración de IPSec -3DES – R1 .....	105
<b>Figura 49 -</b> Configuración de IPSec -3DES – R3.....	105



<b>Figura 50</b> - Configuración de IPSec -AES – R1 .....	106
<b>Figura 51</b> - Configuración de IPSec –AES - R3.....	106
<b>Figura 52</b> - Configuración de IPSec -DES – R1.....	107
<b>Figura 53</b> - Configuración de IPSec -DES – R3.....	107
<b>Figura 54</b> – Ubicación de Archivo a Compartir en PcA.....	108
<b>Figura 55</b> - Copia de Archivo de PcA a PcC.....	108
<b>Figura 56</b> - Inicio de Captura de Tráfico con Wireshark.....	109
<b>Figura 57</b> - Fin de Captura de Tráfico con Wireshark .....	109
<b>Figura 58</b> - Estructura de un Paquete Captura .....	110
<b>Figura 59</b> - Paquetes filtrados por el ip de origen – 192.168.1.3 .....	110
<b>Figura 60</b> - Paquetes filtrados por el ip destino – 192.168.3.3.....	111
<b>Figura 61</b> - Número de paquetes de R1 .....	111
<b>Figura 62</b> - Número de paquetes de R3 .....	112
<b>Figura 63</b> - Ubicación de Archivo a Compartir en PcA.....	113
<b>Figura 64</b> - Copia de Archivo de PcA a PcC.....	113
<b>Figura 65</b> – Inicio de Captura de Tráfico con Wireshark.....	114
<b>Figura 66</b> - Fin de Captura de Tráfico con Wireshark .....	114
<b>Figura 67</b> - Estructura de un paquete Capturado.....	115
<b>Figura 68</b> - Paquetes filtrados por el IP de origen – 192.168.1.3.....	115
<b>Figura 69</b> - Paquetes filtrados por el IP destino – 192.168.3.3 .....	116
<b>Figura 70</b> - Número de paquetes de R1 .....	116
<b>Figura 71</b> - Número de paquetes de R3 .....	117
<b>Figura 72</b> - Ubicación de Archivo a Compartir en PcA.....	118
<b>Figura 73</b> - Copia de Archivo de PcA a PcC .....	118
<b>Figura 74</b> – Inicio de Captura de Tráfico con Wireshark.....	119



<b>Figura 75</b> - Fin de Captura de Tráfico con Wireshark .....	119
<b>Figura 76</b> - Estructura de paquete capturado .....	120
<b>Figura 77</b> - Paquetes filtrados por el Ip de origen - 192.168.1.3 .....	121
<b>Figura 78</b> - Paquetes filtrados por el IP destino - 192.168.3.3 .....	121
<b>Figura 79</b> - Número de paquetes de R1 .....	122
<b>Figura 80</b> - Número de paquetes de R3 .....	122
<b>Figura 81</b> : PcA con Polycom Realpresence.....	123
<b>Figura 82</b> : PcC con Polycom Realpresence .....	123
<b>Figura 83</b> : Inicio de Captura de Voz y Video .....	124
<b>Figura 84</b> : Llamada de PcA a PcC .....	124
<b>Figura 85</b> : Llamada entrante de IP 192.168.1.3 .....	125
<b>Figura 86</b> : Envío de Voz y Video .....	125
<b>Figura 87</b> : Número de paquetes en R1 con 3DES .....	126
<b>Figura 88</b> : Número de paquetes en R3 con 3DES .....	126
<b>Figura 89</b> : Número de paquetes en R1 con AES.....	127
<b>Figura 90</b> : Número de paquetes en R3 con AES.....	127
<b>Figura 91</b> : Número de paquetes en R1 con DES .....	128
<b>Figura 92</b> : Número de paquetes en R3 con DES .....	128



# CAPÍTULO I: EL PROBLEMA DE INVESTIGACIÓN

## 1. El Problema de Investigación

### 1.1. Situación problemática

En la actualidad, nos encontramos en un momento decisivo respecto al uso de las tecnologías para desarrollar y ensanchar la capacidad de comunicación. Las redes nos conectan cada vez más desde cualquier lugar. La necesidad de manipular la información de una manera más segura y confiable, es a través de las llamadas redes privadas virtuales (VPN), que permite vincularnos y tener un enlace privado, el cual va acoplado sobre una red pública, y garantiza la integridad y confidencialidad de la información entre los participantes, gracias a los diversos procesos de autenticación, encriptación y codificación, para poder tener un enlace que garantice la privacidad.

Es en este sentido, la seguridad se ha vuelto un punto vital a la hora de entablar una comunicación, desde su origen han surgido diversas investigaciones en seguridad de la red para la administración de contraseñas, firmas digitales y el encriptamiento de datos con el uso de algoritmos criptográficos. Haciendo de estos un punto fundamental para la configuración de redes privadas virtuales, ya que en un medio como el internet, los datos son vulnerables, y de fácil captura por persona ajenas.

En los últimos años han aparecido diversos tipos de algoritmos para cifrar nuestros datos, todos intentando cubrir una o varias de las características de la seguridad (confidencialidad, integridad, autenticación, no repudio). Siendo difícil evaluar el nivel de cumplimiento de cada algoritmo, ya que pueden ser vulnerables, ante técnicas de ataque diferentes, además la mayoría de los algoritmos pueden trabajar con claves de distintas longitudes



lo que afecta a la seguridad. Por otro lado, tenemos otras características que influyen en el proceso de selección del algoritmo más adecuado para un determinado sistema.

En la actualidad, existen infinidad de algoritmos criptográficos, que partiendo de un documento obtienen otro o un conjunto de información, estos han sido clasificados en grupos como los algoritmos criptográficos simétricos y los algoritmos criptográficos asimétricos. La criptografía simétrica es aquella que utiliza la misma clave para cifrar y descifrar el mensaje de datos, es decir se basa en una misma clave compartida. La criptografía asimétrica es aquella que en lugar de usar una sola clave para realizar el cifrado y descifrado, se utilizan dos claves diferentes; una para cifrar y otra para descifrar.

Hoy en día la criptografía simétrica es muy usada para cifrar todo tipo de datos, observándose un desconocimiento para la elección de que algoritmo utilizar a la hora de cifrar nuestros datos, por no tener en cuenta la velocidad de encriptación, los recursos que utiliza, y lo que más resalta es el nivel de integridad que nos brinda un algoritmo específico.

Hoy en día tenemos la gran responsabilidad de seguir brindando la seguridad necesaria en nuestra comunicación, en los datos que enviamos, en las operaciones que realizamos. Todo esto sabiendo que algoritmo cumple con las características fundamentales de la criptografía.

## 1.2. Formulación del problema

¿De qué manera se podrá saber con qué algoritmo obtendremos mayor integridad de nuestros datos al conectarse a una red privada virtual?

### 1.3. Delimitación de la Investigación

El presente proyecto se desarrolló en el laboratorio de investigación científica de la escuela de ingeniería de sistemas de la universidad Señor de Sipán ubicada en el distrito de Pimentel, Provincia de Chiclayo, Departamento de Lambayeque. Los interesados en esta investigación son el estudiante de la escuela académica de ingeniería de sistemas Denys Ivan Capuñay Puican, y el asesor Ing. Juan Elías Villegas Cubas; logrando así desarrollar este proyecto en un periodo de 10 meses.

### 1.4. Justificación e importancia

#### Justificación Tecnológica

Esta investigación que se realizó es relevante en lo tecnológico porque aborda una temática de tendencia y de cómo nos conectamos hoy en día a un medio tan inseguro como el internet, que resulta ser un tema de investigación constante debido a las nuevas tecnologías que aparecen constantemente.

#### Justificación Social

En la actualidad la comunicación por internet se ha vuelto un tema globalizado, donde muchos convenios, acuerdos y reuniones se dan constantemente vía internet. Esta propuesta trata de ayudar a la sociedad a seguir obteniendo mejores herramientas que garanticen la seguridad, integridad y privacidad de una reunión.

#### Justificación Económica

En lo económico esta propuesta intenta ayudar a reducir el uso de recursos computacionales, reducir el tiempo de cifrado y descifrado de un paquete, etc.

## 1.5. Limitaciones de la Investigación

La investigación que desarrollé no alcanzo el tiempo para implementar varios prototipos de red privada virtual (VPN).

## 1.6. Objetivos de la Investigación

### 1.6.1. Objetivo general

Analizar comparativamente los algoritmos criptográficos existentes para redes privadas virtuales.

### 1.6.2. Objetivos específicos

- a) Seleccionar algoritmos criptográficos para redes privadas virtuales.
- b) Implementar Redes Privadas Virtuales usando IPSec con diferentes algoritmos.
- c) Capturar tráfico de voz, video y datos en los escenarios de la red privada virtual implementada.
- d) Evaluar cuantitativamente los algoritmos implementados en la VPN.



## CAPÍTULO II: MARCO TEÓRICO

## 2. Marco Teórico

### 2.1. A Nivel Internacional

La seguridad es uno de los factores fundamentales y de éxito en la utilización de algoritmos de encriptación, garantiza en todo momento que las comunicaciones sean fiables. Esta hace uso de métodos de autenticación e implementación de VPNs, asegurando que sólo los usuarios autorizados accedan a la VPN de la organización y puedan tener acceso a esta.

Gonzales (2013) en su trabajo de investigación Métodos de encriptación para redes privadas virtuales. El objetivo fue verificar la seguridad de un equipo cuando se conecta de forma remota y las políticas de seguridad adecuadas para que la información no quede expuesta a posibles ataques. En este estudio el autor en mención manifestó que para la implementación de una VPN, existen aspectos fundamentales que deben considerarse: costo, desempeño, confianza y seguridad. De estas características, la seguridad es la más primordial, sin la existencia de esta característica las otras resultan ser improductivos; puesto que no importa qué tan barata, rápida y confiable sea una red, sin la seguridad adecuada, los riesgos causaran la inestabilidad de la red. En adición a los riesgos de seguridad, hay aspectos de Calidad en el Servicio (QoS) concernientes al Internet que se deben de tratar. La calidad en el servicio se refiere al acuerdo de servicio ofrecido por un Proveedor de Servicios de Internet (ISP) a un cliente, que garantiza cierto nivel de desempeño. Se logró investigar que con el uso de protocolos de encriptación, la información que atraviesa Internet lo hace de forma cifrada, de modo que sólo el destinatario seleccionado será capaz de leer la misma. Incluso en el caso de escuchas no permitidas, no será posible la

recuperación de la información original de forma legible sin conocer las claves que sólo los interlocutores legítimos poseen.

Aquí podemos percibir que la criptografía juega un papel importante en un entorno distribuido y abierto como es el internet. Pues la resistencia de la criptografía a los ataques está basada en la dificultad calculatoria de ciertos problemas matemáticos, o en la extrema confusión y dispersión aplicada a la información.

Alvarado (2010) en su trabajo de investigación Estudio comparativo de los mecanismos de seguridad de los protocolos para VPNs. El objetivo principal fue analizar el funcionamiento de los principales protocolos que hacen posible la creación de túneles dentro de una infraestructura pública, llamados accesos VPN. En este estudio el autor en mención investiga acerca de los métodos de seguridad de transporte y control de acceso en medios de difusión pública como Internet. Se da especial énfasis en este trabajo al protocolo de seguridad sobre IP llamado IPSec, el cual reúne la mayoría de las características que hacen que un modelo sea seguro sobre un medio masivo como lo es la Internet. Se estudian además las diferentes formas de implementación de esta alternativa, considerándose de gran seguridad la basada en Firewall, la cual contempla la solución IPSec a los problemas antes mencionados. Y por último se presenta una aplicación a nivel de Cliente VPN, donde el otro extremo basado en Firewall se configura como servidor IPSec VPN de acceso. Se logró investigar que los protocolos que componen las funciones VPN estudiados, ofrecen cada uno diferentes normas de operación, con niveles diferentes tanto en seguridad como en compatibilidad de sistema y entorno. Siendo el más destacable y además

confiable para ser utilizado el protocolo IPSec, el cual se puede implementar en medios IP públicos como lo es la Internet, así se puede realizar una transmisión privada y por ende segura entre dos puntos separados remotamente e sin perder la confiabilidad de un enlace punto a punto.

Aquí posemos apreciar que hay diversos esquemas de implementación de VPN, los cuales varían según tamaño de la red corporativa y seguridad que requiera para sus servidores. Estos pueden estar basados en hardware o software, siendo estos últimos más efectivos al momento de efectuar procesos de autenticación y encriptación, debido a que no adhieren sobrepeso a los servidores dedicados a los enrutamientos dentro de la propia red local, agilizando el trabajo dentro de esta. Además que manejar parámetros bastante potentes de seguridad que sería poco probable implementar como software.

Quizhpe (2011) en su trabajo de investigación Soluciones de Cifrados a las Seguridades Informáticas en Procesos de Auditaje Organizacional. Tiene como objetivo principal Realizar un estudio comparativo de soluciones de cifrados a las seguridades informáticas para ser utilizadas en los procesos de Auditaje Organizacional. En este estudio el autor en mención realizo el estudio comparativo de las Soluciones de Cifrados a las Seguridades Informáticas para dar a conocer de una manera clara los diferentes maneras de resguardar la información utilizando los diferentes tipos de cifrados que tenemos para encriptar la información, sobre todo las contraseñas de los usuarios lo que nos va a servir para tener protegidos nuestros equipos y también se realizó este estudio para que toda persona que se interese en este tema aprenda en forma rápida y simple a valorar lo importante que es



la información, tanto para las grandes como pequeñas y medianas empresas y contar con sistemas de seguridad que alejen visitas de posibles hackers. Es importante recordar que es muy fácil poder encriptar nuestras contraseñas utilizando los software que los encontramos en el Internet gratuitamente, lo cual nos es una herramienta muy eficaz para poder mantener segura la Información.

En este trabajo de investigación podemos apreciar que realiza un estudio comparativo de los diferentes tipos de cifrados para determinar cuál es el más conveniente para la utilización en las organizaciones, proponiendo el cifrado más confiable para asegurar la información de las organizaciones.

Moya (2015) en su trabajo de investigación Desarrollo de una aplicación para encriptar información en la transmisión de datos en un aplicativo de mensajería web. Tiene como objetivo principal el desarrollo de una aplicación para encriptar datos en web. En este estudio el autor en mención aplica todas las herramientas investigadas durante el desarrollo de este trabajo, utiliza metodologías conocidas como el método de SCRUM ya que con este los entregables son pequeños y se pueden revisar periódicamente, haciendo más efectiva la identificación de errores y cambios, además de que Scrum se enfoca en la entrega de productos y no tanto en la calidad del código como Xtreme Programming, como no se va a hacer algo que parta desde cero y más bien se va a adaptarlo a nuestras preferencias además se va a reutilizar herramientas ya existentes en caso de necesitarlas. Para el desarrollo iremos probando herramientas como Dreamweaver, PHP, HTML, Visual Studio, ASP. NET y gestores de bases de datos como MySQL, Microsoft SQL Server, PostgreSQL que nos permiten realizar cambios hasta

poder obtener nuestro objetivo final para nuestra disertación.

En esta investigación se hace para tener un claro ejemplo de la vulnerabilidad en la información de hoy en día. Por lo que en los últimos años ha adquirido un auge el estudio e implementación de diferentes modelos de encriptación para asegurar la confidencialidad en el intercambio de información. La investigación trata de abordar la protección desde un punto de vista que proporcione información sobre el funcionamiento de algunos algoritmos de cifrado.

## 2.2. Estado del Arte

Muhammad (2015) en su trabajo de investigación Concepción de redes privadas virtuales mediante IPsec conjunto de protocolos, análisis comparativo de consultas de bases de datos distribuidas utilizando diferentes modos de cifrado IPsec. Enfrento problemas como Encontrar soluciones fiables para protegerse de las actividades que desconfiadas y por la ciberdelincuencia. Lo que logró fue Presentar una extensión de una red privada virtual hecha a través de características adicionales como encapsular los paquetes de datos con una cabecera en ambos extremos, a lo largo de las líneas de la comunicación, así como a través de túneles de comunicación. Lo hizo ofreciendo un conjunto de túneles de comunicación de datos seguras simuladas junto con una comparación de los resultados de las variables de la velocidad medidos en contra de la seguridad a través de diferentes protocolos de cifrado entre LAN remota. Sus resultados fueron la Prestación de un servicio rápido, eficiente y al mismo tiempo el medio ambiente de trabajo seguro mediante la protección de sus activos de la organización.



Pandillas (2011) en su trabajo de investigación sobre el Sistema Red VPN utilizando el protocolo IPSec. Enfrento un problema como los Mecanismo de comunicación pocos seguros y poco fiables, con costos considerablemente líneas arrendadas. Lo que hizo fue Estudiar el método de construcción de túneles en el sistema de IPSec. El protocolo IPSec lo estudia y pone en práctica, y analiza la seguridad en redes VPN haciendo grandes avances. Propuso usar una red VPN por las características en cuanto a su seguridad de, Construye túneles usando el sistema de IPSec. Los resultados que obtuvo fueron Mecanismo de comunicación segura y fiable, reduciendo considerablemente el costo de líneas arrendadas.

Simion (2013) en su trabajo de investigación Consideración de eficiencia para los paquetes de datos de cifrado dentro de VPN inalámbrico de túnel para Video Streaming. Enfrento un problema como El acceso a los diferentes datos está disponible para los usuarios legítimos, así como para los ilegítimos, por esta razón que necesita de la seguridad de datos adicional. Lo que hizo fue Presentar una solución para la calidad de servicio y confidencialidad de los datos es Virtual Private Network (VPN); maneras, en el que podemos reducir los costos operativos, aumentar la productividad, simplificar la topología de red y ampliar el área de conectividad. Esto se hizo con un análisis de los diferentes protocolos utilizados y la forma en que los paquetes de datos de vídeo se encapsulan y se cifran para un alto nivel de calidad de servicio en una conexión VPN. Obteniendo como resultado reducción de los costos operativos, aumentar la productividad, simplificar la topología de red y ampliar el área de conectividad.



Xenakis (2010) en su trabajo de investigación Una caracterización genérica de los gastos generales impuestas por IPsec y algoritmos criptográficos asociados. Enfrento problemas como el Alto impacto en términos de calidad de la comunicación (retardo añadido para el usuario final) y el consumo de recursos (ancho de banda adicional en la interfaz de radio). Lo que hizo fue Presentar una evaluación de los gastos generales de comunicación de IPsec y evalúa la viabilidad de la implementación en dispositivos de mano para la arquitectura UMTS. Considerando algoritmos criptográficos. Esto se desarrolló llevando a cabo un análisis cuantitativo basado en un modelo de simulación detallada de un dispositivo de mano permitido IPsec. Verificando resultados de la simulación mediante la comparación contra los resultados analíticos obtenidos de un modelo analítico aproximada. Obteniendo nuevas consideraciones en el procesamiento y paquetización de los gastos generales introducidas por estos algoritmos y cuantificación de su impacto en términos de calidad de la comunicación.

Tzon-Sun (2014) en su trabajo de investigación Proxy demostrablemente seguro convertible esquema de cifrado basado en RSA autenticada. Enfrenta un problema de como demostrar un diseño de esquemas criptográficos eficientes y demostrablemente seguros que cumplan con los requisitos de firmante original sea propietario de las claves de firma de proxy y así puede crear firmas proxy anteriores esto es crucial y beneficioso para implementaciones prácticas. El autor Presenta el esquema proxy CAE propuesto basado en RSA suposición. El esquema se puede dividir en cuatro fases: configuración del sistema, generación de credencial de delegado (PCG), proxy autenticado generación texto cifrado (PACG), y





recuperación firma proxy y verificación (PSRV) fases. Lo hace calculando la clave de firma proxy a partir de la clave privada del firmante original basado en algunos supuestos criptográficos intratables tales como problemas de logaritmos discretos. Es computacionalmente imposible para cualquier adversario para deducir la clave privada del firmante original de una clave de firma de proxy dado. Obteniendo como resultado el esquema de CAE de proxy cumple con el requisito de seguridad de la confidencialidad del mensaje si el proxy autenticado texto cifrado generado es computacionalmente indistinguibles con respecto a dos textos planos candidatos

## 2.3. Bases teórico científicas

### 2.3.1. Algoritmo

Vancells (2002) define al algoritmo como “Procedimiento de calculo que consiste en cumplir una serie o conjunto ordenado y finito de instrucciones que conducen, una vez especificados los datos, a la solución que el problema genérico en cuestión tiene para los datos considerados” (pag. 7).

Martínez (2003) refirió “el concepto de algoritmo como un conjunto finito de procesos a su vez finitos y bien definidos que conducen a un resultado” (pag. 41).

Diccionario de la Real Academia Española - DRAE (2015) define que es un “Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema”.

Podemos decir que un algoritmo es una serie de reglas o pasos para solucionar un problema en específico.

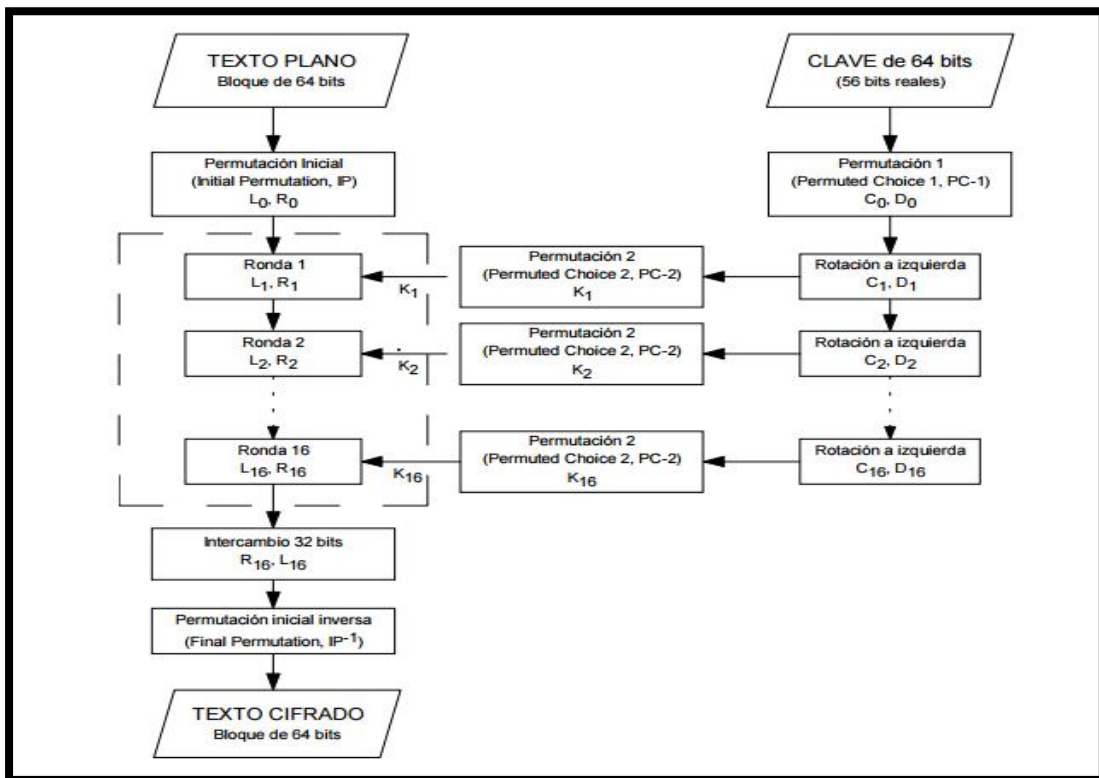


### 2.3.2. Algoritmo Data Encryption Stándar (DES)

DES es un algoritmo desarrollado originalmente por IBM a requerimiento del NBS (Oficina Nacional de Estandarización, en la actualidad denominado NIST, Instituto Nacional de Estandarización y Tecnología) de EE.UU. Trabajaba sobre bloques de 128 bits, teniendo la clave igual longitud. Se basaba en operaciones lógicas booleanas y podía ser implementado fácilmente, tanto en software como en hardware.

Tras las modificaciones introducidas por el NBS, consistentes básicamente en la reducción de la longitud de clave y de los bloques, DES cifra bloques de 64 bits, mediante permutación y sustitución y usando una clave de 64 bits, de los que 8 son de paridad (esto es, en realidad usa 56 bits), produciendo así 64 bits cifrados.

Figura 1 - Esquema general del algoritmo DES



Fuente: Jean-Marc R. (2004). Seguridad en la informática de empresas.

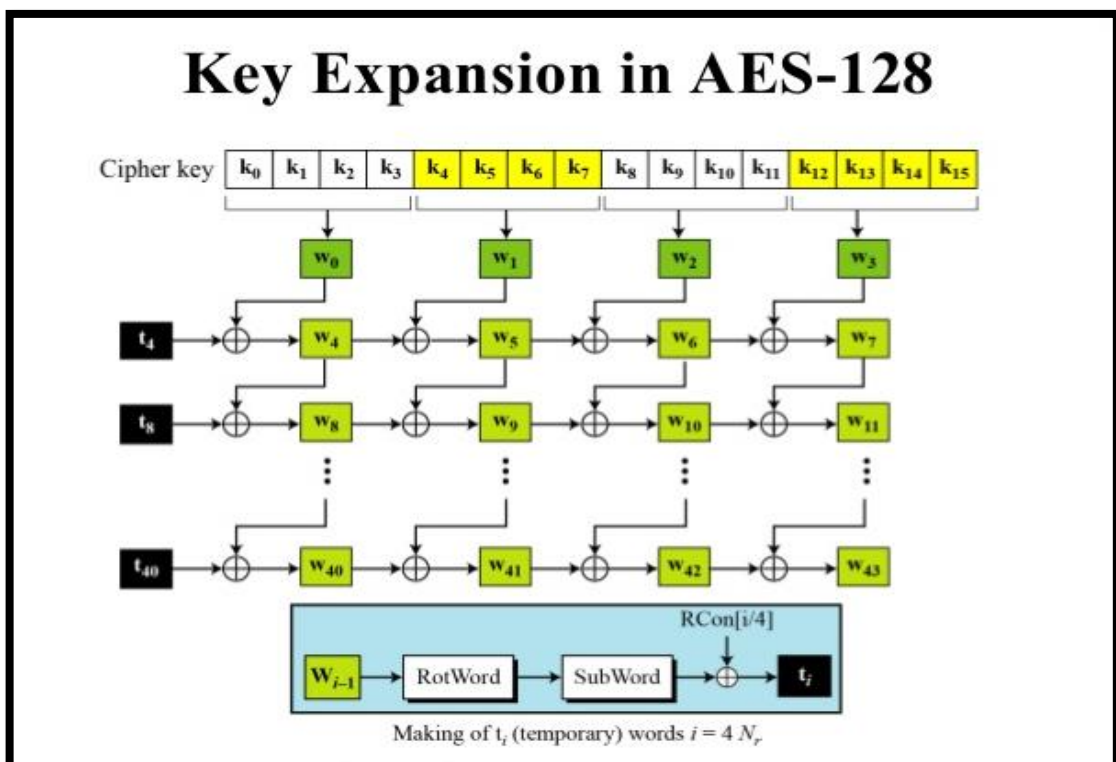


### 2.3.3. Algoritmo Advanced Encryption Standard (AES)

Este algoritmo es el más conocido entre los usuarios de routers, ya que WPA opera con AES como método de cifrado; este cifrado puede implementar tanto en sistemas hardware como en software. El sistema criptográfico AES opera con bloques y claves de longitudes variable, hay AES de 128bits, de 192 bits y de 256 bits.

El resultado intermedio del cifrado constituye una matriz de bytes de cuatro filas por cuatro columnas. A esta matriz se le vuelve a aplicar una serie de bucles de cifrado basado en operaciones matemáticas (sustituciones no lineales de bytes, desplazamiento de filas de la matriz, combinaciones de las columnas mediante multiplicaciones lógicas y sumas XOR en base a claves intermedias).

Figura 2- Esquema del algoritmo de AES



Fuente: Jean-Marc R. (2004). Seguridad en la informática de empresas.



## PUNTOS IMPORTANTES EN LA HISTORIA DE AES

- En el año 1997, el Instituto Nacional de Estándares y Tecnología de EEUU (NIST), emprende un proceso abierto para la selección de un nuevo algoritmo de cifrado.
- Los criterios de evaluación y requisitos mínimos que debían cumplir todos los algoritmos: El algoritmo debe ser público, debe ser un algoritmo de cifrado en bloque simétrico, la longitud de la clave debe ser como mínimo 128 bits, su diseño debe permitir aumentar la longitud de la clave según las necesidades, debe ser implementable tanto en HW como en SW.
- Durante todo el desarrollo del proceso AES, todos los algoritmos y criterios de diseño estuvieron disponibles de forma pública y abierta.
- En Agosto de 1998 comenzó la primera ronda aceptándose quince candidatos durante la *“Primera Conferencia de candidatos a AES”*.
- En Marzo de 1999, se celebraría la segunda conferencia de Candidatos a AES, en la que se discutió los resultados de las numerosas pruebas y criptoanálisis realizados a los quince candidatos iniciales. Quedando solo 5 algoritmos: MARS, RC6, RIJNDAEL, SERPENT, TWOFISH.
- En abril del 2000 se celebró la *“Tercera Conferencia de Candidatos AES”* en Nueva York.
- El 2 de octubre de 2000, el NIST anunció el algoritmo ganador: RIJNDAEL con 86 votos.

#### 2.3.4. Criptografía

Silva (2005) se refiere “Como una rama de las matemáticas que estudia la transformación legible en información que se puede leer directamente, sino que debe descifrarse antes de ser leída” (pag.8).

Evaristo (1999) la define como “la acción de reescribir un texto para que sólo personas autorizadas por el autor del texto puedan descifrarla. “ (s.p)

Diccionario de la Real Academia Española - DRAE (2015) define como el “Arte de escribir con clave secreta o de un modo enigmático.”

Definiremos a la criptografía como una técnica matemática para cifrar o descifrar mensajes, de manera que nadie pueda ver el mensaje sin tener las claves para cifrado o descifrado.

#### 2.3.5. Redes Privadas Virtuales

Cobo (2009) la define como “una extensión de una red privada que utiliza enlaces a través de redes públicas o compartidas como internet y que posibilita la transmisión de datos como si de un enlace punto a punto se tratase.”(Pag. 179)

Cisco (2015) refiere “Una red privada virtual (VPN) es una red privada construida dentro de una infraestructura de red pública, tal como la red mundial de Internet.”

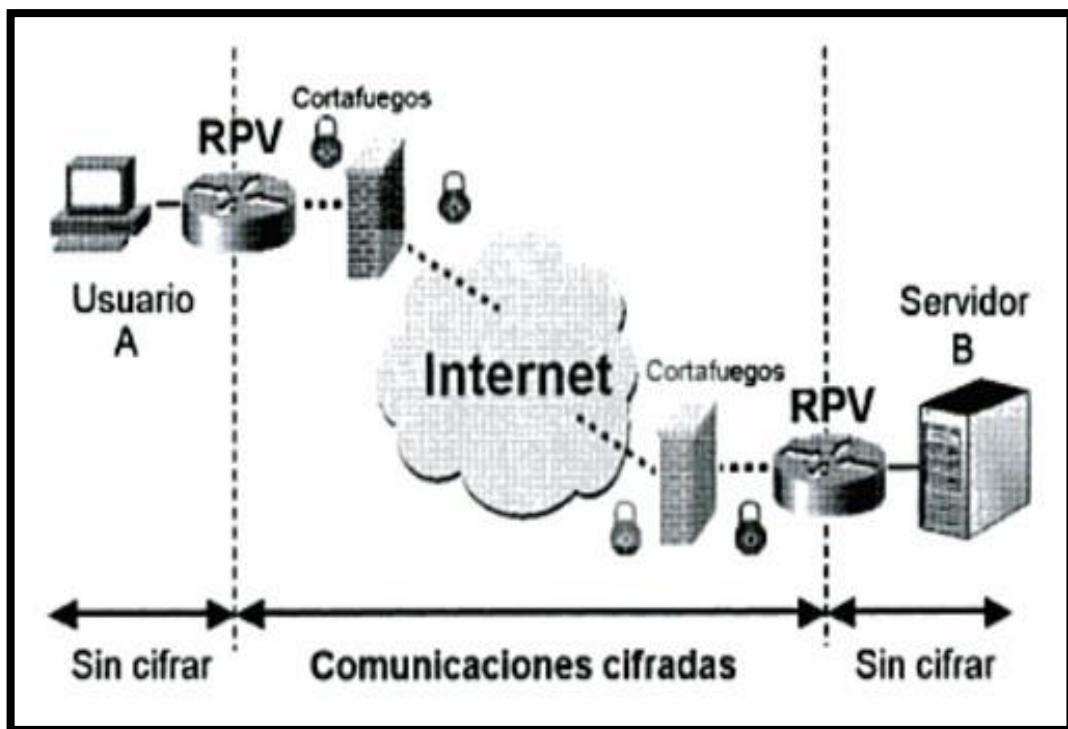
Una Red Privada Virtual (llamada RPV o. en inglés, VPN para Virtual Private Network) es un canal seguro entre dos redes.

Una vez implementada, todos los datos que lo atraviesan se cifran, por lo que pueden transitar con bajo peligro por conexiones de red potencialmente arriesgadas como Internet.



En la Figura 3, Imaginemos un usuario (A) que se encuentra en el interior de una filial situada en Ciudad1, que desea conectarse a un servidor (B) situado en la sede social de la empresa en Ciudad2. Para ello, deberá comunicarse a través de Internet pero, anteriormente, atravesará el servidor VPN (A) que cifrará los datos. A la llegada, el VPN (B) descifrará los datos que se transmitirán sin cifrar al servidor.

*Figura 3 - Red Privada Virtual*



**Fuente:** Jean-Marc R. (2004). *Seguridad en la informática de empresas*.

La operación es transparente, tanto para el usuario A como para el servidor B. No es necesaria ninguna otra configuración en ninguna de las dos máquinas.

La VPN permite cifrar de manera global todas las comunicaciones que circulan entre el usuario y el servidor, independientemente del protocolo

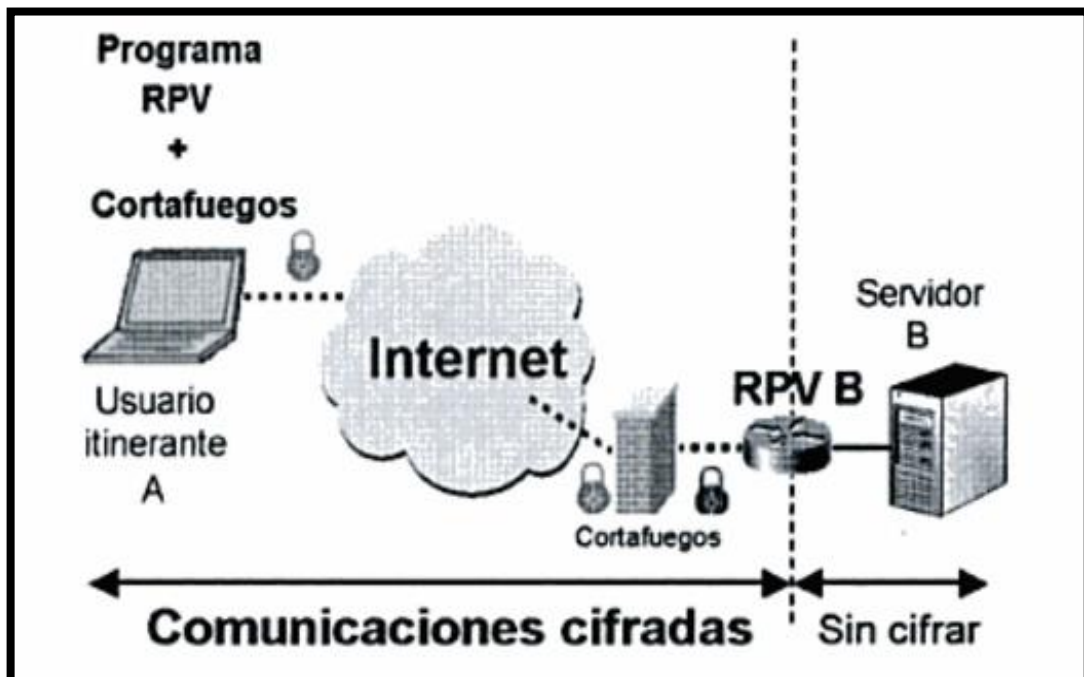
utilizado (Web, mail, ftp, etc.).

Así, implementando una VPN en el interior de una empresa, se tiene la posibilidad en una sola operación de asegurar la confidencialidad de todas las comunicaciones que circulan entre los dos sitios.

La implementación de una VPN también se adapta a muchos otros casos. Citemos, por ejemplo, el caso en que algunos usuarios, comerciales itinerantes, tengan necesidad de acceder desde el exterior a datos que se encuentran en servidores internos a la empresa.

Disponen de ordenadores portátiles y llaman con un módem conectado a Internet. Así es posible proteger su conexión instalando, en cada portátil, un programa que haga tanto de cortafuegos como de VPN. Todas las comunicaciones salientes del portátil serán cifradas por la VPN del usuario y luego descifradas por la de la empresa.

*Figura 4 - Red Privada Virtual –Conexión desde internet*



*Fuente: Jean-Marc R. (2004). Seguridad en la informática de empresas.*

Prestar atención a configurar el cortafuego y las aplicaciones del servidor de modo que limiten el acceso de los usuarios itinerantes sólo a los datos que les son indispensables.

No olvide que es totalmente posible que se les robe el portátil a algunos usuarios. En ese caso, el ladrón dispondría de un medio externo de acceso a la red de su empresa. Con la misma intención, también se recomienda vigilar que todos los portátiles estén protegidos por una contraseña a nivel de la BIOS de la máquina y, si es posible, que los discos duros de los portátiles estén a su vez cifrados.

La ventaja de esta solución es que el acceso a la red está íntimamente ligado al uso del programa VPN. Además del cifrado de los datos, este programa también puede permitir autenticar al usuario. Ya no hay ninguna contraseña que pueda ser interceptada por un tercero. Para utilizar la VPN y conectarse a la red de la empresa, debe disponer físicamente del ordenador portátil en el que ha sido instalado el programa VPN.

### **2.3.6. Internet Protocol Security (IPSec)**

Stewart (2010) se refiere como “conjunto de protocolos basados en estándares diseñados específicamente para asegurar las comunicaciones de protocolo de Internet (IP). IPSec autentica y encripta cada paquete IP de un flujo de datos IP. IPSec tiene protocolos que pueden establecer la autenticación mutua y la negociación de claves criptográficas durante una sesión” (pag. 351).

Mathon (2001) define como “un protocolo que permite asegurar una cierta protección de los datos IP y, por tanto, protegerse de posibles ataques





(análisis del tráfico por analizador de trama, modificación de los datos). Se trata de un protocolo estandarizado por el IETF cuya definición se encuentra en varias RFC, entre las que encontramos las RFC 2401, 2402, 2406, 2408” (pag. 288).

Cisco (2015) describe que IPsec es un marco de estándares abiertos que detalla las reglas para las comunicaciones seguras. IPsec no se limita a ningún tipo específico de cifrado, autenticación, algoritmo de seguridad ni tecnología de creación de claves. En realidad, IPsec depende de algoritmos existentes para implementar comunicaciones seguras. IPsec permite que se implementen nuevos y mejores algoritmos sin modificar los estándares existentes de IPsec.

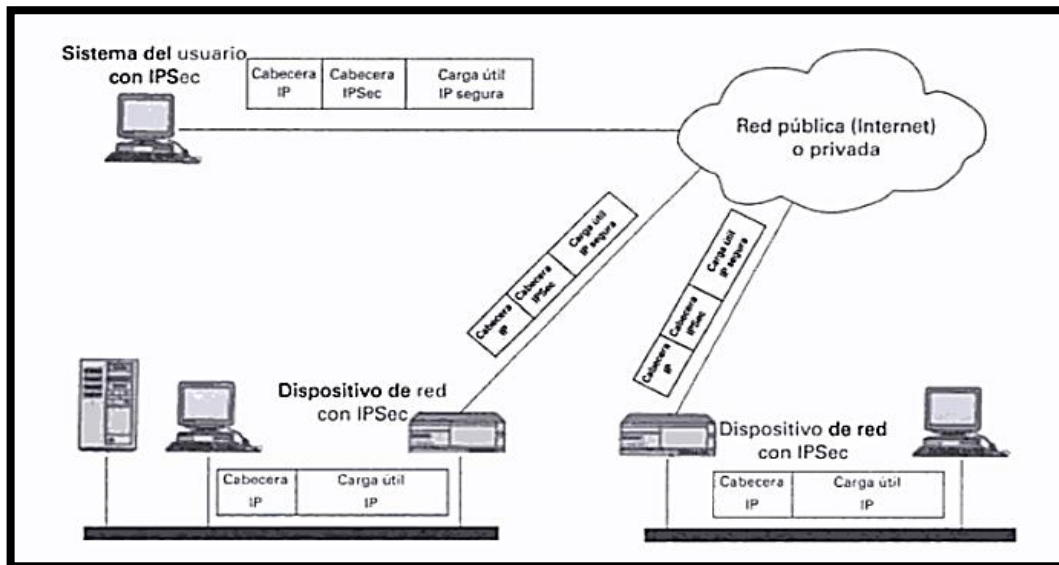
Además refiere que IPsec funciona en la capa de red, por lo que protege y autentica los paquetes IP entre los dispositivos IPsec participantes, también conocidos como “peers”. IPsec protege una ruta entre un par de gateways, un par de hosts o un gateway y un host. Como resultado, IPsec puede proteger prácticamente todo el tráfico de una aplicación, dado que la protección se puede implementar desde la capa 4 hasta la capa 7.

Todas las implementaciones de IPsec tienen un encabezado de capa 3 de texto no cifrado, de modo que no hay problemas de routing. IPsec funciona en todos los protocolos de capa 2, como Ethernet, ATM o Frame Relay.

La característica principal de IPsec que permite dar soporte a esta variedad de aplicaciones es que puede cifrar y/o autenticar todo el tráfico en el nivel IP. Por lo tanto, pueden asegurarse todas las aplicaciones distribuidas,

incluyendo conexión remota, cliente/servidor, correo electrónico, transferencia de ficheros, acceso a la web. etc.

**Figura 5 - Entorno de Seguridad IP**



**Fuente:** Stallings WR. (2004). *Fundamentos de seguridad en redes*

En la figura 5 representa un ejemplo común del uso de IPsec. Una organización tiene algunas LAN en lugares dispersos. En cada LAN hay tráfico IP que no es seguro. Los protocolos IPsec se utilizan para el tráfico exterior, a través de una WAN privada o pública. Estos protocolos operan en dispositivos de red, como por ejemplo un router o un cortafuego, que conecta cada LAN al mundo exterior.

El dispositivo de red IPsec cifrará y comprimirá todo el tráfico que entre en la WAN, y descifrará y descomprimirá todo el tráfico que provenga de ella; estas operaciones son transparentes a las estaciones de trabajo y a los

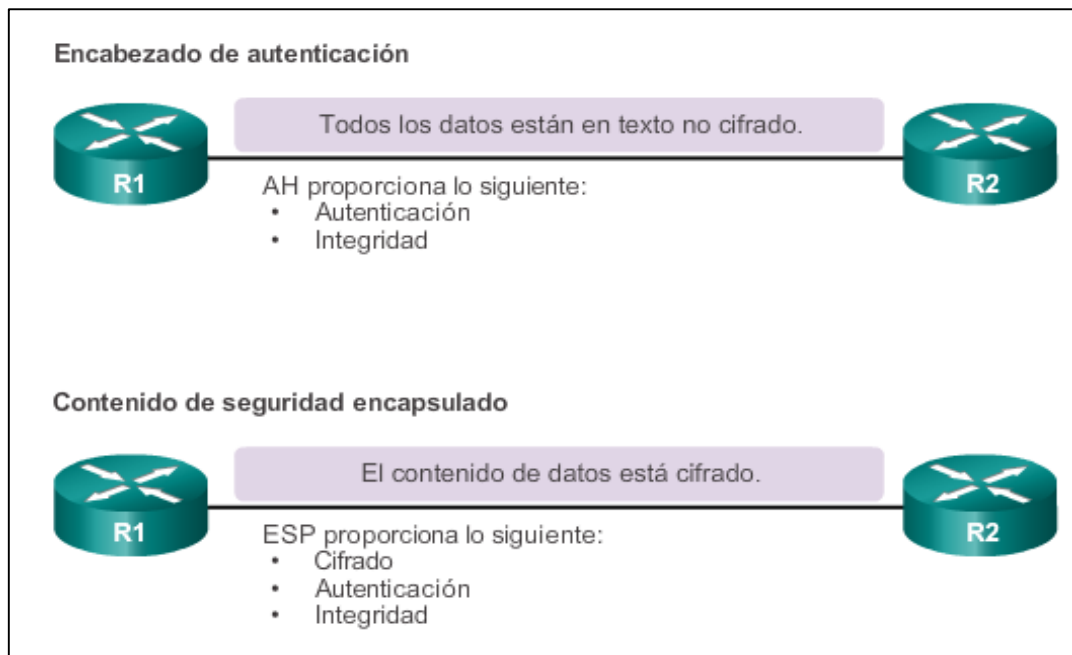


servidores en la LAN. También es posible la transmisión segura con usuarios individuales que se conectan a la WAN. Dichas estaciones de trabajo de usuarios deben implementar los protocolos IPSec para proporcionar seguridad.

**MARCO DEL PROTOCOLO IPSEC**

Cisco CCNA se refiere que el marco del protocolo IPSec describe la mensajería para proteger las comunicaciones, pero depende de los algoritmos existentes.

*Figura 6 – Marco de IPSEC*



**Fuente:** Cisco (2015). CCNA 4 v5.2

En la figura 6, se describen dos protocolos IPSec principales:

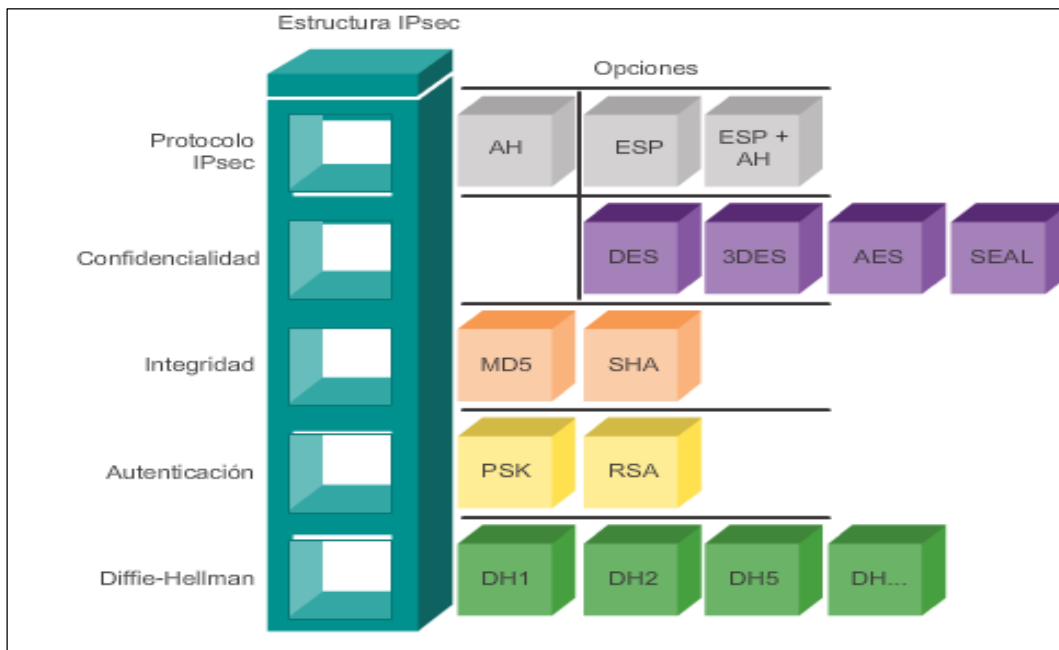
- **Encabezado de autenticación (AH):** AH es el protocolo que se debe utilizar cuando no se requiere o no se permite la confidencialidad. Proporciona la autenticación y la integridad de datos para los paquetes IP que se transmiten entre dos sistemas. Sin embargo, AH no proporciona la confidencialidad (el cifrado) de datos de los paquetes. Todo el texto se



transporta como texto no cifrado. Cuando se utiliza solo, el protocolo AH proporciona una protección poco eficaz.

- **Contenido de seguridad encapsulado (ESP):** es un protocolo de seguridad que proporciona confidencialidad y autenticación mediante el cifrado del paquete IP. El cifrado de paquetes IP oculta los datos y las identidades del origen y el destino. ESP autentica el paquete IP y el encabezado ESP internos. La autenticación proporciona la autenticación del origen de los datos y la integridad de los datos. Si bien el cifrado y la autenticación son optativos en ESP, se debe seleccionar, como mínimo, uno de ellos.

Figura 7 - Marco de IPsec



Fuente: Cisco (2015). CCNA 4 v5.2

En la figura 7, se muestran los componentes de la configuración de IPsec. Se deben seleccionar cuatro componentes básicos del marco de IPsec.

- **Protocolo del marco de IPsec:** al configurar un gateway IPsec para proporcionar servicios de seguridad, se debe seleccionar un protocolo



IPsec. Las opciones son una combinación de ESP y AH. En realidad, las opciones de ESP o ESP+AH casi siempre se seleccionan porque AH en sí mismo no proporciona el cifrado.

- **Confidencialidad (si se implementa IPsec con ESP):** el algoritmo de cifrado elegido se debe ajustar al nivel deseado de seguridad (DES, 3DES o AES).
- **Integridad:** garantiza que el contenido no se haya alterado en tránsito. Se implementa mediante el uso de algoritmos de hash. Entre las opciones se incluye MD5 y SHA.
- **Autenticación:** representa la forma en que se autentican los dispositivos en cualquiera de los extremos del túnel VPN. Los dos métodos son PSK o RSA.
- **Grupo de algoritmos DH:** representa la forma en que se establece una clave secreta compartida entre los peers. Existen varias opciones, pero DH24 proporciona la mayor seguridad.

La combinación de estos componentes es la que proporciona las opciones de confidencialidad, integridad y autenticación para las VPN con IPsec.

## SERVICIOS DE IPSEC

Cisco (2015) refiere que los servicios de seguridad IPsec proporcionan cuatro funciones fundamentales, las cuales se muestran en la ilustración:

- **Confidencialidad (cifrado):** en una implementación de VPN, los datos privados se transfieren a través de una red pública. Por este motivo, la confidencialidad de los datos es fundamental. Esto se puede lograr



mediante el cifrado de los datos antes de transmitirlos a través de la red. Este es el proceso de tomar todos los datos que una computadora envía a otra y codificarlos de una manera que solo la otra computadora pueda decodificar. Si se intercepta la comunicación, el pirata informático no puede leer los datos. IPsec proporciona características de seguridad mejoradas, como algoritmos de cifrado seguros.

- Integridad de datos: el receptor puede verificar que los datos se hayan transmitido a través de Internet sin sufrir ningún tipo de modificaciones ni alteraciones. Si bien es importante que los datos a través de una red pública estén cifrados, también es importante verificar que no se hayan modificado cuando estaban en tránsito. IPsec cuenta con un mecanismo para asegurarse de que la porción cifrada del paquete, o todo el encabezado y la porción de datos del paquete, no se haya modificado. IPsec asegura la integridad de los datos mediante checksums, que es una comprobación de redundancia simple. Si se detecta una alteración, el paquete se descarta.
- Autenticación: verifica la identidad del origen de los datos que se envían. Esto es necesario para la protección contra distintos ataques que dependen de la suplantación de identidad del emisor. La autenticación asegura que se cree una conexión con el compañero de comunicación deseado. El receptor puede autenticar el origen del paquete mediante la certificación del origen de la información. IPsec utiliza el intercambio de claves de Internet (IKE) para autenticar a los usuarios y dispositivos que pueden llevar a cabo la comunicación de manera independiente. IKE utiliza varios tipos de autenticación, por ejemplo, nombre de usuario y

contraseña, contraseña por única vez, biometría, clave previamente compartida (PSK) y certificados digitales.

- Protección antirreproducción: es la capacidad de detectar y rechazar los paquetes reproducidos, y ayuda a prevenir la suplantación de identidad. La protección antirreproducción verifica que cada paquete sea único y no esté duplicado. Los paquetes IPsec se protegen mediante la comparación del número de secuencia de los paquetes recibidos con una ventana deslizante en el host de destino o el gateway de seguridad. Se considera que un paquete que tiene un número de secuencia anterior a la ventana deslizante tiene un retraso o está duplicado. Los paquetes duplicados y con retraso se descartan.

### **2.3.7. IKE (Intercambio de claves de Internet):**

Cisco (2015) Protocolo híbrido que utiliza una parte del protocolo Oakley y otra parte de un conjunto de protocolos llamado SKEME en el marco de la Asociación de seguridad en Internet y el Protocolo de administración de claves (ISAKMP). IKE (Internet Key Exchange) se utiliza para establecer una política de seguridad compartida y las claves autenticadas para los servicios (como IPSec) que requieren una clave. Antes de que se pueda transmitir cualquier tráfico de IPSec, cada router, firewall o host debe ser capaz de identificar la identidad de su par: es posible realizarlo manualmente introduciendo claves previamente compartidas en ambos hosts, por un servicio de CA, o el próximo DNS seguro (DNSSec). Este es el protocolo que antiguamente se conocía como ISAKMP/Oakley, y se define en RFC 2409: Intercambio de claves de Internet (IKE). Un punto de confusión importante

es que ambos acrónimos, "ISAKMP" e "IKE", se utilizan en el software Cisco IOS para referirse al mismo concepto. Sin embargo, estos dos elementos son algo diferentes.

### **2.3.8. ISAKMP**

Cisco (2015) Asociación de seguridad en Internet y Protocolo de administración de claves. Estructura de protocolo que define el mecanismo de implementación de un protocolo de intercambio de claves y la negociación de las políticas de seguridad. ISAKMP (Internet Security Association and Key Management) se define en la Asociación de seguridad en Internet y el Protocolo de administración de claves.

Las conexiones IPsec se forman en dos etapas. ISAMPK fase 1 y fase 2.

#### **ISAKMP/IKE - Fase 1**

Durante la primera fase se establece una conexión segura llamada conexión de control que se usa para negociar los parámetros requeridos para establecer la segunda fase de la conexión. Esta primera conexión utiliza el protocolo UDP con puerto destino 500. Durante esta fase el dispositivo que inicia el proceso envía sus pólizas ISAKMP. Una póliza ISAKMP es una lista que contiene diversas opciones que se utilizarán a la hora de asegurar la conexión:

- Grupo de DH: Se especifica que grupo se usara para realizar el intercambio de claves.
- Método de autenticación: Los dispositivos pueden autenticarse de tres





maneras: Con certificados, Claves simétricas o utilizando RSA encrypted nonce.

- Encriptación: Los métodos de encriptación posibles son: DES, 3DES. AES
- Función H-MAC: Eliges que función se usa para validar la integridad de los paquetes. Las opciones son MD5 y SH1.

El receptor de la sesión va comparando la primera opción propuesta por el iniciador con todas las opciones posibles que él tiene configuradas en sus pólizas ISAKMP. Si no ha encontrado una igualdad, el receptor comparará su opción dos con todas las opciones que tiene configuradas el iniciador, y así sucesivamente. Para que la conexión sea posible los dos dispositivos tienen que coincidir en todas las opciones de al menos una de sus pólizas ISAKMP.

Existen dos maneras en las que los dispositivos pueden construir las conexiones de control:

- Main mode: Se realiza en tres pasos. Primero los dispositivos acuerdan como van a proteger la conexión intercambiando sus pólizas. Después ejecutan el algoritmo DII acordado anteriormente para intercambiar las claves simétricas que se usaran en las funciones H-MAC y de encriptación acordadas anteriormente. Por último los dispositivos se autentican.
- Agresivo mode: Se realiza en dos pasos. El iniciador envía al receptor su identidad, su lista de pólizas ISAKMP, la clave pública para realizar DH, su certificado o método de autenticación. Después el receptor le contesta diciendo si la conexión es posible o no.
- Este método es más rápido pero menos seguro debido que la información relativa a la identidad de la entidad viaja sin ser protegida.



En resumen, el proceso para conexiones Site-to-Site (L2L) main mode es el siguiente:

- Un dispositivo iniciador envía un paquete UDP con puerto destino 500 al receptor solicitando establecer una conexión segura de control.
- Se intercambian las pólizas ISAKMP para acordar como van a proteger la conexión
- Los dispositivos llevan a cabo el algoritmo DH para intercambiar las claves simétricas que usarán en los algoritmos de encriptación y H-MAC
- Si la autenticación se realiza mediante claves simétricas, los dispositivos se identifican para saber que clave simétrica van a utilizar.
- Se autentican usando la clave simétrica u otro medio de autenticación como puede ser usando certificados de identidad.

Las conexiones de acceso remoto pasan por algunos puntos más antes de iniciar la segunda fase:

- Autenticación del usuario (XAUTH): Además de autenticar el dispositivo desde el que se conecta un usuario, este usuario tiene su propia password para poder acceder al sistema.
- Políticas de grupo- Se aplican las políticas específicas para el grupo al que pertenece el usuario. Un ejemplo de estas podría ser especificar que tráfico ha de viajar por el túnel y cual viaja de manera externa a él, que servidores DNS usará el cliente, de que pool de IP's obtendrá la suya. etc.
- Inyección de rutas (RRI): EL cliente puede inyectar su o sus rutas IP al dispositivo al que se conecta (receptor). De esta manera el receptor puede compartir esta información con otros Router de la red para que puedan alcanzar el otro extremo del túnel y por lo tanto al cliente.



## ISAKMP/IKE - Fase 2

Utilizando la existente conexión de control los dispositivos negocian y establecen dos conexiones más, una entrante y otra saliente. Estas conexiones pueden tener las mismas características o no y son las que se utilizan para llevar el tráfico de información que se desea proteger.

La negociación de la seguridad de las conexiones se lleva a cabo mediante el intercambio de los Transform Set. Este concepto es muy similar al de las pólizas ISAKMP que hemos utilizado en la fase 1. En los Transform Set se especifica cómo se va a encriptar el tráfico y como se van a autenticar los paquetes que lo conforman. La encriptación o la autenticación de paquetes son opcionales.

También necesitamos saber que protocolo de transporte de seguridad vamos a utilizar. Las opciones son AH y ESP.

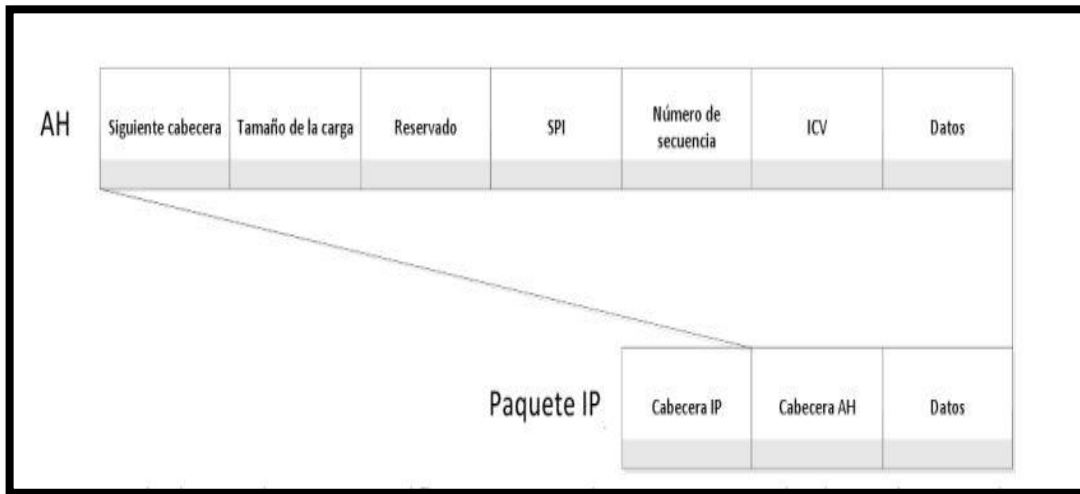
Una vez que sabemos cómo se va a proteger el tráfico necesitamos saber cuál es el tráfico que vamos a proteger y que modo de encapsulación vamos a usar, túnel o transporte.

La selección del tráfico lo hacemos mediante las Crypto ACL's. Todo el tráfico que cumpla las condiciones citadas en una Crypto ACL será encriptado y o autenticado por IPsec.

- Protocolos de seguridad: Los dos protocolos de seguridad que podemos elegir para crear una conexión IPsec son AH y ESP. AH solo proporciona autenticación de paquetes mediante una función H-MAC tal como SHA1 o MD5. Esta es su estructura:



Figura 8 - Estructura de AH



Fuente: Márquez, Guillermo (2015). IPsec y Redes Privadas Virtuales

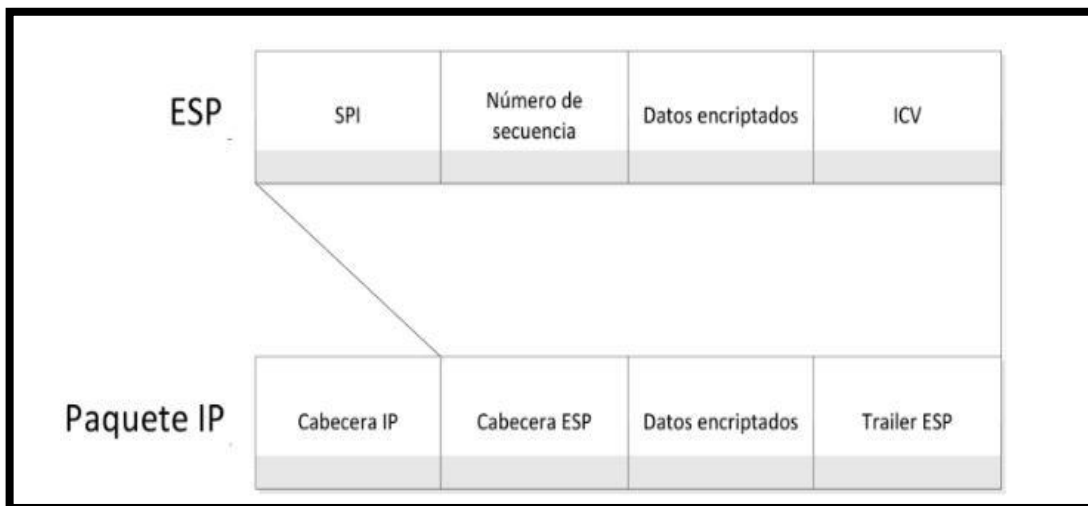
- Siguiete cabecera: Especifica que protocolo se está encapsulando en el campo de datos.
- Tamaño de la carga: Especifica el tamaño de la cabecera AH con los datos o SPI: Es un identificador que identifica únicamente una conexión.
- Número de secuencia: Es un número único para cada paquete que va cambiando. Se usa para evitar ataques de repetición de paquetes
- ICV: Este campo contiene el hash H-MAC y proporciona autenticación para el paquete (comprobación de su integridad) En este campo están protegidos todos los campos del paquete IP tales como la dirección IP, la cabecera AH, los datos del cliente y exceptúa los campos variables en las cabeceras IP y AH. Esta característica proporciona un alto grado de seguridad pero también nos impide el uso de NAT ya que cambiaría la dirección IP del paquete y al llegar este a su destino no pasaría la prueba de comprobación del ICV. Esto es así incluso si estamos trabajando en



modo túnel porque la cabecera IP que se añade en este modo también está protegida.

El otro protocolo de seguridad es ESP. Este puede proporcionar encriptación además de autenticación de paquetes. La encriptación la realiza mediante los algoritmos DES, 3DES o AES y la autenticación de paquetes mediante las funciones H-MAC SHA1 o MD5. Esta es su estructura:

**Figura 9 - Estructura de ESP**



*Fuente: Márquez, Guillermo (2015). IPSec y Redes Privadas Virtuales*

El campo ICV solo contempla la integridad de los datos encriptados y de la cabecera ESP, por lo tanto, ESP si funciona a través de un dispositivo que haga NAT. ESP soporta NAT pero no PAT ya que no utiliza puertos como lo hacen TCP o UDP. Para solucionar esto existe una variación llamada NAT-T. Lo que hace NAT-T es encapsular la cabecera ESP con los datos encriptados en una cabecera UDP con puerto destino 4500.



**Figura 10 - Estructura de NAT- T**



*Fuente: Márquez, Guillermo (2015). IPsec y Redes Privadas Virtuales*

## SOFTWARE PARA CONFIGURAR ROUTER Y SWITCHC

### 2.3.9. PuTTY

PuTTY es un cliente de red que soporta los protocolos SSH, Telnet y Rlogin y sirve principalmente para iniciar una sesión remota con otra máquina o servidor. Es de licencia libre y está diseñado y mantenido principalmente por Simón Tatham desde Gran Bretaña. A pesar de su sencillez es muy funcional y configurable.

Algunas características de PuTTY son:

- El almacenamiento de hosts y preferencias para uso posterior.
- Control sobre la clave de cifrado SSH y la versión de protocolo.
- Control sobre el Re direccionamiento de puertos con SSH, incluyendo manejo empotrado de reenvío X11.
- Completos emuladores de terminal xterm, VT102, y ECMA-48.
- Soporte IPv6, Soporte 3DES, AES, RC4, Blowfish, DES.
- Soporte de autenticación de clave pública.

El nombre PuTTY proviene de las siglas Pu: Port unique TTY: terminal type.

Su traducción al castellano sería: Puerto único de tipo terminal.



## SOFTWARE PARA CAPTURAR TRÁFICO DE RED

### 2.3.10. Wireshark

Wireshark es más importante analizador de protocolos de red del mundo. Le permite ver lo que está sucediendo en su red a nivel microscópico. Es el estándar de facto (ya menudo de iure) a través de muchas industrias y las instituciones educativas. Wireshark desarrollo prospera gracias a los aportes de la creación de redes de expertos en todo el mundo. Es la continuación de un proyecto que comenzó en 1998.

Wireshark tiene un rico conjunto de características que incluye lo siguiente:

- Inspección profunda de cientos de protocolos, con más que se añade todo el tiempo.
- Captura en vivo y análisis fuera de línea.
- De tres paneles estándar explorador de paquetes.
- Multiplataforma: Se ejecuta en Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, y muchos otros.
- Datos de red capturados se pueden consultar a través de una interfaz gráfica de usuario, o por medio de la utilidad TTY-mode TShark.
- Poderosos filtros de visualización en la industria
- Análisis VoIP Rich.
- Leer / escribir muchos diferentes formatos de archivo de captura: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Red Sniffer® general (comprimido y sin comprimir), Sniffer® Pro y NetXray®, Redes Visuales Visual UpTime, WildPackets EtherPeek / TokenPeek / AiroPeek, y muchos otros.
- Datos en tiempo real se pueden leer desde Ethernet, IEEE 802.11, PPP /

HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, y otros (dependiendo de la plataforma).

- Apoyo descifrado para muchos protocolos, incluyendo IPsec, ISAKMP, Kerberos, SNMPv3, SSL / TLS, WEP y WPA / WPA2.
- Reglas para colorear se pueden aplicar a la lista de paquetes para, análisis intuitivo rápida.
- La salida puede ser exportado a XML o texto sin formato.

### 2.3.11. Tcpxtract

Tcpxtract es una herramienta para extraer los archivos de tráfico de red basado en firmas de archivo. La extracción de archivos basado en los encabezados y pies de página de tipo de archivo (a veces llamada "talla") es una técnica de recuperación de datos de la vejez. Herramientas como Foremost emplean esta técnica para recuperar archivos de secuencias de datos arbitrarios. Tcpxtract utiliza esta técnica específicamente para la aplicación de interceptar archivos transmitidos a través de una red. Otras herramientas que llenan una necesidad similar son redes de deriva y Etherpeg. Redes de deriva y Etherpeg son herramientas para el seguimiento y la extracción de archivos gráficos en una red y es comúnmente utilizado por los administradores de red para vigilar la actividad en Internet de sus usuarios. Las principales limitaciones de las redes de deriva y Etherpeg es que sólo admiten tres tipos de archivos y no hay forma fácil de añadir más. También La técnica de búsqueda que utilizan no es escalable y no busca a través de límites de paquetes. tcpxtract cuenta lo siguiente:

- Soporta 26 formatos de archivo populares fuera de la caja. Los nuevos



formatos se pueden añadir simplemente editando su fichero de configuración.

- Con una conversión rápida, puede utilizar el archivo de configuración Foremost edad con tcpextract.
- Algoritmo de búsqueda personalizada escrita es la velocidad del rayo y muy escalable.
- La búsqueda de algoritmos a través de límites de paquetes para una cobertura total y la calidad forense.

### **2.3.12. Acrylic WIFI**

Acrylic WiFi puede ver y escanear las redes WiFi que hay a tu alcance, obtener información de seguridad de la red y obtener contraseñas WiFi genéricas gracias un sistema de plugins incluido, incluso en redes 802.11ac.

Acrylic WiFi es un scanner WiFi gratis para windows.

- Nivel de señal: Gráficas de nivel de señal de los puntos de acceso.
- Inventario: Asignación de nombre a dispositivos WiFi conocidos.
- Contraseñas: Contraseñas WiFi y claves WPS configuradas de fábrica.
- Seguridad: Información de seguridad WEP, WPA o WPA2.
- Hardware: No es necesario hardware especial para su funcionamiento.

Para obtener los mejores resultados recomendamos varios modelos de tarjetas WiFi.

Entre sus funcionalidades únicas en Acrylic WiFi que no te puedes perder y que no verás en ningún otro programa de análisis de redes inalámbricas.

Redes Ocultas: El único escáner WiFi que muestra información detallada de redes WiFi ocultas.



Visor de paquetes: Funciona como un sniffer WiFi mostrando los paquetes de red capturados de redes WiFi cercanas.

Integración: El innovador driver de Acrylic se integra automáticamente con Wireshark permitiéndole capturar tráfico WiFi en windows en modo monitor.

## **METODOLOGÍAS DE INVESTIGACIÓN**

### **2.3.13. Método Descriptivo**

Consiste en describir, analizar e interpretar sistemáticamente un conjunto de hechos relacionados con otras variables tal como se dan en el presente. El método descriptivo apunta a estudiar el fenómeno en su estado actual y en su forma natural; por tanto las posibilidades de tener un control directo sobre las variables de estudio son mínimas por lo cual su validez interna es discutible. A través del método descriptivo se identifica y conoce la naturaleza de una situación en la medida que ella existe durante el tiempo de estudios. Por consiguiente no hay administración o control manipulativo o un tratamiento específico. Su propósito básico es: describir cómo se presenta y qué existe con respecto a las variables o condiciones en una situación.

### **2.3.14. Método Analítico**

El método analítico da cuenta del objeto de estudio del grupo de investigación que en este trabajo se ocupa, con una rigurosa investigación documental, del método mismo que orienta su quehacer. Este método, empleado particularmente en las ciencias sociales y humanas, se define en el libro como un método científico aplicado al análisis de los discursos que pueden tener diversas formas de expresión, tales como las costumbres, el

arte, los juegos lingüísticos y, de manera fundamental, la palabra hablada o escrita. Para analizar y sistematizar los datos de la realidad y de la base teórica científica.

### **2.3.15. Método Deductivo**

Con el método deductivo se suele decir que se pasa de lo general a lo particular, de forma que partiendo de unos enunciados de carácter universal y utilizando instrumentos científicos, se infieren enunciados particulares, pudiendo ser axiomático-deductivo, cuando las premisas de partida están constituidas por axiomas, es decir, proposiciones no demostrables, o hipotéticos-deductivo, si las premisas de partida son hipótesis contrastables. Para establecer la síntesis de los antecedentes, teorías de los antecedentes, teorías y elaboración de la propuesta.

### **2.3.16. Método inductivo – deductivo.**

Consiste en provocar el fenómeno sometido a estudio para que pueda ser observado en condiciones óptimas. Ésta se utiliza para comprobar o examinar las características de un hecho o fenómeno. Consiste en proyectar la atención del participante sobre objetos, hechos o fenómenos, tal y como se presentan en la realidad, puede ser tanto de objetos materiales, de hechos u otros fenómenos. Esta se limita a la descripción y registro de los fenómenos sin modificarlos, ni emitir juicios de valor.

Para obtener las conclusiones. El tratamiento de los datos se lleva a cabo teniendo en cuenta los siguientes pasos:

- Paso 1: Construcción de una Matriz de Datos

Se elabora teniendo en cuenta la necesidad de seleccionar y almacenar, en forma primaria, la información obtenida.

- Paso 2: Utilización de los instrumentos de la Tecnología Informativa

La información almacenada en la Matriz de Datos, se trasladó a una computadora para que puedan realizarse los tratamientos textuales y estadísticos necesarios, utilizando los programas más adecuados para cumplir tal propósito.

- Paso 3: Aplicación de las Pruebas Estadísticas

Se aplicaron las pruebas estadísticas requeridas, de tal forma que se adaptaran y que fueran las más apropiadas para el trabajo, en función de los datos obtenidos y el propósito plasmado en el diseño de la investigación.

Esto permite realizar el Análisis concreto, que tuvo como finalidad estudiar en detalle las características más relevantes respecto al objeto de investigación.

La interpretación fue el paso necesario para unir de manera adecuada, y con carácter científico. De esta forma, el análisis y la interpretación de los resultados y la contextualización otorgada por las Teorías y Doctrinas referentes al tema, sirvieron para fundamentar las conclusiones finales del trabajo de investigación.

## TÉCNICAS DE RECOLECCIÓN DE DATOS

### 2.3.17. Observación- Encuesta

Son procedimientos de observación indirecta tales como la aplicación de cuestionarios, inventarios, test, etc.; se recogen datos relativamente

limitados de un número grande de casos que generalmente representan la muestra de una población. El propósito de la encuesta es recolectar información acerca de variables, antes que información acerca de individuos. Cuando la encuesta recoge información de toda una población se le denomina censo y cuando se recoge información de solo una parte representativa de esta población se le denomina encuesta por muestreo”.

Entrevista: Se utilizó esta técnica por que se usaron preguntas dirigidas a las personas especialistas en el tema de redes y seguridad informática.

Observación: Se utilizó la técnica de la observación porque permitió determinar la realidad de los algoritmos y su importancia en la VPN.

### **2.3.18. Observación - Entrevista Estructurada**

Modalidad que consta de una lista de cuestiones o aspectos que han de ser explorados durante la entrevista. El entrevistador queda libre para adaptar la forma y el orden de las preguntas. El estilo suele ser coloquial, espontaneo e informal. La entrevista estructurada garantiza que no se omitan áreas importantes y permite aprovechar al máximo el escaso tiempo de que se dispone en la mayoría de las entrevistas. Permite una cierta sistematización al delimitar los aspectos que serán tratados.

## **2.4. Definición de Terminología**

### **2.4.1. Encriptado**

Proceso de codificación y ocultación de paquetes de datos para impedir su lectura por terceros y asegurar la confidencialidad de determinadas transacciones.



#### **2.4.2. Clave Privada:**

En un Sistema Asimétrico de Cifrado es la clave que solo el emisor del mensaje conocen para cifrar o descifrar un mensaje.

#### **2.4.3. IPsec (Internet Protocol Security):**

Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

#### **2.4.4. Hash**

Función unidireccional que coge un mensaje de entrada con una longitud arbitraria y produce un resumen con una longitud fija. Cisco utiliza tanto Secure Hash Algorithm (SHA) como Message Digest 5 (MD5) en la implementación de la estructura IPsec.

#### **2.4.5. MD5 (Message-Digest Algorithm 5)**

Algoritmo de generación de hash unidireccional que produce un hash de 128 bits. Tanto MD5 como el Algoritmo de hash seguro (SHA) son variaciones del MD4, que se diseñó para reforzar la seguridad de este algoritmo de generación de hash. SHA es más seguro que MD4 y MD5. Cisco utiliza hashes para la autenticación dentro del marco IPsec.

#### **2.4.6. Algoritmo de hash seguro (SHA)**

Hash unidireccional propuesto por NIST. SHA se basa en MD4 y produce un digest de 160 bits. Puesto que SHA produce un digest de 160 bits, es más



resistente a los ataques que los hashes de 128 bits (como el MD5), pero es más lento.

#### **2.4.7. Encabezado de autenticación (AH)**

AH es el protocolo que se debe utilizar cuando no se requiere o no se permite la confidencialidad. Proporciona la autenticación y la integridad de datos para los paquetes IP que se transmiten entre dos sistemas. Sin embargo, AH no proporciona la confidencialidad (el cifrado) de datos de los paquetes. Todo el texto se transporta como texto no cifrado. Cuando se utiliza solo, el protocolo AH proporciona una protección poco eficaz.

#### **2.4.8. Contenido de seguridad encapsulado (ESP)**

Es un protocolo de seguridad que proporciona confidencialidad y autenticación mediante el cifrado del paquete IP. El cifrado de paquetes IP oculta los datos y las identidades del origen y el destino. ESP autentica el paquete IP y el encabezado ESP internos. La autenticación proporciona la autenticación del origen de los datos y la integridad de los datos. Si bien el cifrado y la autenticación son optativos en ESP, se debe seleccionar, como mínimo, uno de ellos.

#### **2.4.9. ISAKMP**

Estructura de protocolo que define el mecanismo de implementación de un protocolo de intercambio de claves y la negociación de las políticas de seguridad. ISAKMP se define en la Asociación de seguridad en Internet y el Protocolo de administración de claves.

#### **2.4.10. Advanced Encryption Standard (AES):**

AES se finalizó como un algoritmo criptográfico aprobado de la norma de procesamiento de información federal (FIPS) para proteger la transmisión de datos electrónicos (FIPS PUB 197).

AES se basa en el algoritmo Rijndael, que especifica cómo utilizar las claves con una longitud de 128, 192 o 256 bits para cifrar bloques de 128, 192 o 256 bits (las nueve combinaciones de longitud de clave y bloque son posibles).

#### **2.4.11. Data Encryption Standard (DES)**

DES se publicó en 1977 por la oficina nacional de estándares y es un esquema de cifrado de claves secretas basado en el algoritmo Lucifer de IBM. El contraste de DES es una clave pública. Cisco utiliza DES en la criptografía clásica (longitudes de clave de 40 y 56 bits), cifrado de IPsec (clave de 56 bits) y en el Firewall PIX (clave de 56 bits).

#### **2.4.12. HTML (HyperText Markup Language):**

Formato especial de archivos sobre el que está basada la estructura de la aplicación WWW (World Wide Web).

#### **2.4.13. Internet**

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





## CAPÍTULO III: MARCO METODOLÓGICO

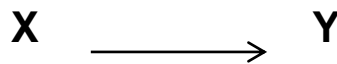
### 3. Marco metodológico

#### 3.1. Tipo y diseño de la investigación

##### 3.1.1. Tipo de Investigación

El estudio planteado es del tipo descriptiva-comparativa, por un lado se describe los algoritmos para redes privadas virtuales objeto de este estudio y enuncia sus características, por el otro lado se elaboró un software para encriptar datos y poder enviar estos a través de una red privada virtual. Comparando con que algoritmos aumenta el nivel de integridad de los datos.

X= (Algoritmos criptográficos)    Y= (Medir la Confidencialidad)



##### 3.1.2. Diseño de la investigación

La investigación que abordo se demostró mediante el envío de datos encriptado y sin encriptar a través de una red privada virtual. Capturando en tráfico en un determinado tiempo.

**Tabla 1 - Diseño de la Investigación**

Var. Independiente	Var. Dependiente	Resultado
ALGORITMOS CRIPTOGRÁFICOS	ANÁLISIS COMPARATIVO PARA MEDIR LA INTEGRIDAD Y CONFIDENCIALIDAD EN REDES PRIVADAS VIRTUALES	Con el análisis comparativo de redes privadas virtuales se lograra obtener algoritmos criptográficos más seguros.
		Con el análisis comparativo de redes privadas virtuales se podrá disminuir el uso de



		recursos computacionales.
		Con el análisis comparativo de redes privadas virtuales aumentara el nivel de integridad de los datos.
		Con el análisis comparativo de redes privadas virtuales disminuirémos el tiempo de encriptación de los datos.

Fuente: Elaboración Propia.

### 3.2. Población y muestra

#### 3.2.1. Población:

Esta investigación se tomó como población todo el tráfico que pasa por una red en un día (24h).

#### 3.2.2. Muestra:

Para el cálculo de la muestra se utilizó la siguiente formula:

$$n = \frac{(N)(K^2)(p)(q)}{(e^2(N - 1)) + (K^2)(p)(q)}$$

Probabilidad de Éxito (p): 0.5

Probabilidad de Fracaso (q): 0.5

Error Máximo (e): 5% (0.05)

Confiabilidad (K): 1.96

Universo (N): 24 horas



$$n = \frac{(24)(1.96^2)(0.5)(0.5)}{(0.05^2(24 - 1)) + (1.96^2)(0.5)(0.5)} = 5 \text{ horas}$$

El número de horas que se obtuvo como muestras para capturar el tráfico de red fue de 5 horas.

### 3.3. Hipótesis

La implementación de algoritmos criptográficos permitió mejorar la integridad de una red privada virtual.

A fin de validar esta hipótesis y evaluar el impacto real de los algoritmos en la integridad y seguridad de los datos, se analizó y evaluó la misma en una red privada virtual, haciendo ataques de captura de tráfico y descriptando, todo esto en contextos similares a escenarios reales.

### 3.4. Operacionalización:

*Tabla 2 - Operacionalización de las variables en estudio*

<b>Variables dependiente</b>	<b>Dimensión</b>	<b>Indicadores</b>	<b>Técnicas e instrumentos</b>
INTEGRIDAD DE LOS DATOS EN UNA RED PRIVADA VIRTUAL	Archivo	Tiempo de envío, Tamaño del archivo	Algoritmos de encriptación. Software para capturar de información. Reporte de software.
	Paquete	Número paquetes Encapsulados y Desencapsulados	
	Encriptación	Número de paquetes Encriptados	
	Desencriptación	Número de paquetes Desencriptados	

**Fuente:** Elaboración Propia.



### 3.5. Métodos, técnicas e instrumentos de recolección de datos

#### 3.5.1. Métodos de Investigación

Los métodos de investigación que utilicé para recolección de datos han sido Experimental.

Se usó este método porque permite manipular las variables en función que permite la recolección de datos, conociendo el tipo de encriptación que ofrece cada algoritmo.

#### 3.5.2. Técnicas de recolección de datos

Observación: Se utilizó esta técnica para poder investigar y conocer los algoritmos para redes privadas virtuales.

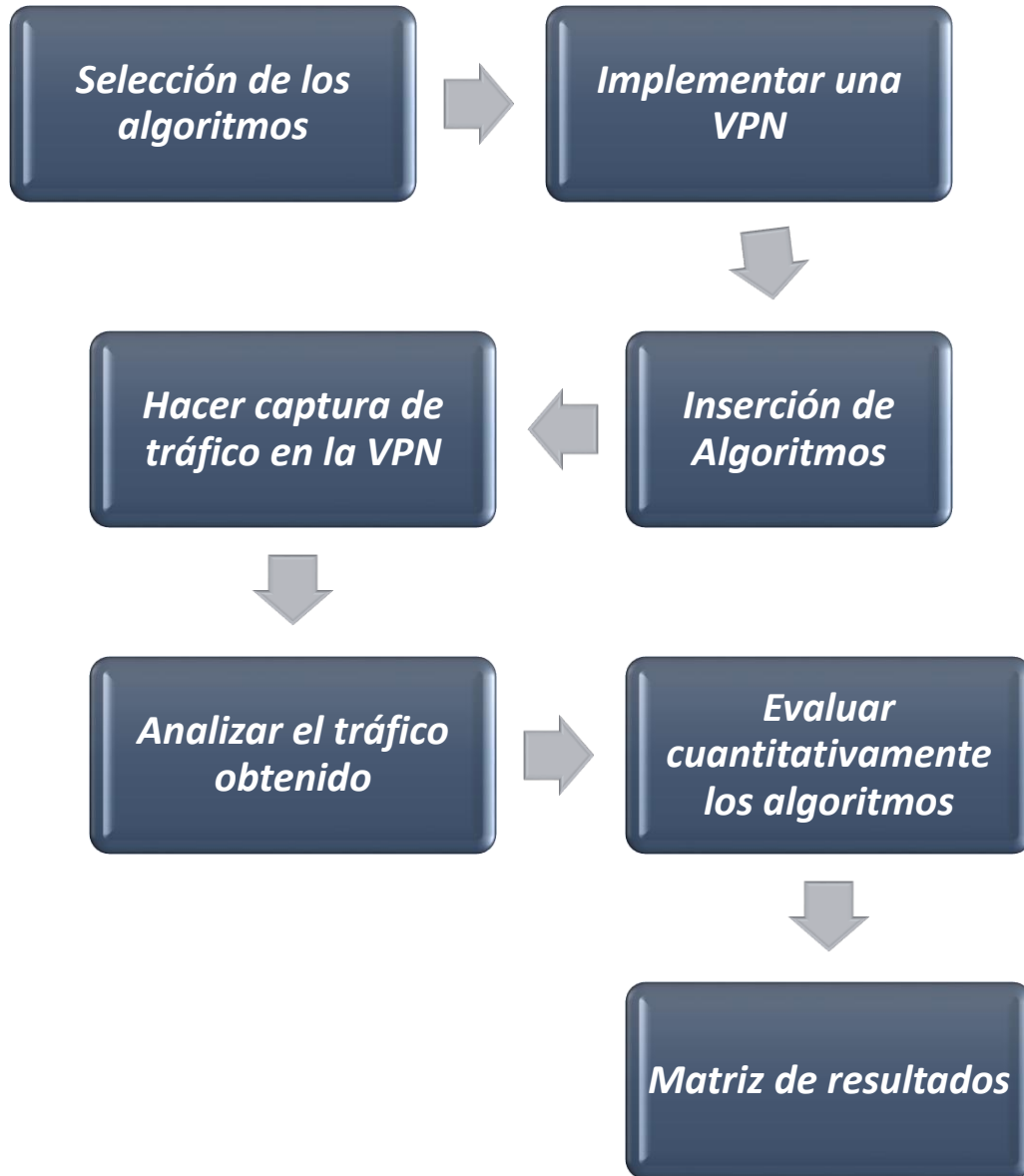
Entrevistas: Entrevisté a ingenieros en redes y telecomunicaciones experto en el tema, obteniendo de manera más detalla que algoritmo se utilizan más, y cual ofrece más seguridad.

#### 3.5.3. Instrumentos de recolección de datos

- a) Wireshark: Le permite ver lo que está sucediendo en su red a nivel microscópico.
- b) Tcpxtract: Es una herramienta para extraer los archivos de tráfico de red basado en firmas de archivo.
- c) Acrylic WIFI: Acrylic WiFi puede ver y escanear las redes WiFi que hay a tu alcance, obtener información de seguridad de la red y obtener contraseñas WiFi genéricas gracias un sistema de plugins incluido, incluso en redes 802.11ac.

### 3.6. Procedimiento para la recolección de datos

Figura 11 - Proceso de Recolección de Datos



**Fuente:** Elaboración Propia.

### 3.7. Análisis Estadístico e interpretación de los Datos

La información obtenida se le hará un análisis estadístico utilizando las siguientes fórmulas para procesar nuestros datos:



**Tiempo de Demora del Envió:** Es la resta entre el tiempo de Inicio y tiempo final. Siendo su unidad de medida en segundos o minutos.

$$Td = Tf - Ti$$

**Donde:**  $Td =$  Tiempo de demora;  $Tf =$  Tiempo Final;

$Ti =$  Tiempo Inicial

**Total de paquetes capturados, encriptados y desencriptados:** Es la suma de los paquetes encriptados y los paquetes desencriptación.

$$TP = Pe + Pd$$

$$Pe = TP - Pd$$

$$Pd = TP - Pe$$

**Donde:**  $TP =$  Total de paquetes;  $Pe =$  Paquetes Encriptados;

$Pd =$  Paquetes Desencriptados

**Total de paquetes capturados, encapsulados y desencapsulados:** Es la suma de los paquetes encriptados y los paquetes desencriptación.

$$TP = pE + pD$$

$$pE = TP - pD$$

$$pD = TP - pE$$

**Donde:**  $TP =$  Total de paquetes;  $pE =$  Paquetes Encapsulados;

$pD =$  Paquetes Desencapsulados

**Porcentaje de Tiempo de Encriptación:** Es la suma de todos los valores de Tiempo de Encriptación, divididos por su número.

$$PTE = \frac{\sum PTE}{n}$$



### 3.8. Criterios Éticos

El criterio ético que se usó en esta tesis es la responsabilidad, porque en nuestro tema de investigación está orientado a la responsabilidad que debemos asumir todos los que llevamos una carrera orientada a las TI con la seguridad de la información, gran parte del mundo ya no es ajena a la inseguridad que se viene día a día cuando nos conectamos a internet, pudiendo ser víctimas de robo de información, suplantación, etc. haciendo que el usuario desconfíe de las nuevas tecnologías que se inventan a diario. Y es aquí donde la responsabilidad entra a tallar, porque desde nosotros debe nacer el compromiso de apoyar y mantener la seguridad hasta donde esté a nuestro alcance.

### 3.9. Criterios de rigor Científico

- Validez:

Sobre la validez Interna: Hay factores que interactúan y encubren la realidad cuando se elige un algoritmo para una red privada virtual. En esta tesis queremos evitar esa confusión; utilizando una Estrategia de Evaluación y selección.

- Generalizabilidad: también llamada validez externa.

Sobre la validez externa: hay muchos cambios debido al contexto de la inseguridad informática o de los participantes. En esta tesis queremos evitar la singularidad, utilizando una estrategia de muestras de la probabilidad en la integridad de datos en los algoritmos.





- Fiabilidad:

En cuanto a la fiabilidad tenemos el peligro de que la evaluación no este dada en un tiempo preciso en la captura de tráfico. Así que necesitamos evitar la inestabilidad. Entre nuestras estrategias está realizar y comprobar que la captura de tráfico se de en tiempo indicado.

- Replicabilidad:

En cuanto a lo que respecta en replicabilidad tenemos el riesgo de ser influida la tesis por el criterio del investigador, Así que necesitamos evitar ese perjuicios, Entre nuestra estrategia están replicar y consultar con diferentes investigadores o ingenieros concedores del tema.



## CAPÍTULO IV: ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

#### 4. Análisis e Interpretación de los Resultados

##### 4.1. Resultados en Tablas

##### 4.1.1. Selección de algoritmos

En este objetivo se seleccionó algoritmos para Redes Privadas Virtuales utilizando el protocolo IPSec.

- **DES (Data Encryption Standar)**
- **AES (Advanced Encryption Standar)**
- **3DES (Triple Data Encryption Standard)**

A continuación se detalla la estructura que tiene cada algoritmo:

*Tabla 3 - Algoritmo de DES*

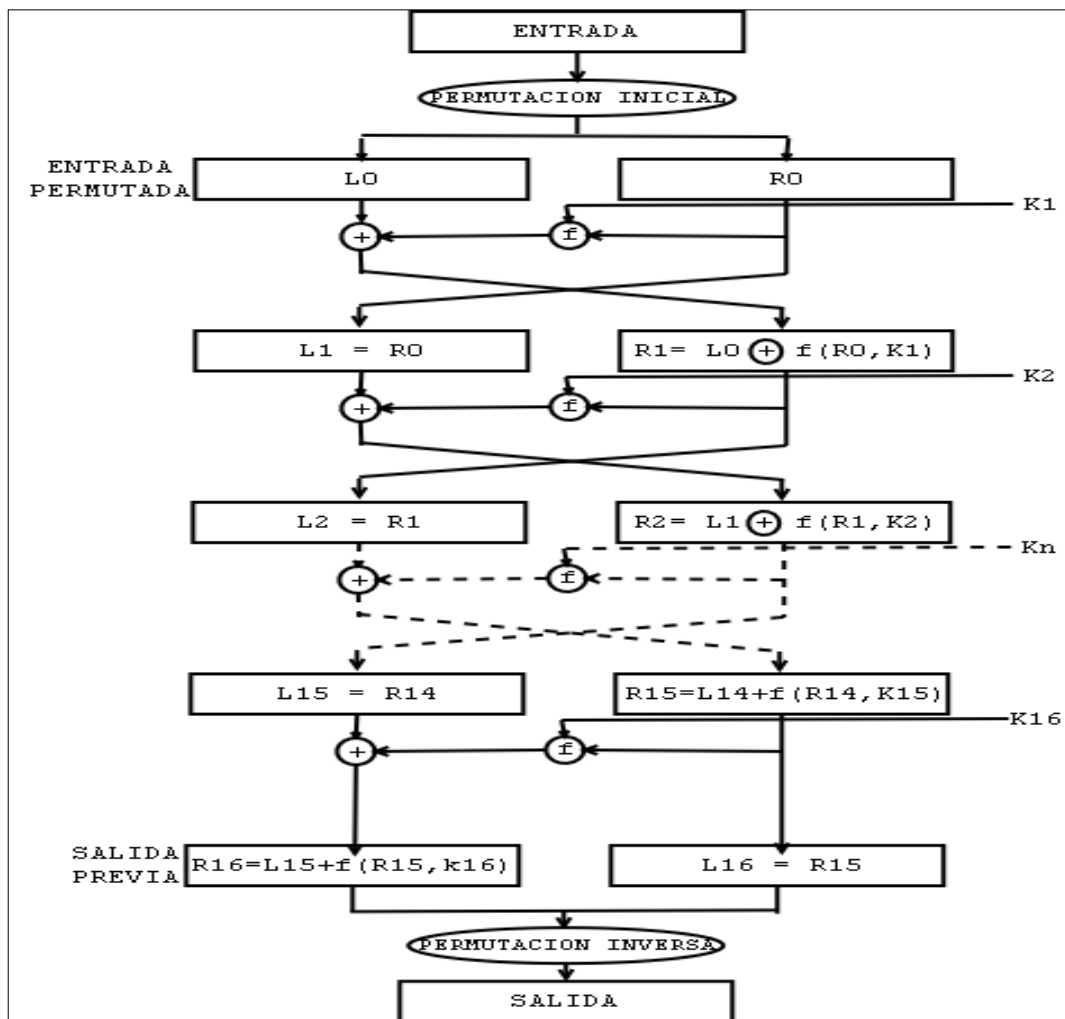
ALGORITMO: <b>DES</b> (DATA ENCRYPTION STANDARD)	
Estructura	<ul style="list-style-type: none"> <li>- ENTRADA: bloque de texto plano de longitud 64 bits y la clave <math>K</math>.</li> <li>- Bloque de texto plano se divide en dos mitades: <math>L_0</math> y <math>R_0</math></li> <li>- Las mitades pasan a través de <math>n</math> redondeos (fases)</li> <li>- Finalmente se combinan para producir el bloque cifrado.</li> <li>- <i>Formula</i></li> <li>- REDONDEOS:                             <ul style="list-style-type: none"> <li>• Cada redondeo <math>i</math> tienen como entradas:                                     <ul style="list-style-type: none"> <li>○ <math>L_{i-1}</math> y <math>R_{i-1}</math> del redondeo previo.</li> <li>○ La sub clave <math>K_i</math> derivada de la clave <math>K</math> (las <math>K_i</math> son diferentes de <math>K</math> y entre sí).</li> </ul> </li> <li>• Estructura de los redondeos (redondeo <math>i</math>):                                     <ul style="list-style-type: none"> <li>○ Se realiza una sustitución sobre la mitad izquierda de los datos (<math>L_{i-1}</math>)</li> <li>○ Se aplica la función de redondeo <math>F</math> a la mitad derecha (<math>R_{i-1}</math>)</li> <li>○ Se hace XOR de la salida de esa función con la mitad izquierda (<math>L_{i-1}</math>)</li> </ul> </li> <li>• Después de esta sustitución, se realiza una permutación que intercambia las dos mitades (<math>L_i</math> y <math>R_i</math>).</li> <li>• La función de redondeo <math>F</math> tiene la misma estructura para cada redondeo                                     <ul style="list-style-type: none"> <li>○ Está parametrizada por la correspondiente <math>K_i</math>.</li> </ul> </li> </ul> </li> <li>- El último redondeo se sigue de un intercambio que deshace la permutación del último redondeo.</li> </ul>

**Fuente:** *Elaboración propia*



En la figura 12 se muestra el funcionamiento del algoritmo de DES, teniendo un bloque de entrada de 64 bits a la cual se le aplica permutación inicial, obteniendo una entrada permutada, esta se divide en dos partes; izquierda y derecha, cada una de 32 bits, a estas partes se le aplica una serie de sustituciones y transformaciones en 16 internaciones distintas (16 rondas). Una vez de realizada las rondas tenemos una salida a la cual se le aplica una permutación inversa para que el algoritmo sirva para encriptar y desenscriptar obteniendo una salida de una bloque cifrado de 64 bits.

Figura 12 - Esquema de Algoritmo DES



Fuente: Gargallo, J. (2015). Seguridad Informática.



ECUACIÓN MATEMATICA DEL ALGORITMO DE DES:

Una vez realizada la permutación, los 64 bits se dividen en dos sub-bloques *Left* y *Right* ( $L_i$  y  $R_i$ ) de 32 bits, los bits que forma el sub-bloque  $L_i$  se encuentra formado por los primeros 32 bits y los bits restantes forma el sub-bloque  $R_i$ . En estas condiciones, el cifrado DES está definido por las ecuaciones:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f ( R_{i-1} , K_i )$$

La salida de  $R_0$  es de 32 bits, se utiliza la permutación  $E$ , con el propósito de expandir a 48 bits y así poder realizar la suma  $OR$  exclusiva con la clave  $K_i$ . Una vez realizada la permutación, los 56 bits se dividen en dos sub-bloques  $C_i$  y  $D_i$  de 28 bits. En estas condiciones, la clave está definida por las ecuaciones:

$$C_i = LS (C_{i-1}) \quad D_i = LS(D_{i-1})$$

$$K_i = PC2 (C_i , D_i)$$

El resultado de haber realizado la permutación  $PC2$  es la generación de la clave  $K_1$  siendo:

$$K_1 = PC2 (C_1, D_1)$$

Suma  $OR$  exclusiva Con la clave  $K_i$  y  $E(R_{i-1})$ , se procede a realizar la suma  $OR$  exclusiva, denotada por:

$$R_i = L_i \oplus f ( R_{i-1}, K_i )$$



**Tabla 4 - Algoritmo de 3DES**

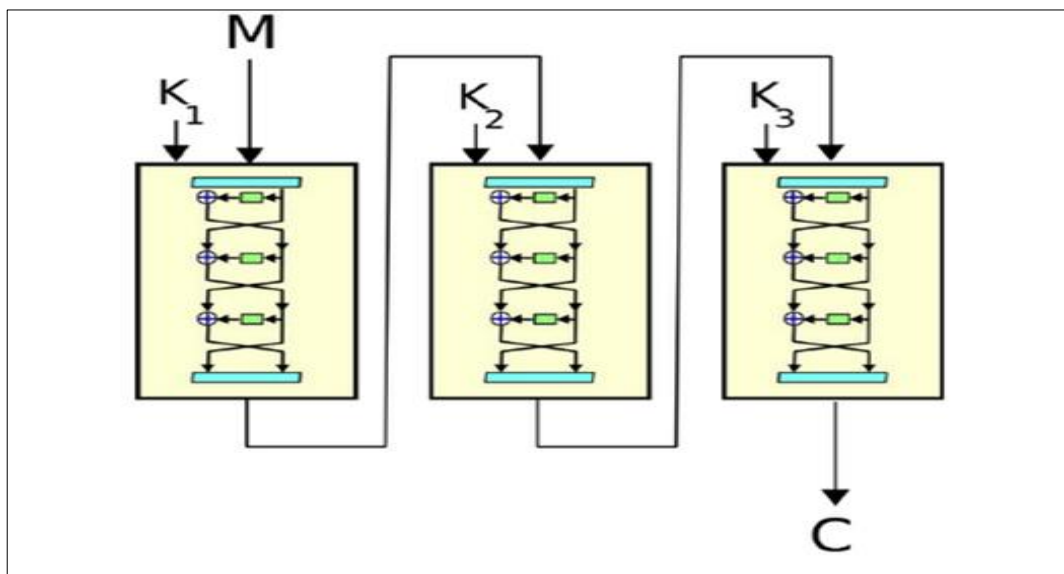
ALGORITMO: <b>3 DES</b> (TRIPLE DATA ENCRYPTION STANDARD)	
<b>Arquitectura</b>	<p>Se basa en aplicar el algoritmo DES tres veces, la clave tiene una longitud de 128 bits. Si se cifra el mismo bloque de datos dos veces con dos llaves diferentes (de 64 bits), aumenta el tamaño de la clave.</p> <p>3DES aumenta de forma significativa la seguridad del sistema de DES, pero requiere más recursos del ordenador.</p> <p>El esquema básico de estos tipos de algoritmos de clave privada es: Mensaje + Clave = Código (encriptación), Código + Clave = Mensaje (des encriptación)</p>
<b>Estructura</b>	<ul style="list-style-type: none"> <li>- Fraccionamiento del texto en bloques de 64 bits (8 bytes)</li> <li>- Permutación inicial de los bloques,</li> <li>- Partición de los bloques en dos partes: izquierda y derecha, denominadas I y D respectivamente,</li> <li>- Fases de permutación y de sustitución repetidas 16 veces (denominadas rondas),</li> <li>- Reconexión de las partes izquierda y derecha, seguida de la permutación inicial inversa.</li> </ul> <p><i>Formula:</i></p> <p style="text-align: center;"><b>Figura 13- Formula de 3 DES</b></p> <div style="border: 1px solid black; padding: 10px; width: fit-content; margin: 0 auto;"> <math display="block">C = E_{DES}^{k_3} \left( D_{DES}^{k_2} \left( E_{DES}^{k_1} (M) \right) \right)</math> </div> <p><b>Fuente:</b> Gargallo, J. (2015). <i>Seguridad Informática</i>.</p> <ul style="list-style-type: none"> <li>• <b>DONDE:</b> <ul style="list-style-type: none"> <li>• Donde M es el mensaje a cifrar</li> <li>• K1 y K2 y K3 las respectivas claves DES.</li> <li>• C es el texto cifrado</li> <li>• E es la clave de Encriptado</li> <li>• D es la clave de Des encriptado.</li> <li>• En la variante 3TDES las tres claves son diferentes; en la variante 2TDES, la primera y tercera clave son iguales.</li> </ul> </li> </ul> <p>Por lo general, se reconocen diversos tipos de cifrado triple DES:</p> <ul style="list-style-type: none"> <li>- DES-EEE3: Cifrado triple DES con 3 claves diferentes,</li> <li>- DES-EDE3: una clave diferente para cada una de las operaciones de triple DES (cifrado, descifrado, cifrado),</li> <li>- DES-EEE2 y DES-EDE2: una clave diferente para la segunda operación (descifrado).</li> </ul>

**Fuente:** *Elaboración Propia*



Ya que DES no tiene estructura de grupo, por lo que se puede aplicar varias veces el algoritmo con diferentes claves, entonces en el Algoritmo 3DES se cifra primero el mensaje con la clave  $K_1$ , después desciframos con la clave  $K_2$  y después volvemos a cifrar con la clave  $K_1$ . Entonces la clave total está formada por la concatenación de las claves  $K_1$  y  $K_2$  y tiene una longitud de 112 bits

Figura 14 - Esquema de Algoritmo 3 DES



Fuente: Gargallo, J. (2015). Seguridad Informática.

ECUACIÓN MATEMÁTICA DEL ALGORITMO DE 3DES:

El 3DES usa tres claves y tres ejecuciones del algoritmo DES. La función

$$\text{sigue la secuencia cifrar-descifrar-cifrar: } C = E_{K_3} \left[ D_{K_2} \left[ E_{K_1} [P] \right] \right]$$

Donde  $C$  = texto cifrado y  $P$  = texto claro

El descifrado es simplemente la misma operación con las claves en orden inverso:

$$P = D_{K_1} \left[ E_{K_2} \left[ D_{K_1} [C] \right] \right]$$



**Tabla 5 - Algoritmo de AES**

<b>ALGORITMO: AES (ADVANCED ENCRYPTION STANDARD)</b>	
<b>Arquitectura</b>	<p>También conocido como Rijndael, este algoritmo es el más conocido entre los usuarios de Router, ya que WPA opera con AES como método de cifrado. Este cifrado puede implementar tanto en sistemas hardware como en software. El sistema criptográfico AES opera con bloques y claves de longitudes variable, hay AES de 128bits, de 192 bits y de 256 bits.</p>
<b>Estructura</b>	<p>Expansión de la clave usando el esquema de claves de Rijndael.</p> <p>Etapa inicial:</p> <ol style="list-style-type: none"> <li>1. AddRoundKey</li> </ol> <p>Rondas:</p> <ol style="list-style-type: none"> <li>1. SubBytes: En este paso se realiza una sustitución no lineal donde cada byte es reemplazado con otro de acuerdo a una tabla de búsqueda.</li> <li>2. ShiftRows En este paso se realiza una transposición donde cada fila del «state» es rotada de manera cíclica un número determinado de veces.</li> <li>3. MixColumns: Operación de mezclado que opera en las columnas del «state», combinando los cuatro bytes en cada columna usando una transformación lineal.</li> <li>4. AddRoundKey: Cada byte del «state» es combinado con la clave «round»; cada clave «round» se deriva de la clave de cifrado usando una iteración de la clave.</li> </ol> <p>Etapa final:</p> <ol style="list-style-type: none"> <li>1. SubBytes</li> <li>2. ShiftRows</li> <li>3. AddRoundKey</li> </ol>

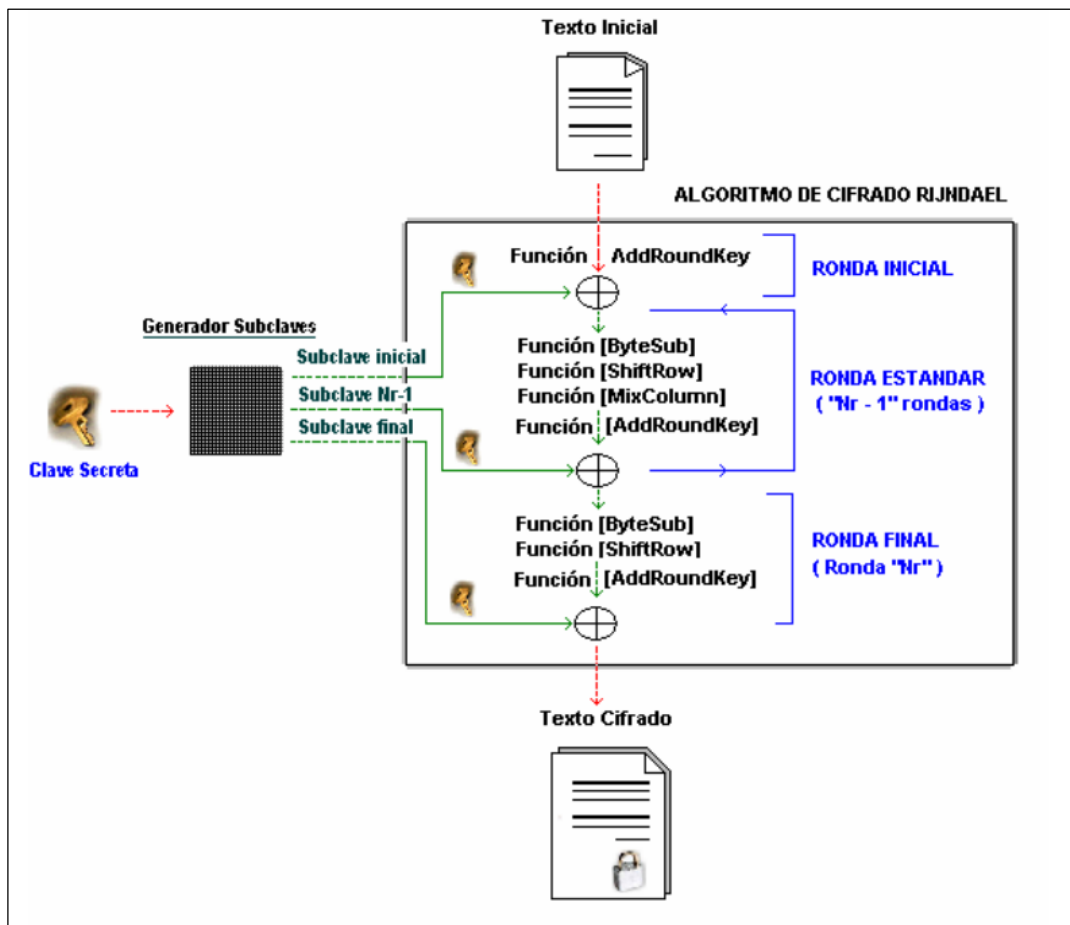
**Fuente:** *Elaboración Propia*





El proceso de cifrado de AES consiste en la aplicación de 4 funciones matemáticas invertibles sobre la información que se desea cifrar. Estas transformaciones se realizan de forma reiterativa para cada ronda o vuelta defina. En la figura se describe el proceso de cifrado con el algoritmo Rijndael como:

Figura 15 - Algoritmo de Rijndael - AES



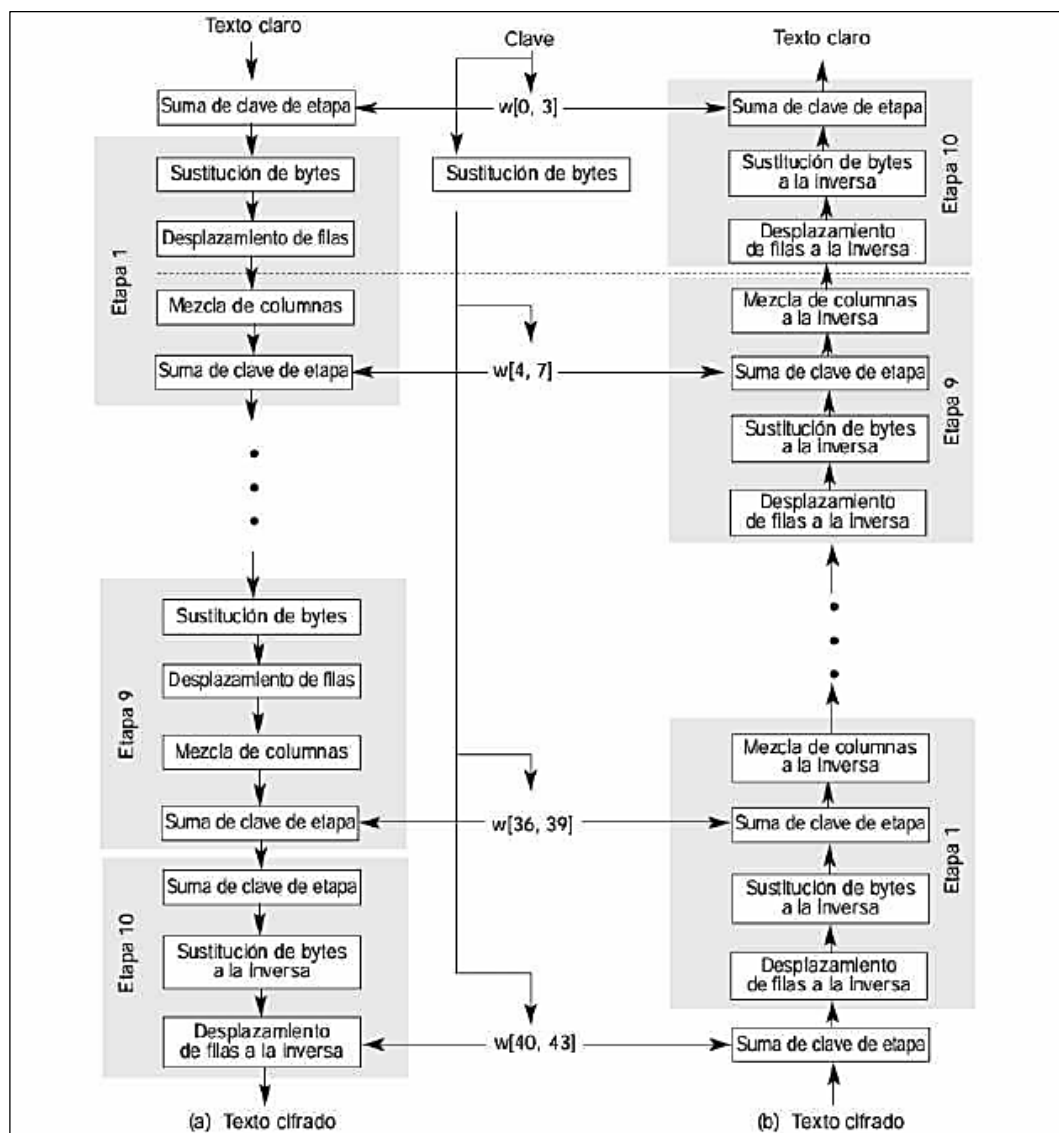
Fuente: Muñoz, A. (2004). Seguridad europea para EEUU

En esencia la información a cifrar se va mapeando en la matriz de Estado. Esta matriz de Estado se introduce al cifrador, y sufre una primera transformación, en la ronda inicial, que consiste en una operación or-exclusiva (AddRoundKey) entre una Subclave generada y la matriz de



Estado. A continuación, a la matriz de Estado resultante se le aplican 4 transformaciones invertibles, repitiéndose este proceso “Nr-1” veces, en lo que se conoce como Ronda Estándar. Finalmente se le aplica una última ronda o vuelta a la matriz de Estado resultante de las “Nr-1” rondas anteriores, aplicando las funciones ByteSub, ShiftRow y AddRoundKey en este orden. El resultado de la ronda final da el bloque cifrado deseado.

**Figura 16 - Cifrado y Descifrado de AES**



**Fuente:** Stallings, W. (2004). *Fundamentos de Seguridad en Redes*.



ECUACIÓN MATEMATICA DEL ALGORITMO DE AES:

AES está diseñado para trabajar en bytes. Sin embargo, cada byte se interpreta como una representación del polinomio:

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$$

Donde cada  $b_i$  es 0 o 1.

*Add Round Key*, se convierte entonces en o-exclusiva, pero la multiplicación se define como polinomio módulo de multiplicación  $x^7 + x^4 + x^3 + x + 1$ .

*SubBytes Routine*, En esta rutina, cada byte de estado se sustituye de acuerdo con la siguiente fórmula:

Para cada bit  $i$ , establezca  $b_i$  a  $b_i$  O exclusiva  $b(i + 4) \bmod 8$  xor  $b(i + 5) \bmod 8$  xor  $b(i + 6) \bmod 8$  xor  $b(i + 7) \bmod 8 + c$  donde  $c = 63$  hex.

*MixColumns*, Esta función mezcla seguridad de los datos en cada columna de acuerdo con las siguientes fórmulas:

Conjunto  $s_0, c$  de  $2 * s_0, c$  xor  $3 * s_1, c$  xor  $s_2, c$  xor  $s_3, c$

Conjunto  $s_1, c$  a  $0, c$  xor  $2 * s_1, c$  xor  $3 * s_2, c$  xor  $s_3, c$

Conjunto  $s_2, c$  a  $s_0, c$  xor  $s_1, c$  xor  $2 * s_2, c$  xor  $3 * s_3, c$

Conjunto  $s_3, c$  de  $3 * s_0, c$  xor  $s_1, c$  xor  $s_2, c$  xor  $2 * s_3, c$

*Rutina AddRoundKey*, Esta función hace un XOR entre cada columna del estado y una palabra de 32 bits de la programación de llave.



En siguiente tabla se presenta un estudio comparativo entre los algoritmos DES, 3DES y AES donde se presentaron diez factores.

**Tabla 6:** Estudio comparativo entre DES, 3DES y AES

FACTORES	AES	DES	3DES
LOGITUD DE LA CLAVE	128,192 y 256 bits	K1 ,K2 YK3 168 bits (k1 y k2 168 bits (k1 y k2 es mismo) 112bits	56 bits
TIPO DE CIFRAS	Simétrica bloques de Cifrado	Simétrica bloques de Cifrado	Simétrica bloques de Cifrado
TAMAÑO DE BROQUE	128,192.0 256 Bits	64 BITS	64 BITS
DESARROLLO	2000	1978	1977
RESISTENCIA CRIPTOANÁLISIS	Diferencial En Contra De Fuerte, truncado Diferencial e Interpolación Lineal y Plazas de Ataques	Vulnerable al diferencial De fuerza Bruta Atacante Podría Ser Analizada de texto Plano con Criptoanálisis diferencial	Vulnerables a diferencial Y lineal criptoanálisis! Las tablas de sustitución Débiles
SEGURIDAD	Considerado Seguro	Sólo uno débil Que Es Salir En Des	Resultado insuficiente
POSIBLES CLAVES	2 <sup>n</sup> 2 <sup>m</sup> y 95~	2 <sup>n</sup> , y 2 <sup>m</sup>	2 <sup>n</sup> *
IMPRIMIBLE REVISIÓN TODA LA LLAVE EN 50 MIL MILLONES DE CLAVES	para una clave de 128 Bits 5 x 10 Años	Para Una Clave de 112 Bits 800 Dias	Para Una Clave de 56 Bits 400 Días
RONDA	10 (128-Bist) ,12 (192 Bits),	48	16
RENDIMIENTO (ENCRIPCIÓN DESENCRIPTACIÓN)	4.174 / 6.452	3.45 / 5. 665	4.01 / 6347

**Fuente:** Medina, Y. (2015). *Comparación de Algoritmos Basados en la Criptografía Simétrica DES, AES y 3DES*



#### 4.1.2. Evaluación Cuantitativa de los Algoritmos

Para la evaluación de envío de datos se utilizó un Archivo de Prueba:

#### 4.53 MB

- a) Por el tamaño del archivo: Se utilizó el mismo archivo para hacer las pruebas con los tres algoritmos

*Tabla 7 - Evaluación por el tamaño de archivo*

Algoritmo	3 DES	AES	DES
Tamaño de archivo	4.53 MB	4.53 MB	4.53 MB

Fuente: *Elaboración propia*

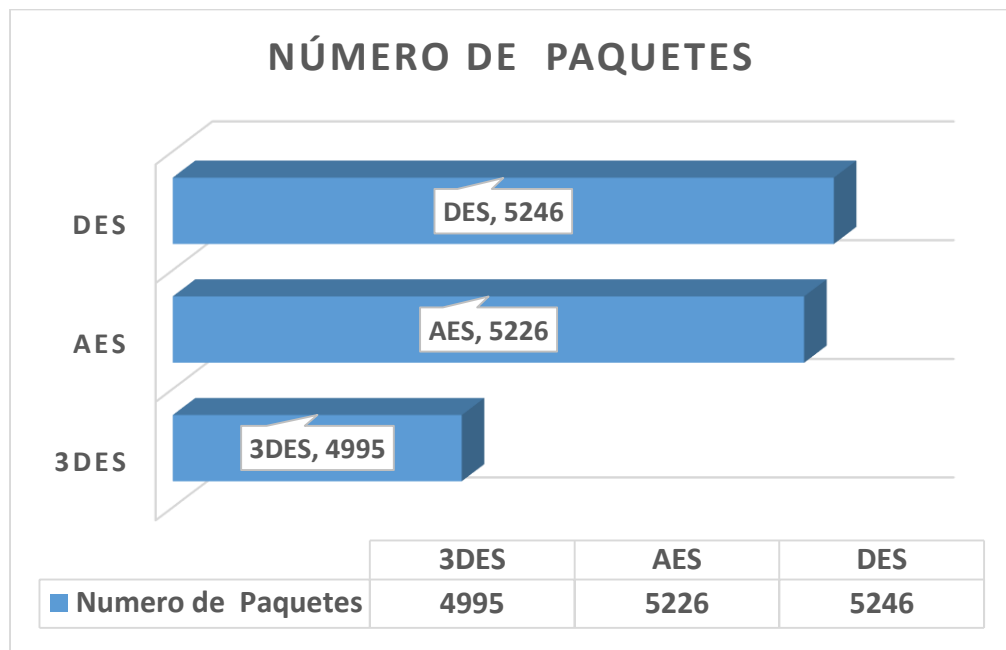
- b) Por el número de paquetes.

*Tabla 8 - Evaluación por el número de paquetes*

Algoritmo	3 DES	AES	DES
Número de paquetes	4995	5226	5246

Fuente: *Elaboración propia*

*Figura 17 - Evaluación por el número de paquetes*



Fuente: *Elaboración propia*



c) Por el tiempo de envío.

**Tabla 9** - Evaluación por el tiempo de envío.

Algoritmo	3 DES	AES	DES
Tiempo de Envío.	00:04:26:59	00:04:21:42	00:04:25:07

Fuente: *Elaboración propia*

El algoritmo AES necesita menos tiempo para enviar el mismo archivo, optimizando los recursos del computador.

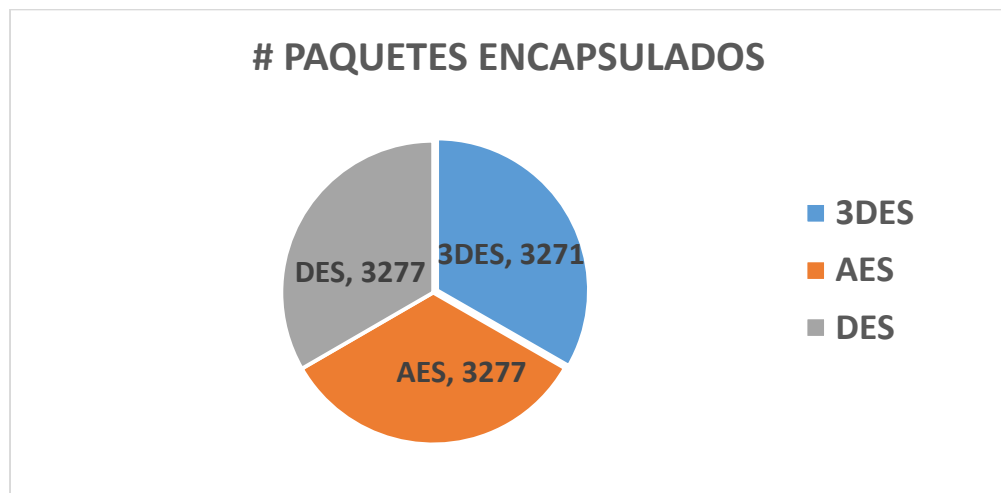
d) Por el número de paquetes encapsulados

**Tabla 10** - Evaluación por el # de paquetes encapsulados

Algoritmo	3 DES	AES	DES
# Paquetes encapsulados	3271	3277	3277

Fuente: *Elaboración propia*

**Figura 18** - Evaluación por el # de paquetes encapsulados



Fuente: *Elaboración propia*

e) Por el número de paquetes desencapsulados.

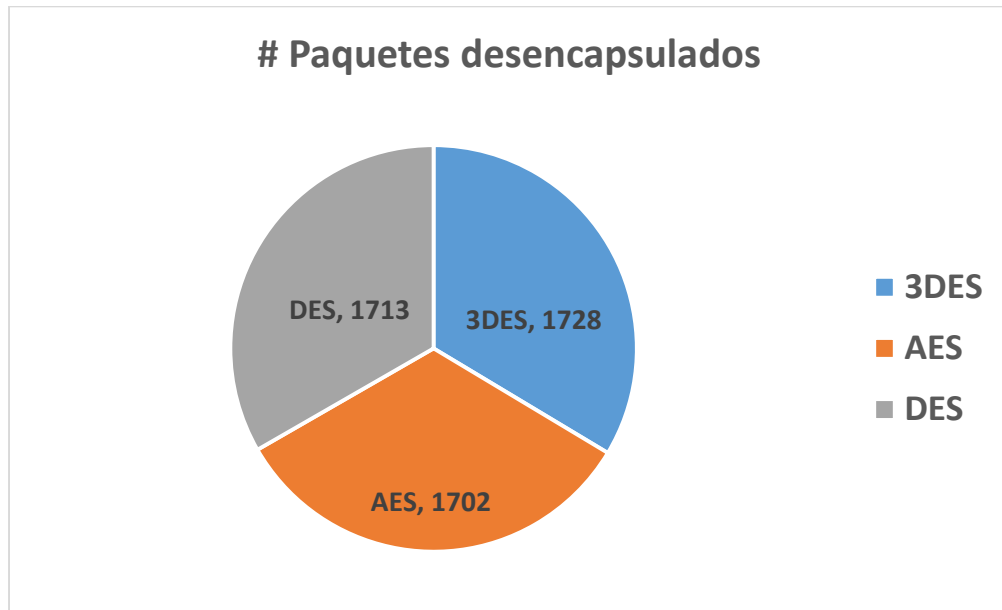
**Tabla 11** - Evaluación por el # de paquetes desencapsulados

Algoritmo	3 DES	AES	DES
# Paquetes desencapsulados	1728	1702	1713

Fuente: *Elaboración propia*



**Figura 19 - Evaluación por el # de paquetes desencapsulados**



Fuente: *Elaboración propia*

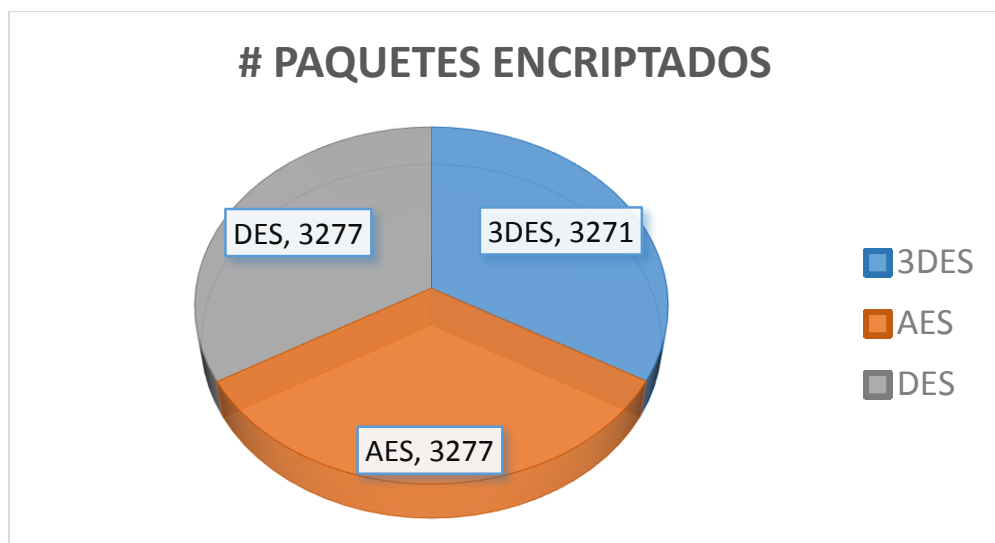
f) Por el número de paquetes encriptados

**Tabla 12 - Evaluación por el # de paquetes encriptados**

Algoritmo	3 DES	AES	DES
# Paquetes encriptados	3271	3277	3277

Fuente: *Elaboración propia*

**Figura 20 - Evaluación por el # de paquetes encriptados**



Fuente: *Elaboración propia*



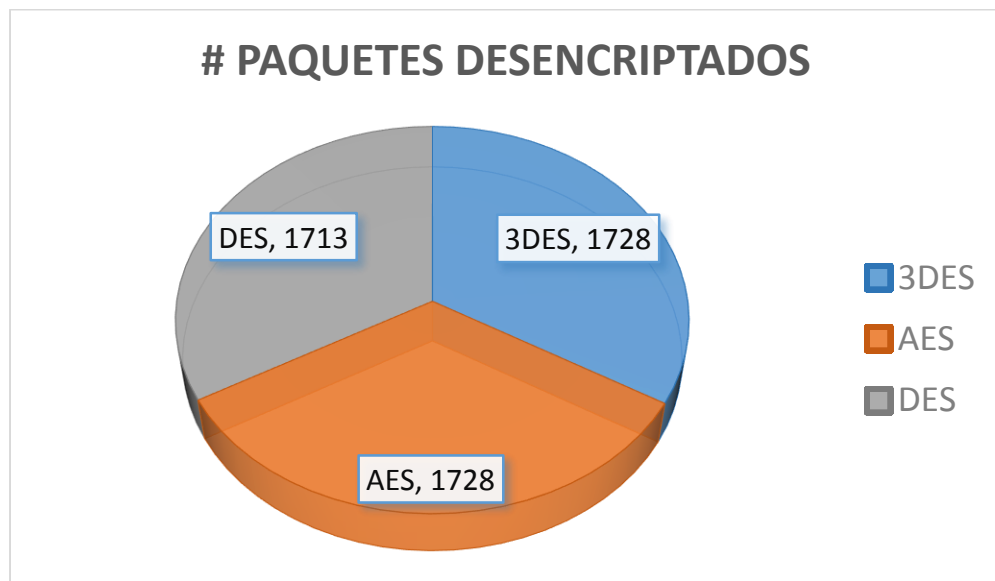
g) Por el número de paquetes descriptados.

*Tabla 13 - Evaluación por el # de paquetes descriptados*

Algoritmo	3 DES	AES	DES
# Paquetes descriptados	1728	1728	1713

Fuente: *Elaboración propia*

*Figura 21 - Evaluación por el # de paquetes descriptados*



Fuente: *Elaboración propia*

Para la evaluación de envío de voz y video se utilizó una llamada de video presencia de prueba de: **6 Minutos.**

h) Por el tiempo de Video Presencia: Se utilizó el mismo tiempo para hacer las pruebas con los tres algoritmos.

*Tabla 14 - Evaluación por el tamaño de archivo*

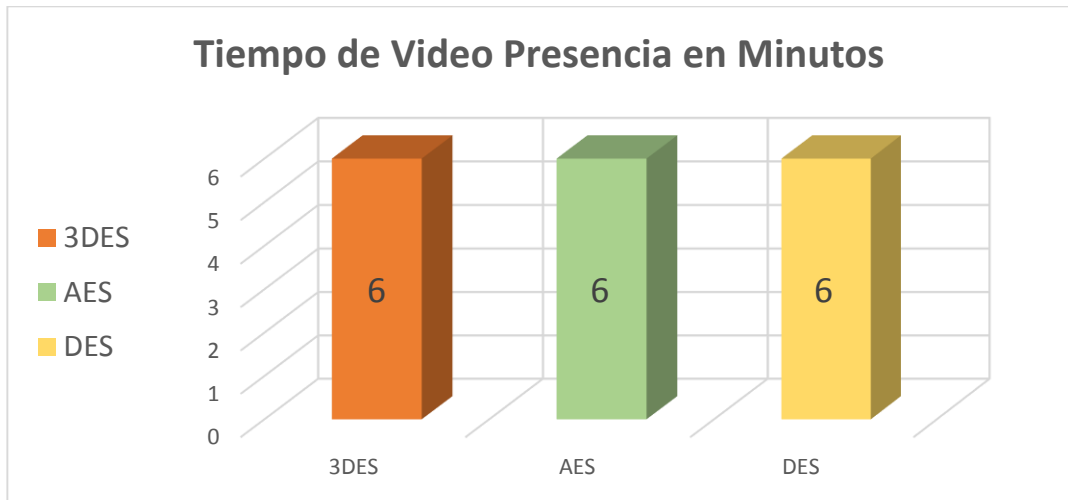
Algoritmo	3 DES	AES	DES
Tiempo de Video en Minutos	6	6	6

Fuente: *Elaboración propia*





**Figura 22: Tiempo de Video Presencia**



**Fuente:** *Elaboración propia*

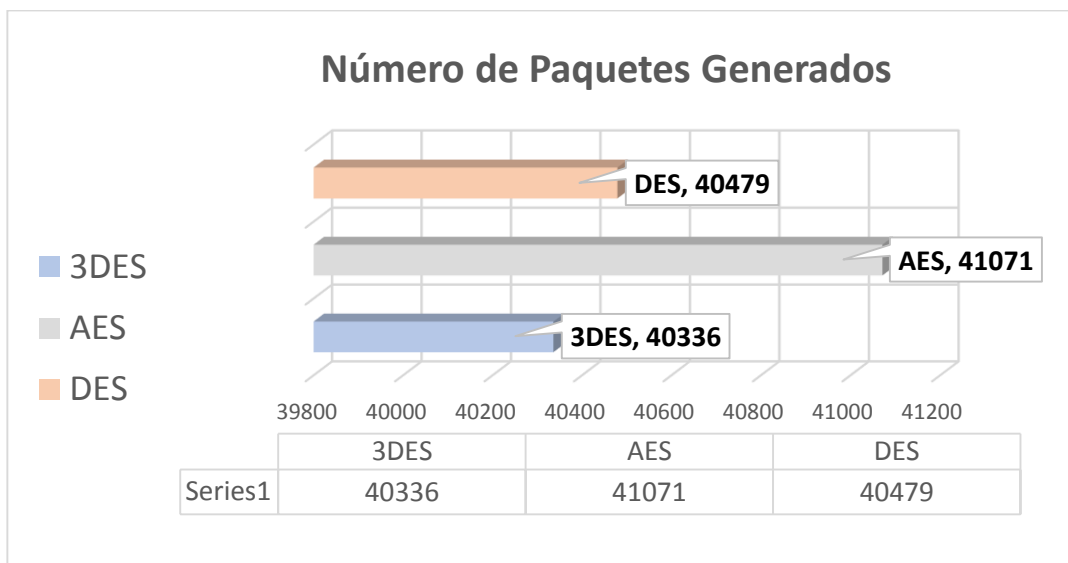
i) Por el número de paquetes que se generó para entablar la video presencia.

**Tabla 15: Por el número de paquetes**

Algoritmo	3 DES	AES	DES
Numero de paquetes	40336	41071	40479

**Fuente:** *Elaboración propia*

**Figura 23: Número de Paquetes Generados**



**Fuente:** *Elaboración propia*



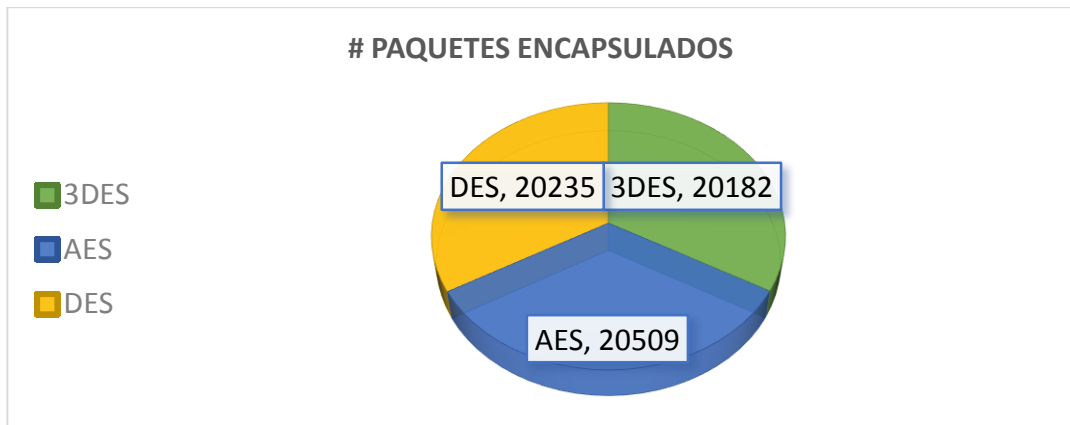
j) Por el número de paquetes encapsulados

**Tabla 16:** Por el número de paquetes encapsulados

Algoritmo	3 DES	AES	DES
# Paquetes encapsulados	20182	20509	20235

Fuente: *Elaboración propia*

**Figura 24:** Por el número de paquetes encapsulados



Fuente: *Elaboración propia*

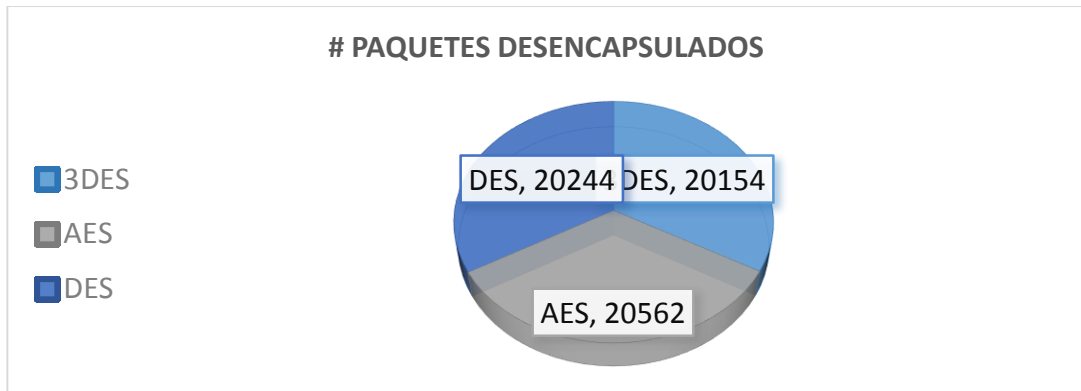
k) Por el número de paquetes desencapsulados

**Tabla 17:** Por el número de paquetes desencapsulados

Algoritmo	3 DES	AES	DES
# Paquetes desencapsulados	20154	20562	20244

Fuente: *Elaboración propia*

**Figura 25:** Por el número de paquetes desencapsulados



Fuente: *Elaboración propia*



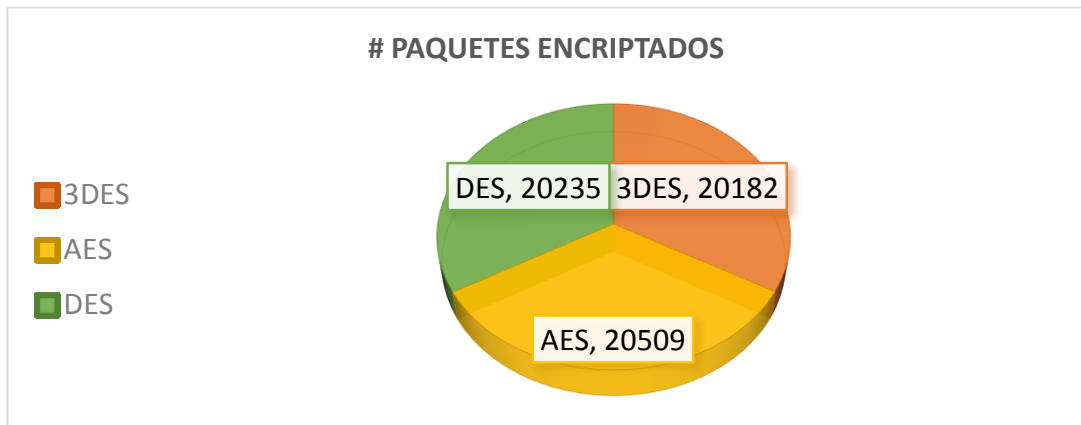
l) Por el número de paquetes encriptados

**Tabla 18:** Por el número de paquetes encriptados

Algoritmo	3 DES	AES	DES
# Paquetes encriptados	20182	20509	20235

Fuente: *Elaboración propia*

**Figura 26:** Por el número de paquetes encriptados



Fuente: *Elaboración propia*

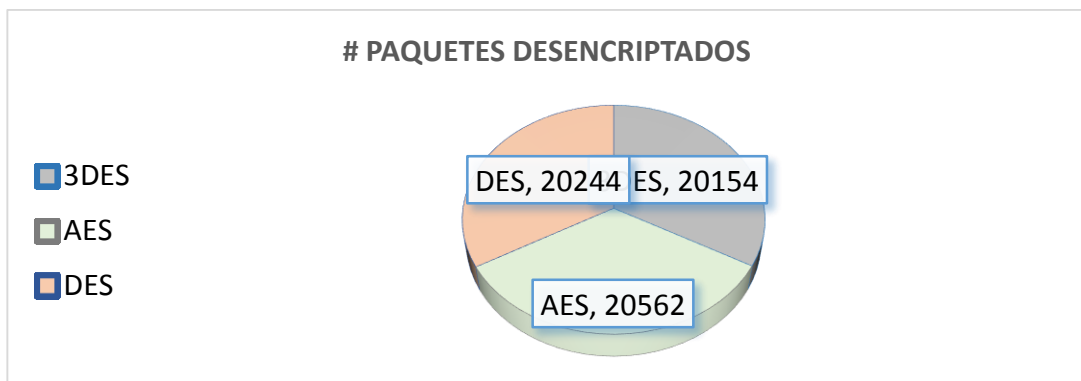
m) Por el número de paquetes descriptados

**Tabla 19:** Por el número de paquetes descriptados

Algoritmo	3 DES	AES	DES
# Paquetes descriptados	20154	20562	20244

Fuente: *Elaboración propia*

**Figura 27:** Por el número de paquetes descriptados



Fuente: *Elaboración propia*



#### 4.1.3. Resume de evaluación cuantitativa de los algoritmos.

En la tabla 20 se muestra el resumen de la evaluación de tráfico de datos.

**Tabla 20** - Tabla resumen de evaluación de algoritmos para Datos

Algoritmo	3 DES	AES	DES
Tamaño de archivo	4.53 MB	4.53 MB	4.53 MB
Número de paquetes	4995	5226	5246
Tiempo de Envió	00:04:26:59	00:04:21:42	00:04:25:07
# Paquetes encapsulados	3271	3277	3277
# Paquetes desencapsulados	1728	1702	1713
# Paquetes encriptados	3271	3277	3277
# Paquetes desencriptados	1728	1728	1713

**Fuente:** *Elaboración propia*

Como resultados en la tabla N° 20 se obtuvo que para enviar el archivo de una pc a otra con el algoritmo AES necesita menor tiempo en comparación que los demás algoritmos.

Además algoritmo AES partió el archivo en un mayor número de paquetes y lo envió en menos tiempo posible. Lo contrario del algoritmo DES que partió el archivo en más paquetes pero necesito más tiempo para enviarlo.

Sobre los paquetes encriptados algoritmo AES presentó igual número de paquetes encriptados que el algoritmo DES, pero algoritmo AES desencriptó mas paquetes que el algoritmo DES utilizando menos recursos.



En la tabla 21 se muestra el resumen de la evaluación de tráfico de voz y video.

**Tabla 21:** *Tabla resumen de evaluación de algoritmos para voz y video*

Algoritmo	3 DES	AES	DES
Tiempo de Video en Min	6 min	6 min	6 min
Número de paquetes	40336	41071	40479
# Paquetes encapsulados	20182	20509	20235
# Paquetes desencapsulados	20154	20562	20244
# Paquetes encriptados	20182	20509	20235
# Paquetes desencriptados	20154	20562	20244

**Fuente:** *Elaboración propia*

Como resultados en la tabla N° 21 se obtuvo que para enviar voz y video, el algoritmo AES partió la video presencia en un mayor número de paquetes esto hizo que la trama fuera más pequeña. Lo contrario de los algoritmo 3DES y DES que partió la video presencia en menos paquetes haciendo más larga la trama.

Sobre los paquetes encriptados algoritmo AES presentaron mayor número de paquetes encriptados y desencriptados que los algoritmo DES y 3DES, esto hizo que aumentara la seguridad de la transmisión.



# CAPÍTULO V: PROPUESTA DE INVESTIGACIÓN

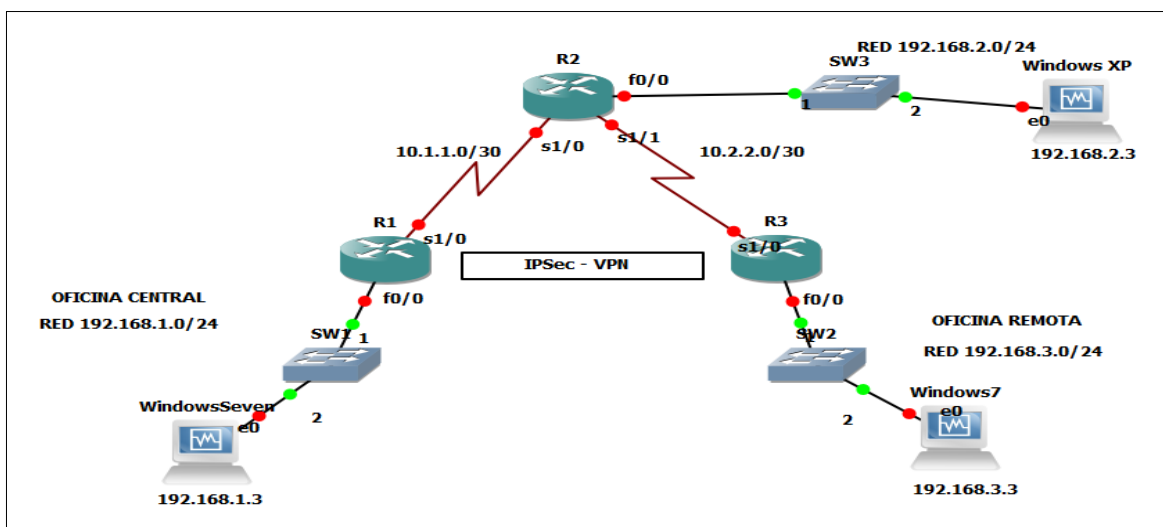
## 5. Propuesta de Investigación

### 5.1. VPN Implementada.

Modelo de la VPN, hecha en Cisco Packet Tracer Student v6.2 y se implementó en equipos reales en el Laboratorio de Sistemas Inteligentes y Seguridad Informática de la Universidad Señor de Sipán (LABSIS).

#### 5.1.1. Modelo de VPN implementada.

Figura 28 - Red VPN



Fuente: CCNA 4 - Cisco

#### 5.1.2. Equipos para la Implementación de VPN.

**Router Cisco 2900.** Dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra.

Figura 29 - Router Cisco 1900



Fuente: Cisco.



**Switch Cisco.** Dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro

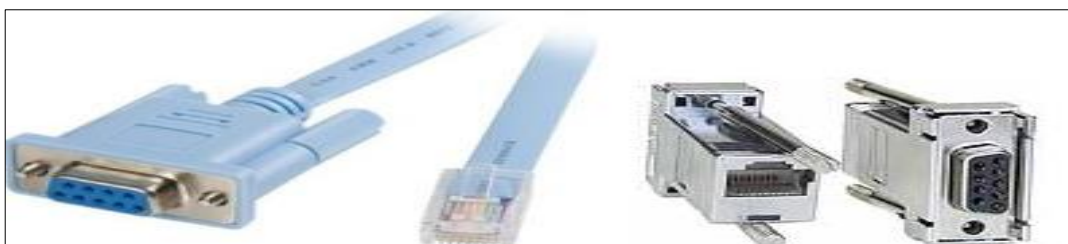
*Figura 30 - Switch Cisco 24 puertos*



Fuente: Cisco.

**Cable Consola.** Dispositivo o servicio que proporciona acceso a la consola del sistema de un equipo informático a través de tecnologías de interconexión.

*Figura 31 - Cable Consola*



Fuente: CCNA1.

**Cable Serial.** Se Utiliza para transferir información entre dos dispositivos que utilizan un protocolo de comunicación serie. La forma de conectores depende del tipo de puerto serie usado en particular.





*Figura 32 - Cable Serial*



Fuente: CCNA1.

**Cables Directo.** Utilizados para montar una red, de este se conectan los computadores a un switch y de un computador a otro computador.

*Figura 33 - Cable Directo*



Fuente: CCNA1.



## 5.2. Configuración de Router Cisco

### 5.2.1. Configuración de Router 1

En las figuras 34, 35 y 36 se realizó la configuración de acceso, configuración de interfaces y enrutamiento en el router R1.

*Figura 34 - Configuración de Acceso a R1*

```
Router>enable
Router#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#enable password cisco
Router(config)#enable secret cisco
Router(config)#
Router(config)#line vty 0 4
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
```

Fuente: *Elaboración Propia*

*Figura 35 - Configuración de Interfaces de R1*

```
Router(config)#hostname R1
R1(config)#interface fa0/0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
*Mar 1 00:15:02.371: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 00:15:03.371: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
R1(config)#interface s1/0
R1(config-if)#ip add 10.1.1.2 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown
R1(config-if)#exit
```

Fuente: *Elaboración Propia*

*Figura 36 - Enrutamiento con EIGRP en R1*

```
R1(config)#
R1(config)#router eigrp 100
R1(config-router)#network 10.1.1.0 0.0.0.3
R1(config-router)#exit
R1(config)#
*Mar 1 00:15:35.971: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
*Mar 1 00:15:36.975: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0,
R1(config)#
```

Fuente: *Elaboración Propia*



### 5.2.2. Configuración de Router 2

En las figuras 37, 38 y 39 se realizó la configuración de acceso, configuración de interfaces y enrutamiento en el router R2.

*Figura 37 - Configuración de Acceso a R2*

```
Router#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#line console 0
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#
Router(config)#enable password cisco
Router(config)#enable secret cisco
The enable secret you have chosen is the same as your enable password.
This is not recommended. Re-enter the enable secret.

Router(config)#
Router(config)#line vty 0 4
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#
Router(config)#hostname R2
```

Fuente: *Elaboración Propia*

*Figura 38 - Configuración de Interfaces de R2*

```
R2(config)#interface fa0/0
R2(config-if)#ip add 192.168.2.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
*Mar 1 00:14:55.171: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 00:14:56.171: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R2(config)#
R2(config)#interface s1/0
R2(config-if)#ip add 10.1.1.1 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
*Mar 1 00:15:31.003: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
*Mar 1 00:15:32.007: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
R2(config)#
R2(config)#interface s1/1
R2(config-if)#ip add 10.2.2.1 255.255.255.252
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown
R2(config-if)#exit
```

Fuente: *Elaboración Propia*

*Figura 39 - Enrutamiento con EIGRP en R2*

```
R2#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#
R2(config)#router eigrp 100
R2(config-router)#network 10.1.1.0 0.0.0.3
R2(config-router)#
*Mar 1 00:20:35.943: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 10.1.1.2 (Serial1/0)
R2(config-router)#network 10.2.2.0 0.0.0.3
R2(config-router)#exit
*Mar 1 00:21:01.983: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 10.2.2.2 (Serial1/1)
R2(config)#exit
R2#
```

Fuente: *Elaboración Propia*



### 5.2.3. Configuración de Router 3

En las figuras 40, 41 y 42 se realizó la configuración de acceso, configuración de interfaces y enrutamiento en el router R3.

*Figura 40 – Configuración de Acceso a R3*

```
Router>enable
Router#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#line console 0
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#
Router(config)#enable password cisco
Router(config)#enable secret cisco
The enable secret you have chosen is the same as your enable password.
This is not recommended. Re-enter the enable secret.

Router(config)#
Router(config)#line vty 0 4
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#
```

Fuente: *Elaboración Propia*

*Figura 41 - Configuración de Interfaces en R3*

```
Router#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3
R3(config)#
R3(config)#interface fa0/0
R3(config-if)#ip add 192.168.3.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#
*Mar 1 00:06:05.879: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 00:06:06.879: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
R3(config)#
R3(config)#interface s1/0
R3(config-if)#ip add 10.2.2.2 255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#
```

Fuente: *Elaboración Propia*

*Figura 42 - Enrutamiento con EIGRP en R3*

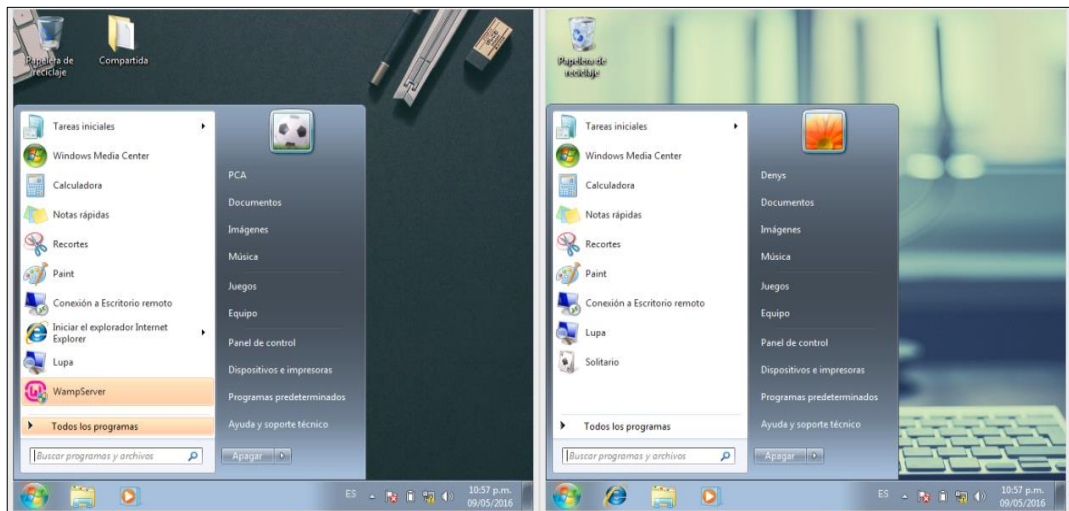
```
R3#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#
R3(config)#router eigrp 100
R3(config-router)#network 10.2.2.0 0.0.0.3
R3(config-router)#exit
R3(config)#
```

Fuente: *Elaboración Propia*

### 5.2.4. Comprobación de Conectividad entre HOST

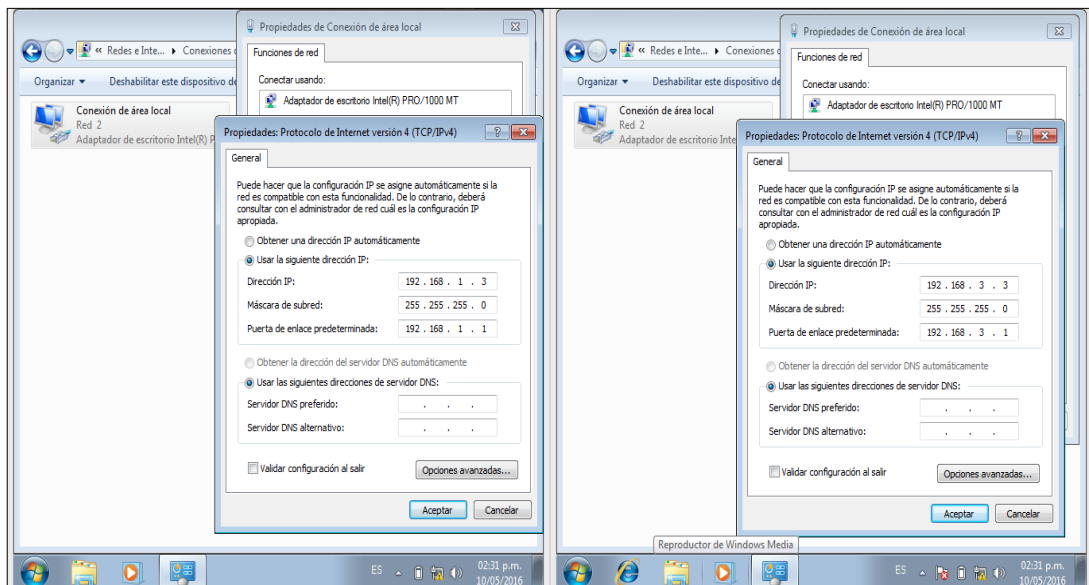
Para la comprobación de la conectividad entre host se asignó una ip a cada computadora conectada a la red, y se continuó con un ping entre las PC conectadas. Para la PcA se le asignó la ip 192.168.1.3, para la PcC se le asignó la ip 192.168.3.3 y se comprobó la conectividad entre los host.

Figura 43 - Conectar dos PC a la RED



Fuente: *Elaboración Propia*

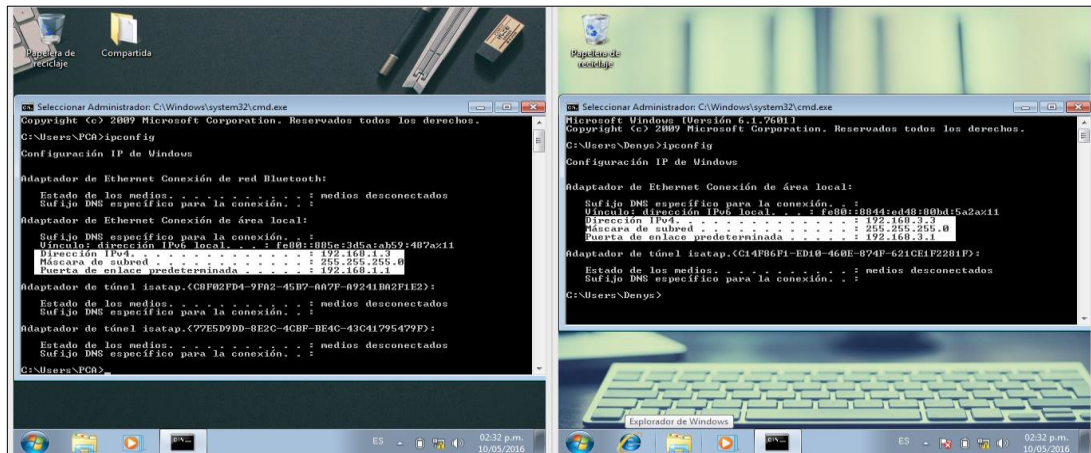
Figura 44 - Configurar las IP en las PC



Fuente: *Elaboración Propia*

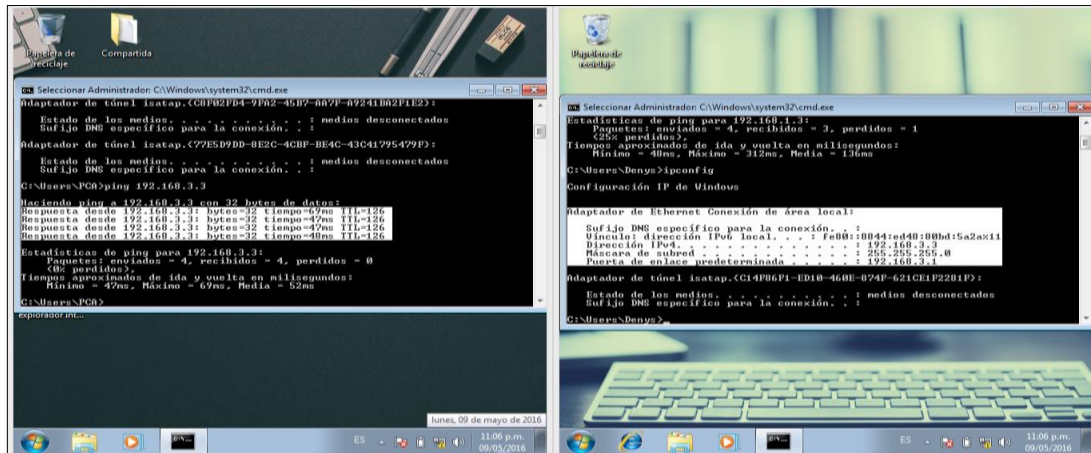


Figura 45 - Comprobar las IP Asignadas



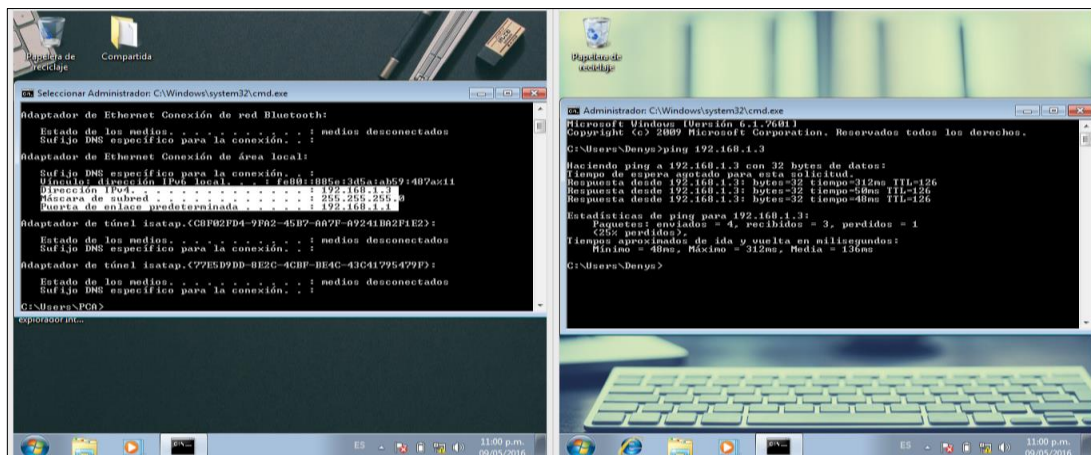
Fuente: *Elaboración Propia*

Figura 46 - Conectividad de PC-A y PC-C



Fuente: *Elaboración Propia*

Figura 47 - Conectividad de PC-C y PC-A



Fuente: *Elaboración Propia*



### 5.3. Configuración de IPSec en Router.

Para la inserción de los Algoritmos 3DES, AES, y DES; primero se activó la licencia del paquete de tecnología de seguridad (módulo securityk9) en los Router y reiniciamos.

```
R1 (config)# license boot module c2900 technology-package securityk9
```

```
R1 (config)# end
```

```
R1# copy running-config startup-config
```

```
R1# reload
```

Después se configuró la ACL 110 para identificar como primordial el tráfico proveniente de la LAN en el R1 a la LAN en el R3. Este tráfico primordial activa la VPN con IPSec para que se implemente cada vez que haya tráfico entre las LAN de los routers R1 y R3. El resto del tráfico que se origina en las LAN no se cifra.

```
R1 (config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
```

```
R3 (config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
```

Seguidamente se inició con la fase 1 de configurar IPSec, se configuró las propiedades de la política criptográfica ISAKMP 10 en el R1 junto con una clave criptográfica compartida. Después se configuró el algoritmo de cifrado, el método de intercambio de claves y el método DH.

```
R1 (config)# crypto isakmp policy 10
```

```
R1 (config-isakmp)# encryption (aes, 3 des y des)
```

```
R1 (config-isakmp)# authentication pre-share
```

```
R1 (config-isakmp)# group 2
```

```
R1 (config-isakmp)# exit
```

```
R1 (config)# crypto isakmp key cisco address 10.2.2.2
```

En la fase 2 de IPsec se creó el conjunto de transformaciones VPN-SET para usar esp-3des y esp-sha-hmac. Seguidamente, se creó la asignación criptográfica VPN-MAP que vincula todos los parámetros de la fase 2. Se usó el número de secuencia 10 se identificó como una asignación ipsec-isakmp.

```
R1 (config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
```

```
R1 (config)# crypto map VPN-MAP 10 ipsec-isakmp
```

```
R1 (config-crypto-map)# description VPN connection to R3
```

```
R1 (config-crypto-map)# set peer 10.2.2.2
```

```
R1 (config-crypto-map)# set transform-set VPN-SET
```

```
R1 (config-crypto-map)# match address 110
```

```
R1 (config-crypto-map)# exit
```

Por último, se vinculó la asignación criptográfica VPN-MAP a la interfaz de salida Serial 1/0.

```
R1(config)# interface S1/0
```

```
R1(config-if)# crypto map VPN-MAP
```

Para verificar el túnel que se configuró se hizo uso de los comandos:

```
R1 # show run y
```

```
R1 # show crypto ipsec sa
```



### 5.3.1. Configuración de IPSec – 3DES

Configuración e inserción de IPSec y el algoritmo 3DES.

*Figura 48 - Configuración de IPSec -3DES – R1*

```
R1(config)#access-
R1(config)#$ 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#cryp
R1(config)#crypto isakmp poli
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encry
R1(config-isakmp)#encryption ?
  3des  Three key triple DES
  aes   AES - Advanced Encryption Standard.
  des   DES - Data Encryption Standard (56 bit keys).

R1(config-isakmp)#encryption 3des
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#exit
R1(config)#
R1(config)#crypto isakmp key cisco address 10.2.2.2
R1(config)#crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R1(cfg-crypto-trans)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#description VPN connection to R3
R1(config-crypto-map)#set peer 10.2.2.2
R1(config-crypto-map)#set transform-set VPN-SET
R1(config-crypto-map)#match address 110
R1(config-crypto-map)#exit
R1(config)#
R1(config)#interface s1/0
R1(config-if)#crypto map VPN-MAP
R1(config-if)#
*Mar  1 00:09:23.423: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ONexit
R1(config)#exit
***
```

Fuente: *Elaboración Propia*

*Figura 49 - Configuración de IPSec -3DES – R3*

```
R3(config)#
R3(config)#$ 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#encryption ?
  3des  Three key triple DES
  aes   AES - Advanced Encryption Standard.
  des   DES - Data Encryption Standard (56 bit keys).

R3(config-isakmp)#encryption 3des
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 2
R3(config-isakmp)#exit
R3(config)#
R3(config)#crypto isakmp key cisco address 10.1.1.2
R3(config)#crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R3(cfg-crypto-trans)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R3(config-crypto-map)#description VPN connection to R1
R3(config-crypto-map)#set peer 10.1.1.20
R3(config-crypto-map)#set peer 10.1.1.2
R3(config-crypto-map)#set transform-set VPN-SET
R3(config-crypto-map)#match address 110
R3(config-crypto-map)#exit
R3(config)#
R3(config)#interface s1/0
R3(config-if)#crypto map VPN-MAP
R3(config-if)#exit
R3(config)#
```

Fuente: *Elaboración Propia*



### 5.3.2. Configuración de IPSec – AES

Configuración e inserción de IPSec y el algoritmo AES.

*Figura 50 - Configuración de IPSec -AES – R1*

```
R1(config)#
R1(config)#$ 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
access list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
^
% Invalid input detected at '^' marker.

R1(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#exit
R1(config)#crypto isakmp key cisco address 10.2.2.2
R1(config)#crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R1(cfg-crypto-trans)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R1(config-crypto-map)#description VPN connection to R3
R1(config-crypto-map)#set peer 10.2.2.2
R1(config-crypto-map)#set transform-set VPN-SET
R1(config-crypto-map)#match address 110
R1(config-crypto-map)#exit
R1(config)#
R1(config)#interface s1/0
R1(config-if)#crypto map VPN-MAP
R1(config-if)#
*Mar 1 01:26:09.739: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config)#
```

Fuente: *Elaboración Propia*

*Figura 51 - Configuración de IPSec –AES - R3*

```
R3#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#$ 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
access list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
^
% Invalid input detected at '^' marker.

R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#encryption aes
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 2
R3(config-isakmp)#exit
R3(config)#
R3(config)#crypto isakmp key cisco address 10.1.1.2
R3(config)#crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R3(cfg-crypto-trans)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R3(config-crypto-map)#description VPN connection to R1
R3(config-crypto-map)#set peer 10.1.1.2
R3(config-crypto-map)#set transform-set VPN-SET
R3(config-crypto-map)#match address 110
R3(config-crypto-map)#exit
R3(config)#
R3(config)#interface s1/0
R3(config-if)#crypto map VPN-MAP
R3(config-if)#e
*Mar 1 01:24:58.267: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is O
R3(config-if)#exit
```

Fuente: *Elaboración Propia*



### 5.3.3. Configuración de IPSec – DES

Configuración e inserción de IPSec y el algoritmo DES.

*Figura 52 - Configuración de IPSec -DES – R1*

```
R1(config)#
R1(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption des
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#exit
R1(config)#
R1(config)#crypto isakmp key cisco address 10.2.2.2
R1(config)#crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R1(cfg-crypto-trans)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R1(config-crypto-map)#description VPN connection to R3
R1(config-crypto-map)#set peer 10.2.2.2
R1(config-crypto-map)#set transform-set VPN-SET
R1(config-crypto-map)#match address 110
R1(config-crypto-map)#exit
R1(config)#
R1(config)#interface s1/0
R1(config-if)#crypto map VPN-MAP
R1(config-if)#end
*Mar 1 00:10:48.739: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1#
```

**Fuente:** *Elaboración Propia*

*Figura 53 - Configuración de IPSec -DES – R3*

```
R3#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#$ 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#encryption des
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 2
R3(config-isakmp)#exit
R3(config)#
R3(config)#crypto isakmp key cisco address 10.1.1.2
R3(config)#crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R3(cfg-crypto-trans)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R3(config-crypto-map)#description VPN connection to R1
R3(config-crypto-map)#set peer 10.1.1.2
R3(config-crypto-map)#set transform-set VPN-SET
R3(config-crypto-map)#match address 110
R3(config-crypto-map)#exit
R3(config)#
R3(config)#interface s1/0
R3(config-if)#crypto map VPN-MAP
R3(config-if)#
*Mar 1 00:28:35.883: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)#end
```

**Fuente:** *Elaboración Propia*



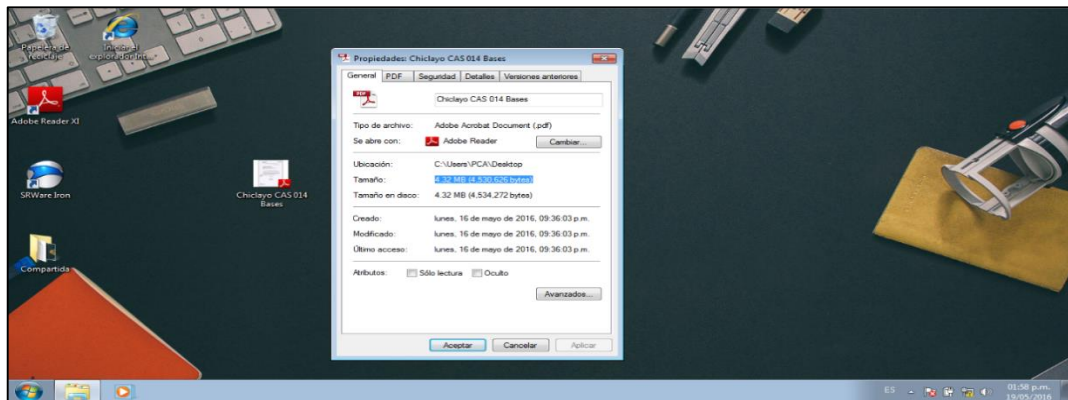
#### 5.4. Captura de Tráfico en VPN

Para el desarrollo de este objetivo se necesitó tener conectados todos los equipos antes mencionados, y la VPN debidamente configurada, además de contar con la Herramienta Wireshark para hacer la Captura Tráfico de voz, video y datos en los escenarios de la red privada virtual implementada.

##### 5.4.1. Captura de tráfico de datos con IPSec y 3DES

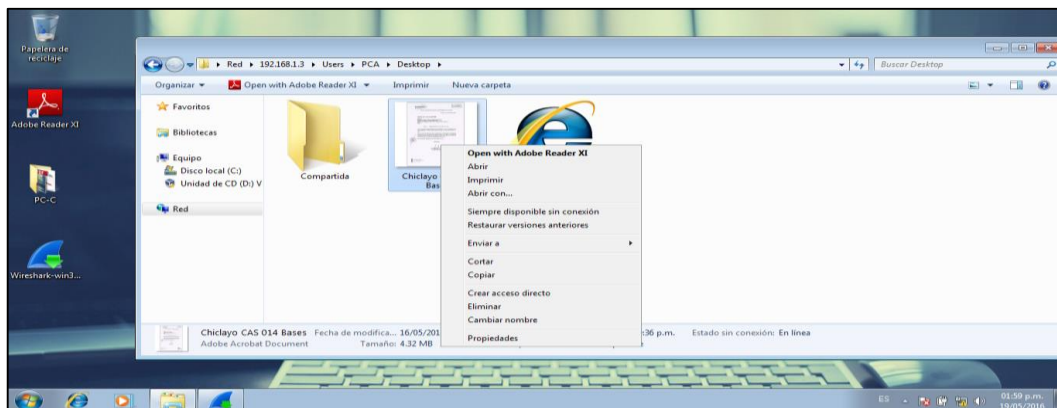
Para la captura de tráfico en la VPN con el Algoritmo de 3DES primero se ubicó el archivo a capturar, se conectó mediante la ip remotamente y se procedió a copiar y a la vez a capturar tráfico con el software Wireshark.

*Figura 54 – Ubicación de Archivo a Compartir en PcA*



Fuente: *Elaboración Propia*

*Figura 55 - Copia de Archivo de PcA a PcC*

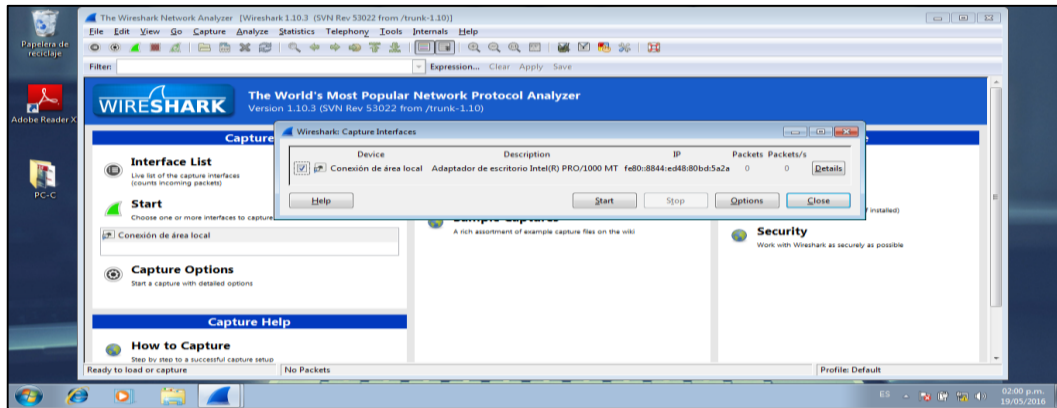


Fuente: *Elaboración Propia*



En la figura 56 se realizó el inicio de la captura de tráfico la PcC haciendo uso del software Wireshark

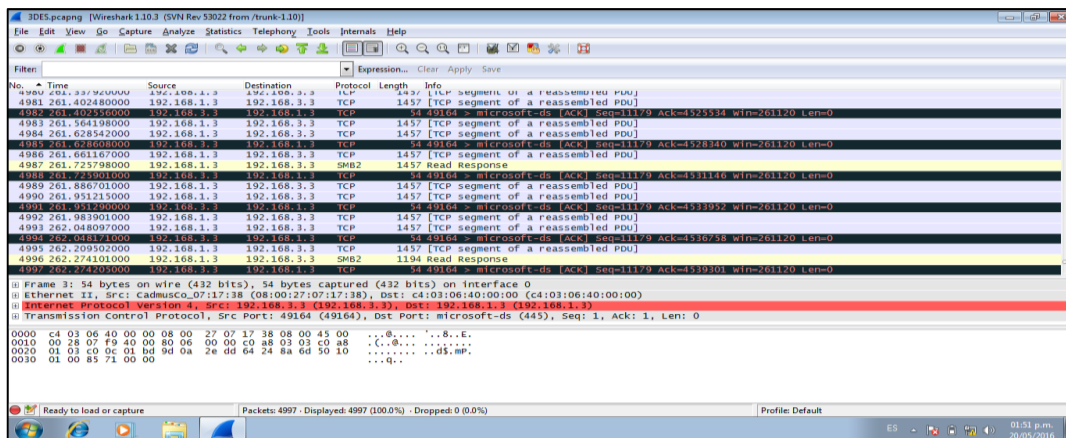
Figura 56 - Inicio de Captura de Tráfico con Wireshark



Fuente: Wireshark

En la figura 57 se realizó la finalización de la captura de tráfico la PcC haciendo uso del software Wireshark. Obteniendo un total de 4997 paquetes capturados para el algoritmo 3DES.

Figura 57 - Fin de Captura de Tráfico con Wireshark

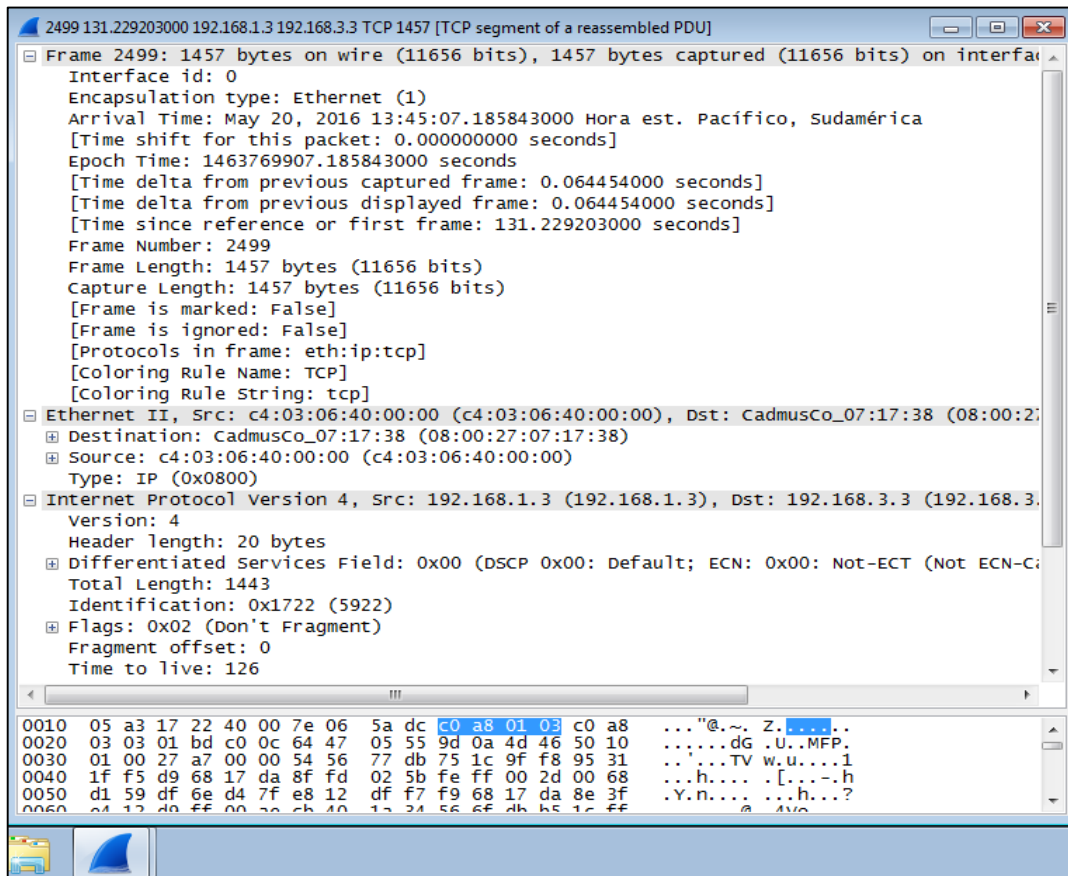


Fuente: Wireshark

En la Figura 58 se obtuvo el paquete capturado número 2499, con un tamaño de 1403 bytes.

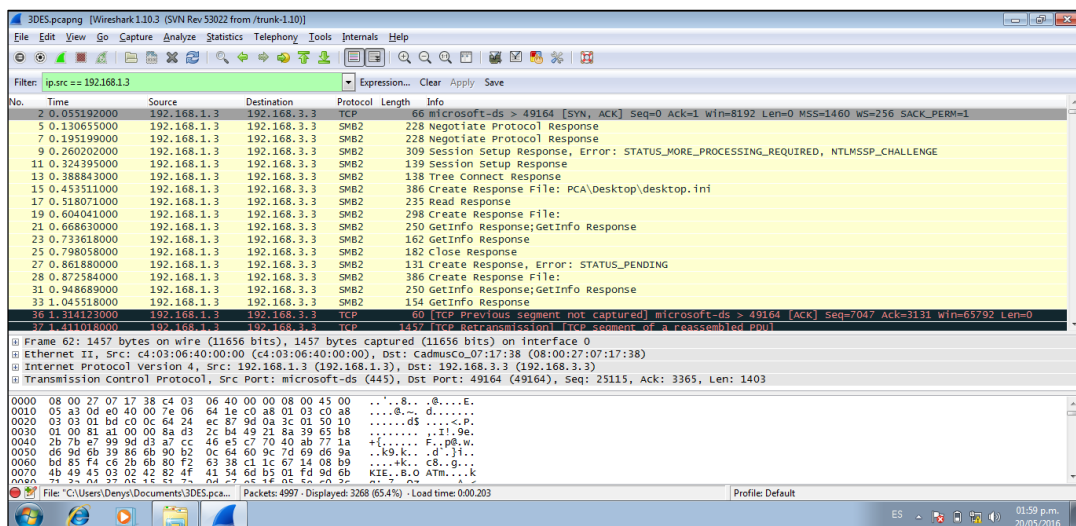


Figura 58 - Estructura de un Paquete Captura



Fuente: Wireshark

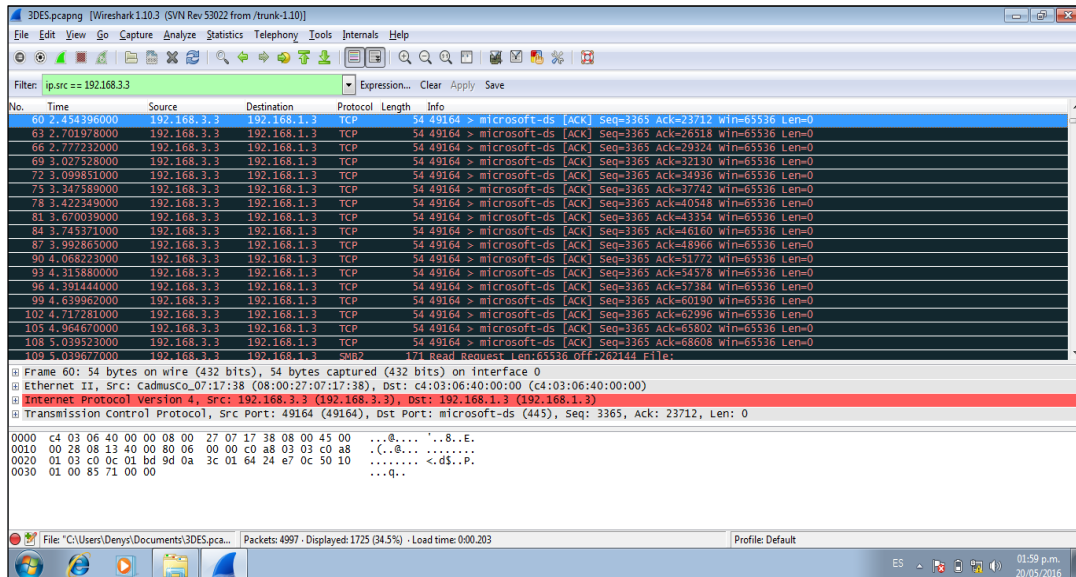
Figura 59 - Paquetes filtrados por el ip de origen – 192.168.1.3



Fuente: Wireshark



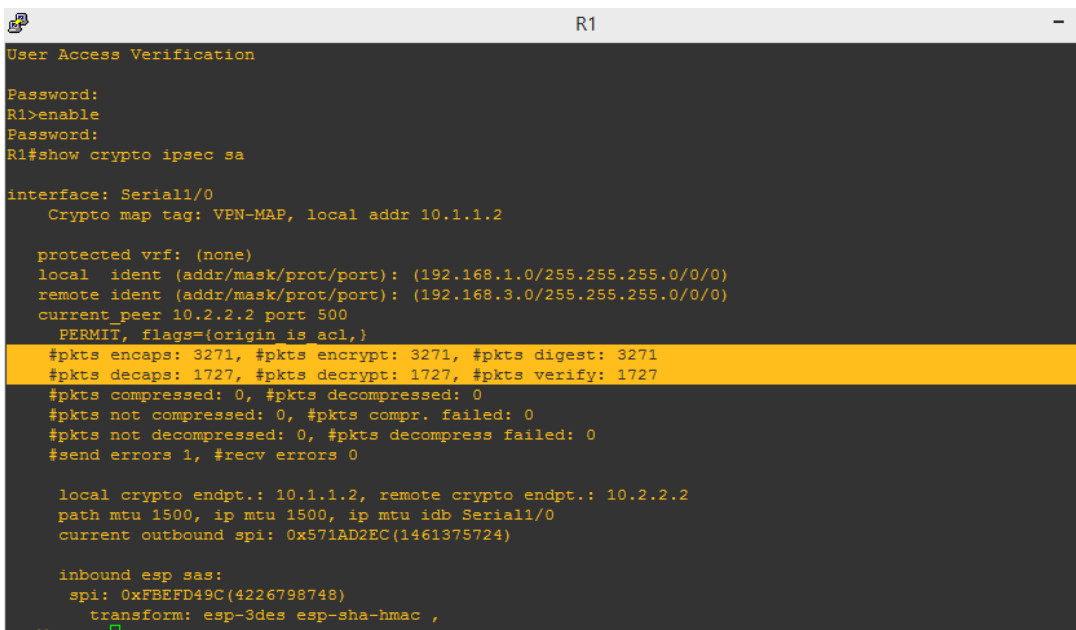
**Figura 60 - Paquetes filtrados por el ip destino – 192.168.3.3**



Fuente: *Wireshark*

En la figura 61, se muestra a través del software PuTTY el router 1, donde se encontró el número de paquetes encapsulados y encriptados que fueron 3271 y el número de paquetes de desencapsulados y descryptados que fueron 1721, todos estos en el router 1.

**Figura 61 - Número de paquetes de R1**



Fuente: *PuTTY*



En la figura 62 se obtuvo el número de paquetes encapsulados, encriptados que fueron 3271 y el número de paquetes de desencapsulados y desencriptados que fueron 1728, todos estos del router 3.

**Figura 62 - Número de paquetes de R3**

```

R3
User Access Verification
Password:
R3>enable
Password:
R3#show crypto ipsec sa

interface: Serial1/0
  Crypto map tag: VPN-MAP, local addr 10.2.2.2

  protected vrf: (none)
  local ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
  current_peer 10.1.1.2 port 500
    PERMIT, flags={origin is acl,}
    #pkts encaps: 1728, #pkts encrypt: 1728, #pkts digest: 1728
    #pkts decaps: 3271, #pkts decrypt: 3271, #pkts verify: 3271
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 2, #recv errors 0

  local crypto endpt.: 10.2.2.2, remote crypto endpt.: 10.1.1.2
  path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
  current outbound spi: 0xFBFEFD49C(4226798748)

  inbound esp sas:
    spi: 0x571AD2EC(1461375724)
      transform: esp-3des esp-sha-hmac ,
  --More--
    
```

Fuente: PuTTY

Tiempo de Copia del Archivo: **00:04:26:59**

Tamaño de Archivo: 4.53 MB

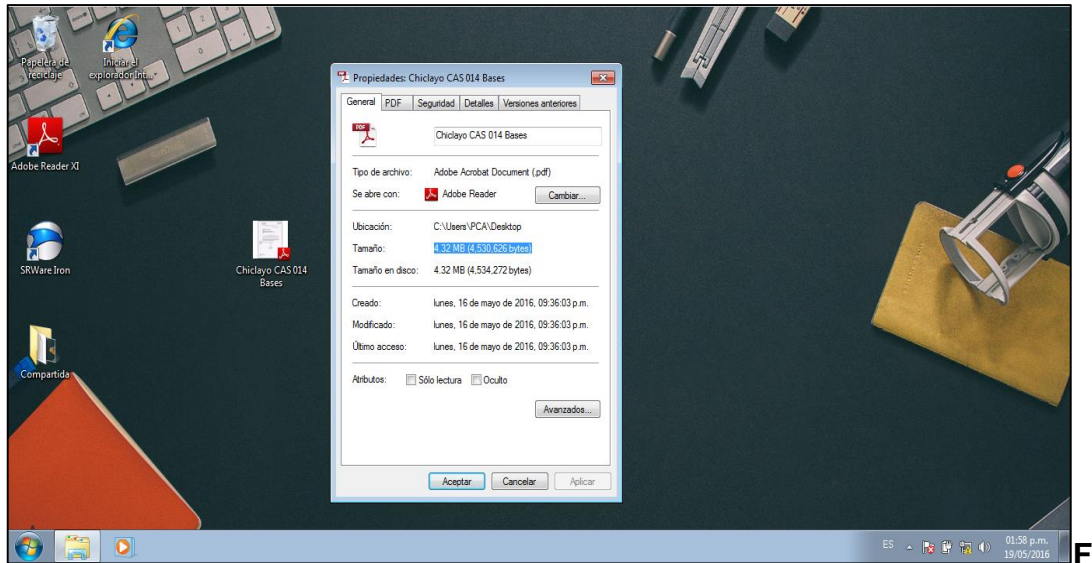




### 5.4.2. Captura de tráfico de datos con IPsec y AES

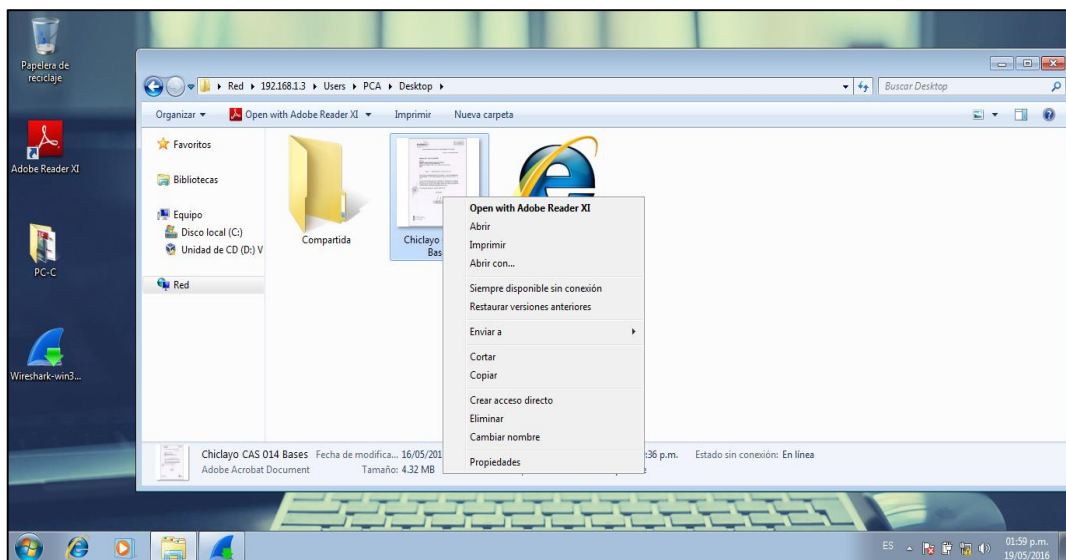
Para la captura de tráfico en la VPN con el Algoritmo de AES primero se ubicó el archivo a capturar, se conectó mediante la ip remotamente y se procedió a copiar y a la vez a capturar tráfico con el software Wireshark.

Figura 63 - Ubicación de Archivo a Compartir en Pca



Fuente: *Elaboración Propia*

Figura 64 - Copia de Archivo de Pca a PcC

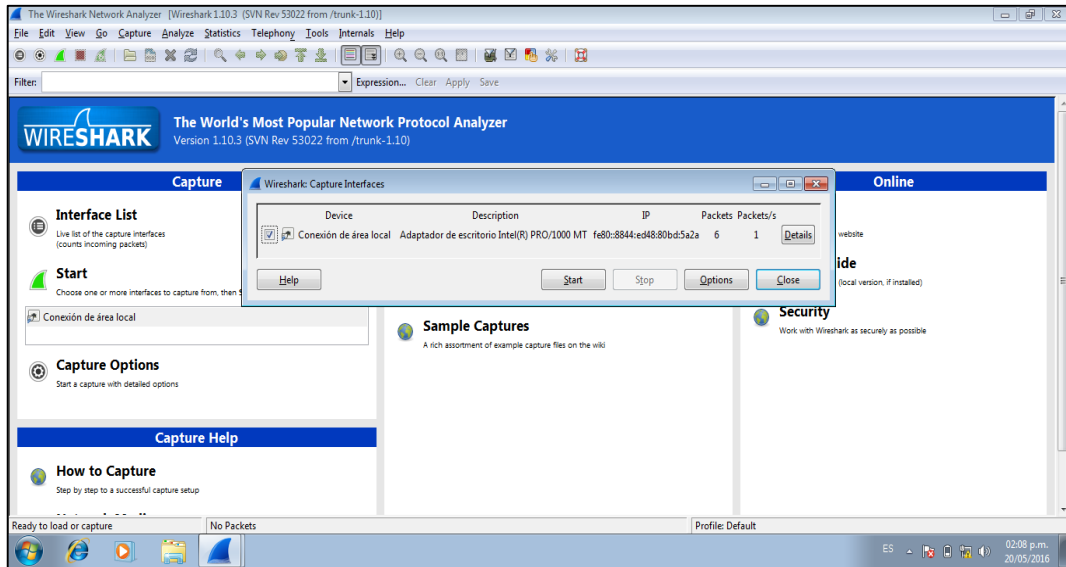


Fuente: *Elaboración Propia*



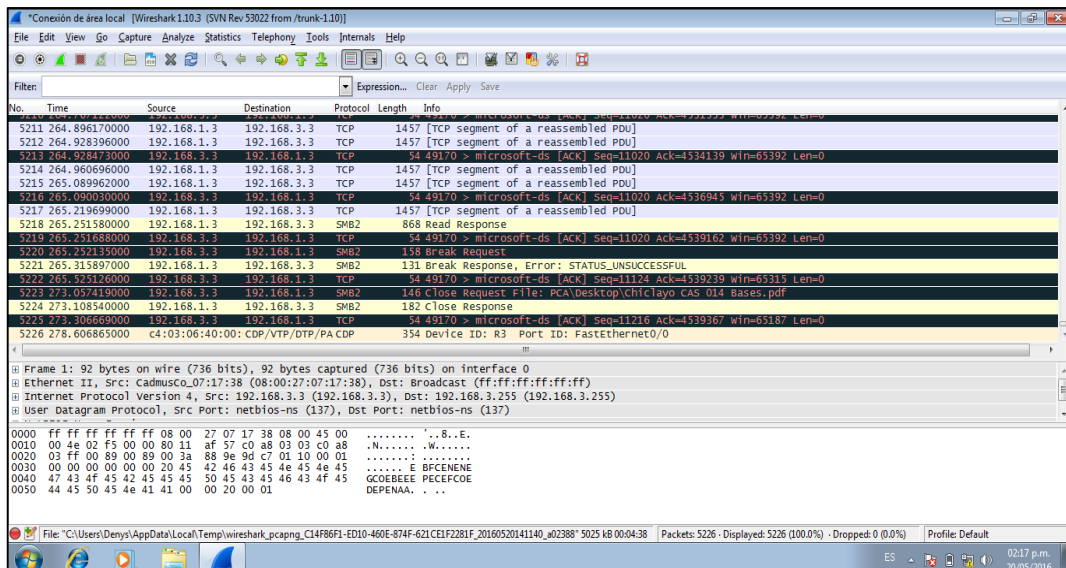
En la figura 65 se realizó el inicio de la captura de tráfico la PcC haciendo uso del software Wireshark.

Figura 65 – Inicio de Captura de Tráfico con Wireshark



Fuente: Wireshark

Figura 66 - Fin de Captura de Tráfico con Wireshark

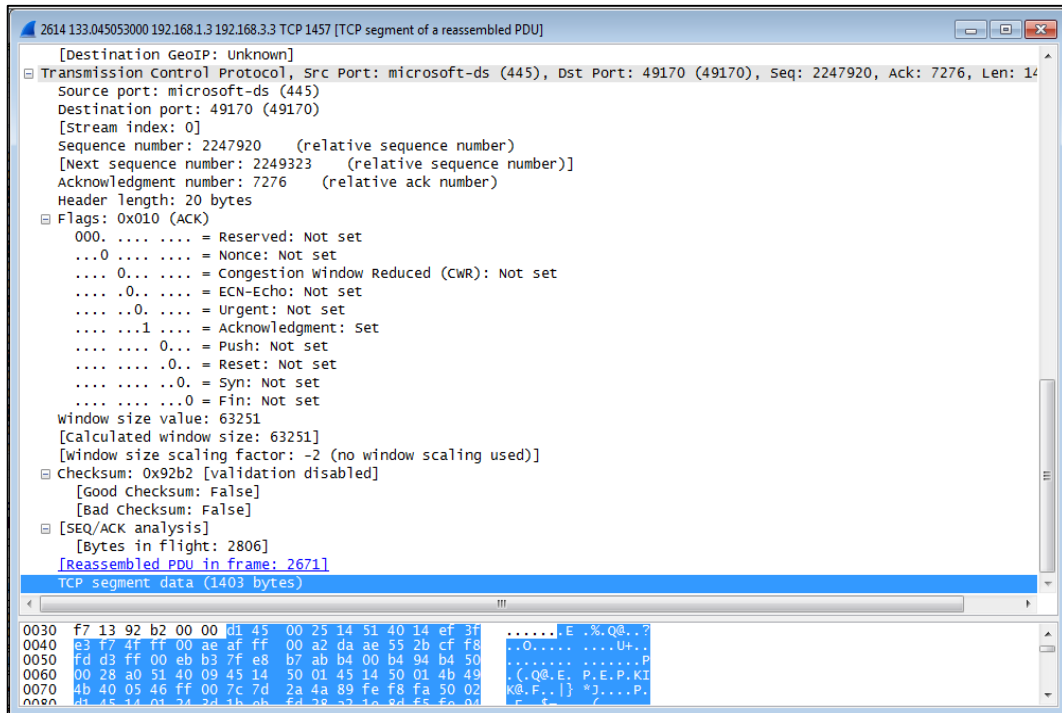


Fuente: Wireshark



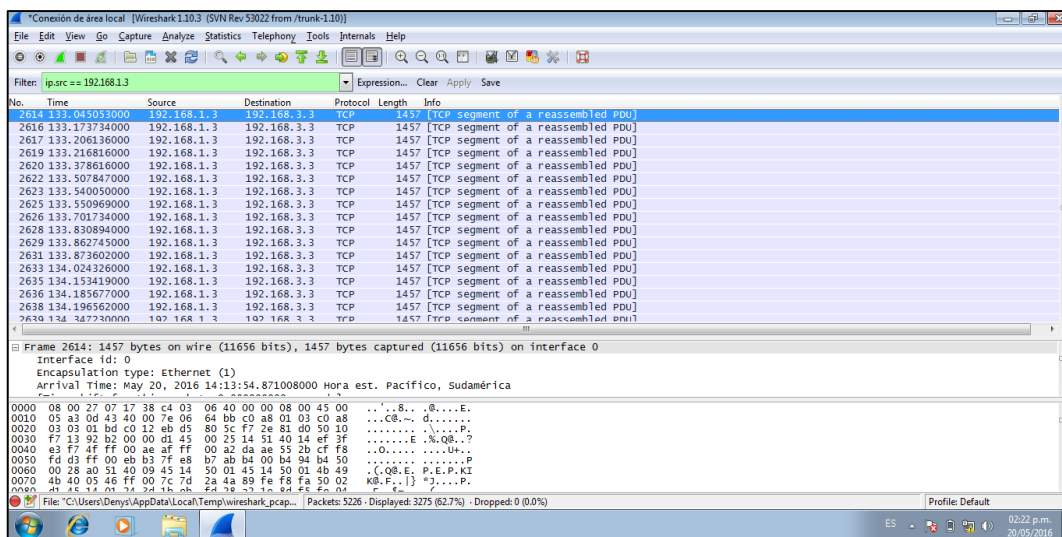
En la Figura 67 se obtuvo el paquete capturado número 2614, con un tamaño de 1403 bytes.

Figura 67 - Estructura de un paquete Capturado



Fuente: Wireshark

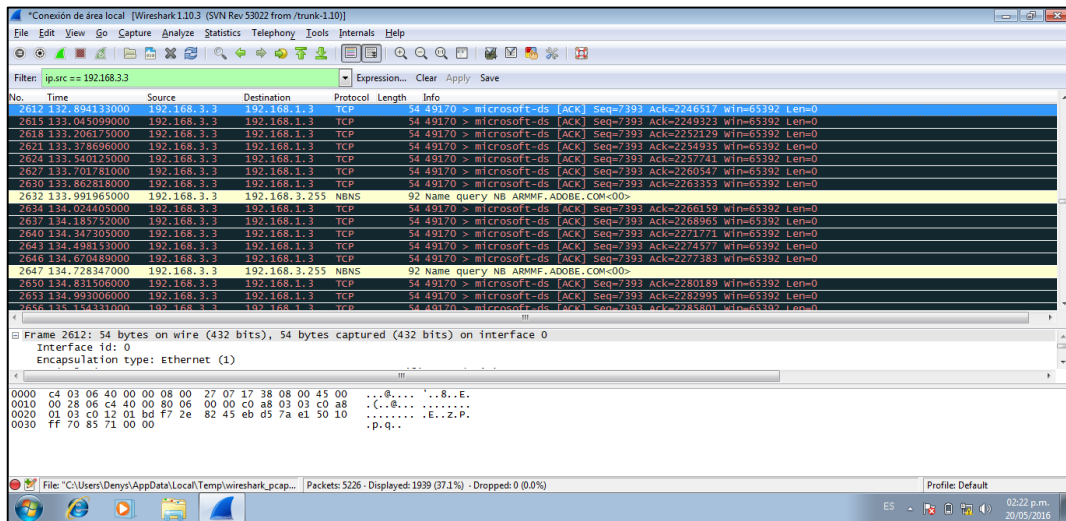
Figura 68 - Paquetes filtrados por el IP de origen – 192.168.1.3



Fuente: Wireshark



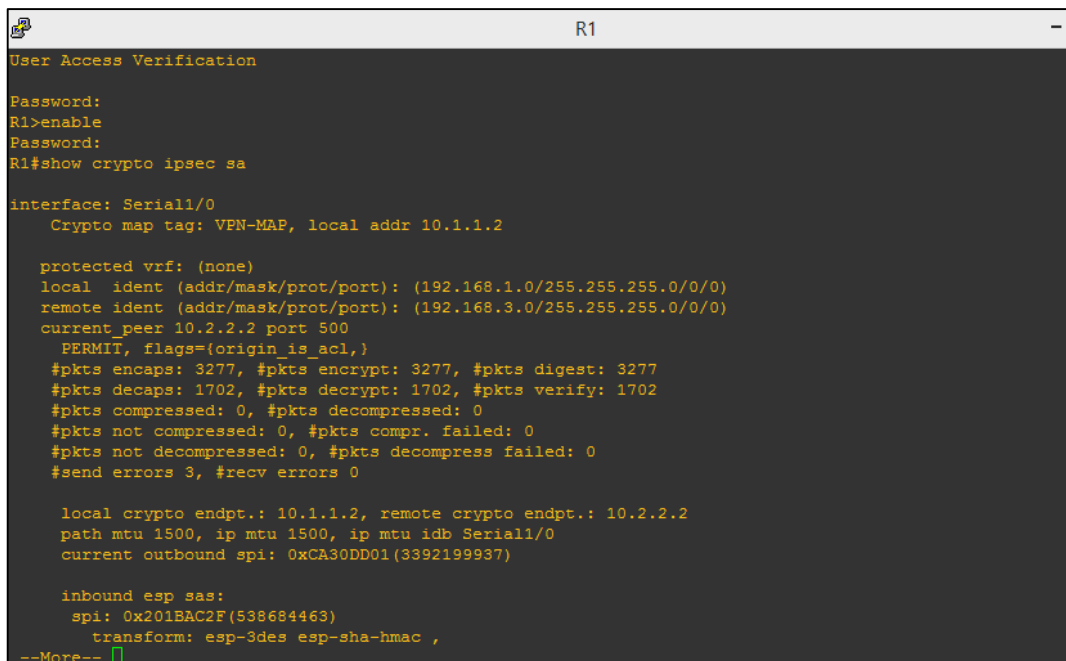
Figura 69 - Paquetes filtrados por el IP destino – 192.168.3.3



Fuente: Wireshark

En la figura 70, se muestra a través del software PuTTY el router 1, donde se encontró el número de paquetes encapsulados y encriptados que fueron 3277 y el número de paquetes de desencapsulados y desenscriptados que fueron 1702, todos estos del router 1.

Figura 70 - Número de paquetes de R1



Fuente: PuTTY



En la figura 71, se muestra a través del software PuTTY el router 3, donde se encontró el número de paquetes encapsulados y encriptados que fueron 3277 y el número de paquetes de desencapsulados y desenscriptados que fueron 1702, todos estos del router 3.

**Figura 71 - Número de paquetes de R3**

```

R2
User Access Verification
Password:
R3>enable
Password:
R3#show crypto ipsec sa

interface: Serial1/0
  Crypto map tag: VPN-MAP, local addr 10.2.2.2

  protected vrf: (none)
  local ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
  current_peer 10.1.1.2 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 1702, #pkts encrypt: 1702, #pkts digest: 1702
    #pkts decaps: 3277, #pkts decrypt: 3277, #pkts verify: 3277
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 2, #recv errors 0

  local crypto endpt.: 10.2.2.2, remote crypto endpt.: 10.1.1.2
  path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
  current outbound spi: 0x201BAC2F(538684463)

  inbound esp sas:
    spi: 0xCA30DD01(3392199937)
      transform: esp-3des esp-sha-hmac ,
  --More--
    
```

Fuente: PuTTY

Tiempo de Copia del Archivo: **00:04:21:42**

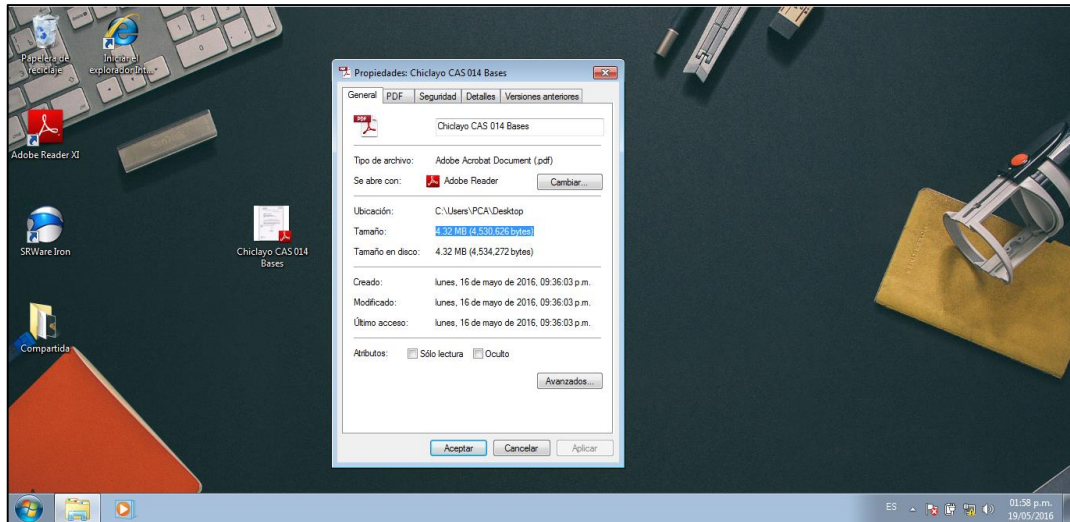
Tamaño de Archivo: 4.53 MB



### 5.4.3. Captura de tráfico de datos con IPsec y DES

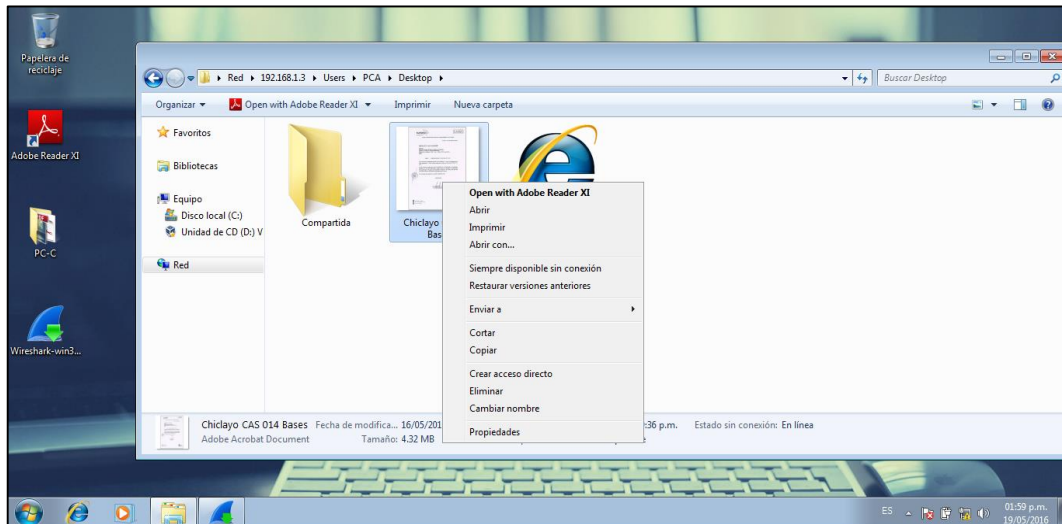
Para la captura de tráfico en la VPN con el Algoritmo de DES primero se ubicó el archivo a capturar, se conectó mediante la ip remotamente y se procedió a copiar y a la vez a capturar de tráfico con el software Wireshark.

*Figura 72 - Ubicación de Archivo a Compartir en Pca*



Fuente: *Elaboración Propia*

*Figura 73 - Copia de Archivo de Pca a Pcc*

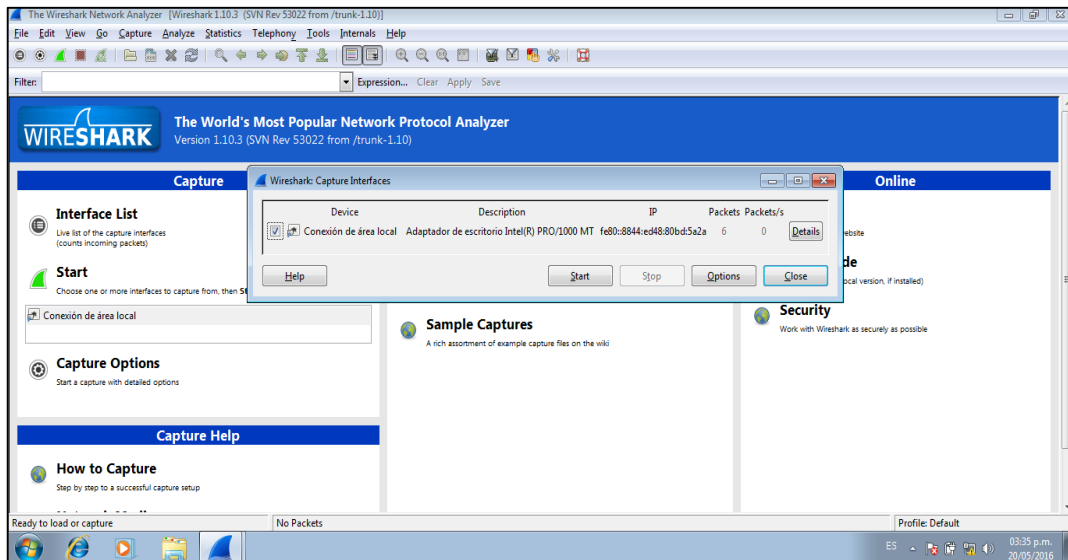


Fuente: *Elaboración Propia*



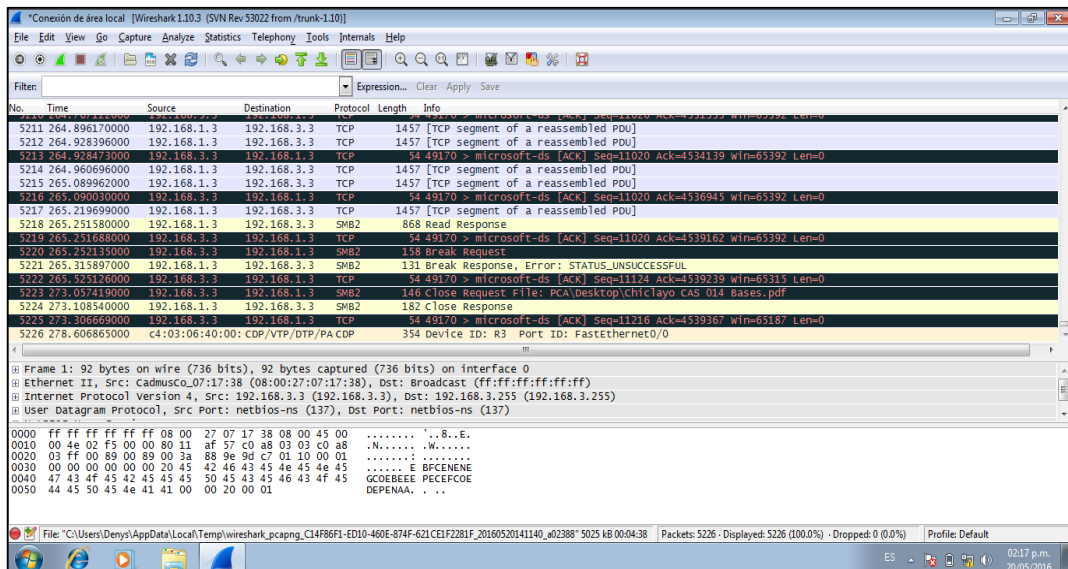
En la figura 74, se realizó el inicio de la captura de tráfico la PcC haciendo uso del software Wireshark.

Figura 74 – Inicio de Captura de Tráfico con Wireshark



Fuente: Wireshark

Figura 75 - Fin de Captura de Tráfico con Wireshark

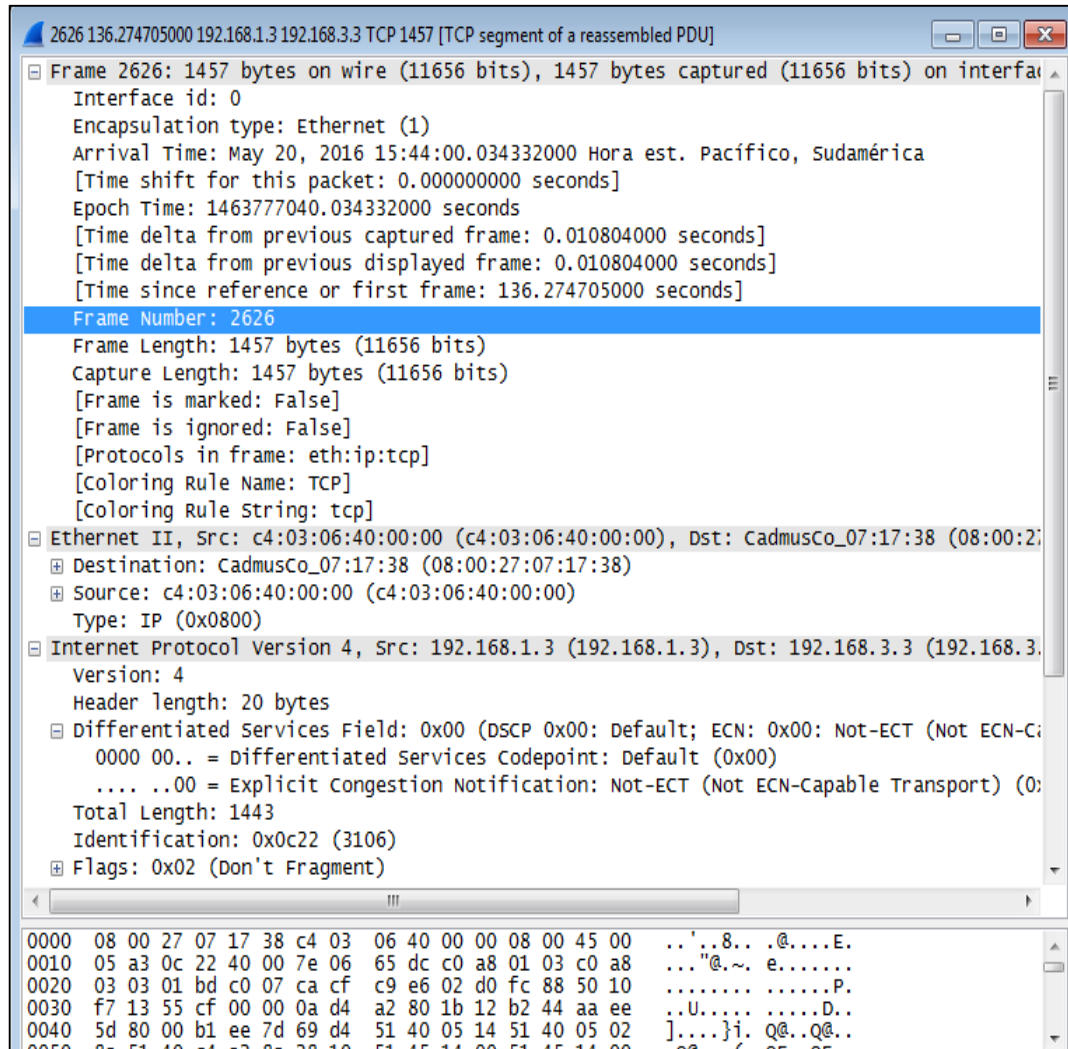


Fuente: Wireshark



En la Figura 76, se obtuvo el paquete capturado número 2614, con un tamaño de 1403 bytes.

**Figura 76 - Estructura de paquete capturado**

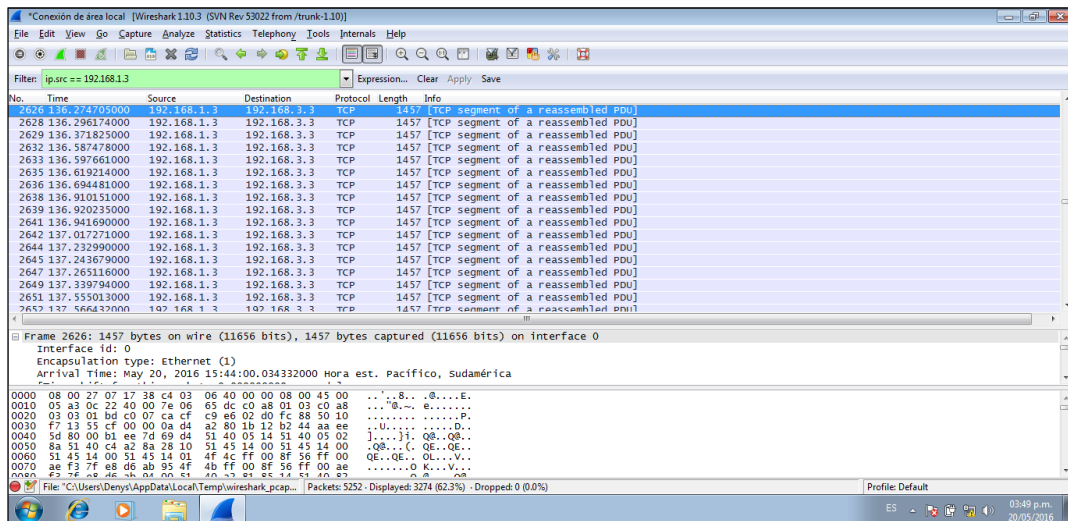


Fuente: *Wireshark*



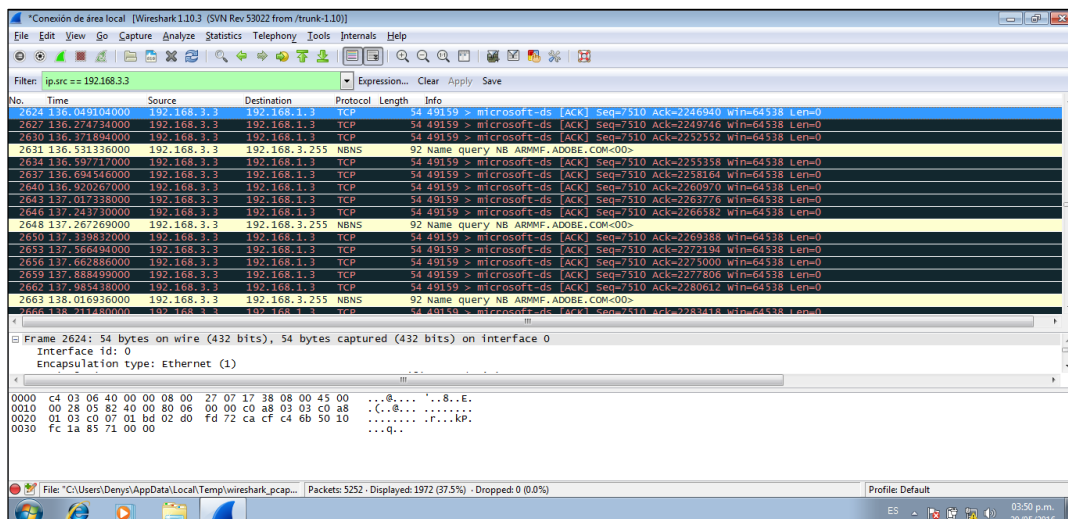


Figura 77 - Paquetes filtrados por el Ip de origen - 192.168.1.3



Fuente: Wireshark

Figura 78 - Paquetes filtrados por el IP destino - 192.168.3.3



Fuente: Wireshark

En la figura 79, se muestra a través del software PuTTY el router 1, donde se encontró el número de paquetes encapsulados y encriptados que fueron 3277 y el número de paquetes de desencapsulados y descriptados que fueron 1713, todos estos en el router 1.



**Figura 79 - Número de paquetes de R1**

```

R1
R1>enable
Password:
R1#show crypto ipsec sa

interface: Serial1/0
  Crypto map tag: VPN-MAP, local addr 10.1.1.2

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
current_peer 10.2.2.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 3277, #pkts encrypt: 3277, #pkts digest: 3277
#pkts decaps: 1713, #pkts decrypt: 1713, #pkts verify: 1713
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.1.2, remote crypto endpt.: 10.2.2.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
current outbound spi: 0x5CD7E414(1557652500)

inbound esp sas:
  spi: 0x5F0F771A(1594849050)
    transform: esp-3des esp-sha-hmac ,
  
```

Fuente: PuTTY

En la figura 80, se muestra el número de paquetes encapsulados y encriptados que fueron 3277 y el número de paquetes de desencapsulados y desenscriptados que fueron 1713, todos estos del router 3.

**Figura 80 - Número de paquetes de R3**

```

R3
R3>enable
Password:
R3#show crypto ipsec sa

interface: Serial1/0
  Crypto map tag: VPN-MAP, local addr 10.2.2.2

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
current_peer 10.1.1.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 1713, #pkts encrypt: 1713, #pkts digest: 1713
#pkts decaps: 3277, #pkts decrypt: 3277, #pkts verify: 3277
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 2, #recv errors 0

local crypto endpt.: 10.2.2.2, remote crypto endpt.: 10.1.1.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
current outbound spi: 0x5F0F771A(1594849050)

inbound esp sas:
  spi: 0x5CD7E414(1557652500)
    transform: esp-3des esp-sha-hmac ,
  
```

Fuente: PuTTY

Tiempo de Copia del Archivo: **00:04:25:07**

Tamaño de Archivo: 4.53 MB



**5.4.4. Captura tráfico de voz y Video con IPsec y 3DES**

Para la captura de tráfico de Voz y Video en la red privada virtual se usó la herramienta de *Polycom Realpresence*. Con la cual se consiguió entablar una comunicación de voz y video con los dos host de la VPN.

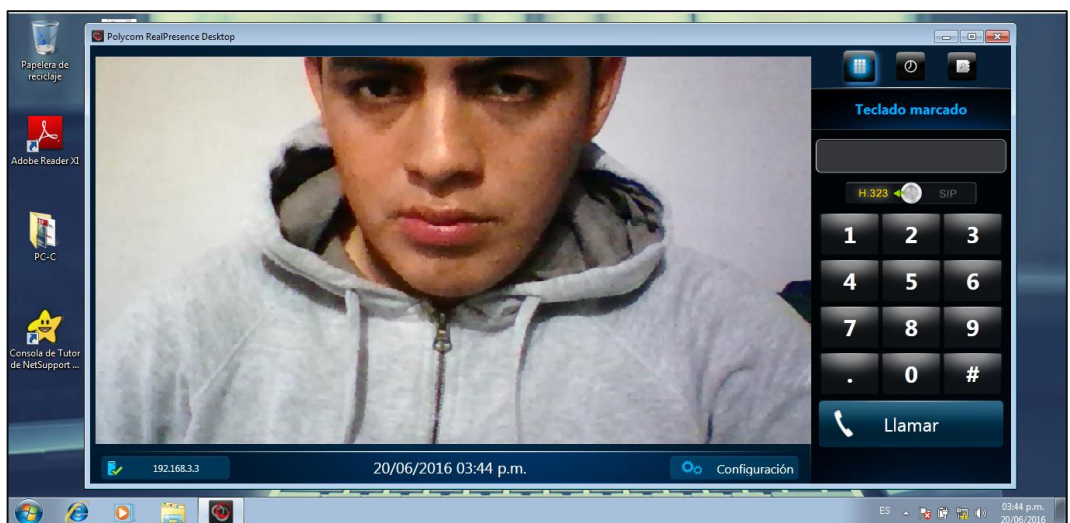
En la figura 81 y 82 se realizó la instalación de la herramienta Polycom RealPresence en los dos host. En la parte derecha se colocó la IP con la cual estableció la comunicación.

*Figura 81: PcA con Polycom Realpresence*



Fuente: *Elaboración Propia*

*Figura 82: PcC con Polycom Realpresence*

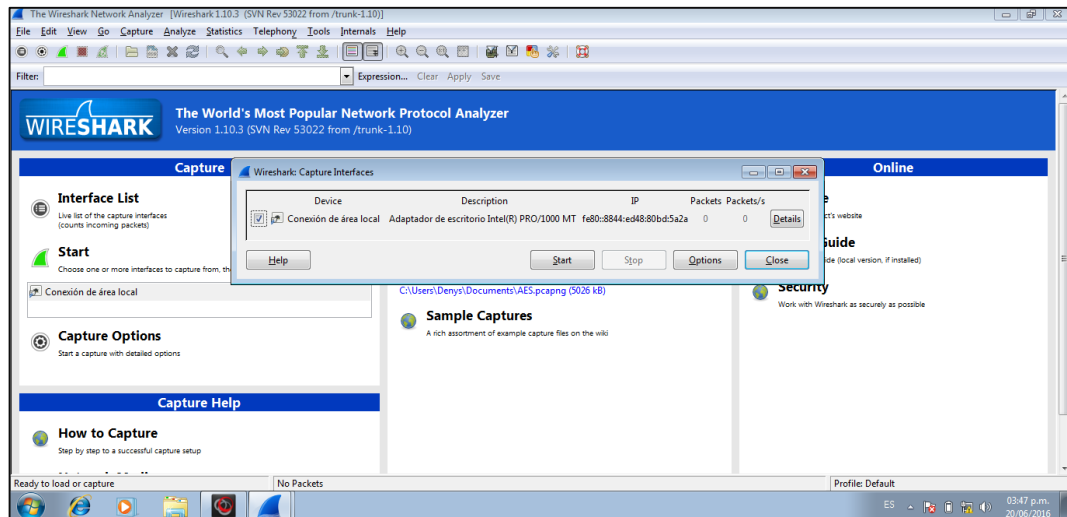


Fuente: *Elaboración Propia*



En la figura 83, se muestra el inicio de la captura de tráfico de voz y video en la PcA con IP 192.168.1.3 y utilizó el algoritmo de 3DES.

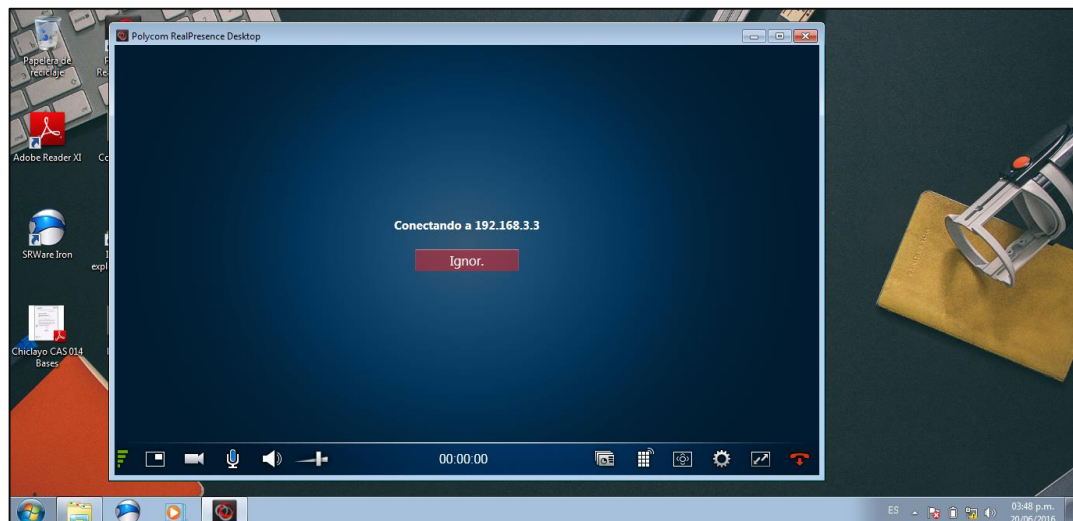
**Figura 83: Inicio de Captura de Voz y Video**



Fuente: *Elaboración Propia*

En la figura 84, se realizó la llamada del host con IP 192.168.1.3 al host con la IP 192.168.3.3 que corresponde a la PcC.

**Figura 84: Llamada de PcA a PcC**

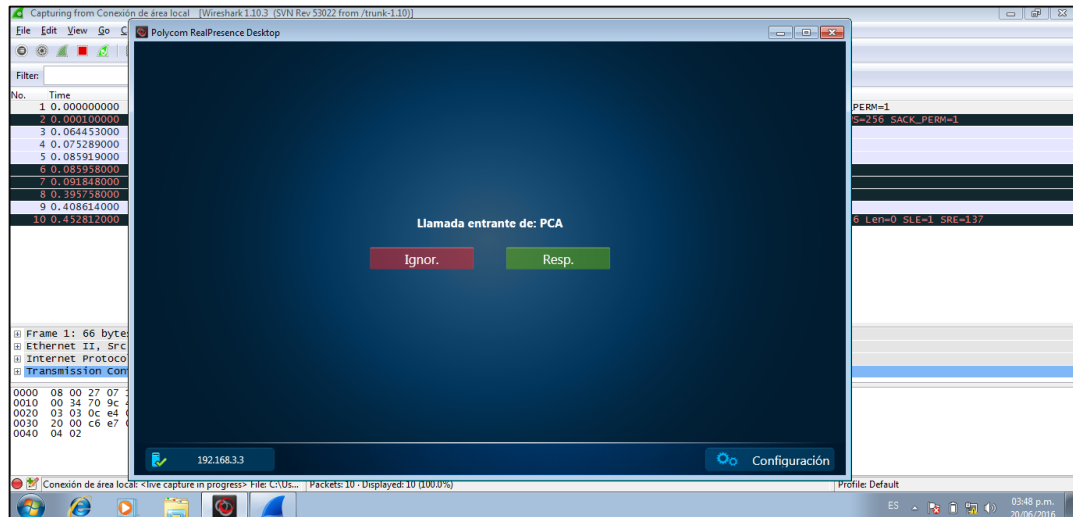


Fuente: *Elaboración Propia*



En la figura 85, se realizó la llamada del host con IP 192.168.1.3 al host con la IP 192.168.3.3 que corresponde a la PcC.

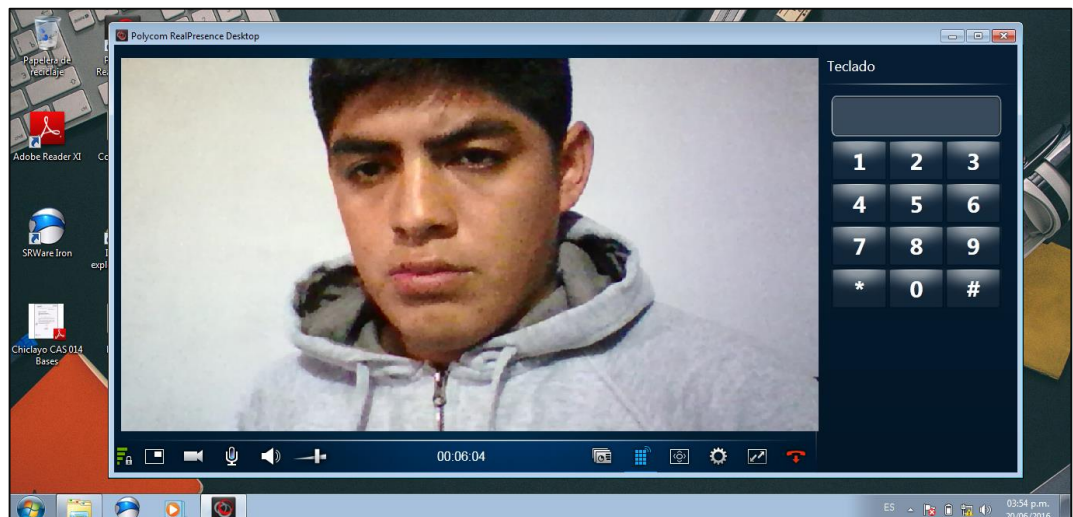
**Figura 85:** Llamada entrante de IP 192.168.1.3



Fuente: *Elaboración Propia*

En la figura 86, se realizó el envío de voz y video de Pca hacia la PcC durante 6 minutos que corresponden a la muestra.

**Figura 86:** Envío de Voz y Video



Fuente: *Elaboración Propia*

Después del que se finalizó el envío de voz y video por la VPN, se procedió



a conectarse al Router R1 a través del software PuTTY (Figura 87), donde se encontró el número de paquetes encapsulados y encriptados que fueron 20182 y el número de paquetes desencapsulados y desencriptados que fueron 20154, todo esto en Router 1 y con el algoritmo de 3DES.

**Figura 87:** Número de paquetes en R1 con 3DES

```

R1
Password:
R1#show crypto ipsec sa

interface: Serial1/0
  Crypto map tag: VPN-MAP, local addr 10.1.1.2

  protected vrf: (none)
  local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
  current_peer 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 20182, #pkts encrypt: 20182, #pkts digest: 20182
    #pkts decaps: 20154, #pkts decrypt: 20154, #pkts verify: 20154
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 2, #recv errors 0

  local crypto endpt.: 10.1.1.2, remote crypto endpt.: 10.2.2.2
  path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
  current outbound spi: 0x6CE422DD(1826890461)
    
```

Fuente: PuTTY

**Figura 88:** Número de paquetes en R3 con 3DES

```

R3
R3>enable
Password:
R3#show crypto ipsec sa

interface: Serial1/0
  Crypto map tag: VPN-MAP, local addr 10.2.2.2

  protected vrf: (none)
  local ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
  current_peer 10.1.1.2 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 20154, #pkts encrypt: 20154, #pkts digest: 20154
    #pkts decaps: 20182, #pkts decrypt: 20182, #pkts verify: 20182
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

  local crypto endpt.: 10.2.2.2, remote crypto endpt.: 10.1.1.2
  path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
    
```

Fuente: PuTTY



#### 5.4.5. Captura tráfico de voz y Video con IPsec y AES

Para la captura de tráfico con el algoritmo AES que realizó el mismo procedimiento de configuración en los host y se usó la herramienta *Polycom Realpresence* (Figuras 81, 82, 83, 84, 85 y 86). Después que se finalizó el envío de voz y video por la VPN, se procedió a conectarse al Router R1 a través del software PuTTY (Figura 89), donde se encontró el número de paquetes encapsulados y encriptados que fueron 20509 y el número de paquetes desencapsulados y descryptados que fueron 20562, todo esto en Router 1 y con el algoritmo de AES.

**Figura 89:** Número de paquetes en R1 con AES

```

R1
User Access Verification
Password:
R1>enable
Password:
R1#show crypto ipsec sa

interface: Serial1/0
  Crypto map tag: VPN-MAP, local addr 10.1.1.2

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
current_peer 10.2.2.2 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 20509, #pkts encrypt: 20509, #pkts digest: 20509
  #pkts decaps: 20562, #pkts decrypt: 20562, #pkts verify: 20562
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 2, #recv errors 0
    
```

Fuente: PuTTY

**Figura 90:** Número de paquetes en R3 con AES

```

R3#show crypto ipsec sa

interface: Serial1/0
  Crypto map tag: VPN-MAP, local addr 10.2.2.2

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
current_peer 10.1.1.2 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 20562, #pkts encrypt: 20562, #pkts digest: 20562
  #pkts decaps: 20509, #pkts decrypt: 20509, #pkts verify: 20509
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0
    
```

Fuente: PuTTY



#### 5.4.6. Captura tráfico de voz y Video con IPsec y DES

Para la captura de tráfico con el algoritmo DES que realizó el mismo procedimiento de configuración en los host y se usó la herramienta Polycom Realpresence (Figuras 81, 82, 83, 84, 85 y 86). Después del que se finalizó el envío de voz y video por la VPN, se procedió a conectarse al Router R1 a través del software PuTTY (Figura 91), donde se encontró el número de paquetes encapsulados y encriptados que fueron 20235 y el número de paquetes desencapsulados y desencriptados que fueron 20244, todo esto en Router 1 y con el algoritmo de DES.

*Figura 91: Número de paquetes en R1 con DES*

```

R1
R1#show crypto ipsec sa
interface: Serial1/0
  Crypto map tag: VPN-MAP, local addr 10.1.1.2

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
current_peer 10.2.2.2 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 20235, #pkts encrypt: 20235, #pkts digest: 20235
  #pkts decaps: 20244, #pkts decrypt: 20244, #pkts verify: 20244
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
    
```

Fuente: PuTTY

*Figura 92: Número de paquetes en R3 con DES*

```

R3
Password:
R3#show crypto ipsec sa
interface: Serial1/0
  Crypto map tag: VPN-MAP, local addr 10.2.2.2

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
current_peer 10.1.1.2 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 20244, #pkts encrypt: 20244, #pkts digest: 20244
  #pkts decaps: 20235, #pkts decrypt: 20235, #pkts verify: 20235
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
    
```

Fuente: PuTTY





## CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

## 6. Conclusiones y Recomendaciones

### 6.1. Conclusiones

Se concluyó que el algoritmo AES es el mejor algoritmo de encriptamiento en cuanto a tiempo de envío, en número de paquetes de encriptación y en el número de paquetes de desencriptación con el protocolo IPSec.

- a) Se seleccionaron los algoritmos criptográficos; concluyendo que los algoritmos que fueron seleccionados para este estudio fueron: AES (Advanced Encryption Standar), DES (Data Encryption Standar) y 3DES (Triple Data Encryption Standar).
- b) Se concluyó con la implementación de tres redes privadas virtuales en el laboratorio de investigación de la escuela (LABSIS), utilizando una topología de red propietaria estándar con el protocolo IPSec.
- c) Se hizo captura de tráfico en las tres redes implementadas con IPsec y con los algoritmos AES, DES y 3DES; obteniendo como conclusión el número de paquetes que genera cada algoritmo, el número de paquetes que encripta y desencripta, también se obtuvo el número de paquetes que encapsula y desencapsula por cada algoritmo.
- d) Se concluyó en la evaluación de datos, voz y video obteniendo el tamaño de los paquetes, número de paquetes, el grado de encriptación y desencriptación. Logrando una matriz de resultados.

Se concluyó que el algoritmo AES es el mejor protocolo de encriptamiento en cuanto a tiempo de envío, número de paquetes de encriptación y en el número de paquetes de desencriptación, número de paquetes de encapsulación y en el número de paquetes de desencapsulación.



## 6.2. Recomendaciones

- a) Se recomienda hacer la comparativa a nivel de protocolos para, denotar así que protocolo ofrece mayor confidencialidad, integridad, vinculación y autenticación de nuestros datos.
- b) Se recomienda implementar en las empresas, redes privadas virtuales, utilizando el algoritmo AES para asegurar la integridad y seguridad de sus datos.
- c) Se recomienda utilizar otras topologías de red e implementar otros protocolos y algoritmos para obtener una evaluación general de los protocolos existentes para redes privadas virtuales.
- d) Se recomienda hacer la captura de tráfico de red en redes inalámbricas y medir cual es el comportamiento los algoritmos AES, DES y 3DES con el protocolo IPSec en estas.

**REFERENCIAS BIBLIOGRÁFICAS:**

Gonzales, P. (2013). *Métodos de encriptación para redes privadas virtuales*.

Universidad Mayor de San Andrés. La Paz – Bolivia.

Tanenbaum, A. (2003). *Redes de Computadoras*. (4° edición). México: Editorial

Pearson Educación.

Cobo, A. (2009). *Estudio científico de las redes de ordenadores*. Madrid: Visión

libros.

Vancells, J. (2002). *Algoritmos y programas*. España: Editorial UOC.

Martínez, F. (2003). *Introducción a la programación estructurada en C*. España:

Universidad de Valencia.

Silva, S. (2005). *Internet y correo electrónico/ Internet and Email*. España: Ideas

Propias Editorial S.L.

Stewart, J. (2010). *Network Security, Firewalls, and VPNs*. Estados Unidos:

Jones & Bartlett Publishers.

Stallins, W. (2004). *Fundamentos de seguridad en redes, aplicaciones y*

*estándares*. Madrid: Editorial Pearson Educación.

Gutierrez, J. (2003). *Protocolos criptográficos y seguridad en redes*. España,

Cantabria: Ediciones Santander.

Alvarado, R. (2010). *Estudio Comparativo de los Mecanismos de Seguridad de*

*los Protocolos para VPNs*. Ecuador, Escuela Superior Politécnica de

Chimborazo.

- Jean-Marc R. (2004). *Seguridad en la informática de empresas*. Barcelona: Ediciones ENI.
- Muhammad, E., Bujar, R.(2015) *Conception of Virtual Private Networks Using IPsec Suite of Protocols, Comparative Analysis of Distributed Database Queries Using Different IPsec Modes of Encryption*. Macedonia: South East European University.
- Gang, Z. (2011). *Research on VPN Network System using IPSec Protocol*. China: School of Computer Science.
- Simion, D., Ursuleanu, M., Graur, A., Potorac, A., Lavric, A. (2013). *Efficiency Consideration for Data Packets Encryption within Wireless VPN Tunneling for Video Streaming*. China: International Journal of computers communications & control.
- Xenakis, C., Laoutaris, N., Merakos, L., Stavrakakis, I. (2006). *A generic characterization of the overheads imposed by IPsec and associated cryptographic algorithms*. Iran: Iran university.
- Perez, M. (2009). *Windows Server 2008: instalación, configuración y administración*. España: RC Libros.
- Romero, M., Sivianes, F., Sanchez, G., Rivera, O., Benjumea, J. (2010). *Sistemas microinformáticos y redes*. España: Editorial Paraninfo.
- Márquez, G. (2015). *IPSec y Redes Privadas Virtuales*. España: Editorial Perfect-bound

Muñoz, A. (2004). *Seguridad europea para EEUU – Algoritmo Criptográfico Rijndael*. Madrid: Editorial Kriptolis

William, S. (2004). *Fundamentos de Seguridad en Redes – Aplicaciones y Estándares*. Madrid: Editorial Pearson Educación. 2° Edi.

Medina, Y., Miranda, H. (2015). *Comparación de Algoritmos Basados en la Criptografía Simétrica DES, AES y 3DES*. Colombia: Revista Mundo FES. Edición N° 9.

# ANEXOS

ANEXO 1: ENTREVISTA JUICIO DE EXPERTOS

**Objetivo:** ANALIZAR COMPARATIVAMENTE ALGORITMOS CRIPTOGRÁFICOS PARA REDES PRIVADAS VIRTULES

Fecha:..... Lugar: ..... Hora Inicio: ..... Hora término: .....

Datos Generales:

Nombre del entrevistado: .....

Profesión u ocupación: ..... Edad: .....

Donde labora: .....

- ¿Ha tenido usted alguna experiencia usando o configurando Redes Privadas Virtuales (VPNs), describa cuáles?  
.....  
.....
- ¿Conoce Usted algoritmos de encriptación para Redes Privadas Virtuales (VPNs), menciónelos, y diga porque los usa?  
.....  
.....
- ¿Cree usted que al analizar comparativamente cada algoritmo criptográfico existente para VPN mejore la integridad de los datos?  
.....  
.....
- ¿Qué criterios usa para elegir que algoritmo implementara en una VPN?  
.....  
.....
- ¿Piensa usted que se debería tener una evaluación de cada algoritmo?  
.....  
.....
- ¿Cree que es necesario utilizar algoritmos para encriptar nuestros datos?  
.....  
.....
- ¿Le gustaría tener una ficha de evaluación de los algoritmos criptográficos para VPN?  
.....  
.....





ANEXO 2: CARACTERISTICAS DE LOS PROTOCOLOS DE ENRUTAMIENTO

Característica	RIPv1	RIPv2	EIGRP	IS-IS	OSPF	BGP
Vector Distancia	✓	✓	✓	X	X	✓
Estado de	X	X	X	✓	✓	X
Direccionamiento sin clase	X	✓	✓	✓	✓	✓
VLSM	X	✓	✓	✓	✓	✓
Sumarización automática	✓	✓	✓			✓
Sumarización manual	X	✓	✓	✓	✓	✓
Requiere diseño jerárquico	X	X	X	✓	✓	X
Tamaño de la red	Pequeño	Pequeño	Grande	Grande	Grande	Muy Grande
Métrica	Saltos	Saltos	Compuesta	Métrica	Costo	Atributos de ruta
Tiempo de convergencia	Lento	Lento	Muy rápido	Rápido	Rápido	Muy lento
Distancia administrativa (AD)	120	120	5/90/170	115	110	20/200
Número de protocolo	X	X	88	124	89	X
Número de	X	520 UDP	X	X	X	179 TCP
Entrada en la tabla de enrutamiento	R	R	D (*)	i	O (*)	B
Tipos de paquetes	Query Update	Query Update	Hello Update Query Reply Ack	Hello Link State Sequence	Hello DBD LSR LSU LSAck	Open Keepalive Update Notification
Temporizadores	Update Invalid Holddown Flush	Update Invalid Holddown Flush	Hello Holdtime Active	CSNP Hello Holding LSP Retransmit	Hello Dead Interval	ConnectRetry Hold Time Keepalive MinASOriginatio nInterval MinRouteAdverti sementInterval



Observaciones de los protocolos de enrutamiento:

1. BGP también se conoce como un protocolo de vector de ruta.
2. En EIGRP, la AD es de 5 para rutas sumariadas, 90 para rutas internas y 170 para rutas externas (redistribuidas dentro de EIGRP)
3. En BGP, la AD para las sesiones BGP externas (eBGP) es de 20 y para las internas (iBGP) es 200
4. En la tabla de enrutamiento, D corresponde a DUAL, el algoritmo principal de EIGRP. Puede aparecer como D EX (Ruta Externa)
5. En la tabla de enrutamiento, OSPF puede aparecer como O IA (Inter Area), O E1 (Ruta externa tipo 1, que incrementa la métrica), O E2 (externa tipo 2, que no incrementa la métrica)
6. En la tabla de enrutamiento es posible encontrar entradas con "o" (en minúscula).

Estas rutas corresponden a ODR (On-demand Routing). No confundir con O (mayúscula) de OSPF



## Solicitud: Acceso a Equipos de Laboratorio de Investigación

Director de Escuela de Ingeniería de Sistemas

**Ing. Tuesta Monteza Víctor Alexci.**

Es grato dirigirme a usted para saludarlo cordialmente y manifestarle, Siendo alumno del 10° ciclo de la carrera de Ingeniería de Sistemas de la Facultad de Ingeniería, Arquitectura y Urbanismo de la Universidad Señor de Sipán, **Denys Ivan Capuñay Puican**, identificado con **DNI 47085290**.

Cursando el curso de TESIS II, teniendo como tema de tesis **ANALISIS COMPARATIVO DE ALGORITMOS CRIPTOGRAFICOS PARA REDES PRIVADAS VIRTUALES**, pido se me **autorice realizar mis pruebas en los equipos de redes existentes en el Laboratorio de Investigación** perteneciente a la escuela.

Siendo estos equipos:

- a) 3 Router Cisco
- b) 2 Switch Cisco
- c) 1 Cable Consola
- d) 4 Cables UTP Norma 568-A
- e) 2 Cables UTP Norma 568-A y 568-B

Sin otro particular me despido de Usted expresándole las muestras de mi especial consideración y estima.

Atentamente,

Denys Ivan Capuñay Puican  
DNI: 47085290

UNIVERSIDAD SEÑOR DE SIPÁN  
MB. VICTOR ALEXCI TUESTA MONTEZA  
DIRECTOR DE INGENIERÍA DE SISTEMAS