



UNIVERSIDAD  
NACIONAL  
DE LOJA

ENSA-CIS-UNL



*Facultad de la Energía, las Industrias y los Recursos Naturales No Renovables*

CARRERA DE INGENIERÍA EN SISTEMAS

**“Desarrollo de un Prototipo de  
Seguridad de la Información Aplicando  
la Técnica de Esteganografía en la  
Capa de Red”**

*“Tesis previa a la Obtención del título de  
Ingeniero en Sistemas”.*

***Autor:***

- Luis Omar Solano Solano

***Director:***

- Ing. Gastón René Chamba Romero, Mg. Sc.

***LOJA-ECUADOR***

***2018***

# **CERTIFICACIÓN DEL DIRECTOR**

Loja, 08 de agosto de 2018

Ing. Gastón René Chamba Romero, Mg. Sc.

**DOCENTE DE LA CARRERA DE INGENIERÍA EN SISTEMAS DE LA FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES DE LA UNIVERSIDAD NACIONAL DE LOJA.**

**CERTIFICA:**

Que el señor Luis Omar Solano Solano, egresado de la carrera de Ingeniería en Sistemas y cuyo tema de trabajo de titulación versa sobre “**Desarrollo de un Prototipo de Seguridad de la Información Aplicando la Técnica de Esteganografía en la Capa de Red**”, ha sido monitoreado, revisado y orientado bajo mi asesoramiento, con pertinencia y con la rigurosidad científica que el trabajo de investigación debe cumplir, por lo cual autorizo su presentación y sustentación.



---

Ing. Gastón René Chamba Romero, Mg. Sc.

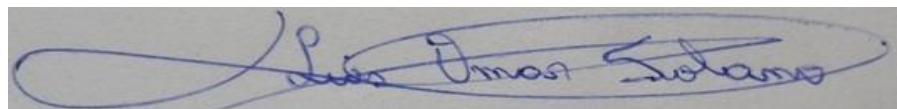
**DIRECTOR DEL TRABAJO DE TITULACIÓN**

## **AUTORÍA**

Yo **LUIS OMAR SOLANO SOLANO** declaro ser autor del presente trabajo de titulación, previo a la obtención del título de Ingeniero en Sistemas denominado "**DESARROLLO DE UN PROTOTIPO DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA TÉCNICA DE ESTEGANOGRAFÍA EN LA CAPA DE RED**", y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales por el contenido de la misma.

Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de la tesis en el Repositorio Institucional – Biblioteca Virtual.

Firma:

A handwritten signature in blue ink, appearing to read "Luis Omar Solano". It is written over a horizontal line and enclosed within a light blue oval.

Cédula: 1105161861

Fecha: 11/10/2018

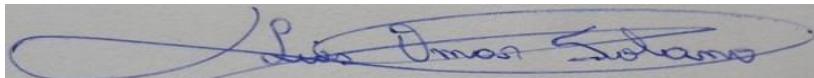
# **CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DEL AUTOR, PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL Y PUBLICACIÓN DEL TEXTO COMPLETO**

Yo, **LUIS OMAR SOLANO SOLANO**, declaro ser el autor de la tesis titulada: **DESARROLLO DE UN PROTOTIPO DE SEGURIDAD DE LA INFORMACIÓN APlicando LA TÉCNICA DE ESTEGANOGRAFÍA EN LA CAPA DE RED**, como requisito para optar al título de **INGENIERO EN SISTEMAS**; autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional:

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia de la tesis que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja a los 9 días del mes de octubre del dos mil dieciocho.



**Firma:** .....

**Autor:** Luis Omar Solano Solano

**Cédula:** 1105161861

**Dirección:** Loja, (Paraguay y España)

**Correo Electrónico:** losolanos@unl.edu.ec

**Teléfono:** Celular: 0968008206

## **DATOS COMPLEMENTARIOS**

**Director de Tesis:** Ing. Gastón René Chamba Romero, Mg. Sc.

**Tribunal de Grado:** Ing. Edison Leonardo Coronel Romero, Mg. Sc.

Ing. Hernán Leonardo Torres Carrión, Mg. Sc.

Ing. Angel Freddy Ganazhapa Malla, Mg. Sc.

## **AGRADECIMIENTO**

Manifiesto mis sinceros agradecimientos a mi madre, mi padre y mi hermano por su apoyo incondicional.

Al personal técnico y administrativo que trabaja en la Universidad Nacional de Loja, en la Facultad de la Energía, las Industrias y los Recursos Naturales no Renovables y en la Carrera de Ingeniería en Sistemas que con sugerencias e ideas me ayudaron en el desarrollo del proyecto de mi tesis.

Así mismo agradezco a mi director de proyecto de tesis al Ing. Gastón René Chamba Romero, el cual con su conocimiento y experiencia me guio y superviso mi trabajo, convirtiéndose en el pilar fundamental para alcanzar mi meta propuesta, obteniendo los resultados esperados.

Igualmente, expreso mi agradecimiento a los docentes que me impartieron su conocimiento, anécdotas y consejos en el trascurso de estos cinco años de estudio universitario los cuales fueron de gran ayuda para poder cumplir con mi objetivo de formación profesional.

## **DEDICATORIA**

Este presente trabajo le dedico a Dios, quien me ha dado fuerzas, valentía y coraje por seguir adelante en los momentos más difíciles teniendo fe en él he podido superar mis temores y mis miedos.

A mis padres, Hermelinda Solano y Hugo Gonza por su apoyo en cada etapa de mi vida, los cuales me han dado un ejemplo de constancia y superación, gracias a sus consejos pude establecer mis objetivos en mi vida y he aquí he logrado uno de ellos. A mi hermano quien ha estado pendiente en toda esta jornada universitaria brindándome su total apoyo.

A mi esposa y mi hija que son la fuente de inspiración logrando darme la fuerza necesaria para no decaer y lograr lo que anhelaba.

A mis compañeros los cuales conocí en los diferentes ciclos de estudio, compartiendo ideas, experiencias, apoyo mutuo, pero sobre todo lo que perdurara siempre una gran amistad.

Luis Solano

# **ÍNDICE DE CONTENIDOS**

<b>CERTIFICACIÓN DEL DIRECTOR .....</b>	I
<b>AUTORÍA .....</b>	II
<b>CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DEL AUTOR .....</b>	III
<b>AGRADECIMIENTO.....</b>	IV
<b>DEDICATORIA .....</b>	V
<b>ÍNDICE DE CONTENIDOS.....</b>	VI
<b>ÍNDICE DE FIGURAS .....</b>	XI
<b>ÍNDICE DE TABLAS .....</b>	XV
<b>a. TÍTULO.....</b>	1
<b>b. RESUMEN.....</b>	2
<b>SUMMARY .....</b>	3
<b>c. INTRODUCCIÓN .....</b>	4
<b>d. REVISIÓN DE LITERATURA .....</b>	5
1. Seguridad de la Información en la actualidad.....	5
2. Revisión bibliográfica .....	6
2.1. Definición de problema.....	6
2.2. Búsqueda, Organización y Análisis de Trabajos .....	7
3. Seguridad de la Información .....	13
3.1. Seguridad Informática.....	13
3.2. Seguridad de red .....	13
4. Amenazas a la información .....	14
4.1. Tipos de Amenazas.....	14
4.1.1. Amenazas Pasivas .....	14
4.1.2. Amenazas Activas.....	15

4.2.	Métodos de ataques a la información .....	16
5.	Criptografía .....	16
5.1.	Criptografía simétrica.....	17
5.1.1.	Algoritmos de Criptografía Simétrica.....	18
5.2.	Criptografía Asimétrica .....	19
5.2.1.	Algoritmos de Criptografía Asimétrica.....	20
5.3.	Certificado Digital.....	20
5.3.1.	Uso de los certificados digitales.....	21
5.4.	Firma Digital .....	21
5.5.	OpenSSL .....	22
5.6.	Aplicación de la criptografía simétrica utilizando OpenSSL.....	22
6.	Esteganografía .....	24
6.1.	Principio de Esteganografía .....	24
6.2.	Tipos de esteganografía .....	26
6.3.	Portadores.....	27
6.4.	Características de Esteganografía .....	27
7.	Esteganografía de Red .....	28
7.1.	Canal encubierto .....	28
7.2.	Características de los canales en cubiertos .....	29
7.3.	Métodos de esteganografía de red.....	30
8.	Esteganografía en la Actualidad.....	30
8.1.	Ocultar en un archivo comprimido (.rar) en una imagen (.jpg). ....	30
8.2.	Ocultar un archivo de texto (.txt) en un archivo ejecutable (.exe).....	33
9.	Sistema de Archivos .....	37
9.1.	Sistema de archivos de nueva tecnología (NTFS) .....	37
9.1.1.	Características de NTFS.....	37
9.1.2.	Almacenamiento NTFS.....	38
9.1.3.	Tipos de Atributos NTFS.....	38
10.	Flujo Alternativo de Datos (ADS) .....	40
10.1.	Características del Flujo Alternativo de Datos .....	41

10.2.	Estructura del Flujo Alternativo de Datos en una Tabla Maestra de Archivos .....	41
10.3.	Ventajas del Flujo Alternativo de Datos.....	42
10.4.	Desventajas del Flujo Alternativo de Datos .....	43
10.5.	Comandos Básicos que utiliza el Flujo Alternativo de Datos .....	43
10.6.	Manipulación del Flujo Alternativo de Datos .....	44
10.6.1.	Insertar texto en un flujo alternativo de datos, utilizando como fichero principal un archivo de texto .....	45
10.6.2.	Visualizar texto insertado en un flujo alternativo de datos.....	46
10.6.3.	Insertar un texto en un flujo alternativo de datos por medio de un script php .....	47
10.6.4.	Insertar una Imagen en un flujo alternativo de datos, utilizando como fichero principal un archivo de texto .....	48
10.6.5.	Visualizar una Imagen insertada en un flujo alternativo de datos .....	49
10.6.6.	Insertar una imagen en un flujo alternativo de datos, usando como fichero principal un archivo ejecutable.....	51
10.6.7.	Insertar un archivo ejecutable en un ADS, utilizando como fichero principal un archivo de texto .....	53
10.6.8.	Ejecutar un archivo tipo exe dentro de un ADS.....	54
11.	Red de computadoras.....	55
11.1.	Tipos de Redes .....	56
11.2.	Topologías de Redes .....	57
11.3.	Protocolo de red .....	57
11.4.	Modelos de Arquitectura de red.....	58
11.5.	Modelo OSI.....	58
11.6.	Modelo TCP/IP .....	59
11.6.1.	Capa de acceso a la red.....	60
11.6.1.1.	Protocolo ARP .....	60
11.6.2.	Capa de Internet .....	60
11.6.2.1.	Protocolo IP.....	61
11.6.2.2.	Protocolo ICMP .....	63
11.6.3.	Capa de Transporte.....	67
11.6.3.1.	Protocolo TCP.....	67

11.6.4.    Capa de Aplicación .....	70
11.6.4.1.    Protocolos de la capa de aplicación .....	70
<b>e. MATERIALES Y MÉTODOS .....</b>	<b>71</b>
1.    Materiales .....	71
1.1.    Talento Humano .....	71
1.2.    Bienes.....	71
1.3.    Servicios .....	72
1.4.    Imprevisto .....	73
1.5.    Total de Recursos.....	73
2.    Métodos y técnicas .....	73
2.1.    Métodos .....	74
2.2.    Técnicas.....	74
2.3.    Metodología de la Ingeniería .....	75
<b>f. RESULTADOS.....</b>	<b>78</b>
Fase 1. Desarrollar una descripción clara y concisa del problema. ....	78
Fase 2. Identificar, al menos de manera tentativa, los factores importantes que afectan al problema o que puedan jugar un papel en su solución.....	79
Fase 3. Proponer un modelo para el problema, utilizando conocimientos científicos o de la ingeniería del fenómeno de bajo estudio consignar todas las limitaciones o supuesto del modelo.....	80
Fase 4. Realizar experimentos apropiados y recolectar datos para probar o validar el modelo tentativo o las conclusiones planteadas en la Fase 2 y la Fase 3.....	82
Fase 5. Manipular el modelo para contribuir a desarrollar una solución del problema. ....	85
Fase 6. Realizar un experimento apropiado para confirmar que la solución propuesta al problema es efectiva y eficiente .....	90
Fase 7. Obtener conclusiones y/o recomendaciones con base a la solución propuesta.....	108
<b>g. DISCUSIÓN.....</b>	<b>109</b>
<b>h. CONCLUSIONES.....</b>	<b>111</b>
<b>i. RECOMENDACIONES .....</b>	<b>112</b>

<b>j. BIBLIOGRAFÍA .....</b>	<b>113</b>
<b>k. ANEXOS .....</b>	<b>116</b>

## ÍNDICE DE FIGURAS

<b>Fig. 1</b> Ilustración grafica de la problemática [Fuente Propia].....	7
<b>Fig. 2</b> Ataque pasivo [Fuente propia].....	15
<b>Fig. 3</b> Ataque activo [Fuente propia].....	15
<b>Fig. 4</b> Criptografía Simétrica [Fuente propia] .....	17
<b>Fig. 5</b> Criptografía Asimétrica [Fuente propia] .....	19
<b>Fig. 6</b> Firma digital [23] .....	21
<b>Fig. 7</b> Esquema de criptografía simétrica [Fuente propia].....	22
<b>Fig. 8</b> Ejecución de openssl en cmd [Fuente propia] .....	23
<b>Fig. 9</b> Crear una clave aleatoria [Fuente propia] .....	23
<b>Fig. 10</b> Cifrar el archivo "Rol_Pagos.docx" [Fuente propia] .....	23
<b>Fig. 11</b> Descifrar la información del archivo "Rol_Pagos.encrypted" [Fuente propia].....	24
<b>Fig. 12</b> Archivo portador "Ibbox.jpg" y archivo a ocultar "Tprueba.rar" [Fuente propia].....	31
<b>Fig. 13</b> Archivo portador + archivo a ocultar = archivo resultante [Fuente propia].....	31
<b>Fig. 14</b> Estructura hexadecimal del archivo "Ibbox.jpg" [Fuente propia].....	32
<b>Fig. 15</b> Estructura del archivo "resultado.jpg" [Fuente propia].....	33
<b>Fig. 16</b> Recuperación del archivo oculto [Fuente propia] .....	33
<b>Fig. 17</b> Archivo portador "calc.exe" y archivo a ocultar "Usuarios_Contra.txt" [Fuente propia] .....	34
<b>Fig. 18</b> Archivo portador ejecutable + archivo a ocultar texto = archivo resultante [Fuente propia] .....	34
<b>Fig. 19</b> Nuevo objeto de la suma binaria "calc_texto.exe" [Fuente propia] .....	34
<b>Fig. 20</b> Estructura hexadecimal del archivo "calc.exe" [Fuente propia] .....	35
<b>Fig. 21</b> Estructura del archivo "calc_texto.exe" [Fuente propia] .....	36
<b>Fig. 22</b> Recuperación de archivo oculto [Fuente propia] .....	36
<b>Fig. 23</b> Registro tabla maestra de archivo sin un flujo alternativo de datos [31] .....	41
<b>Fig. 24</b> Registro tabla maestra de archivo con un flujo alternativo de datos [31] .....	42
<b>Fig. 25</b> Estructura de un fichero principal con archivos ocultos [Fuente propia] .....	44
<b>Fig. 26</b> Creación (ads – fichero principal) insertar (archivo de texto) [Fuente propia] .....	45

<b>Fig. 27</b> Visualización del texto del fichero principal usando el comando “type” [Fuente propia] .....	46
<b>Fig. 28</b> Visualizar el texto insertado en un ads usando el comando “more” [Fuente propia] .....	46
<b>Fig. 29</b> Visualizar el texto de un ads con el programa " Notepad" [Fuente propia].....	47
<b>Fig. 30</b> Script php “scriptPHP.php” [Fuente propia].....	47
<b>Fig. 31</b> Insertar texto en un ads utilizando un script php [Fuente propia] .....	48
<b>Fig. 32</b> Archivo imagen y archivo de texto [Fuente propia] .....	48
<b>Fig. 33</b> Insertar un archivo imagen en un ads, oculto en un fichero principal de tipo texto [Fuente propia].....	49
<b>Fig. 34</b> Visualizar una imagen con el comando "more" [Fuente propia] .....	49
<b>Fig. 35</b> Visualizar un archivo de imagen insertado en un ads utilizando “Paint” [Fuente propia] .....	50
<b>Fig. 36</b> Visualizar una imagen insertada en un ads por medio de un script php [Fuente propia] .....	51
<b>Fig. 37</b> Fichero principal y archivo de imagen [Fuente propia].....	51
<b>Fig. 38</b> Insertar y visualizar una imagen en un ads de tipo exe [Fuente propia] .....	52
<b>Fig. 39</b> Enlistar los ads contenidos en un fichero principal utilizando el comando "dir/r" [Fuente propia].....	52
<b>Fig. 40</b> Fichero principal (FPnetexe.txt) y archivo ejecutable (net.txt) [Fuente propia] .....	53
<b>Fig. 41</b> Insertar un archivo ejecutable en un ads, contenido en un fichero principal de tipo texto [Fuente propia] .....	53
<b>Fig. 42</b> Ejecución de un archivo ejecutable insertado en un ads [Fuente propia] .....	54
<b>Fig. 43</b> Red de computadoras [Fuente Propia] .....	55
<b>Fig. 44</b> Red de computadoras [Fuente Propia] .....	58
<b>Fig. 45</b> Datagrama del protocolo de internet [35] .....	62
<b>Fig. 46</b> Datagrama IP / paquete ICMP [36].....	64
<b>Fig. 47</b> Metodología de la ingeniería [42].....	75
<b>Fig. 48</b> Descripción grafica del problema en la red [Fuente propia] .....	78
<b>Fig. 49</b> Prototipo de seguridad de la información [Fuente propia] .....	<b>¡Error! Marcador no definido.</b>

<b>Fig. 50</b> Configuración del router “TP-LINK” [Fuente Propia].....	86
<b>Fig. 51</b> Ejecución de openssl [Fuente Propia].....	87
<b>Fig. 52</b> Ejecución de scapy [Fuente Propia] .....	89
<b>Fig. 53</b> Generación de clave aleatoria [Fuente Propia] .....	91
<b>Fig. 54</b> Cifrado de archivos de la carpeta “Documentos_1” [Fuente Propia] .....	92
<b>Fig. 55</b> Cifrado de archivos de la carpeta “Documentos_2” [Fuente Propia] .....	92
<b>Fig. 56</b> Cifrado de archivos de la carpeta “Documentos_3” [Fuente Propia] .....	92
<b>Fig. 57</b> Cifrado de archivos de la carpeta “Archivos_Ejecutable” [Fuente Propia] .....	92
<b>Fig. 58</b> Cifrado de archivos de la carpeta “Archivos_Multimedia” [Fuente Propia] .....	92
<b>Fig. 59</b> Archivos cifrados en el fichero principal "Fichero_principal_documentos_1.txt" [Fuente Propia] .....	94
<b>Fig. 60</b> Archivos cifrados en el fichero principal "Fichero_principal_documentos_2.txt" [Fuente Propia] .....	94
<b>Fig. 61</b> Archivos cifrados en el fichero principal "Fichero_principal_documentos_3.txt" [Fuente Propia] .....	95
<b>Fig. 62</b> Archivos cifrados en el fichero principal "Fichero_principal_ejecutable.txt" [Fuente Propia].....	95
<b>Fig. 63</b> Archivos cifrados en el fichero principal "Fichero_principal_multimedia.txt" [Fuente Propia].....	96
<b>Fig. 64</b> Direcciones ip del receptor 1 [Fuente Propia].....	96
<b>Fig. 65</b> Direcciones ip de receptor 2 [Fuente Propia].....	97
Fig. 66 Direcciones ip del emisor [Fuente Propia] .....	97
<b>Fig. 67</b> Transmisión de ficheros principales al receptor 1, versión IPV4 [Fuente Propia]..	98
<b>Fig. 68</b> Transmisión de ficheros principales al receptor 1, versión IPV6 [Fuente Propia].	98
<b>Fig. 69</b> Transmisión de ficheros principales al receptor 2, versión IPV4 [Fuente Propia].	99
<b>Fig. 70</b> Estadística de tiempos de transmisión [Fuente Propia] .....	99
<b>Fig. 71</b> Transmisión de la clave al receptor 1, versión IPV4 [Fuente Propia] .....	101
<b>Fig. 72</b> Transmisión de la clave al receptor 1, versión IPV6 [Fuente Propia] .....	101
<b>Fig. 73</b> Transmisión de la clave al receptor 2, versión IPV4 [Fuente Propia] .....	101
<b>Fig. 74</b> Recepción de ficheros principales receptor 1 [Fuente Propia].....	102
<b>Fig. 75</b> Recepción de ficheros principales receptor 2 [Fuente Propia].....	102

<b>Fig. 76</b> Archivos cifrados insertado en los ficheros principales del receptor 1 [Fuente Propia].....	102
<b>Fig. 77</b> Archivos cifrados insertado en los ficheros principales del receptor 2 [Fuente Propia].....	103
<b>Fig. 78</b> Filtro de paquetes ICMP por el receptor 1, versión IPV4 [Fuente Propia] .....	103
<b>Fig. 79</b> Filtro de paquetes ICMP por el receptor 2, versión IPV4 [Fuente Propia] .....	104
<b>Fig. 80</b> Filtro de paquetes ICMP por el receptor 1, versión IPV6 [Fuente Propia] .....	104
<b>Fig. 81</b> Creación de accesos directos, de archivos cifrados [Fuente Propia] .....	105
<b>Fig. 82</b> Accesos directos creados [Fuente Propia].....	106
<b>Fig. 83</b> Extracción de archivos cifrados de los accesos directos [Fuente Propia].....	106
<b>Fig. 84</b> Archivos cifrados [Fuente Propia] .....	106
<b>Fig. 85</b> Descifrar archivos con openssl [Fuente Propia] .....	107
<b>Fig. 86</b> Archivos descifrados [Fuente Propia].....	108

## **ÍNDICE DE TABLAS**

<b>TABLA I ECUACIONES DE BÚSQUEDA .....</b>	<b>8</b>
<b>TABLA II ORGANIZACIÓN Y ANÁLISIS DE LOS TRABAJOS DE REVISIÓN BIBLIOGRÁFICA.....</b>	<b>9</b>
<b>TABLA III ÁREAS QUE CUBRE LA SEGURIDAD INFORMÁTICA.....</b>	<b>13</b>
<b>TABLA IV MATRIZ QUE UTILIZARON LOS PRISIONEROS DE VIETNAM [26] .....</b>	<b>25</b>
<b>TABLA V CARACTERÍSTICAS DE NTFS .....</b>	<b>38</b>
<b>TABLA VI ALMACENAMIENTO NTFS.....</b>	<b>38</b>
<b>TABLA VII ATRIBUTOS NTFS.....</b>	<b>39</b>
<b>TABLA VIII IDENTIFICADORES DEL FLUJO ALTERNATIVO DE DATOS.....</b>	<b>40</b>
<b>TABLA IX COMANDOS BÁSICOS PARA CREAR, MODIFICAR Y VER FLUJO ALTERNATIVO DE DATOS .....</b>	<b>43</b>
<b>TABLA X TIPOS DE REDES.....</b>	<b>56</b>
<b>TABLA XI CLASES DE DIRECCIONES DE RED.....</b>	<b>61</b>
<b>TABLA XII TIPOS DE MENSAJES ICMP .....</b>	<b>64</b>
<b>TABLA XIII ENCABEZADO DE MENSAJE ECHO REPLY Y ECHO REQUEST .....</b>	<b>66</b>
<b>TABLA XIV CABECERA TCP .....</b>	<b>68</b>
<b>TABLA XV TALENTO HUMANO .....</b>	<b>71</b>
<b>TABLA XVI BIENES.....</b>	<b>72</b>
<b>TABLA XVII SERVICIOS .....</b>	<b>72</b>
<b>TABLA XVIII IMPREVISTO.....</b>	<b>73</b>
<b>TABLA XIX TOTAL RECURSOS.....</b>	<b>73</b>
<b>TABLA XX MÉTODOS DE LA TÉCNICA DE CRIPTOGRAFÍA .....</b>	<b>79</b>
<b>TABLA XXI MÉTODOS DE LA TÉCNICA DE ESTEGANOGRAFÍA .....</b>	<b>79</b>
<b>TABLA XXII DESCRIPCIÓN DE CRIPTOGRAFÍA SIMÉTRICA Y ASIMÉTRICA.....</b>	<b>82</b>
<b>TABLA XXIII COMPARACIÓN DE PROTOCOLOS DE RED.....</b>	<b>83</b>
<b>TABLA XXIV INSTALACIONES DE HERRAMIENTAS DE SOFTWARE .....</b>	<b>85</b>
<b>TABLA XXV ARCHIVOS DE EXPERIMENTOS .....</b>	<b>90</b>
<b>TABLA XXVI CREACIÓN DE FICHEROS PRINCIPALES .....</b>	<b>93</b>
<b>TABLA XXVII TABLA DE TIEMPOS DE CONTROL DE TRANSMISIÓN DE ARCHIVOS</b>	<b>99</b>

**a. TÍTULO**

**“DESARROLLO DE UN PROTOTIPO DE SEGURIDAD DE  
LA INFORMACIÓN APLICANDO LA TÉCNICA DE  
ESTEGANOGRÁFÍA EN LA CAPA DE RED”**

## **b. RESUMEN**

En la actualidad, la información es vulnerable a muchos ataques ciberneticos, que tienen como propósito obtener información confidencial y utilizarla en actos no éticos que afecten a las instituciones u organizaciones. La seguridad en la red es uno de los aspectos que tiene gran importancia, al momento en que dos o más personas establezcan una comunicación y transmitan información por la misma. Dicha información pueda extraviarse, extraerse, o ser modificada mostrando debilidad de seguridad ante un ataque; por ello existen varias técnicas que permiten brindar seguridad a los datos que se trasmitten por la red como son las técnicas de esteganografía y criptografía.

El presente trabajo de titulación trata sobre el desarrollo de un prototipo de seguridad de la información aplicando la técnica de esteganografía en la capa de red. Para el desarrollo del prototipo se implementa una Red de Área Local (**Local Area Network**), se hará uso de dos métodos de la técnica de esteganografía, el primer método que se utiliza es el Flujo Alternativo de Datos (**Alternate Data Stream**) conocido como ADS, que permite ocultar archivos de diferentes extensiones dentro de un fichero principal y adicionalmente se utilizara el método de cifrado simétrico de la técnica de criptografía, su función es generar una clave única que permita al emisor cifrar y al receptor descifrar la información de los archivos.

El segundo método hace uso de la esteganografía de red cuyo propósito es utilizar campos de la cabecera de un protocolo que no son utilizados, en este caso se hará uso del Protocolo de Control y Error de Mensajes (**Internet Control Message Protocol**) conocido como ICMP, aprovechando su campo DATA como canal encubierto para insertar la clave generada por el método de criptografía simétrica, la clave se transmitirá al receptor de forma inapreciable a una tercera persona.

Al finalizar el desarrollo del trabajo de titulación, se realizará las respectivas pruebas del prototipo estableciendo una red LAN en el laboratorio de redes y sistemas operativos del bloque 12, de la Facultad de Energía, las Industrias y los Recursos Naturales No Renovables, de la Universidad Nacional de Loja, los resultados que se obtendrán nos permitirán determinar qué tan eficiente es nuestro prototipo y que trabajos futuros se pueden implementar.

## **SUMMARY**

At present, information is vulnerable to many cyber attacks, which are intended to obtain confidential information and use it in unethical acts that affect institutions or organizations. The network security is one of the aspects that have great importance, at the moment in which two or more people establish a communication and transmit information by it. That information may be lost, extracted, or modified showing weakness of security in the face of an attack; For this reason, there are several techniques that allow to provide security to the data transmitted through the network, such as steganography and cryptography techniques.

The present work deals with the development of a prototype of information security applying the steganography technique in the network section. For the development of the prototype a Local Area Network (Local Area Network) is implemented, using two methods of the steganography technique, the first method used is the Alternative Data Flow (Alternate Data Stream) known as ADS, which allows to hide files of different extensions within a main file and additionally the symmetric encryption method of the cryptography technique will be used, its function is to generate a unique key that allows the sender to encrypt and the receiver to decrypt the information of the files.

The second method makes use of the network steganography whose purpose is to use fields of the head of a protocol that are not used, in this case it will make use of the Control Protocol and Error of Messages (Internet Control Message Protocol) known as ICMP, taking advantage of its DATA field as an undercover channel to insert the key generated by the symmetric cryptography method, the key will be transmitted to the receiver in a negligible way to a third person.

At the end of the final course work, the prototype tests will be carried out, establishing a LAN network in the network and operating systems laboratory of block 12, in the Facultad de Energía, las Industrias y los Recursos Naturales No Renovables, de la Universidad Nacional de Loja, the results that will be obtained will allow us to determine how efficient our prototype is and what future works can be implemented.

## **C. INTRODUCCIÓN**

En el presente vivimos en una era tecnológica, donde la información digital se ha convertido en uno de los bienes más importantes para instituciones, organizaciones y personas. Se invierten grandes cantidades de dinero en medidas que permitan la seguridad de la información en la red, como son los sistemas de seguridad privativos o pagados, pero, así como existen individuos que realizan soluciones factibles de seguridad, hay otros que se especializan en vulnerar este tipo de seguridades teniendo como objetivo principal lucrar de la información que se transmite en una comunicación establecida entre un emisor y uno o varios receptores, la información puede utilizarse para fines maliciosos futuros que afecten la integridad de la institución u organización, por tal motivo se propone un prototipo fácil y económico utilizando técnicas y métodos implementados con software gratuitos que permitan la seguridad de transmisión de información por la red.

Una de las técnicas que ha sido utilizada desde hace mucho tiempo para mantener la información segura es la criptografía, cuyo objetivo principal es cifrar la información en un tipo de lenguaje que no sea fácil de comprender; una de las herramientas de software libre que utiliza el método de criptografía y que se propone en el presente trabajo es OpenSSL.

El arte de ocultar las cosas es el objetivo de la técnica de esteganografía, que utiliza un portador para ocultar la información de forma que no sea percibida o detectada por una persona ajena a la recepción de dicha información, este concepto lo abarca una de las características del Sistemas de archivos de nueva tecnología (New Technology File System) sus siglas son NTFS, esta característica es el Flujo Alternativo de Datos (Alternate Data Stream) más conocido como ADS.

La esteganografía de red utiliza el mismo concepto de esteganografía, donde su diferencia radica en el portador, en este caso se utiliza un campo de la cabecera (canal encubierto) de un protocolo de red como portador, en este campo se inserta la información y se envía por la red a uno o varios receptores.

La combinación de la técnica de criptografía y la técnica de esteganografía permite desarrollar un prototipo factible en la transferencia de archivos por la red, por parte del emisor al receptor o receptores generando seguridad en la información.

## **d. REVISIÓN DE LITERATURA**

En esta sección se realiza una introducción de la situación actual de cómo ha sido afectada o vulnerada la seguridad de la red en instituciones u organizaciones, se abordará la problemática que se presenta cuando los datos fluyen a través de una red. Se realizará una revisión bibliográfica de literatura aplicando la metodología de [1] con la finalidad de identificar qué impacto o utilidad ha tenido la técnica de esteganografía de red en la seguridad de la información, se tiene como propósito encontrar métodos, aplicación de técnicas, ventajas, desventajas de esteganografía de red y casos de éxito.

### **1. Seguridad de la Información en la actualidad**

Uno de los casos más impactantes que da a conocer que en la actualidad la información se encuentra vulnerable es lo sucedido en las elecciones de Estados Unidos, donde hackers fueron capaces de lucrar cuentas, robar claves, entregar malware, obtener correos electrónicos y documentos los cuales fueron utilizados para lanzar evidencia potencialmente condenatoria sobre los políticos durante las elecciones, todo este lucro de información se realizó a través de una combinación de ataques de phishing [2].

Los troyanos y el ataque phishing siguen siendo las principales amenazas que se introducen en las empresas cuando un usuario ingresa a un enlace incompleto, accede a sitios web peligrosos o descarga archivos dañinos a través de email o redes sociales, estas amenazas permiten ocasionar daños en el sistema o vulnerar la seguridad de la información [3].

Una de las muchas tendencias preocupantes en los oscuros mercados web negros es la compra y venta de información de salud protegida por PHI (Protected Health Information). Se trata de datos obtenidos ilegalmente de hospitales, clínicas y otras instituciones sanitarias por piratas informáticos que aprovechan las debilidades de su ciberseguridad. Por lo general, la PHI incluye los números de la seguridad social, las fechas de nacimiento, los nombres de familiares, procedimientos médicos y resultados, y en algunos casos información financiera y de facturación o antecedentes penales [4].

Otro caso que se puede mencionar es la de un hacker que obtuvo acceso a la cuenta de GitHub de la criptomoneda de Syscoin y reemplazó el cliente oficial de Windows con una versión que contenía malware. El cliente de Windows Syscoin envenenado contenía Arkei Stealer, una cepa de malware especializada en eliminar y robar claves privadas de billetera. Este malware también se detecta como Trojan: Win32 / Feury.B! CI [5].

La actividad de DYMALLOY se remonta a 2015 e incluye asociaciones con actividad en 2011. La actividad se centra en la recopilación de inteligencia de redes de sistemas de control industrial con un propósito desconocido. DYMALLOY utiliza comportamientos malintencionados comunes, como las campañas de spear phishing, para atacar directamente las comunicaciones digitales de las personas y los ataques de abrevaderos que colocan malware en sitios web relacionados con la industria en un esfuerzo por robar credenciales corporativas [6].

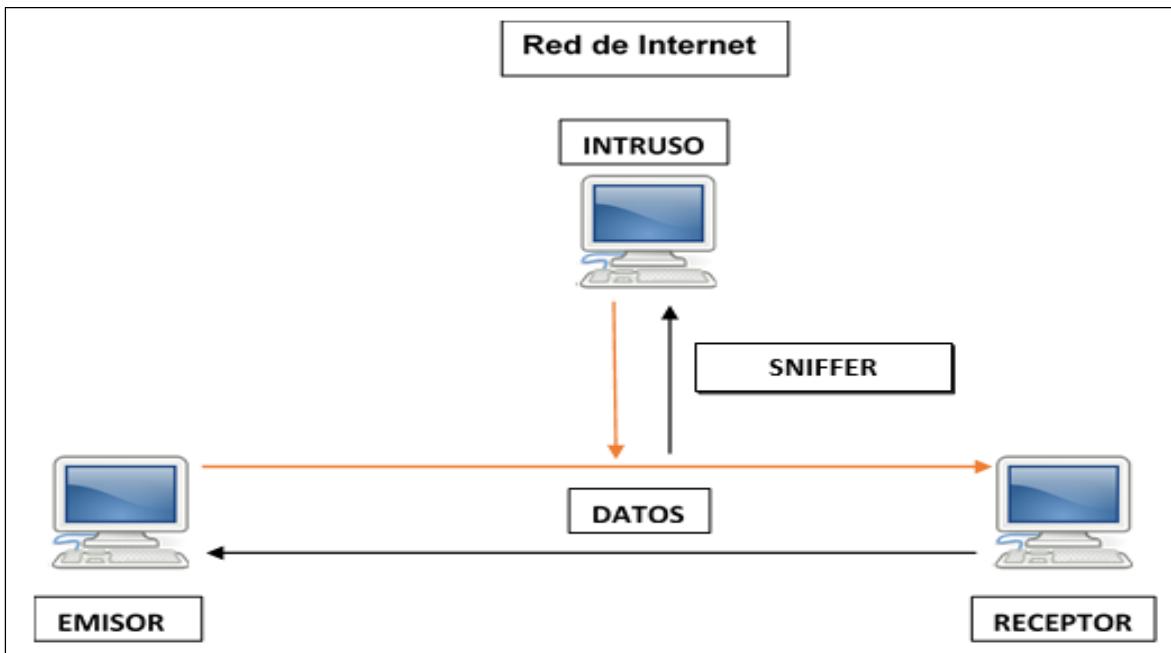
Finalmente se puede mencionar que HealthEquity, sufrió una violación de datos por parte de hackers que lograron comprometer la cuenta de correo electrónico de un empleado de HealthEquity y acceder a ciertos datos, esto permitió que se robara información como ID de los miembros de HealthEquity, nombres de sus empleadores, eliminar varias cuentas de atención médica, números de seguridad social y más [7].

## **2. Revisión bibliográfica**

La revisión bibliográfica tiene como base la metodología plateada por [1] donde se detalla el desarrollo de cada uno de los procesos teniendo como objetivo obtener información relevante y necesaria para el trabajo de titulación.

### **2.1. Definición de problema**

Una comunicación confidencial entre un emisor y uno o varios receptores que intercambian información por la red, es interferida (sniffer) por una tercera persona con la finalidad de lucrar los datos, en la Fig. 1 se representa el problema de forma gráfica.



**Fig. 1 Ilustración grafica de la problemática [Fuente Propia]**

## 2.2. Búsqueda, Organización y Análisis de Trabajos

La búsqueda de trabajos se basó en como los autores utilizan la esteganografía de red para dar solución a la problemática planteada y tratar de establecer una comunicación de datos segura, las siguientes fuentes bibliográficas fueron utilizadas para la búsqueda de información:

- **ScienceDirect**
- **ACM Digital Library**
- **IEEE Digital Library**
- **Scholar Google**

Se hace uso de ecuaciones de búsqueda, las ecuaciones están estructuradas por palabras claves combinadas con operadores lógicos (AND - OR) formando una cadena de búsqueda más profundizada, enfocándose en trabajos recientes entre el año 2015 y 2018, estos trabajos pueden ser artículos, reportes técnicos, patentes, revistas especializadas, memorias de conferencias, simposios y tesis doctorales, en la TABLA I se describe las ecuaciones que se utilizaron.

**TABLA I ECUACIONES DE BÚSQUEDA**

Ecuaciones de Búsqueda
steganography AND layer AND network
steganography AND protocol
steganography AND transmission data
steganography OR internet
steganography AND techniques AND network
steganography AND network

Dentro de la organización se realizó una selección minuciosa de trabajos, con el objetivo de encontrar información importante que sea de ayuda en el trabajo de titulación, uno de los puntos más relevantes tomados en consideración fue el año de publicación dentro del intervalo del año 2015 - 2018, en este punto se busca obtener investigaciones actuales donde se puede encontrar métodos, técnicas y aplicaciones de la esteganografía de red , cada trabajo fue revisado cuidadosamente y se redactó un resumen en el cual se destaca el método usado, el portador y la capa del modelo TCP/IP que aplica esteganografía, la combinación de la técnica de esteganografía con la técnica de criptografía y trabajos futuros tal como se observa en la TABLA II. Como último paso de la revisión bibliográfica se realiza un análisis de todos los trabajos investigados para determinar qué temas son relevantes y útiles para el desarrollo de un prototipo de seguridad de la información aplicando la técnica de esteganografía en la capa de red.

**TABLA II ORGANIZACIÓN Y ANÁLISIS DE LOS TRABAJOS DE REVISIÓN BIBLIOGRÁFICA**

Título de trabajo	Año	Resumen
<b>Secure Quantum Steganography Protocol for Fog Cloud Internet of Things</b>	2018	El autor [8] presenta un nuevo enfoque que permite mantener segura la información de IOT (Internet de las Cosas), el enfoque consiste en aplicar esteganografía de red a la información, el emisor inserta los datos en un protocolo de estados cuánticos entrelazados, lo envía por la red, el receptor utiliza la función de hash para autenticar el mensaje insertado en el protocolo cuántico, el enfoque permite tener seguridad en diferentes ataques en la red.
<b>Securing Data Transfer in IoT Employing an Integrated Approach of Cryptography &amp; Steganography</b>	2017	El presente artículo [9] tiene como prioridad mantener la integridad de los datos que IOT (Internet de las Cosas) trasmite a un servidor o a la red, los datos que genera IOT son cifrados con un algoritmo de clave pública (DES) , luego se obtiene un resumen de los datos utilizando el Algoritmo Message Digest 5 (MD5), los datos cifrados, la clave y el resumen de los datos se insertan en una imagen utilizando el método LSB (Bit Menos Significativo) este método pertenece a la técnica de esteganografía, al recibir el servidor la imagen aplica esteganografía inversa extrayendo el resumen de los datos (datos cifrados y la clave), luego utiliza la clave para descifrar los datos, calcula el resumen utilizando (MD5) y si los resúmenes son iguales lo datos han mantenido su integridad.
<b>Inter-Protocol Steganography for Real-Time Services and Its</b>	2017	En el presente ensayo de conferencia el autor [10] se enfoca en brindar seguridad a los datos en tiempo real (VoIP) que son trasmítidos por la red, utiliza el método de esteganografía de inter protocolo PadSteg, este método utiliza el

<b>Detection Using Traffic Coloring Approach</b>		relleno de datos arbitrarios en los campos de la cabecera de los protocolos de RTC (Protocolo en tiempo real) y RTCP (Protocolo de control en tiempo real) el relleno consiste en insertar información en tiempo real de VoIP.
<b>Steganography in social networks</b>	2017	En el presente ensayo de conferencia el autor [11] utiliza funciones de una red social para poder transmitir información oculta y segura por internet, el método se centra en el ejemplo de “Vkontakte” que utiliza un gráfico para ocultar datos usando la función "Aregar Amigo " esta función permite la conexión entre dos cuentas de usuario, la estructura del gráfico se conforma de la siguiente manera: las cuentas de usuarios son los vértices y los links de cuentas de amigos son los bordes.
<b>APISteg: An active IP identification based steganographic method</b>	2016	El autor [12] propone un método de esteganografía APISteg, este método trabaja con el campo ID (16 bits) de protocolo IP, la función del método es insertar datos en los primeros 12 bits de campo y los 4 restantes utiliza para imitar el tráfico ordinario del protocolo y transmitirlo por la red, la información se transmite de manera imperceptible ante los atacantes, el método PDU funciona de manera muy similar , es menos complejo pero tiene un gran ancho de banda.
<b>Detection Of URL In Image Steganography</b>	2016	El presente artículo [13] muestra un enfoque en que la esteganografía no solo se puede utilizar para seguridad de la información; de hecho, se utiliza también para fines antiéticos, el enfoque se basa en que el emisor inserta una URL que contiene código malicioso en una imagen usado el método LSB (Bit Menos Significativo) de la técnica de esteganografía, al trasmitirse por la red esta URL puede abrirse en un navegador y ocasionar daños a los equipos directamente.

<b>Steganography in data networks based on PDU retransmission</b>	2016	En el presente ensayo de conferencia el autor [14] se centra en realizar pruebas de simulación sobre OMNeT ++ en distintas versiones del protocolo TCP, para determinar que versión es óptima para aplicar esteganografía de red, el protocolo TCP vegas es el protocolo seleccionado por tener mayor ancho de banda al aplicar el método PDU (Unidad de Datos de Protocolos) la función del método es trasmitir datos externos insertados en un canal encubierto, este canal es un campo de la cabecera de un protocolo.
<b>A Novel Approach for Hiding Data in Videos Using Network Steganography Methods</b>	2015	El autor [15] utiliza como portador un archivo de video, este portador permite ocultar mensajes extensos, utiliza el método PDU (Unidad de Datos de Protocolos) de la técnica de esteganografía y el método de criptografía simetría, la combinación de los dos métodos permite al emisor cifrar los datos e insértalos en un archivo de video, este archivo se vuelve a cifrar y se comprime para luego ser insertado en la cabecera del protocolo TCP/IP y se envía por la red, el receptor extrae y descomprime los datos del encabezado de los protocolos y luego descifra los datos y obtiene el video del emisor, en este video el receptor obtiene nuevamente los datos insertados y se vuelven a descifrar obteniendo la información real, en el proceso de cifrar y descifrar el emisor y el receptor deben ponerse de acuerdo en utilizar una misma clave.
<b>Optimal matrix embedding for Voice-over-IP steganography</b>	2015	En artículo [16] presenta un esquema para lograr una incrustación optima de datos en el protocolo VoIP (Voz sobre protocolo de internet) para transmitir en tiempo real los datos por la red, el esquema utiliza una matriz ajustable de codificación (AME) la cual proporciona una estructura ordenada para insertar

		datos, el esquema ayuda a que no se generen problemas de lentitud, perdida o sobrecarga de paquetes incrustados en el protocolo.
<b>Secure Data Communication Using Protocol Steganography in IPv6</b>	2015	En el presente ensayo de conferencia el autor [17] muestra que la criptografía (Algoritmo RSA) y esteganografía de red es aplicable al protocolo IPV4, la esteganografía utiliza el método PDU (Unidad de Datos de Protocolo) para modificar los siguientes campos e insertar información cifrada: IP Flags, Ip indetification File, IP fragment offset e IP Options. Las técnicas de criptografía y esteganografía también son aplicadas al protocolo IPV6, un campo optimo es la “etiqueta de flujo” con un tamaño 20 bits utilizado como canal encubierto.

En la TABLA II se analizó diez trabajos en los que constan conferencias, revistas y artículos tratando el tema de esteganografía, un principio en común en nuestro proyecto de titulación y los trabajos analizados, es el buscar proporcionar seguridad a la información que se transmite por la red, en el desarrollo del prototipo se utilizará la combinación de dos técnicas criptografía y esteganografía tal como las presentan los autores [9], [15], [17], donde a través de la técnica de criptografía se cifra la información y se proporciona una clave para su seguridad, y luego con el método de esteganografía de red se transmite dicha clave de forma oculta. La esteganografía de red utiliza como portador un protocolo de red, en el protocolo se aprovecha un canal encubierto este canal se refiere a un campo de su cabecera que no es usado, en este campo se inserta la clave, algo similar se presenta en [8], [10], [12], [14], [16], [17] y así mismo proporciona un método que permite manipular los campos de la cabecera de un protocolo, este método es conocido como PDU (Unidad de Datos de Protocolos) y es utilizado por los autores [12], [14], [15], [17]. La esteganografía de red es aplicable en diversas capas del protocolo TCP/IP, la capa que se utilizará en el presente trabajo es la capa de red, ya que sus protocolos ya han aplicado esteganografía de red obtenido resultados satisfactorios [10],[13], [16], [17].

### **3. Seguridad de la Información**

La Seguridad de la Información ha crecido mucho en estos últimos tiempos, debido al robo de información que puede ser utilizada con fines fraudulentos. La Seguridad de la Información, según ISO27001, se refiere a la confidencialidad, la integridad, la disponibilidad de la información y los datos importantes, para una empresa u organización independientemente del formato que tengan, estos pueden ser: digitales, en papel, audio, video y otros [18].

#### **3.1. Seguridad Informática**

La seguridad informática es esencial dentro de una institución, donde se busca prevenir al máximo el lucro de datos tales como números de cuentas bancarias, información de tarjetas de crédito, claves, documentos relacionados con el trabajo, hojas de cálculo, etc. La seguridad informática es el nombre genérico para el conjunto de herramientas diseñadas con el fin de proteger los datos almacenados en un equipo y evitar ataques de piratas informáticos.

La seguridad informática cubre cuatro áreas principales como se muestra en la TABLA III que permiten el bienestar de la información.

**TABLA III ÁREAS QUE CUBRE LA SEGURIDAD INFORMÁTICA**

Áreas	Definición
<b>Confidencialidad</b>	Usuarios autorizados pueden acceder a la información.
<b>Integridad</b>	Usuarios autorizados pueden modificar la información.
<b>Disponibilidad</b>	Información disponible cuando el usuario lo necesite.
<b>Autenticación</b>	Comunicación segura entre usuarios.

#### **3.2. Seguridad de red**

Internet ha llegado a convertirse en la actualidad en uno de las formas de comunicación más importantes, extendiéndose entre personas, instituciones, organizaciones y empresas, la red de internet también cuenta con desventajas que son las amenazas al momento de establecer una comunicación.

En una comunicación en la red de internet siempre habrá información que se transmitirá entre dos o más personas (Emisor – Receptor(s)), la información que se transmite mucha de las veces es interceptada por personas ajena a la comunicación, no necesariamente debe estar en contacto físico con la víctima; los datos pueden ser fácilmente copiados, transmitidos, modificados o destruidos cuando son transmitidos por la red. Seguridad en la red es el nombre genérico para el conjunto de herramientas diseñadas para proteger los datos durante su transmisión a través de una red de telecomunicación.

## 4. Amenazas a la información

Antes de definir que es una amenaza debemos conocer que es una vulnerabilidad, una vulnerabilidad es una debilidad en la seguridad de la información, es una situación existente que por razones desconocidas se encuentra presente en el funcionamiento del sistema.

Las amenazas son las situaciones que desencadenan un incidente en la empresa, realizando un daño material o pérdidas inmateriales de sus activos de información [19].

Una amenaza surge a partir de la existencia de una vulnerabilidad que es aprovechada para lucrar información o interferir en una comunicación que se esté efectuando en una institución.

### 4.1. Tipos de Amenazas

Las amenazas pueden clasificarse según el efecto que ocasionen y la forma en como actúen [20], su clasificación es la siguiente:

- Amenazas Pasivas
- Amenazas Activas

#### 4.1.1. Amenazas Pasivas

El atacante pasivo interviene un canal de comunicación sin modificar ningún dato tal como se muestra en la Fig. 2, el objetivo del atacante es obtener la información que se transmite en la red, se puede efectuar el ataque pasivo mediante la escucha clandestina o un sniffer; existen dos tipos de amenazas pasivas:

- **Espionaje:** Una tercera persona lee, el contenido de la transmisión de la comunicación entre dos usuarios.

- **Análisis de tráfico:** Consiste en interceptar y examinar el flujo de tráfico de mensajes, no importa si se encuentran cifrados, el atacante analiza un gran número de mensajes y determina un patrón en la comunicación de dos usuarios.



**Fig. 2 Ataque pasivo [Fuente propia]**

#### 4.1.2. Amenazas Activas

Son difíciles de detectar, la amenaza activa realiza la modificación del flujo de datos o creación de un flujo de datos falso tal como se muestra en la Fig. 3, un atacante activo amenaza la confidencialidad, autenticación y la integridad de los datos, existen cuatro tipos de amenazas activas:

- **Suplantación de identidad:** El atacante tiene como propósito suplantar la identidad de otro usuario.
- **Repetición:** Un atacante realiza la captura de datos y los retransmite después de conocer su contenido.
- **Modificación del mensaje:** El atacante inserta, modifica o elimina el mensaje original.
- **Denegación de servicios (DDos):** Se le impide al emisor la utilización normal de las actividades de comunicación.



**Fig. 3 Ataque activo [Fuente propia]**

#### **4.2. Métodos de ataques a la información**

Un intruso informático puede realizar diferentes ataques a los ordenadores donde existe información almacenada o cuando se establece una comunicación entre usuarios, algunos de los ataques que más se utilizan son los siguientes.

- **Trashing:** Conocida como basurero, el objetivo del intruso es buscar en la basura digital algún rastro de información que el usuario desechar por equivocación, es la más utilizada hoy en día.
- **Ingeniería Social:** Se basa en el error humano de creer que una clave lo controla todo, este método aprovecha o abre puertas traseras para lograr su objetivo.
- **Phising:** Utiliza email malicioso cuyo objetivo es robar el usuario y clave del propietario.

### **5. Criptografía**

La criptografía es una de las técnicas que ha sido utilizada desde hace algún tiempo, con el fin de mantener segura la información. La R.A.E (Real Academia Española) define criptografía como el arte de escribir con clave secreta o de un modo enigmático.

Con la llegada de la computadora y más aún con la llegada de Internet, fue indispensable el uso de herramientas automatizadas para la protección de archivos y otro tipo de información almacenada en la computadora, algunas de estas herramientas son los cortafuegos, los Sistemas Detectores de Intrusos y el uso de sistemas criptográficos [21].

La criptografía utiliza algoritmos matemáticos que permiten realizar la acción de cifrar información, esta acción consiste en modificar su contenido a un lenguaje diferente, con el objetivo que no sea entendible para un intruso, también permite la acción de descifrar la información que es la manera de como un usuario transforma a su estado original la información que ha sido cifrada.

Un sistema de seguridad criptográfico debe cumplir a cabalidad con los cinco objetivos de la criptografía:

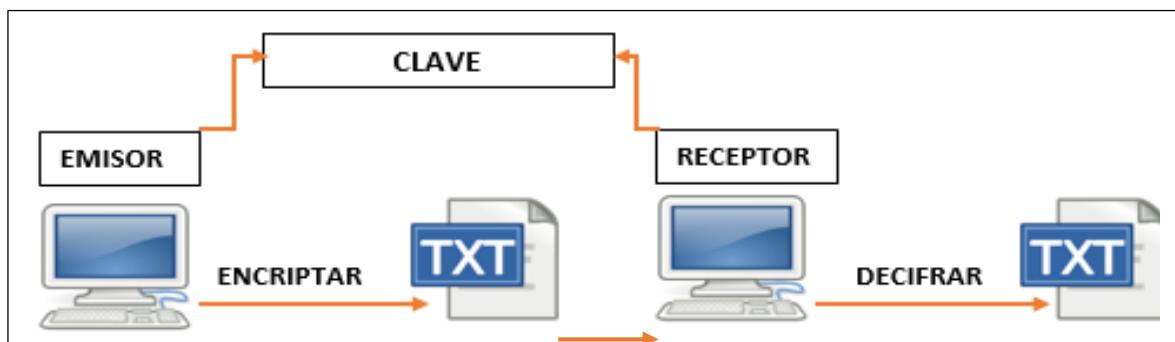
- **Autenticación:** Antes de realizar una comunicación se deberá confirmar la identidad de los usuarios.
- **Privacidad:** Solo el emisor y el receptor sabrán que datos se envían y que datos serán recibidos.
- **Integridad:** El mensaje que recibió el receptor no deberá tener modificación alguna en su contenido.
- **No repudio:** No podrá negar ni el emisor ni el receptor que un mensaje se ha enviado cuando los involucrados tienen conocimiento de su transmisión.
- **Servicios Fiabilidad y Disponibilidad:** Calidad de servicios e información disponible cuando sea requiera por parte de los usuarios.

## 5.1. Criptografía simétrica

La criptografía simétrica utiliza algoritmos criptográficos públicos, su seguridad depende de su complejidad interna y la longitud de la clave, una de las características importantes de la criptografía simétrica es que es más rápida que la criptografía asimétrica.

La criptografía simétrica también conocida como la criptografía de clave única utiliza una sola clave para cifrar y descifrar. En el proceso de trasmisión de archivos cifrados que hace uso de la criptografía simétrica, el emisor y el receptor tienen que ponerse de acuerdo en tener una sola clave secreta que sea compartida entre los dos [22].

El emisor utiliza la clave secreta para cifrar un archivo, el archivo cifrado se lo transmite al receptor, el receptor utiliza la misma clave secreta para descifrar el archivo teniendo como resultado el archivo original tal como se puede observar en la Fig. 4.



**Fig. 4** Criptografía Simétrica [Fuente propia]

### **5.1.1. Algoritmos de Criptografía Simétrica**

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

DES utiliza una clave simétrica de 64 bits, de los cuales 56 son usados para cifrar, mientras que los 8 restantes son de paridad, y se usan para la detección de errores en el proceso. Como la clave efectiva es de 56 bits, son posibles un total de 72.057.594.037.927.936 claves posibles, es decir, unos 72.000 billones de claves, por lo que la ruptura del sistema se puede efectuar por fuerza bruta o diccionario.

#### **RC5**

Utiliza el método de cifrado por bloques, tiene un tamaño variable de bloques de 32, 64 o 128 bits. Proporciona diferentes longitudes de clave hasta un máximo de 2040 bits, y un número variable de iteraciones de hasta 255, el grado de seguridad de este algoritmo depende del número de interacciones.

#### **AES (Advanced Encryption Standard)**

Conocido como el algoritmo Rijndael, hace uso del método cifrado por bloques, puede cifrar bloques de datos de 128 bits utilizando claves simétricas de 128, 192, o 256. Este algoritmo se considera muy seguro y eficiente y sirve para cifrar los datos de todo tipo y por eso, se suele usar en varios protocolos y técnicas de transmisión un ejemplo es que AES es usado por openssl, openvpn y en los cífrados Wireless de los routers de los hogares.

La forma en que se gestionan estos bloques de mensaje, se denomina “modo de cifrado”. En openssl se utilizan las siguientes librerías de criptografía.

- **ECB (Electronic Code Book Mode):** En este modo los datos se dividen en bloques de 64 bits y cada bloque se cifra uno a la vez. Cifrados y separados en diferentes bloques son totalmente independientes entre sí.
- **CBC (Cipher Block Chaining):** Este modo de cifrado es una extensión de ECB que añade cierta seguridad. El modo de cifrado CBC divide el mensaje en bloques y usa XOR para combinar el cifrado del bloque anterior con el texto plano del bloque actual. El primer bloque a cifrar no tiene texto cifrado anterior, por lo que el texto plano es XOR con un número de 64 bits llamado vector de inicialización, o IV, para abreviar.

- **OFB (Output Feed Back):** En este caso el keystream se genera cifrando el bloque anterior del keystream, dando lugar al siguiente bloque. El primer bloque de keystream se crea cifrando un vector de inicialización IV.
- **CFB (Cipher Feed Back):** Se hace igual que en OFB, pero para producir el keystream, se cifra el último bloque de cifrado en lugar del último bloque del keystream como hace OFB. Un bit erróneo en el texto cifrado genera  $1+64/m$  bloques de texto claro incorrectos (siendo  $m$  la longitud del flujo en el que se divide el bloque).

## 5.2. Criptografía Asimétrica

La criptografía asimétrica también se conoce como la criptografía de clave pública es más segura que la criptografía simétrica pero más lenta. Se utiliza dos claves: clave pública conocida por algunas personas en general para cifrar y la clave privada conocida sólo por el usuario propietario de esa clave el cual la utiliza para descifrar [22].

El receptor genera dos claves una privada y una pública, la clave pública es entregada al emisor, con esta clave pública el emisor podrá cifrar un archivo y lo transmitirá al receptor, el receptor hará uso de su clave privada para descifrar el archivo y obtener el archivo original tal como se puede observar en la Fig. 5.

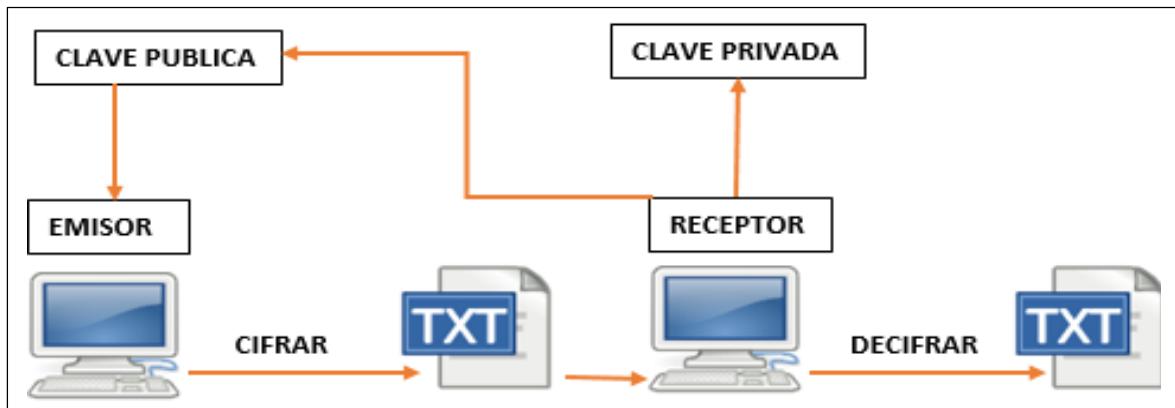


Fig. 5 Criptografía Asimétrica [Fuente propia]

### **5.2.1. Algoritmos de Criptografía Asimétrica**

#### **RSA**

Inventado en 1977 por Ron Rivest, Adi Shamir, y Leonard Adleman. La seguridad de este algoritmo reside en la dificultad que supone la factorización de un número compuesto por factores primos muy grandes. Si un criptoanalista fuera capaz de encontrar los factores primos sería capaz también de determinar la clave privada y, por lo tanto, descifrar el mensaje. Sin embargo, el problema de factorización se considera imposible de resolver en la práctica, y cuanto más grande sean los números utilizados, es decir las longitudes de las claves, mayor dificultad se alcanza.

#### **DSA (Digital Signature Algorithm)**

Emplea un algoritmo de firma y cifrado distinto al del RSA, aunque ofrece el mismo nivel de seguridad. Está basado en el problema de los logaritmos discretos y únicamente puede emplearse para las firmas digitales. A diferencia del RSA, que puede emplearse también para cifrar.

#### **Diffie-Hellman**

No se considera un algoritmo asimétrico, es utilizado para generar una clave privada simétrica a ambos extremos de un canal de comunicación inseguro. Se emplea para obtener la clave secreta con la que posteriormente se pueda cifrar la información, junto con un algoritmo de cifrado simétrico.

#### **Gamal**

Utiliza un esquema de cifrado basado en problemas matemáticos de algoritmos discretos, se basa en la idea de Diffie-Hellman ya que funciona de forma parecida, es utilizado tanto para generar firmas digitales como para cifrar o descifrar.

### **5.3. Certificado Digital**

Un certificado digital es un DNI (Documento de Identificación Nacional) único dentro de la red de internet que permite la autenticación de un individuo, permitiendo al individuo que demuestre quien dice ser y que tiene la clave privada asociada a su certificado.

### 5.3.1. Uso de los certificados digitales

Los certificados digitales tienen muchos usos y aplicaciones, ofreciendo beneficios que garantizan la identidad y seguridad de la información a los individuos o instituciones.

- **Firma Electrónica de Documentos.** - Permite la firma de facturas, de recetas, de expedientes, contratos, de proyectos, de cuentas financieras entre otros documentos que necesiten legalidad y autenticidad de un individuo.
- **Autenticación Web.** - En el ámbito informático se garantiza la identidad de un individuo o institución hacia una tercera persona, para realizar el pago de impuestos, la prestación de declaraciones, el registro de documentos electrónicos, etc.

### 5.4. Firma Digital

La firma digital es utilizada para asegurar la integridad de la información a través de un código de verificación tal como se observa en la Fig. 6. La firma digital no asegura que la información del documento este cifrado, el documento puede ser leído por otras personas tal como sucede cuando se realiza una firma entre la presencia de dos personas [23].

- El emisor genera una huella digital del mensaje mediante una función hash, esta huella proporciona un único número que permite identificar a ese documento.
- La huella digital se cifra con una clave privada del emisor, esta combinación es lo que se llama firma digital, la firma digital es enviada adjunta al mensaje original.
- El receptor generara una huella digital del mensaje o documento recibido.
- Descifrará la firma digital utilizando la clave pública del emisor, y obtendrá la huella digital del mensaje original, si las huellas coinciden el mensaje es el original.

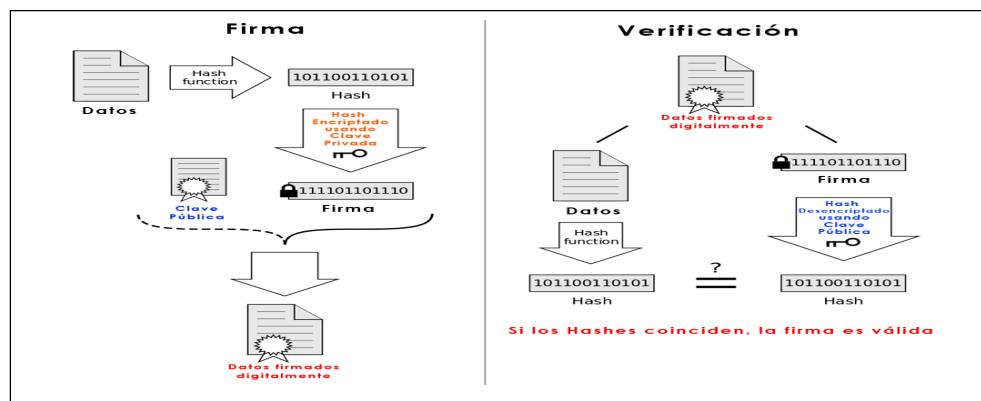


Fig. 6 Firma digital [23]

## 5.5. OpenSSL

OpenSSL es de código libre cuenta con varias herramientas que permiten tener seguridad en la información con todas las características para los protocolos Transport Layer Security (TLS) y Secure Sockets Layer (SSL), se considera un robusto paquete de herramientas de administración y bibliotecas relacionadas con la criptografía simétrica y asimétrica [24].

## 5.6. Aplicación de la criptografía simétrica utilizando OpenSSL

Se requiere cifrar un documento que cuenta con información confidencial muy importante para la institución, la información solo puede ser vista por el emisor y el receptor, el esquema de cifrado simétrico se presenta en la Fig. 7 donde se detalla su procedimiento.

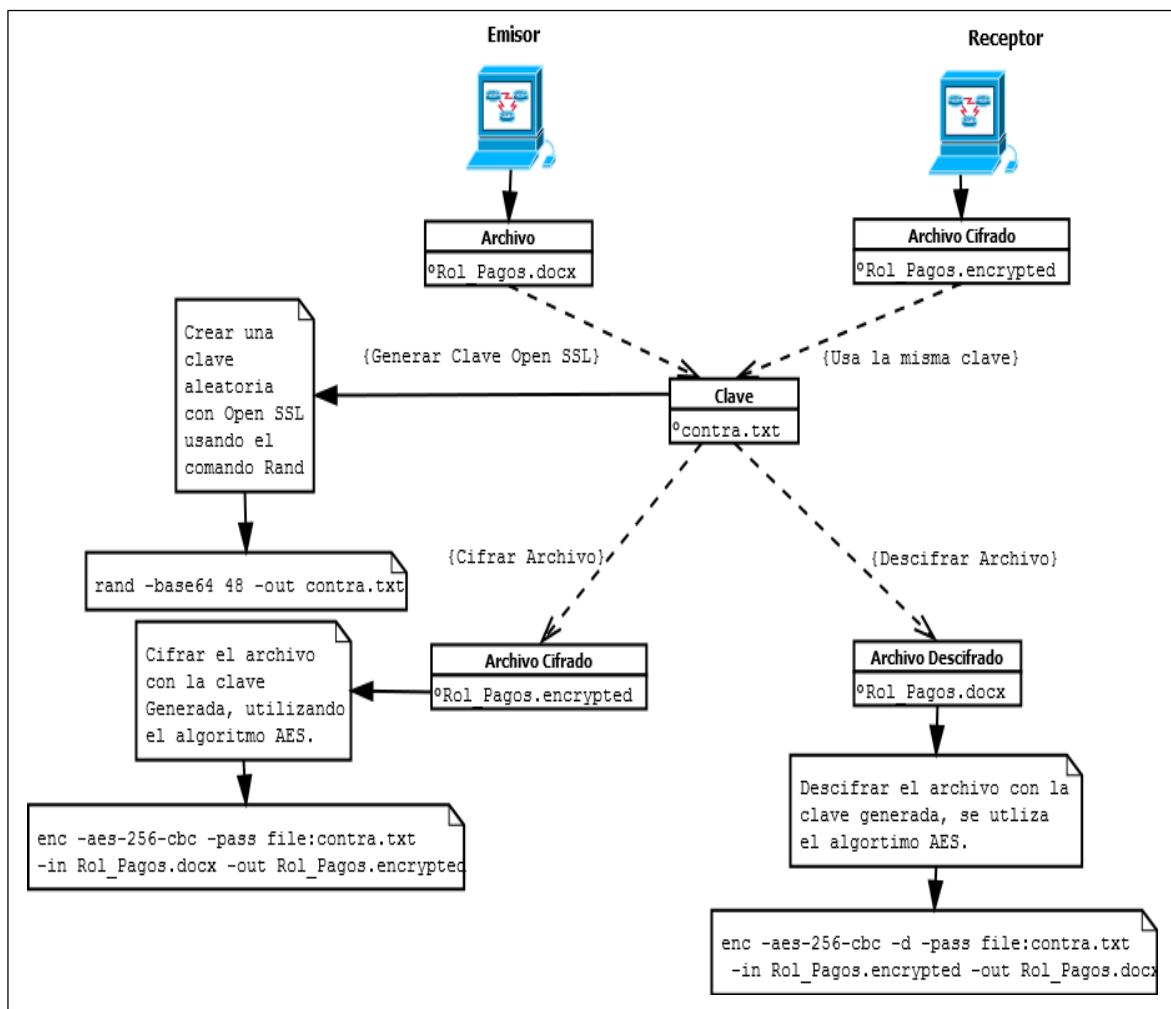


Fig. 7 Esquema de criptografía simétrica [Fuente propia]

1. Instalar openssl en el sistema operativo Windows
2. Abrir la consola de Windows y ejecutar openssl en modo administrador (CMD), en el directorio donde se encuentra el archivo, observe la Fig. 8.

```
C:\Users\b-boy\Desktop\Tesis\Archivo>openssl
OpenSSL>
```

**Fig. 8 Ejecución de openssl en cmd [Fuente propia]**

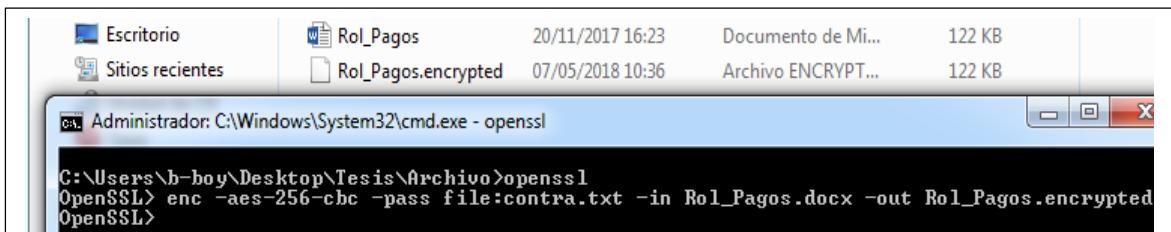
3. Crear una clave aleatoria con una longitud de 48 caracteres, se usa la siguiente línea de comandos “**rand -base64 48 -out contra.txt**” la clave generada se guarda en un archivo de tipo texto, observe la Fig. 9.

```
C:\Users\b-boy\Desktop\Tesis\Archivo>openssl
OpenSSL> rand -base64 48 -out contra.txt
Loading 'screen' into random state - done
OpenSSL>
```

**Fig. 9 Crear una clave aleatoria [Fuente propia]**

4. Cifrar el archivo con la línea de comandos “**enc -aes-256-cbc -pass file:contra.txt -in Rol\_Pagos.docx -out Rol\_Pagos.encrypted**”, en este caso se utiliza un archivo .docx nombrado “**Rol\_pagos.docx**”. La línea de comandos describe lo siguiente:

- Se especifica el algoritmo a utilizar en este caso el AES “**enc -aes-256-cbc**”
- Se utiliza la clave generada en el punto 3 para cifrar el archivo “**Rol\_pagos.docx**”.
- Se ingresa como entrada el nombre del archivo a cifrar y como salida el nombre del archivo cifrado su tipo es encrypted, observe la Fig. 10.



**Fig. 10 Cifrar el archivo "Rol\_Pagos.docx" [Fuente propia]**

5. El archivo de tipo encrypted contiene la información cifrada con la clave, para descifrar la información se utiliza la siguiente línea de comandos “**enc -aes-256-cbc -d -pass file:contra.txt -in Rol\_Pagos.encrypted -out Rol\_Pagos.docx**” es muy similar a la línea de comandos para cifrar, la única diferencia es que se agrega (**-d**) que descifra la información del archivo de entrada en este caso “**Rol\_Pagos.encrypted**” y también se define el documento de salida que será “**Rol\_Pagos.docx**” con la información descifrada observe la Fig.11.

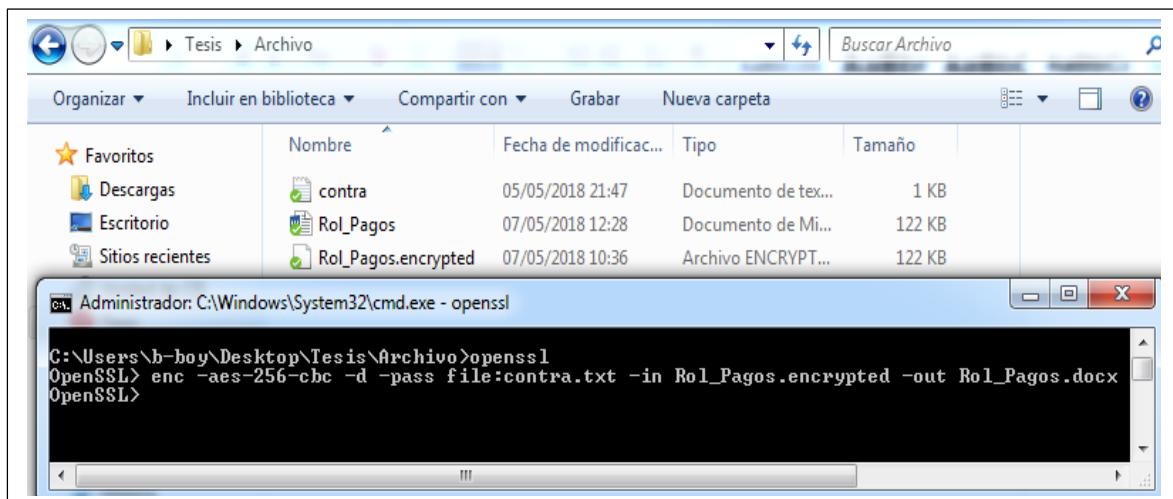


Fig. 11 Descifrar la información del archivo “Rol\_Pagos.encrypted” [Fuente propia]

## 6. Esteganografía

### 6.1. Principio de Esteganografía

La palabra esteganografía proviene del griego: Steganos (oculto, secreto) y Graphy (texto o dibujo). A través de la historia la esteganografía ha sido utilizada de muchas formas con el fin de ocultar información.

Ya en el antigua Grecia, los textos eran escritos en tablas cubiertas de cera, otro método utilizado e igualmente ingenioso consistía en afeitar la cabeza de los mensajeros, tatuar el mensaje y esperar la presencia de cabello para que un individuo pueda transportar la información. En el transcurso del tiempo la esteganografía ha estado presente en épocas significativas, como por ejemplo la primera guerra mundial, donde la escritura de mensajes se realizaba utilizando tinta invisible obtenida de diferentes compuestos (Vinagre, Jugo de

frutas) una vez escrito el mensaje en el papel, se opacaba el mensaje a través de calor convirtiéndolo casi imperceptible para la vista humana. Durante la II Guerra Mundial, comenzó a utilizarse el micro punto; es decir, un mensaje fotográficamente reducido a la medida de un punto y era pegado en una letra como por ejemplo la letra (i), esta letra podría estar en un papel que tenga un mensaje cualquiera [25] .

Un ejemplo que se presenta [26] trata sobre dos prisioneros que fueron mantenidos en prisión en Hoa Lo, conocida por los norteamericanos como "Hanoi Hilton", donde se utilizaban un código para comunicarse el cual no era perceptible por los guardias de la prisión; el código consistía en golpear ciertas barras de metal varias veces para transmitir un mensaje letra por letra. Cada letra está ubicada en una matriz de 5x5 con las 26 letras del alfabeto (K fue representado por C) observe la TABLA IV, donde era necesario alcanzar el número de fila y el número de columna lentamente para representar la letra de comunicación deseada.

**TABLA IV MATRIZ QUE UTILIZARON LOS PRISIONEROS DE VIETNAM [26]**

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

## **6.2. Tipos de esteganografía**

Existen varios métodos de esteganografía que hoy en día se están utilizando para mantener la seguridad de la información en la red, pero no solo se utiliza la esteganografía para fines éticos, sino también para lanzar ataques informáticos como virus o URLs escondidas en imágenes que infectan las computadoras y otros ataques que afectan considerablemente a la seguridad de la información [27].

- **Esteganografía Lingüística**

Se caracteriza por utilizar un lenguaje propio, cambia las palabras dentro del texto para generar secuencias de caracteres aleatorios, básicamente aquí se utiliza el archivo de texto como portador para incrustar la información secreta. Es más vulnerable ante un ataque ya que puede ser fácil para un atacante detectar el patrón.

- **Esteganografía Imagen**

Se utiliza el archivo de imagen como portador para ocultar el mensaje secreto, una imagen digital es una combinación de baja y alta frecuencia. Una región de baja frecuencia está fuertemente relacionada con sus píxeles vecinos, mientras que una región de frecuencia más alta se desvía fuertemente a sus píxeles vecinos. El humano no puede detectar estas modificaciones, el mensaje secreto se incrusta en el píxel de la imagen, dependiendo de la distribución de frecuencia baja o alta.

- **Esteganografía Audio**

Los audios también son un archivo eficaz para actuar como portadores para transmitir información, tras la modificación de bits se puede incrustar mensajes con información confidencial sin modificar su estructura así que al momento de reproducirlo no se detectaría modificación por el oído humano.

- **Esteganografía Video**

El archivo de video es menos propenso a ser detectado o interferido ya que es una combinación de imagen y audio. Un video es una colección de imágenes que se ejecutan a una velocidad constante. Para ocultar la información tenemos que extraer los marcos del video y convertirlos a imagen y aplicar un método de esteganografía de imágenes.

- **Esteganografía Red**

Se caracteriza por utilizar como portador un protocolo de red para transmitir datos ocultos por la red, Por lo tanto, es difícil detectar o eliminar el mensaje oculto, esta característica lo convierte en uno de los métodos más utilizados en la actualidad [27].

### 6.3. Portadores

Los portadores son aquellos objetos usados por la esteganografía para ocultar información aplicando alguna técnica o método, existen dos tipos de portadores, los portadores estructurados y los portadores no estructurados.

#### Portadores Estructurados

Los portadores estructurados tienen una estructura de datos previamente definida y son interpretados por un sistema informático, se aplican reglas semánticas que definen el formato del portador, estos portadores son:

- Documentos
- Protocolo de Red

#### Portadores no Estructurados

Los portadores no estructurados no cuentan con una estructura de datos, ni con un límite de cuanta información se puede ocultar, debido a que su modificación puede estar o no interpretada por el usuario u otras formas de interpretación, este portador puede ser:

- Imágenes
- Audio
- Video

### 6.4. Características de Esteganografía

Existen características esenciales antes de aplicar esteganografía a un tipo de archivo, las características son las siguientes:

- **Capacidad.** La cantidad de datos que se puede insertar en el portador sin modificar su tamaño o estructura.
- **Invisibilidad.** La información oculta en el portador debe ser invisible ante cualquier código, con la finalidad que no advierta la existencia de información.

- **Robusto.** La cantidad de veces que el portador es inmune a las modificaciones por terceras personas antes de perder la información.
- **Seguridad.** Mide la dificultad en que un algoritmo extrae la información oculta en un objeto portador.

## 7. Esteganografía de Red

La esteganografía de red se centra en el transporte de información que se da en la comunicación entre el emisor y el receptor, su objetivo principal es ocultar la información en canales encubiertos de un protocolo de red, estos canales son campos de la cabecera del protocolo que no son utilizados o que al insertar datos no afectan su funcionalidad, la información pasa desapercibida ante terceras personas, esta información puede ser mensajes textuales, datos, comandos o alguna señal que tenga significado para el receptor [27].

La principal diferencia entre la esteganografía clásica y la esteganografía moderna radica en su portador. Por ejemplo, en lugar de usar piel humana y tablas de madera hoy en día se usan archivos multimedia como imágenes, audio, video, protocolos, etc.

La esteganografía está teniendo una amplia área de aplicación como comunicación confidencial, almacenamiento de datos secretos y protección a la alteración de datos, algunas aplicaciones en que la esteganografía podría ser de gran utilidad son:

- Transmitir noticias e información confidencial sin tener miedo a la intercepción.
- Solución para la transmisión de coordenadas de una ubicación secreta.
- Seguridad en la transmisión de una base de datos bancaria.

### 7.1. Canal encubierto

Un canal encubierto es un medio en el que la información se puede insertar, por tal ventaja es aprovechado para transmitir información entre el emisor y el receptor, al utilizar un canal encubierto se viola las políticas de seguridad del sistema, antes de utilizarlo hay que tener en cuenta que en las redes existen modelos de seguridad y esquemas de control de acceso que regulan el uso de canales encubiertos.

La creación de canales encubiertos, se da en la mayoría de los protocolos de red con la finalidad de aplicar la esteganografía, la inserción de los datos es mediante la manipulación del formato de los paquetes a enviar, en si un canal encubierto son los campos reservados o que no son usados de un protocolo.

- **Canal encubierto de almacenamiento**

El emisor y receptor utilizan una variable compartida donde el emisor inserta los datos y el receptor los extrae. En el entorno de la red de internet, los campos del encabezado de un protocolo actúan como variables compartidas donde se inserta la información. Varias herramientas emplean protocolos TCP, IP, ICMP y HTTP para establecer el canal encubierto de almacenamiento.

- **Canal encubierto de temporización**

El receptor y el emisor acuerdan una prioridad en un intervalo de tiempo (un protocolo de inicio) durante cada intervalo de tiempo el emisor transmite un solo paquete y lo mantiene en espera, luego el receptor monitorea cada intervalo para determinar si se recibió un paquete. Tenga en cuenta que los datos brutos que fluyen a través del canal son binarios pero la interpretación real de la secuencia binaria depende de las partes comunicantes.

- **Canales de ordenación**

Se caracterizan por ocultar la información en el orden de llegada de los paquetes.

- **Canales combinados o híbridos**

Son aquellos canales resultantes de la combinación de las técnicas empleadas por algunos de los tipos de canales anteriores.

## **7.2. Características de los canales en cubiertos**

Para la existencia de un canal encubierto se debe cumplir con ciertas características que determinaran que un canal encubierto es apto para insertar información estableciendo una comunicación.

- **Comunicación.** La forma en que el emisor y el receptor pueda establecer una comunicación.
- **Comunicación Restringida.** No se establecerá una comunicación normal debido a las políticas de seguridad.

- **Variable compartida.** Siempre debe existir una variable compartida dentro del sistema de comunicación entre el emisor y el receptor (campo de un protocolo).
- **Alteración de la Variable.** La variable compartida debe permitir su modificación por parte del emisor y ser visible al receptor mostrando su alteración.
- **Sincronización.** El emisor y el receptor deben ser capaces de sincronizar sus operaciones de comunicación entre sí.

### 7.3. Métodos de esteganografía de red

La esteganografía de red hace uso de algunos métodos que son aprovechados para ocultar la información, estos tres métodos permiten ocultar la información y pasar desapercibida ante un intruso [12].

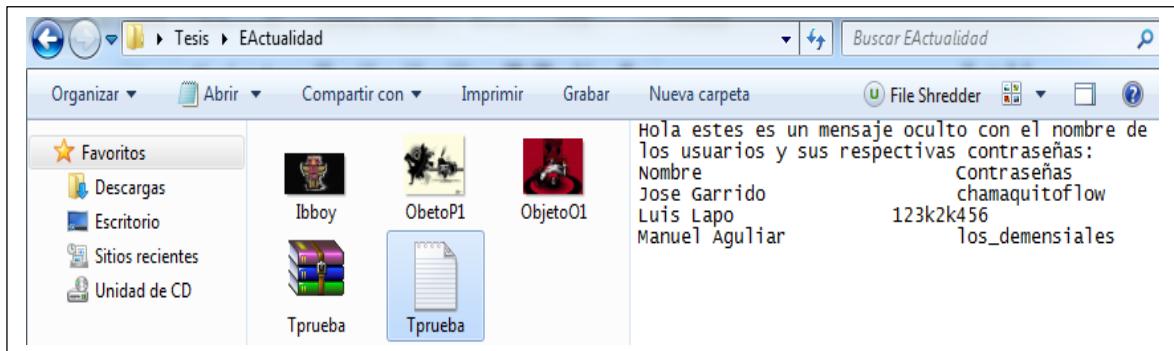
- **Unidad de Datos de protocolo (PDU).** Consiste en insertar datos externos en un campo de la cabecera de un protocolo de red que no sea usado o que la usarlo no afecte su estructura.
- **Comportamiento del protocolo (PB).** Implica la codificación de datos externos mediante la explotación del mecanismo conductual de los protocolos de red.
- **Método basado en Aplicaciones y Servicios (NAS).** Involucra incrustación de datos externos utilizando características de la red, aplicaciones y servicios.

## 8. Esteganografía en la Actualidad

Se utiliza esteganografía en portadores digitales como texto, video, audio, etc. Se detallará algunas de las formas de como ocultar archivos dentro de portadores digitales [13].

### 8.1. Ocultar en un archivo comprimido (.rar) en una imagen (.jpg).

Para realizar el ocultamiento de un archivo comprimido en una imagen, se deberá tener en un directorio los dos archivos, el primero será el portador con el nombre de “lbboy.jpg” y el segundo será el que se va a ocultar con el nombre de “Tprueba.rar”, el archivo comprimido tendrá un sub-archivo de texto llamado “Tprueba.txt”, observe la Fig. 12.



**Fig. 12** Archivo portador “Ibboxy.jpg” y archivo a ocultar “Tprueba.rar” [Fuente propia]

Teniendo el archivo portador y el archivo a ocultar, se aplica un técnica que consiste en realizar una suma binaria a través de la consola de Windows (CMD), la consola debe abrirse en el directorio donde se encuentran los archivos y ejecutar la línea de comandos “**copy /b Ibboxy + Tprueba.rar resultado.jpg**”, la acción que realiza es copiar, listar los archivos, ingresar el nombre del archivo portador, colocar el signo más “+” demostrando que es una suma, ingresar el nombre del archivo a ocultar y especificar el nombre del archivo resultado “resultado.jpg” este archivo es el resultado de haber ocultado el archivo comprimido dentro de la imagen observe la Fig. 13.

```

Microsoft Windows [Versión 6.1.7601]
Copyright © 2009 Microsoft Corporation. Reservados todos los derechos.

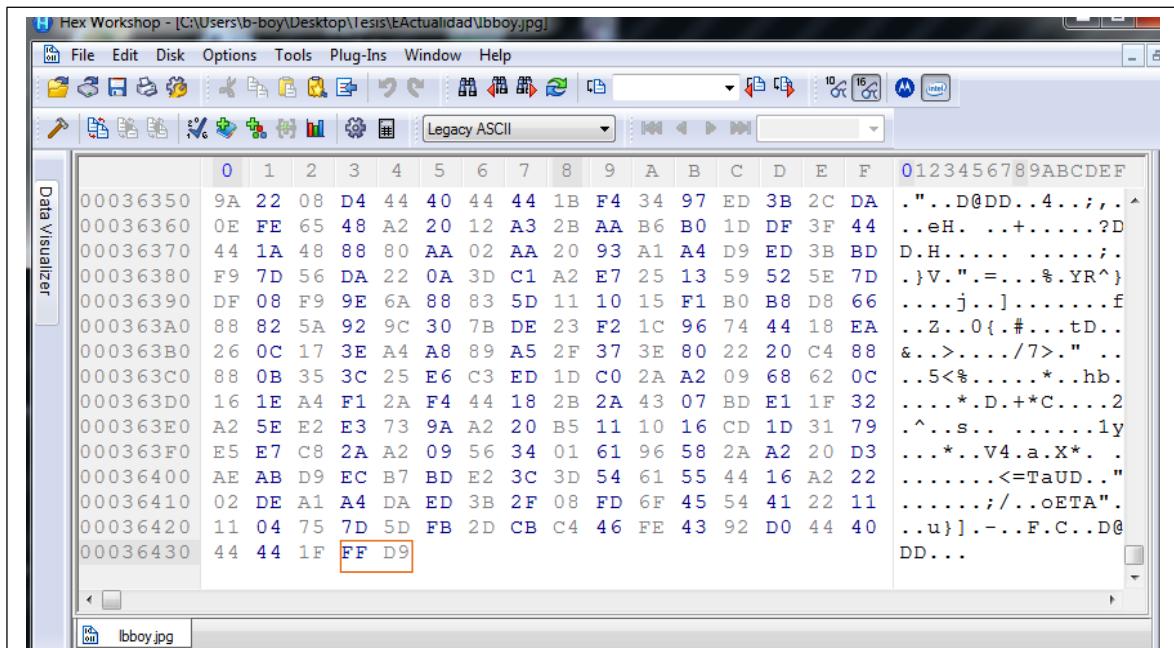
C:\Users\b-boy>cd Desktop
C:\Users\b-boy\Desktop>cd Tesis
C:\Users\b-boy\Desktop\Tesis>cd EActualidad
C:\Users\b-boy\Desktop\Tesis\EActualidad>copy /b Ibboxy.jpg + Tprueba.rar resultado.jpg
Ibboxy.jpg
Tprueba.rar
    1 archivo(s) copiado(s).

C:\Users\b-boy\Desktop\Tesis\EActualidad>

```

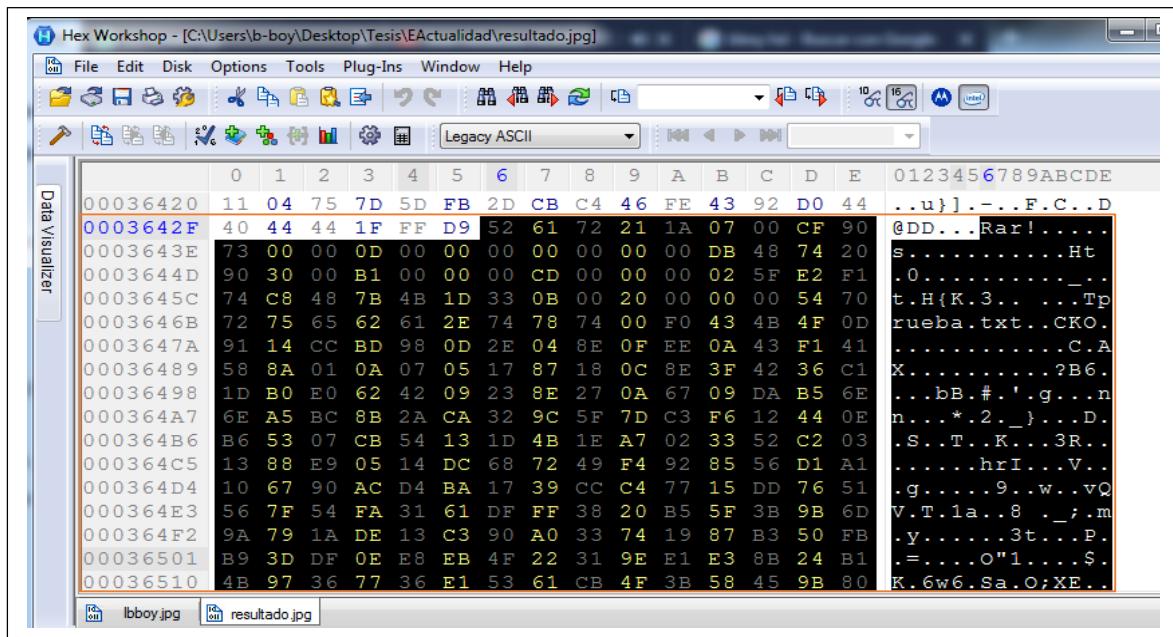
**Fig. 13** Archivo portador + archivo a ocultar = archivo resultante [Fuente propia]

El archivo resultado “resultado.jpg” es igual al archivo portador “Ibbox.jpg” visualmente y también en tamaño, pero para comprobar que el archivo “resultado.jpg” contiene el archivo comprimido oculto, se compara la estructura hexadecimal del archivo portador y el archivo resultado, se abren los archivos en un editor hexadecimal “**Hex Editor**”, la estructura hexadecimal del archivo portador tiene una terminación de FF D9 observe la Fig. 14.

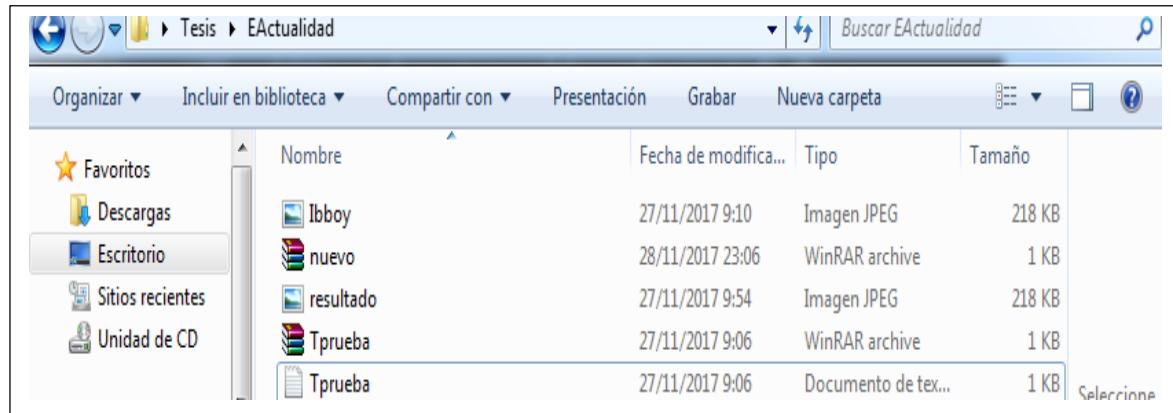


**Fig. 14** Estructura hexadecimal del archivo "Ibbox.jpg" [Fuente propia]

El mismo procedimiento se realiza para el archivo resultado, se puede observar en la Fig. 15 que la estructura hexadecimal del portador termina en FF D9 y luego continua otra estructura hexadecimal la cual corresponde al archivo oculto, para recuperar el archivo comprimido que está oculto se copia la estructura hexadecimal que continua a partir de FF D9 y se guarda en un archivo nuevo de tipo .rar “nuevo.rar” el cual contiene la información que se ocultó observe la Fig. 16.



**Fig. 15 Estructura del archivo "resultado.jpg" [Fuente propia]**



**Fig. 16 Recuperación del archivo oculto [Fuente propia]**

## 8.2. Ocultar un archivo de texto (.txt) en un archivo ejecutable (.exe)

Un archivo ejecutable también es un portador que no levanta sospechas al ocultar información, para ocultar un archivo .txt en un archivo ejecutable, se deberá tener un mismo directorio los dos archivos, el primero será el portador con el nombre de “calc.exe” con un tamaño de 897 KB y el segundo archivo a ocultar será “Usuarios\_Contra.txt” con un tamaño de 515 bytes observe la Fig. 17.

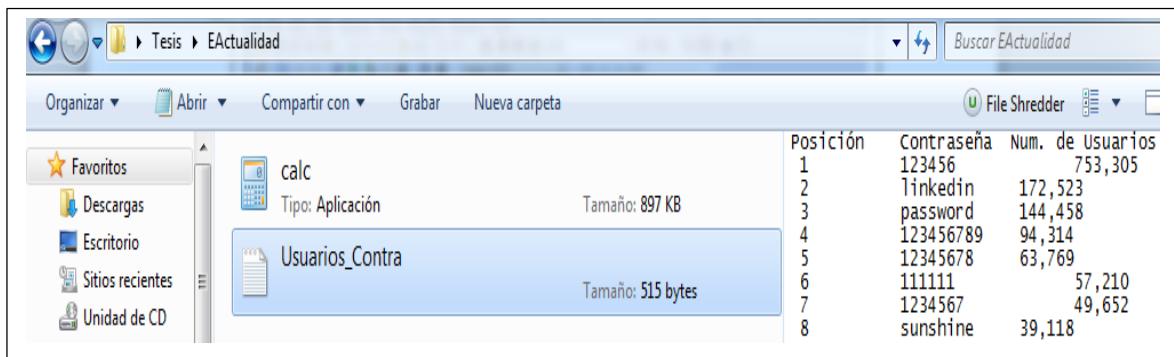


Fig. 17 Archivo portador “calc.exe” y archivo a ocultar “Usuarios\_Contra.txt” [Fuente propia]

Tal como se realiza al ocultar un archivo comprimido en una imagen se sigue el mismo procedimiento para ocultar el texto en un archivo ejecutable, la línea de comandos para este caso es: **“copy /b calc.exe + Usuarios\_Contra.txt calc\_texto.exe”** observe la Fig. 18 muestra el procedimiento en CMD y la Fig. 19 muestra el archivo resultado.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright © 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\b-boy>cd Desktop\Tesis\EActualidad
C:\Users\b-boy\Desktop\Tesis\EActualidad>copy /b calc.exe + Usuarios_Contra.txt
cal_texto.exe
calc.exe
Usuarios_Contra.txt
    1 archivo(s) copiado(s).

C:\Users\b-boy\Desktop\Tesis\EActualidad>
```

Fig. 18 Archivo portador ejecutable + archivo a ocultar texto = archivo resultante [Fuente propia]

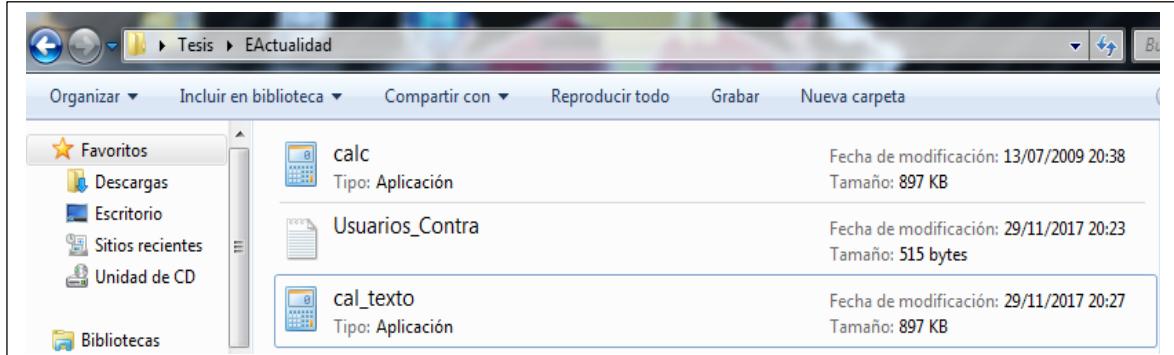


Fig. 19 Nuevo objeto de la suma binaria “calc\_texto.exe” [Fuente propia]

El archivo resultado “cal\_texto.exe” es igual al archivo portador “calc.exe” en tamaño como se observa en la Fig. 19, pero para comprobar que el archivo “cal\_texto.exe” contiene el archivo de texto oculto, se compara la estructura hexadecimal del archivo portador y el archivo resultado, utilizando un editor hexadecimal “Hex Editor”, la estructura hexadecimal del portador tiene una terminación de 00 00 observe la Fig. 20.

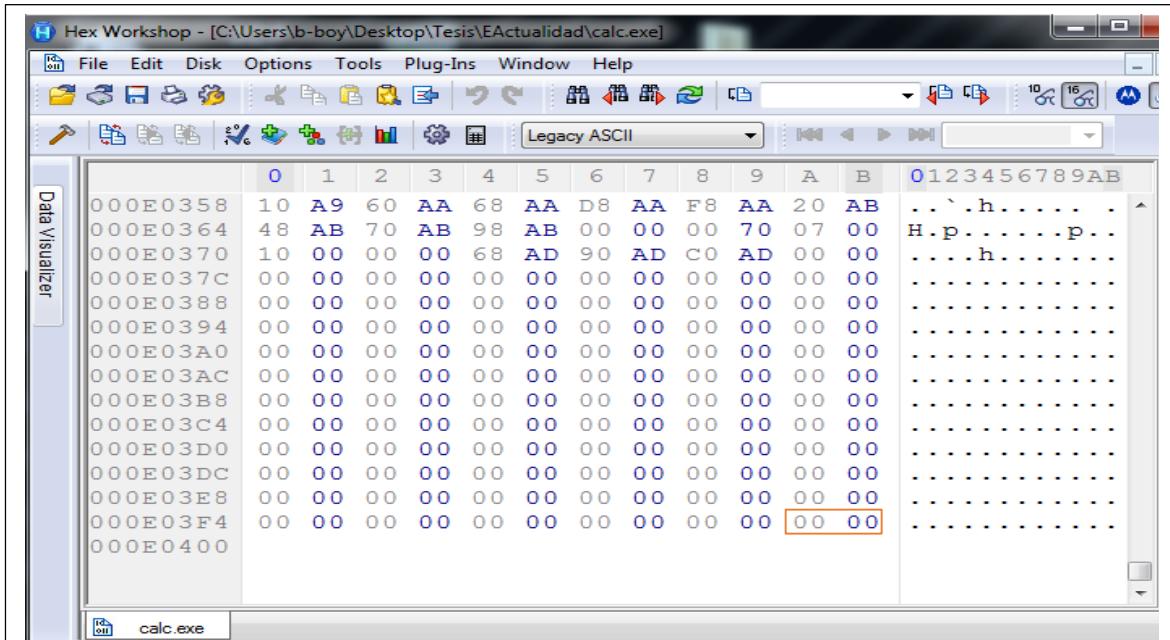


Fig. 20 Estructura hexadecimal del archivo "calc.exe" [Fuente propia]

El mismo procedimiento se realiza para el archivo resultado, en la Fig. 21 se puede visualizar que la estructura hexadecimal del portador termina en 00 00 y luego continua otra estructura hexadecimal la cual corresponde al archivo oculto, para recuperar el archivo texto que está oculto, en el archivo resultado se copia la estructura hexadecimal que continua a partir de 00 00 y se guarda en un archivo nuevo de tipo texto “nuevo.txt” el cual contiene la información que se ocultó, tal como se observa en la Fig. 22.

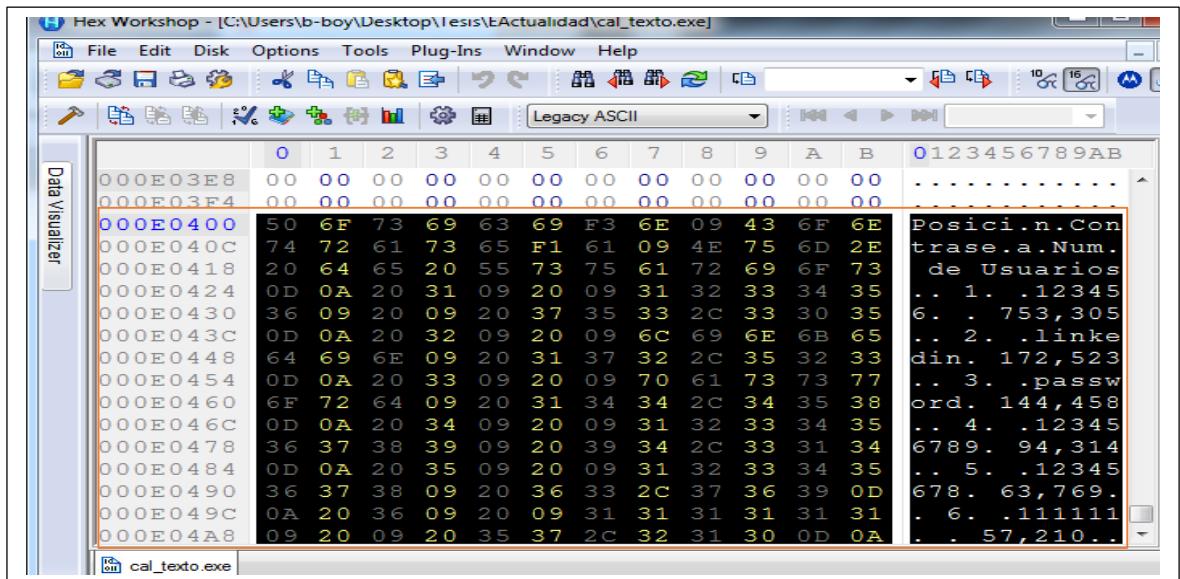


Fig. 21 Estructura del archivo "calc\_texto.exe" [Fuente propia]

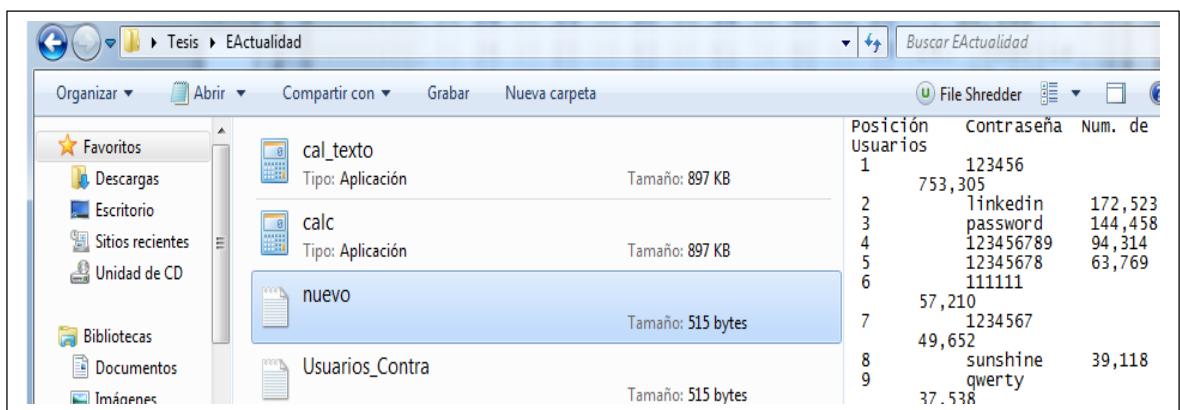


Fig. 22 Recuperación de archivo oculto [Fuente propia]

En estas dos presentaciones se hizo uso de la esteganografía utilizando archivos portadores y archivos a ocultar, teniendo éxito en el ocultamiento de información ya que pasa desapercibida por correo electrónico o por una memoria USB, vulnerando a personas que han tratado de obtener su contenido, este método no tiene un grado de seguridad alto ya que al tener un editor hexadecimal o aplicando estegoanálisis se podría obtener su información.

## **9. Sistema de Archivos**

Un sistema de archivos se refiere a una partición o disco que se utiliza para almacenar información, implementando métodos y estructura que ayudan a un Sistema Operativo a seguir la pista de los archivos que se encuentran almacenados, los cuales pueden ser accedidos por usuarios locales o remotos.

El sistema de archivos es el subsistema que suministra los medios para la organización y el acceso a los datos almacenados en dispositivos de memoria secundaria (disco) los datos que se almacenan en el disco se dividen en bloques de longitud fija, siendo el sistema de archivos el encargado de asignar un número adecuado de bloques a cada archivo, los sistemas de archivos cumplen con algunas funciones que son:

- Crear y borrar archivos
- Permitir el acceso a los archivos para que sean leídos o escritos
- Automatizar la gestión de la memoria secundaria
- Permitir referenciar un archivo por su nombre simbólico
- Proteger los archivos frente a fallos del sistema
- Permitir el uso compartido de archivos a usuarios autorizados

### **9.1. Sistema de archivos de nueva tecnología (NTFS)**

Sistema de archivos de nueva tecnología (New Technology File System) o más conocido NTFS es un sistema de archivos diseñado específicamente para Windows NT, también se utiliza en algunas versiones como Windows 2000, Windows XP y Windows Vista [28].

El objetivo de crear NTFS era crear un sistema de archivos eficiente, robusto y con seguridad incorporada desde su base, el nivel de seguridad que NFTS destaca es permitir que se definan atributos para cada archivo.

#### **9.1.1. Características de NTFS**

NTFS es un sistema de archivos flexible y potente, construido en un modelo de sistema de archivos elegantemente y simple, cuenta con algunas características las cuales se puede observar en la TABLA V.

**TABLA V CARACTERÍSTICAS DE NTFS**

<b>Características</b>	<b>Definición</b>
<b>Recuperación</b>	NTFS permite recuperarse de errores en el sistema, cuando sucede un fallo NTFS reconstruye volúmenes y los devuelve a un estado consistente.
<b>Seguridad</b>	NTFS utiliza el modelo de objetos de Windows para brindar seguridad a los archivos.
<b>Discos y archivos grandes</b>	La forma eficiente de soportar discos o archivos más grandes es lo que lo caracteriza de otros sistemas de archivos
<b>Múltiples flujos de Datos</b>	NTFS permite definir múltiples flujos de datos para un único archivo.
<b>Facilidad General de Indexación</b>	NTFS asocia una colección de atributos con cada archivo.

### **9.1.2. Almacenamiento NTFS**

El almacenamiento NTFS se realiza en diferentes enfoques, en la TABLA VI se mencionan algunos conceptos de almacenamiento en el disco [28].

**TABLA VI ALMACENAMIENTO NTFS**

<b>Almacenamiento</b>	<b>Concepto</b>
<b>Sector</b>	Es la unidad física más pequeña del disco, el tamaño de los datos en bytes es de 512 bytes.
<b>Agrupación</b>	El tamaño de la agrupación es una potencia de 2 y es uno de los sectores más contiguos.
<b>Volúmenes</b>	Es una partición lógica formada por una o más agrupaciones, se forma por la información del sistema de archivos y su tamaño máximo es de $2^{64}$ bytes.

### **9.1.3. Tipos de Atributos NTFS**

NTFS visualiza a cada archivo o directorio como un conjunto de atributos. Tanto el nombre del archivo, información de seguridad o sus datos, son todos atributos. Cada uno de esos

atributos se identifica por un código de tipo de atributo y opcionalmente un nombre [28] observe en la TABLA VII los diferentes atributos de NTFS.

**TABLA VII ATRIBUTOS NTFS**

Atributo	Descripción
<b>Standard Information</b>	Incluye información tal como fecha y hora y número de enlaces.
<b>Attribute List</b>	Muestra la ubicación de todos los registros de atributos que no caben en el registro MFT.
<b>File Name</b>	Contiene el nombre de archivo que puede ser de longitud larga (255 caracteres) o corta (8 caracteres), sin hacer distinción entre mayúsculas y minúsculas.
<b>Security Descriptor</b>	Describe quien es el propietario del archivo y quien lo puede acceder.
<b>Data</b>	Contiene datos de archivo. NTFS permite múltiples atributos de datos por archivo. Cada archivo tiene típicamente un atributo de datos sin nombre. Un archivo también puede tener uno o más llamados atributos de datos, cada uno con una sintaxis particular.
<b>Object ID</b>	Es un volumen único de identificador de archivo. No todos los archivos tienen identificadores de objetos.
<b>Logged Tool Stream</b>	Similar a un flujo de datos, pero las operaciones se registran en el archivo de registro NTFS como cambios en los metadatos de NTFS.
<b>Reparse Point</b>	Se utiliza para los puntos de montaje de volumen
<b>Index Root</b>	Utilizado para implementar directorios y otros

## 10. Flujo Alternativo de Datos (ADS)

El Flujo Alterativo de Datos (Alternate Data Streams) más conocido como ADS, forman parte y se encuentran en todas las versiones de los sistemas de archivos NTFS , su objetivo es almacenar datos dentro de datos “metadatos”, es decir todos los datos en un mismo fichero, su objetivó ha convertido al ADS como una técnica efectiva para ocultar y almacenar archivos [29].

El conocimiento de ADS es bajo cuando se compara con métodos utilizados para ocultar archivos, este método tiene relación con la esteganografía, ya que su finalidad es similar, es decir ocultar información utilizando un portador. Algunos principios de los ADS son:

- Permite ocultar ADS detrás de cualquier archivo de sistema existente.
- Los ADS no se ven afectados moviendo o copiando el archivo.
- El archivo existente no se ve afectado por los ADS.

El ADS se puede usar para ocultar un archivo secreto o malicioso dentro del registro de un archivo de sistema. Los archivos maliciosos pueden estar presentes en su sistema y no ser visibles al usuario. Por lo tanto, se ha convertido en una vulnerabilidad que los hackers pueden explotar fácilmente [30].

Los archivos que se descarga de internet crean automáticamente ADS que contiene un identificador de zona “Zone.Identifier”, que indica a través de un valor determinado su origen en la TABLA VIII se listan los valores.

**TABLA VIII IDENTIFICADORES DEL FLUJO ALTERNATIVO DE DATOS**

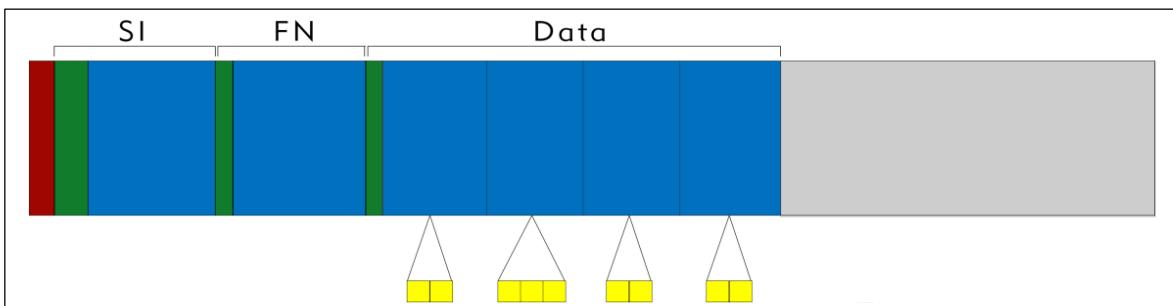
Identificador	Valor
URLZONE_LOCAL_MACHINE	0
URLZONE_INTRANET	1
URLZONE_TRUSTED	2
URLZONE_INTERNET	3
URLZONE_UNTRUSTED	4

### **10.1. Características del Flujo Alternativo de Datos**

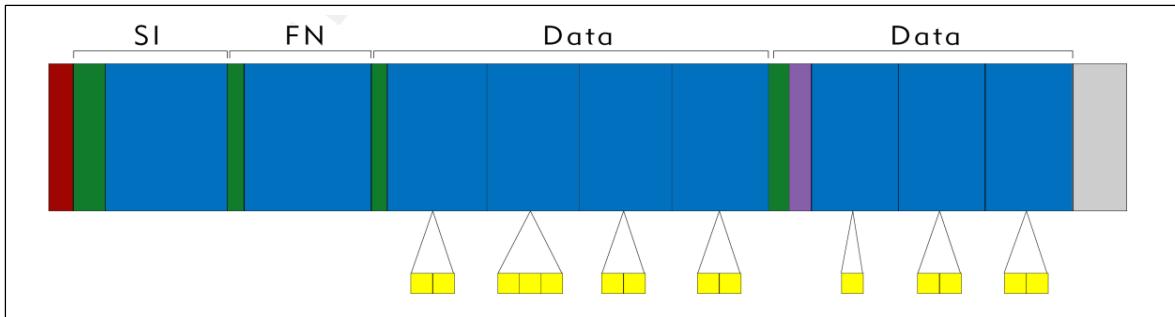
- El flujo alternativo de datos permite adjuntar cualquier tipo de archivo a un archivo o carpeta principal.
- Se puede utilizar para ocultar datos, ya que las utilidades del sistema solo verifican el flujo \$ DATA sin nombre y, por lo tanto, el ADS permanece sin detectar.
- La técnica de ocultación de ADS en NTFS es mucho más simple que cualquier otra técnica de ocultación, otras técnicas requieren el uso de archivos específicos bajo manipulación de programas para ocultar datos.
- Los protocolos de Internet como SMTP, FTP, etc. no admiten flujos de datos alternativos. Implica que las transmisiones de datos alternativas no se pueden intercambiar a través de Internet [31].
- Archivos que contienen datos alternativos en una secuencia se puede intercambiar en la red de área local, si el sistema receptor tiene sistema de archivos NTFS [31].
- Un usuario puede adjuntar cualquier cantidad de archivos a un archivo principal. No hay límite para esto. Las secuencias de datos alternativas pueden ser de cualquier tamaño y su tamaño no se visualiza en Windows.

### **10.2. Estructura del Flujo Alternativo de Datos en una Tabla Maestra de Archivos**

El flujo alternativo de datos (ADS) en si es una característica de NTFS [31] su función principal es almacenar información sobre un fichero sin tener que utilizar otros ficheros. Estos metadatos se escriben en el disco duro a continuación de los datos del fichero, para entenderlo mejor se muestra en la Fig. 23 un registro de la tabla maestra de archivos sin un ADS y la Fig. 24 un registro de la tabla maestra de archivos con un ADS.



**Fig. 23** Registro tabla maestra de archivo sin un flujo alternativo de datos [31]



**Fig. 24** Registro tabla maestra de archivo con un flujo alternativo de datos [31]

Como se puede observar en la Fig. 24 aparece un segundo DATA después de los datos del fichero principal, este DATA es el ADS que contiene los datos ocultos, cada registro en la tabla maestra de archivos de la Fig. 23 y la Fig. 24 cuenta con atributos los cuales son:

- **Atributo de información estándar (SI):** contiene el tiempo de creación del archivo, tiempo de modificación, tiempo de acceso pasado y permisos de archivo estándar de DOS (Sistema, Oculto, Archivar, Solo lectura, etc.). Cada registro solo puede tener un atributo SI.
- **Atributo de nombre de archivo (FN):** contiene un nombre para el archivo o directorio. Este nombre puede ser el nombre de UNICODE regular, el nombre de archivo corto de MSDOS 8.3 o cualquier otro dato de identificación. Múltiples atributos de nombre de archivo pueden existir y ser grabados para contener cada uno de estos posibles nombres.
- **Atributo de datos (DATA):** contiene los datos del archivo. Puede haber múltiples atributos de datos en cada registro.

### 10.3. Ventajas del Flujo Alternativo de Datos

- Se puede usar para ocultar datos aplicando el concepto de esteganografía.
- Permite la compatibilidad de NTFS de Windows con el archivo jerárquico de Macintosh.
- Es utilizado por el sistema de archivos NTFS para almacenar información sobre un archivo como miniaturas, están ocultos como ADS detrás del archivo principal.

#### **10.4. Desventajas del Flujo Alternativo de Datos**

- Los flujos alternativos de datos no pueden ser detectados por los buscadores normales del sistema por lo que se ha convertido en un problema grave ya que proporciona una forma perfecta para ocultar datos maliciosos.
- Cuando se oculta datos maliciosos en un archivo haciendo uso de un flujo alternativo de datos, estos archivos pueden comenzar a ocultar cada vez más datos detrás de un solo archivo cubriendo más y más espacio en disco y causando ataques de denegación de servicio.
- Los programas de antivirus tienen dificultad para detectar ADS
- Los servicios de limpieza de archivos tienen problemas para eliminar ADS

#### **10.5. Comandos Básicos que utiliza el Flujo Alternativo de Datos**

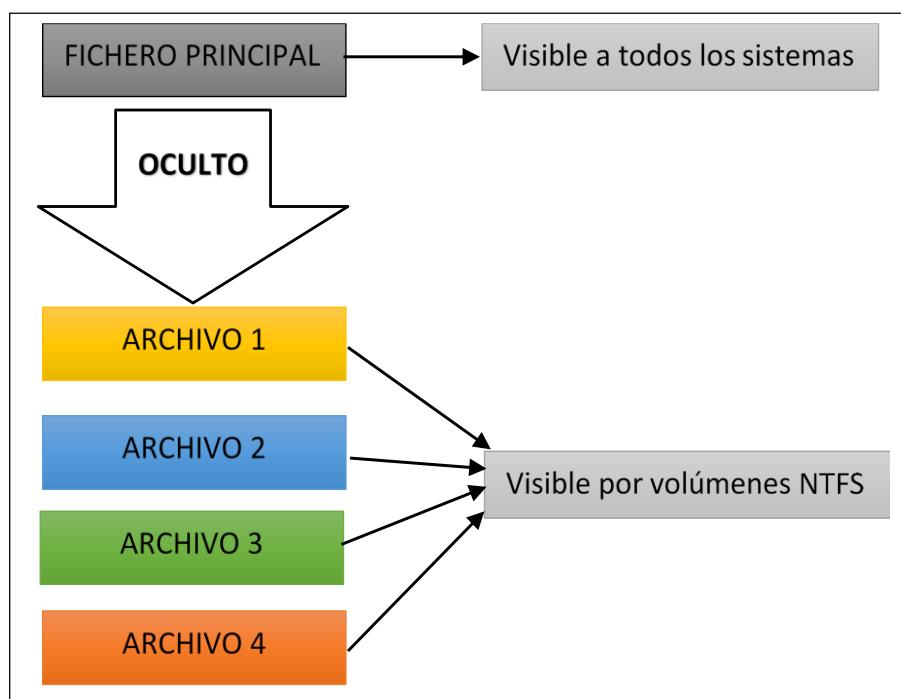
Trabajar con el flujo alternativo de datos es muy simple se hace uso de la consola CMD de Microsoft Windows en modo administrador, de esta manera se obtendrá todos los privilegios como son: obtener acceso a todos los archivos del equipo y realizar cambios, los cambios a los archivos se realizan al ingresar y ejecutar los comandos en la consola de Microsoft Windows que son utilizados para crear, modificar y ver ADS observe la TABLA IX.

**TABLA IX COMANDOS BÁSICOS PARA CREAR, MODIFICAR Y VER FLUJO ALTERNATIVO DE DATOS**

Sintaxis	Concepto
'<', '>'	Operadores de redirección
echo	Muestra mensajes
type	Leer texto plano del fichero principal
more	Leer texto plano de ADS
start	Ejecuta Programas
dir/r	Muestra ADS que existen en un directorio
mklink	Crea vínculos simbólicos y físicos

## 10.6. Manipulación del Flujo Alternativo de Datos

La manipulación de ADS se refiere a la forma de crear, modificar y visualizar datos que se ocultan en un fichero principal, en la Fig. 25. se observa cómo es la estructura de un fichero principal con archivos ocultos. Para desarrollar la manipulación de ADS en el sistema operativo Microsoft Windows es necesario conocer el funcionamiento, estructura, especificaciones, objetivo, comandos y las características del Flujo Alternativo de Datos.



**Fig. 25** Estructura de un fichero principal con archivos ocultos [Fuente propia]

La creación, modificación y visualización de ADS se realizará en el siguiente directorio de trabajo:

C:\Users\b-boy\Desktop\Tesis\PruebasAds

En esta dirección se desarrollarán todas las pruebas y se incluirá los diferentes archivos que se ocultarán y otros que serán ficheros principales, una recomendación muy importante es abrir la consola en modo administrador, para obtener todos los privilegios y prevenir problemas futuros en la ejecución de los comandos.

### **10.6.1. Insertar texto en un flujo alternativo de datos, utilizando como fichero principal un archivo de texto**

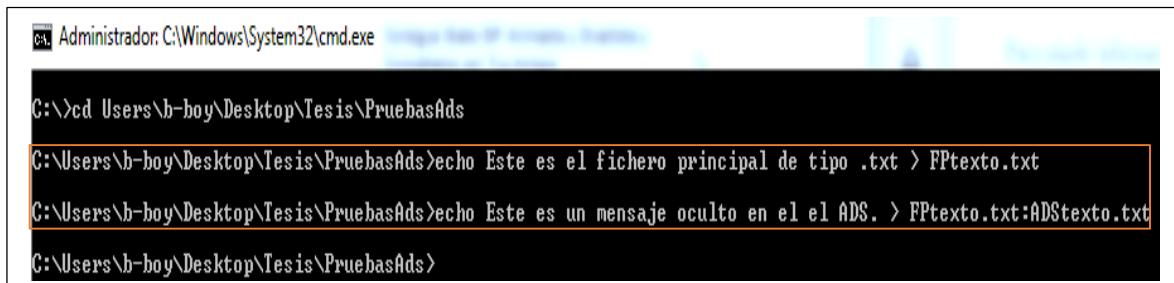
Insertar un texto en un ADS es muy simple, una vez que se abre la consola CMD de Microsoft Windows en modo administrador y se ha situado en la ruta del directorio de trabajo, lo primero que se debe crear es un fichero principal, el fichero principal que se crea se le asigna un nombre, en este caso se llamará “FPtexto.txt” el fichero contendrá un mensaje que será visible ante el usuario y el sistema, esto se realiza usando la siguiente línea de comandos:

***echo Este es el fichero principal de tipo.txt > FPtexto.txt***

Obteniendo el fichero principal se procede a la creación del ADS con el nombre de “ADStexto.txt” una acotación muy importante es que el ADS que se crea tiene que ser del mismo tipo del archivo que se va a ocultar, la forma de ocultar el archivo es sencilla se inserta el nombre del archivo o mensaje a ocultar, luego se inserta el signo “>” de redirección haciendo referencia al fichero principal, se ingresan dos puntos “:” y en segundo plano se hace referencia al ADS, todo este procedimiento se realiza usando la siguiente línea de comandos:

***echo Este es un mensaje oculto en el ADS > FPtexto.txt: ADStexto.txt***

En la Fig. 26 se muestra la creación del ADS y del fichero principal, además se inserta el mensaje de texto en el ADS creado.



```
C:\ Administrador: C:\Windows\System32\cmd.exe
C:\>cd Users\b-boy\Desktop\Tesis\PruebasAds
C:\Users\b-boy\Desktop\Tesis\PruebasAds>echo Este es el fichero principal de tipo .txt > FPtexto.txt
C:\Users\b-boy\Desktop\Tesis\PruebasAds>echo Este es un mensaje oculto en el el ADS. > FPtexto.txt:ADStexto.txt
C:\Users\b-boy\Desktop\Tesis\PruebasAds>
```

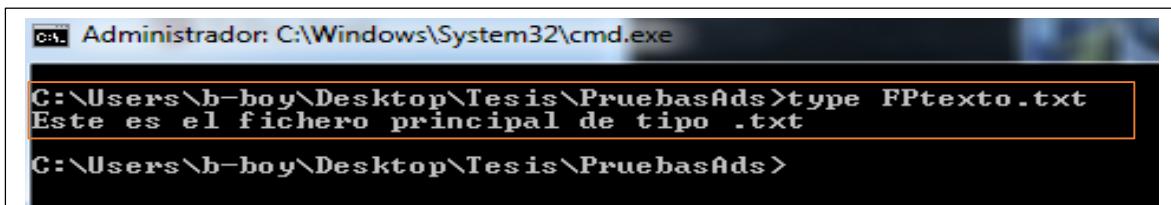
**Fig. 26** Creación (ads – fichero principal) insertar (archivo de texto) [Fuente propia]

Insertado el mensaje de texto en el ADS no afectará al tamaño del fichero principal, no podrá ser visualizado por el usuario y lo mejor de todo no levantará sospecha alguna al momento que se desee copiar o pegar el fichero principal en otro directorio de la máquina.

### 10.6.2. Visualizar texto insertado en un flujo alternativo de datos

Existen varias formas de poder visualizar un texto insertado en un ADS, se detallarán las dos formas más comunes:

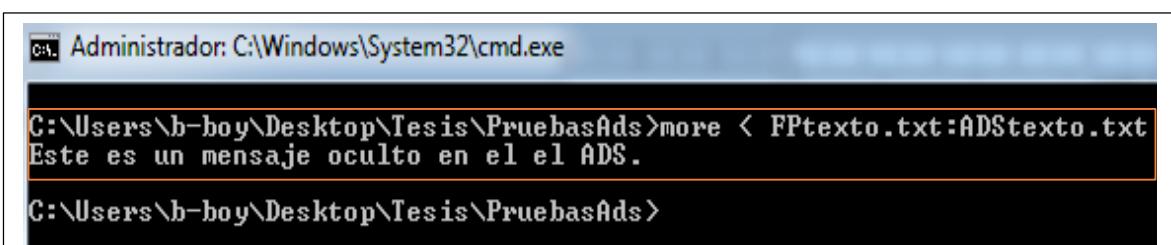
La primera forma de visualizar un texto insertado en un ADS es por medio de la consola CMD, ya que se considera la forma más eficiente para acceder a su contenido. Existen dos comandos que se utilizan para visualizar texto de archivos el comando “type” y el comando “more”, la diferencia en estos dos comandos es que el comando “type” solo nos permite visualizar el texto de un fichero principal que es visible a los usuarios, en la Fig. 27 se puede observar que al ejecutar la línea de comandos se visualiza el mensaje que se insertó al crear el fichero principal “FPtexto.txt”.



```
C:\Users\b-boy\Desktop\Tesis\PruebasAds>type FPtexto.txt
Este es el fichero principal de tipo .txt
C:\Users\b-boy\Desktop\Tesis\PruebasAds>
```

Fig. 27 Visualización del texto del fichero principal usando el comando “type” [Fuente propia]

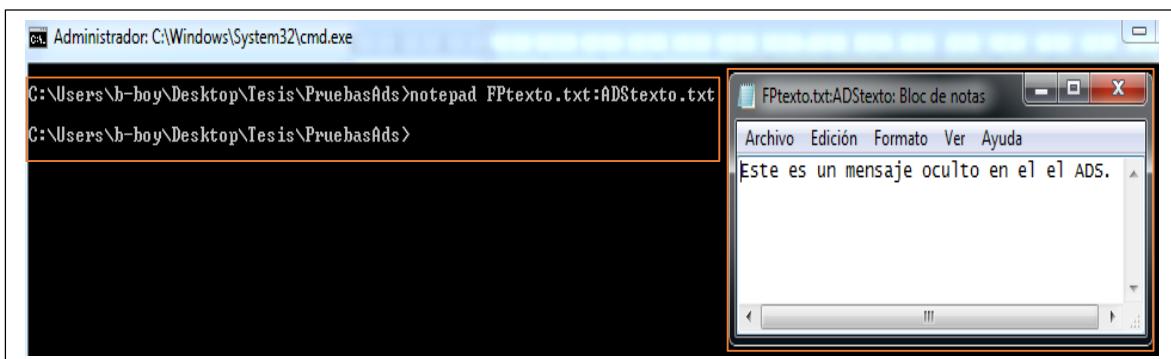
El comando “more” en cambio sí nos permite acceder y visualizar el texto insertado en un ADS tal como se observa en la Fig. 28, lo que realiza la línea de código es insertar el comando “more”, seguido se inserta el signo “<” de redirección, en este caso el signo es inverso por el motivo que no se va insertar un archivo, caso contrario se va acceder a la información del archivo oculto, se debe tener en cuenta que el ADS se encuentra dentro del fichero principal por tal motivo se hace referencia al mismo, se ingresan dos puntos “:” y en segundo plano se ingresa el nombre del ADS, al ejecutarse la línea de código muestra la información que se insertó en el ADS.



```
C:\Users\b-boy\Desktop\Tesis\PruebasAds>more < FPtexto.txt:ADStexto.txt
Este es un mensaje oculto en el el ADS.
C:\Users\b-boy\Desktop\Tesis\PruebasAds>
```

Fig. 28 Visualizar el texto insertado en un ads usando el comando “more” [Fuente propia]

La segunda forma de visualizar un texto insertado en un ADS es mediante el programa “Notepad” como se observa en la Fig. 29, el programa permite acceder a la información y visualizarla, pero únicamente lo hará si se lo ejecuta desde consola CMD de Microsoft Windows, si se intenta buscar directamente el ADS “ADSTexto.txt” no se podrá encontrar, como se explicó en la Fig. 25 el ADS es un metadato oculto en un fichero principal que no pude ser visualizado por los usuarios, la línea de comandos que se utiliza es muy similar a la que utiliza el comando “more” la diferencia está en que en vez de insertar “more” se inserta “Notepad”. Al ejecutar la línea de comandos muestra la información en el programa.



**Fig. 29** Visualizar el texto de un ads con el programa " Notepad" [Fuente propia]

#### 10.6.3. Insertar un texto en un flujo alternativo de datos por medio de un script php

El uso de lenguajes de programación como php, se considera otra manera de insertar texto dentro de un ADS; se crea un script llamado “scriptPHP.php” su sintaxis describe los siguiente; en la variable “\$canal” se abren dos archivos con la función (fopen) el primero es el fichero principal y el segundo al ADS, la variable (fwrite) hace referencia a la variable que abrió los archivos e ingresa el texto, se hace uso de la función (fclose) para cerrar el canal, la sintaxis del script se observa en la Fig.30.

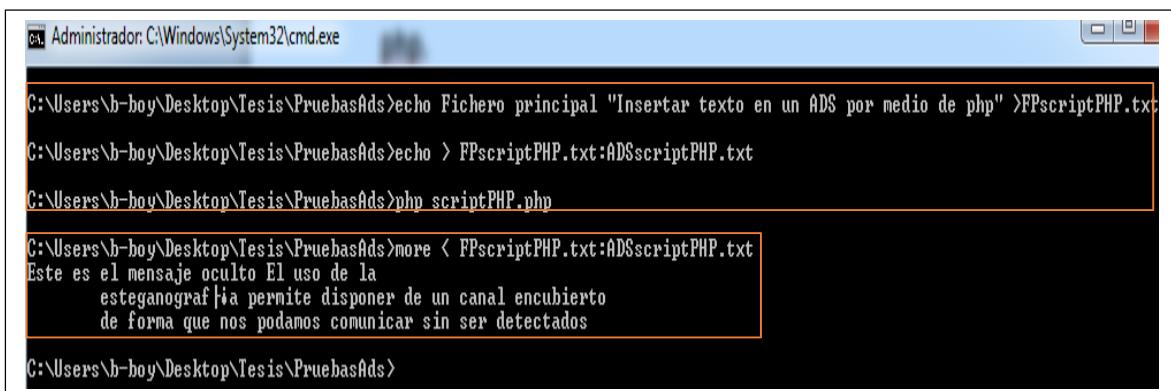
```

1  <?php
2  // Se abre el archivo FPscript.txt y el ADSscript.txt
3  $canal= fopen('FPscript.txt:ADSscript.txt','w');
4  // Se escribe el mensaje oculto
5  fwrite($canal, 'Este es el mensaje oculto : "El uso de la
6  esteganografía permite disponer de un canal encubierto
7  de forma que nos podamos comunicar sin ser detectados."');
8  //Se cierra el canal
9  fclose ($canal);
10 ?>

```

**Fig. 30** Script php “scriptPHP.php” [Fuente propia]

Antes de ejecutar el script en la consola CMD, se tendrá que crear los dos archivos que menciona la variable “\$canal”, se crea el fichero principal con el nombre de “FPscriptPHP.txt” y el ADS con el nombre de “ADSscript.php”, creados los archivos se ejecuta el script “scriptPHP.php” con la finalidad de insertar el texto en el ADS, la forma de comprobar que en el ADS se encuentra el texto, es utilizando el comando “more”, en la Fig. 31 se observa el procedimiento.



```

Administrator: C:\Windows\System32\cmd.exe

C:\Users\b-boy\Desktop\Tesis\PruebasAds>echo Fichero principal "Insertar texto en un ADS por medio de php" >FPscriptPHP.txt
C:\Users\b-boy\Desktop\Tesis\PruebasAds>echo > FPscriptPHP.txt:ADSscriptPHP.txt
C:\Users\b-boy\Desktop\Tesis\PruebasAds>php scriptPHP.php
C:\Users\b-boy\Desktop\Tesis\PruebasAds>more < FPscriptPHP.txt:ADSscriptPHP.txt
Este es el mensaje oculto El uso de la
esteganografia permite disponer de un canal encubierto
de forma que nos podamos comunicar sin ser detectados
C:\Users\b-boy\Desktop\Tesis\PruebasAds>

```

Fig. 31 Insertar texto en un ads utilizando un script php [Fuente propia]

#### 10.6.4. Insertar una Imagen en un flujo alternativo de datos, utilizando como fichero principal un archivo de texto

No solo se puede ocultar archivos de la misma extensión de un fichero principal, la variedad de tipos de archivos a ocultar no tiene límites, en este caso se ocultará un archivo de imagen en un fichero principal de tipo texto, en la Fig. 32 se observa un archivo de imagen “unl.jpg” con un tamaño de 16 KB este archivo será insertado en un ADS, mientras que el archivo “FPImagen.txt” con un tamaño de 1 KB será el fichero principal que contendrá el ADS.

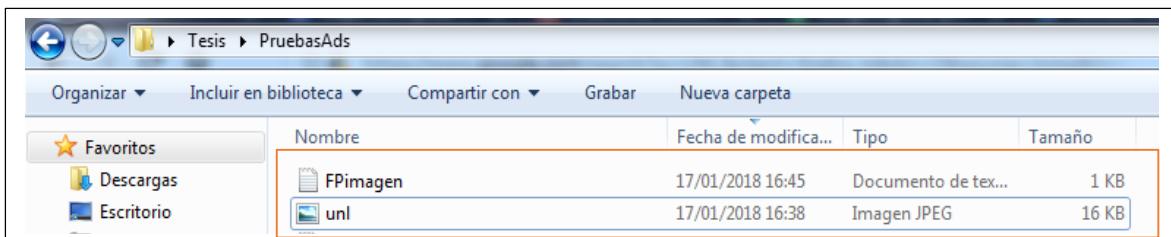


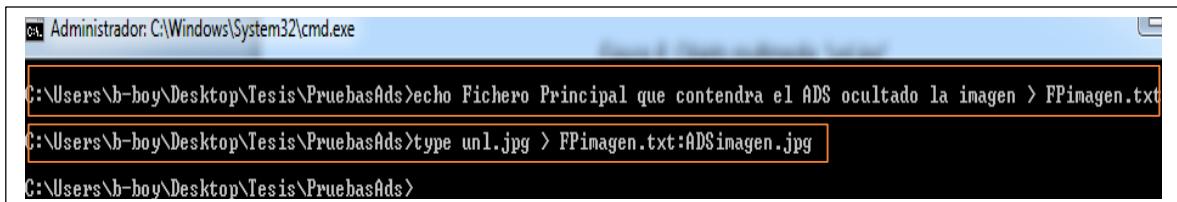
Fig. 32 Archivo imagen y archivo de texto [Fuente propia]

El fichero principal se crea desde la consola CMD junto con el ADS, el fichero principal contendrá el ADS, mientras que en el ADS se insertara el archivo de imagen llamado “ADSimagen.jpg”, en este caso no se utilizará el comando “echo”, se utilizará el comando

“type” por la razón que no se va a insertar un texto, sino un archivo la línea de comandos que se ejecuta es la siguiente:

```
type imagen.jpg > FPImagen.txt: ADSImagen.jpg
```

La línea de comandos describe lo siguiente; se ingresa el comando “type” se menciona el archivo imagen de entrada, se hace referencia al fichero principal y al ADS, cabe mencionar que el ADS será de la misma extensión del archivo que se inserta, en la Fig.33 se observa todo el procedimiento descrito.



The screenshot shows a Windows Command Prompt window titled "Administrador: C:\Windows\System32\cmd.exe". The user has run the command "type unl.jpg > FPImagen.txt: ADSImagen.jpg". The output of the command is visible in the console window, showing the file path and the command itself.

**Fig. 33** Insertar un archivo imagen en un ads, oculto en un fichero principal de tipo texto [Fuente propia]

#### 10.6.5. Visualizar una Imagen insertada en un flujo alternativo de datos

La manera de visualizar una imagen insertada en un ADS es muy diferente a la forma de visualizar un texto, su diferencia consiste en que se utilizan diferentes comandos, para visualizar un texto se utiliza el comando “more”, si se intentara visualizar una imagen con el comando “more” dará como resultado un conjunto de símbolos comenzado con la palabra “JFIF” esta palabra demuestra que la imagen si esta insertada pero no se puede visualizar, tal como se observa en la Fig. 34.



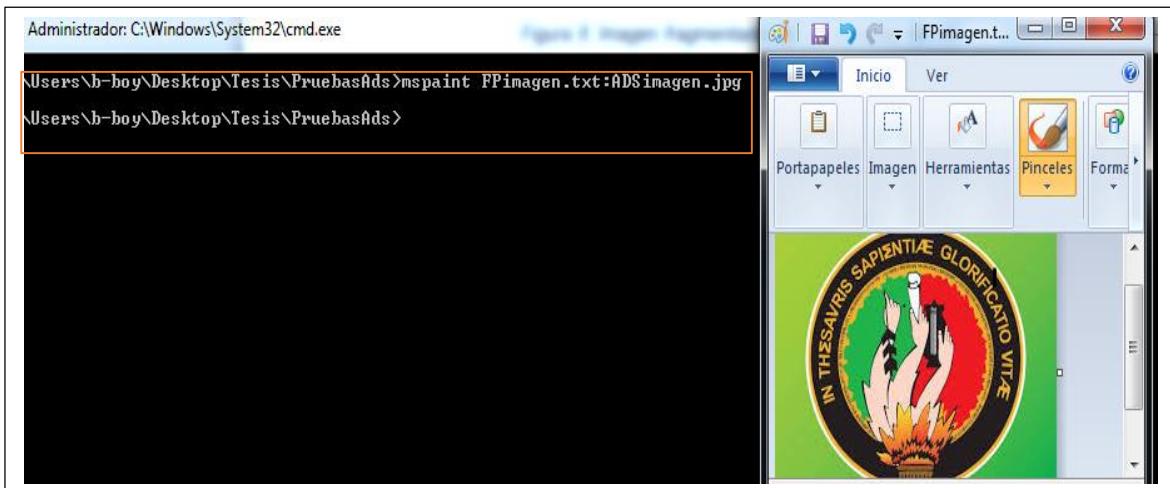
The screenshot shows a Windows Command Prompt window with the command "more < FPImagen.txt: ADSImagen.jpg". The output shows the word "JFIF" followed by a series of binary or encoded characters, indicating that the image data is being processed as text.

**Fig. 34** Visualizar una imagen con el comando "more" [Fuente propia]

Existen dos formas de poder visualizar una imagen, la primera es utilizando el editor de imagen Paint ejecutándolo desde la consola CMD de Windows con la siguiente línea de comandos:

### ***mspaint FPImagen.txt: ADSImagen.jpg***

La línea de comandos describe lo siguiente; se ingresa el comando mspaint que hace referencia al editor de imagen Paint, seguido se escribe el nombre del fichero principal que contiene el ADS, y por último se inserta el nombre del ADS en que se insertó el archivo de imagen, este procedimiento se observa en la Fig. 35.



**Fig. 35** Visualizar un archivo de imagen insertado en un ads utilizando “Paint” [Fuente propia]

La segunda forma de visualizar un archivo de imagen insertado en un ADS es por medio de un lenguaje de programación como php, este mismo lenguaje se utilizó para insertar un texto dentro de un ADS, en este caso se utilizará para visualizar un archivo, se crea un script llamado “imagen.php” se digita la siguiente sintaxis:

```
<?php  
  
$file= file_get_contents('FPImagen.txt:ADSimagen.jpg');  
  
echo $file;  
  
?>
```

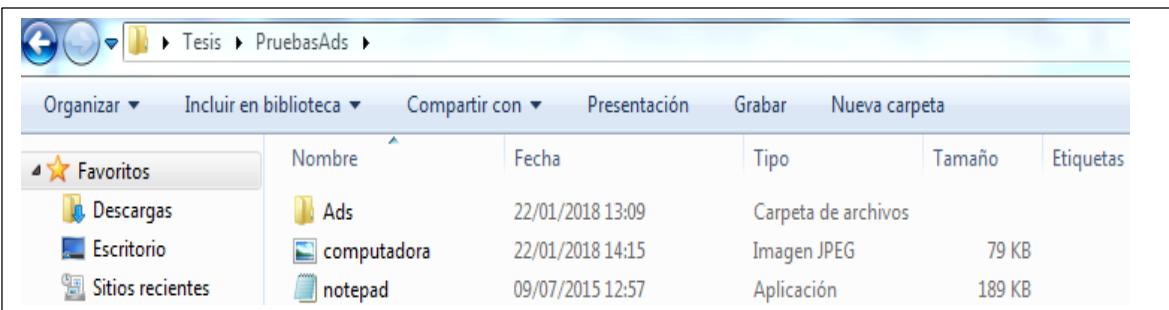
La sintaxis describe los siguientes: la variable “\$file” hace uso de la función (file\_get\_contents) esta función permite obtener el archivo insertado en el ADS oculto en el fichero principal, dando como salida un archivo de extensión “jpg” este archivo será visible por el sistema y los usuarios utilizando cualquier editor de imágenes observemos la Fig. 36.



**Fig. 36** Visualizar una imagen insertada en un ads por medio de un script php [Fuente propia]

#### 10.6.6. Insertar una imagen en un flujo alternativo de datos, usando como fichero principal un archivo ejecutable

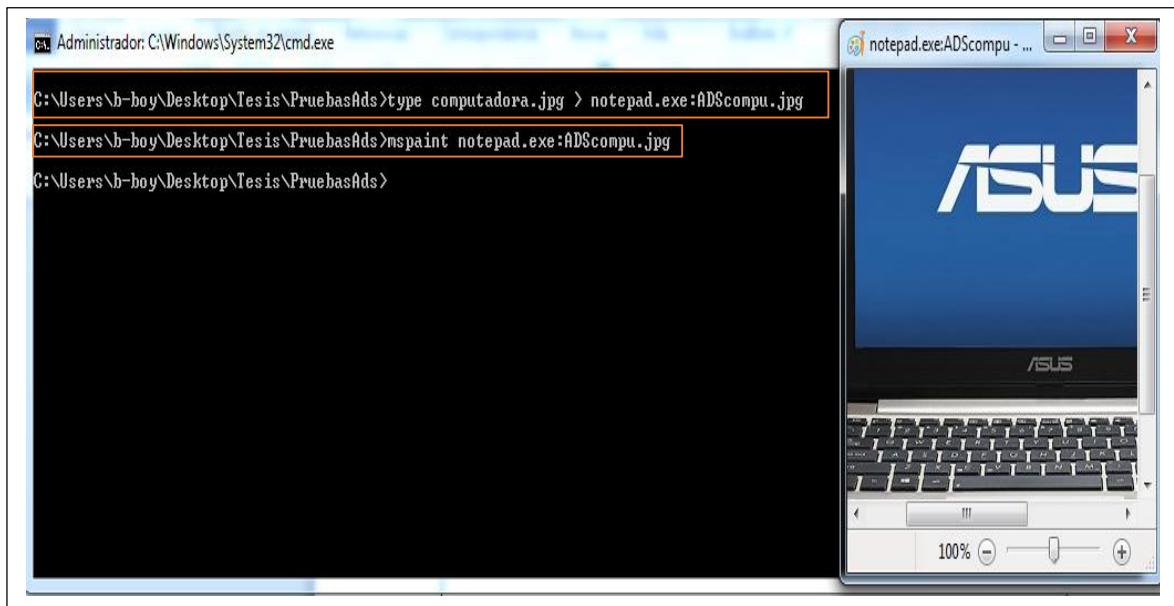
Un archivo ejecutable también puede ser utilizado como un fichero principal para contener un ADS de diferente tipo, en la Fig. 37 se muestran el archivo ejecutable “notepad.exe” este archivo será el fichero principal el cual contendrá el ADS y en el ADS se insertar el archivo de imagen “computadora.jpg”.



**Fig. 37** Fichero principal y archivo de imagen [Fuente propia]

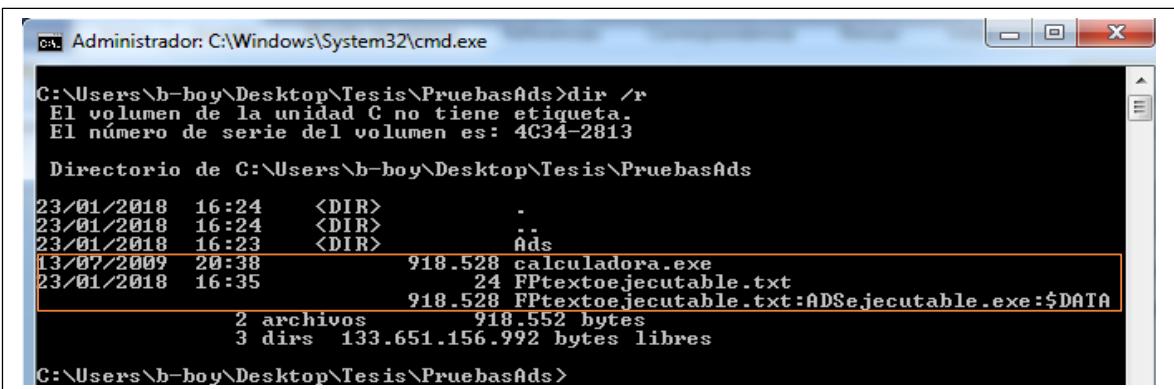
El procedimiento es muy similar a los anteriores. Lo que se pretende demostrar es que cualquier archivo que se encuentre en NTFS puede ser usado como fichero principal y así

mismo tener ocultos diferentes tipos de ADS, en la Fig. 38 se muestra cómo se inserta y se visualiza la imagen en el ADS.



**Fig. 38** Insertar y visualizar una imagen en un ads de tipo exe [Fuente propia]

Una de las maneras de confirmar que un archivo se encuentra insertados en un ADS es utilizando el comando "dir", pero este comando solo enlista los archivos que son visibles para el usuario, para observar los ADS ocultos, se realiza lo siguiente al comando "dir" se le agrega "/r" este comando "dir/r" si permite enlistar los archivos principales conjuntamente con los ADS que contiene alojados, tal como se observa en la Fig. 39.



**Fig. 39** Enlistar los ads contenidos en un fichero principal utilizando el comando "dir/r" [Fuente propia]

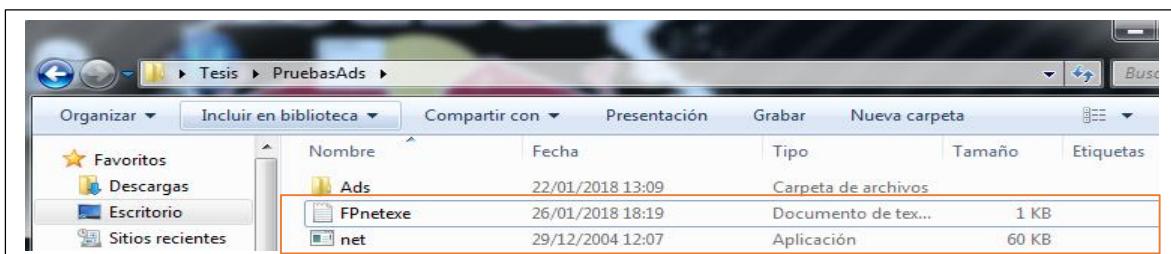
### **10.6.7. Insertar un archivo ejecutable en un ADS, utilizando como fichero principal un archivo de texto**

El uso del flujo alternativo de datos no es utilizado únicamente para mantener seguros los archivos, también es utilizado por hackers que realizan ataques informáticos con fines maliciosos, estos ataques se realizan enviando un archivo ejecutable oculto en un fichero principal de tipo: pdf, imagen, texto, video, audio.

Un archivo de texto puede pasar desapercibido ante un usuario, por tal motivo se lo utiliza como fichero principal, una razón del porque nadie sospecharía es por su tamaño, ya que, ante la vista del usuario, el archivo es muy pequeño para contener un archivo ejecutable.

El comando “type” permite insertar el archivo ejecutable dentro del fichero principal de tipo texto, pero no permite mostrar o ejecutar el archivo por las políticas de Microsoft Windows, que establece que un flujo alternativo de datos no permita su manipulación por un usuario final, solo será usado por los programas que lo necesiten.

En la Fig. 40 se observa un archivo de texto llamado “FPnetexe.txt” con tamaño de 1 KB este archivo será el fichero principal que contendrá el ADS, en el ADS se insertará un archivo ejecutable llamado “net.exe” con un tamaño de 68 KB.



**Fig. 40** Fichero principal (FPnetexe.txt) y archivo ejecutable (net.txt) [Fuente propia]

La forma de insertar un archivo ejecutable dentro de un ADS, es similar a la forma de insertar una imagen, se utiliza el mismo comando “type”, simplemente se debe tener en cuenta de que tipo es el archivo que se va insertar, porque de este tipo se tiene que crear el ADS, tal como se observa en la Fig. 41.

```
C:\Users\b-boy\Desktop\Tesis\PruebasAds>type net.exe > FPnetexe.txt:ADSnetexe.exe
```

**Fig. 41** Insertar un archivo ejecutable en un ads, contenido en un fichero principal de tipo texto [Fuente propia]

#### 10.6.8. Ejecutar un archivo tipo exe dentro de un ADS

Un archivo de extensión .exe no se puede visualizar como un texto o una imagen, pero si se puede ejecutar, por lo cual los comandos “more” y “type” no serían útiles, la forma de ejecutar un archivo .exe es creando un enlace simbólico el cual permite tener un acceso a un directorio o archivo que se encuentra en una determinada ubicación.

***mklink ESnet.exe c:\ruta de la carpeta\FPnetexe.exe: ADSnetexe.exe***

La línea de comandos describe lo siguiente; se ingresa el comando mklink y seguido el nombre que se le dará al enlace simbólico con la extensión del archivo que se encuentra oculto, se escribe la ruta del directorio especificando el fichero principal y el ADS donde está el archivo ejecutable, creado el enlace simbólico se utiliza el comando “start” que permite la ejecución del acceso directo, tal como se observa en la Fig. 42.



The screenshot shows a Windows Command Prompt window titled "Administrador C:\Windows\System32\cmd.exe". The command entered is:

```
C:\Users\b-boy\Desktop\Tesis\PruebasAds>type net.exe > FPnetexe.txt:ADSnetexe.exe  
C:\Users\b-boy\Desktop\Tesis\PruebasAds>mkLink ESnet.exe C:\Users\b-boy\Desktop\Tesis\PruebasAds\FPnetexe.txt:ADSnetexe.exe  
vínculo simbólico creado para ESnet.exe <==> C:\Users\b-boy\Desktop\Tesis\PruebasAds\FPnetexe.txt:ADSnetexe.exe  
C:\Users\b-boy\Desktop\Tesis\PruebasAds>start ESnet.exe  
C:\Users\b-boy\Desktop\Tesis\PruebasAds>
```

The taskbar at the bottom shows the application icon for "C:\Users\b-boy\Desktop\Tesis\PruebasAds\ESnet.exe" and the text "Cmd line:".

**Fig. 42** Ejecución de un archivo ejecutable insertado en un ads [Fuente propia]

Para obtener un archivo que se insertó en un ADS contenido en un flujo alternativo de datos, lo único que se debe realizar, es utilizar es la siguiente línea de comandos:

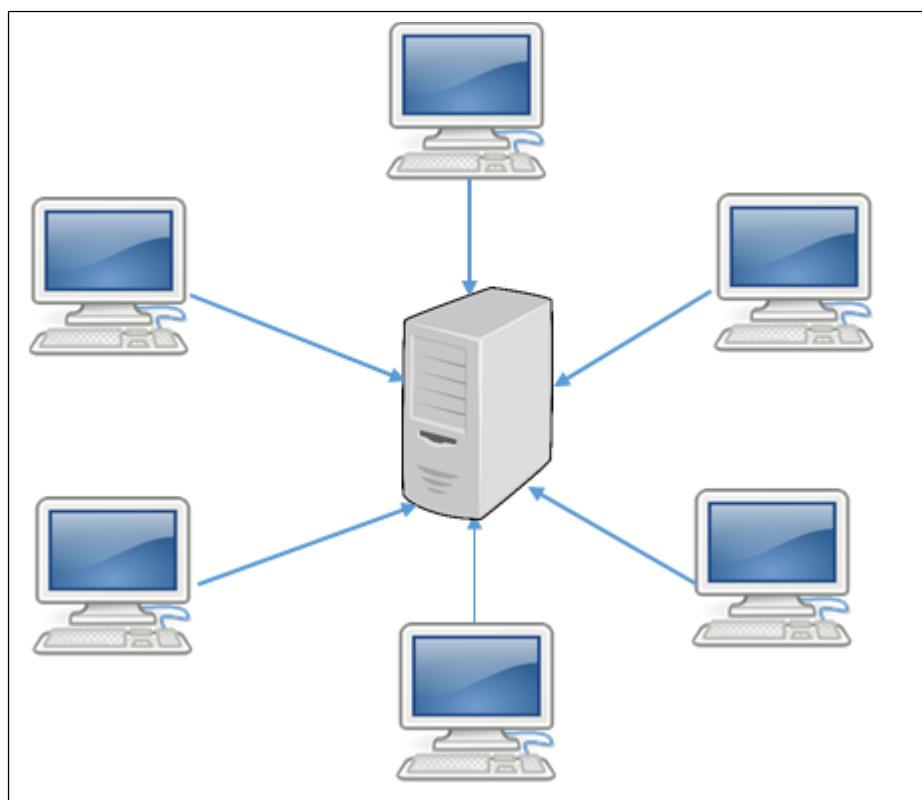
***type “nombre de acceso directo.exe” > “nombre.exe”***

Lo que realiza la línea de comandos es; ingresar el comando “type”, luego insertar el nombre del enlace simbólico con su extensión “tipo del archivo oculto”, utilizar el operador de redirección “>” e insertar un nombre con la extensión del archivo oculto, al ejecutarlo automáticamente se obtendrá el archivo que se encontraba insertado en el ADS.

## 11. Red de computadoras

El origen de las redes se remota en la Universidad de Hawai, en los años setenta a través del Método de Acceso Múltiple con Detección de Portadora y Detección de Colisiones, CSMA/CD (Carrier Sense and Multiple Access with Collision Detection), utilizado actualmente por Ethernet. Este método surgió ante la necesidad de implementar en las islas Hawai un sistema de comunicaciones basado en la transmisión de datos por radio, que se llamó Aloha, y permite que todos los dispositivos puedan acceder al mismo medio, aunque sólo puede existir un único emisor en cada instante [32].

Una red de computadoras es un conjunto de equipos conectados entre sí a través de canales físicos o inalámbricos tal como se observa en la Fig. 43 tiene varios propósitos, como facilitar la comunicación, compartir un único dispositivo electrónico o transmisión de archivos entre dos o más usuarios.



**Fig. 43** Red de computadoras [Fuente Propia]

### **11.1. Tipos de Redes**

Existen diferentes tipos de redes las cuales se diferencian por su tamaño, su velocidad de transmisión y su alcance, en la Tabla X se mencionan los tipos de redes que existen en la actualidad.

**TABLA X TIPOS DE REDES**

<b>TIPO</b>	<b>DESCRIPCIÓN</b>
<b>Redes PAN</b> <b>Red de Área Personal</b> <b>Personal Area Network</b>	La red se conforma por todos los equipos que estén cerca del usuario, permite una comunicación y transmisión de datos sencilla, rápida y efectiva.
<b>Redes LAN</b> <b>Rede de Área Local</b> <b>(Local Area Network)</b>	Generalmente se las utiliza en edificios. Están constituidas normalmente para un conjunto reducido de ordenadores y se limitan físicamente a un espacio geográfico de 100 metros.
<b>Redes MAN</b> <b>Rede de Área Metropolitana</b> <b>(Metropolitan Area Network)</b>	Red de alta velocidad, abarca ciudades enteras, su red se conforma por distintas redes LAN, su extensión es de 100 Km.
<b>Redes WAN</b> <b>Red de Área Extensa</b> <b>(Wide Area Network):</b>	No tienen ninguna limitación geográfica, su extensión se da en países o en continentes, une redes metropolitanas de ciudades enteras permitiendo su comunicación.
<b>Redes SAN</b> <b>Red de Almacenamiento Integral</b> <b>Storage Area Network (SAN)</b>	Realiza el almacenamiento de la red de usuarios comunes y los reorganiza en una red independiente de alto rendimiento.

## 11.2. Topologías de Redes

Las computadoras de una red pequeña están conectadas entre sí por cables de conexión ya sea de par trenzado, cable coaxial, entre otros. Cuando se requiere la conexión de redes extensas se utiliza micro ondas, fibra óptica o incluso satélites.

Todas las conexiones de las redes se realizan a través de una estructura conocida como topología de red, la topología de red no es más que la forma en que lleva a cabo una conexión, existen diferentes tipos de topología como son:

- **Lineal.** Es el modelo más sencillo también se lo conoce como “topología de bus”, utiliza un cable que recorre cada uno de los ordenadores y usa una terminación en cada uno de los extremos, los dispositivos que se conectan a la topología lineal generalmente utilizan un conector en T.
- **Anillo.** Forma una red con dispositivos conectados uno a otro sobre un cable dando la forma de un círculo físico, su función reside en que los paquetes que recibe una computadora que genera un toquen los trasmite a la siguiente computadora hasta terminar el círculo.
- **Estrella.** Cada uno de los ordenadores cuenta con su propio cable dedicado que apunta a una caja de conexiones que permite la interconexión entre los dispositivos.
- **Árbol.** También conocida como “topología estrella distribuida” porque abarca más de una caja de conexión que se conectan en topología de bus, al igual que la topología estrella cada dispositivo se conecta a una caja de conexiones.

## 11.3. Protocolo de red

Es una agrupación de reglas y estándares que tiene como objetivo hacer que la comunicación en la red sea factible y confiable. Las reglas definen la forma en que deben de efectuarse las comunicaciones de las redes, incluyendo la temporización, la secuencia, la revisión y la corrección de errores [33].

Los tres elementos claves dentro de los protocolos son:

- Sintaxis (formato de los mensajes: datos + comandos)
- Semántica (significado de los comandos)

- Secuencia y temporización (adecuado de las acciones que se toman respecto de los comandos)

#### 11.4. Modelos de Arquitectura de red

La comunicación entre redes es muy compleja, en particular resulta tedioso entender del todo su funcionamiento, por ello la arquitectura tiene como propósito dar a conocer como está compuesta y cómo funciona una red.

Los dos modelos de arquitectura de red más conocidos son el modelo OSI y el modelo TCP/IP observe la Fig. 44 la estructura de los modelos está compuesta por niveles que interactúan para resolver problemas y llevar a cabo una comunicación, cada nivel cuenta con funciones y servicios, los niveles inferiores prestan servicios a los niveles superiores, todos los servicios son definidos por los protocolos de red.

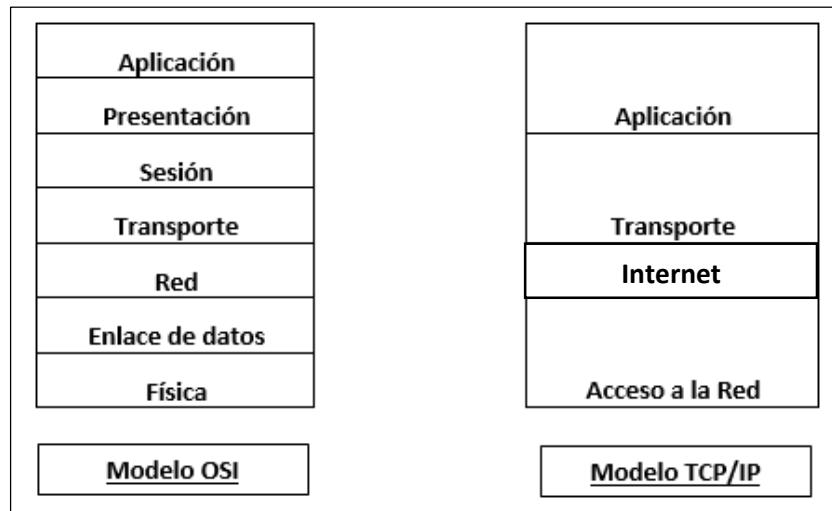


Fig. 44 Red de computadoras [Fuente Propia]

#### 11.5. Modelo OSI

El modelo OSI, Open Systems Interconnection Reference Model (Modelo de Interconexión de Sistemas Abierto), fue aprobado en 1984 bajo la norma ISO 7498, su creación se debió como respuesta ante la necesidad de interconectar sistemas de distintos fabricantes que empleaban sus propios protocolos [34].

El modelo OSI cuenta con siete capas tal como se observa en la Fig. 44, cada capa contiene funciones que permiten la comunicación de sistemas. Las capas poseen arquitectura

jerárquica cada una se apoya de la anterior, la capa inferior realiza su función y ofrece un servicio a la capa superior. La pila del modelo OSI no es más que una jerarquía de pequeños protocolos que trabajan juntos para llevar a cabo la transmisión de los datos de un nodo a otro nodo de la red.

El modelo OSI ofrece los mecanismos y reglas que permiten resolver un sin número de cuestiones. Comprender las distintas capas del modelo OSI no sólo permite internarse en los conjuntos de protocolos de red que actualmente se utilizan, sino que también proporciona un marco de trabajo conceptual del que puede servirse cualquiera para comprender el funcionamiento de dispositivos de redes complejas, como conmutadores, puentes y routers [33].

### **11.6. Modelo TCP/IP**

El modelo TCP/IP (Protocolo de control de transmisión/Protocolo de Internet) fue desarrollado por Vinton Cerf y Robert E. Kahn, en la década de 1970. Fue implantado en la red ARPANET, se ha convertido en el estándar por defecto para la conexión en red. Las redes TCP/IP son ampliamente escalables, por lo que TCP/IP puede utilizarse tanto para redes pequeñas como grandes, así mismo puede ejecutarse en distintas plataformas de software (Windows, UNIX, etc.) y casi todos los sistemas operativos de red lo soportan como protocolo de red predeterminado [34].

TCP/IP consiste de cuatro capas tal como se observa en la Fig.44 cada capa consta de una serie de protocolos diferentes, pero solamente algunos de ellos definen verdaderamente la operación principal de toda la pila. De todos los protocolos claves o fundamentales solamente dos son considerados cruciales o indispensables en todos los sentidos. Estos son el protocolo de internet (IP) y el protocolo de control de transmisión (TCP) [33].

Debido a la importancia de estos dos protocolos, sus abreviaciones representan una suite completa: TCP/IP. IP y TCP son importantes porque muchas de las funciones más críticas son implementadas en la capa 3 y 4. La suite de protocolos tiene un grupo de requerimientos para el funcionamiento de una variedad de protocolos y tecnologías para hacer que una red funcional brinde sus servicios a los usuarios y las aplicaciones que estos necesiten.

### **11.6.1. Capa de acceso a la red**

Esta capa se encuentra en el nivel más bajo de la pila TCP/IP, abarca la capa física y la capa de enlace de datos de modelo OSI, asocia las direcciones lógicas IP a direcciones físicas de los dispositivos adaptadores de red (NIC) permite encapsular un datagrama IP en una trama con la finalidad que pueda ser transmitida por la red.

Una trama es la unidad de datos que utiliza la capa de enlace, viaja de un nodo a otro que está conectado al mismo medio de comunicación y facilitan la sincronización de comunicación entre entidades de la capa de enlace de datos.

#### **11.6.1.1. Protocolo ARP**

Address Resolution Protocol (Protocolo de resolución de direcciones) es el responsable de convertir las direcciones ip a direcciones de red físicas, ARP interroga a los equipos de la red para averiguar sus direcciones físicas y luego crea una tabla de búsqueda entre las direcciones lógicas y físicas en una memoria caché. Cuando un equipo debe comunicarse con otro, consulta la tabla de búsqueda. Si la dirección requerida no se encuentra en la tabla, el protocolo ARP envía una solicitud a la red. Todos los equipos en la red comparan esta dirección lógica con la suya al encontrarla envían la respuesta [33].

### **11.6.2. Capa de Internet**

Es la segunda capa del modelo TCP/IP, contiene la capa de red del modelo OSI, transmite paquetes desde una ip origen hasta una ip destino, la finalidad de la capa es la commutación de paquetes y determinar la mejor ruta de forma que un paquete enviado por la red llegue a su destino de forma rápida y eficiente. El protocolo principal en esta capa es IP existen dos versiones, la primera versión es IPV4 el más utilizado en la mayoría de redes, pero afronta un problema, el crecimiento de las redes ha hecho que el protocolo IPV4 no pueda direccionar todos los equipos que se encuentran en la red, la segunda versión es IPV6 desarrollado para dar solución al problema que afronta IPV4, tiene una capacidad superior de direccionamiento en la red.

### **Clasificación de direcciones de red**

En internet se tiene definido cinco clases de direcciones de red A – B – C – D – E, las clases A – C – D se utiliza para la asignación de nodos TCP/IP en redes extensas, medianas y pequeñas, la clase D es usada en multicast y la clase E se utiliza en forma experimental.

La clase de dirección define los bits que se utilizan para las partes de Id. de red e Id. de host de cada dirección. La clase de dirección también define el número de redes y hosts que se pueden admitir por cada red, tal como se muestra en la TABLA XI.

**TABLA XI CLASES DE DIRECCIONES DE RED**

Clase de direcciones IP.	Valor del primero octeto	Máscara de red	Número de redes	Número de host por red
A	1 – 126	255.0.0.0	126	16,777,214
B	128 – 191	255.255.0.0	16,384	65,534
C	192 – 223	255.255.255.0	2,097,152	254
D	224 – 239	No disponible	No disponible	No disponible
E	240 – 254	No disponible	No disponible	No disponible

#### 11.6.2.1. Protocolo IP

Protocolo de internet (Internet Protocol) conocido como IP, se utiliza en sistemas interconectados de redes de comunicaciones de ordenadores para el intercambio de paquetes, el protocolo ip proporciona los medios necesarios para la trasmisión de bloques de datos llamados datagramas desde el origen al destino, donde origen y destino son hosts identificados por direcciones de longitud fija. El protocolo internet también se encarga, si es necesario, de la fragmentación y el ensamblaje de grandes datagramas para su transmisión a través de redes de trama pequeña [35].

Un datagrama es un fragmento de paquete con la suficiente información para que la red pueda encaminar el fragmento hacia un equipo receptor.

Los datagramas IP como se observa en la Fig. 45 son las unidades principales de información de Internet, los términos trama, mensaje, paquete y segmento también se usan para describir las agrupaciones de información lógica en las diversas capas del modelo de referencia OSI.

0 – 3	4 – 7	8 – 15	16 – 18	19 – 31
Versión	Tamaño cabecera	Tipo de servicio	Longitud total	
Identificador		Indicadores	Posición de Fragmento	
Tiempo		Protocolo	Checksum encabezamiento	
Dirección origen		Dirección destino		
Opciones			Relleno	
Datos				

**Fig. 45** Datagrama del protocolo de internet [35]

Descripción de campos:

- **Versión.** Este campo de 4 bits, se usa para especificar la versión del protocolo IP.
- **Lectura de cabecera (IHL).** Este campo de 4 bits, especifica la longitud de encabezamiento del datagrama indicando el número de palabras de 32 bits.
- **Tipo de Servicio.** Este campo de 8 bits, especifica el servicio al cual pertenece el paquete se divide en cinco campos (Prioridad (3 bits), D (1 bit), T (1 bit), R (1 bit), (No usado)).
- **Longitud total.** Da la longitud total del fragmento del datagrama, incluido el encabezamiento, el paquete más largo que puede enviarse es de 65535.
- **Identificación.** Esta casilla contiene el número de serie del paquete. Esto entra en vigencia cuando un paquete se parte en pedazos más pequeños por el camino (se fragmenta) cada uno de los fragmentos llevará el mismo número de identificación.

- **Control de fragmentación** Estos bits se dividen en: 1 bit de sobra, 1 bit para evitar la fragmentación, 1 bit para indicar que el paquete forma parte de un paquete más grande que se fragmento. Y un último bit de “desplazamiento de fragmento”.
- **Tiempo.** Da a conocer el tiempo máximo que se le permite al datagrama permanecer en la red IP, evitando que datagramas extraviados viajen por la red indefinidamente.
- **Protocolo.** Especifica el tipo de protocolo de alto nivel que soporta los datos que lleva el datagrama.
- **Checksum de la cabecera.** Asegura que el encabezamiento no tiene errores, se forma tratando el encabezamiento como una secuencia de enteros de 16 bits.
- **Direcciones IP origen y destino.** Contiene las direcciones de 32 bits de los “hosts” origen y destino.
- **Opciones.** Algunos datagramas no lo utilizan, se incluye normalmente para depurar la red.
- **Relleno.** Representa octetos conteniendo ceros los cuales permite que el datagrama sea múltiplo exacto de 32.
- **Datos.** - Es la zona de datos del datagrama.

#### 11.6.2.2. Protocolo ICMP

Protocolo de mensajes de control de internet (Internet Control Message Protocol) conocido como ICMP, es denominado un protocolo de control, da aviso de los errores que se generan en el procesamiento de los datagramas del protocolo IP. El protocolo ICMP funciona sobre IP, es decir un paquete ICMP a su vez será un paquete IP, una característica propia de los paquetes ICMP es que no enviarán errores que se generen en otro paquete ICMP ya que si lo hacen se generará un bucle infinito [36].

Los mensajes ICMP son enviados en varias situaciones: por ejemplo, cuando un datagrama no puede alcanzar su destino, cuando una pasarela no dispone de capacidad de almacenamiento temporal para reenviar el datagrama, y cuando la pasarela no puede dirigir al "host" para enviar el tráfico por una ruta más corta [36].

Los paquetes ICMP son trasmítidos junto con los paquetes IP, tal como se puede observar en la Figura. 46.

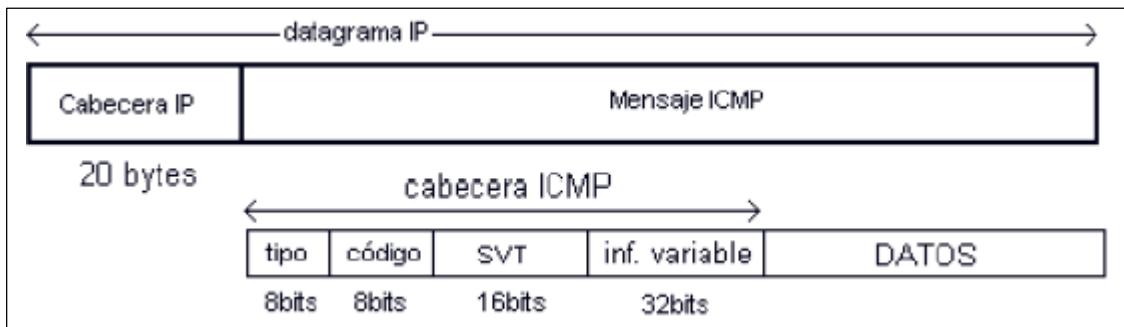


Fig. 46 Datagrama IP / paquete ICMP [36]

Descripción de los campos:

- **Tipo.** Este campo tiene una longitud de 8 bits y especifica el tipo de mensaje ICMP.
- **Código.** Este campo tiene una longitud de 8 bits, permite precisar el motivo exacto por el cual se generó el mensaje, existen algunos códigos tal como se observa en la Tabla XII que nos da a conocer porque se suscitó el problema.
- **Suma de Control (SVT).** Este campo tiene una longitud de 16 bits, proporciona un método para la determinación de la integridad del mensaje.
- **Información variable.** Este campo no es muy utilizado y la mayoría de veces es rellenado con ceros.
- **Datos.** Este dato lo utiliza el "host" para asociar el mensaje al proceso apropiado. Si un protocolo de nivel superior utiliza números de puerto, se asume que están en los primeros 64 bits de datos del datagrama original.

TABLA XII TIPOS DE MENSAJES ICMP

TIPO	NOMBRE	DESCRIPCIÓN
0	<b>Respuesta de Eco</b> (Echo Reply)	Respuesta al mensaje Echo Request
3	<b>Destino Inaccesible</b> ( <i>Destination Unreachable</i> )	El destino no se puede alcanzar, debido a que no se sabe cómo llegar a su dirección IP

4	<b>Cadencia de envío demasiada elevada (Source Quench)</b>	Enviando por un router cuando descarta paquetes de entrada porque su cola de salida se ha llenado.
5	<b>Redirección (Redirect)</b>	Enviado por un router a un host para indicarle una mejor puerta de enlace para llegar al destino deseado.
8	<b>Petición de eco (Echo Request)</b>	Solicitud de eco, generada por comando “ping”
9	<b>Aviso de router (Router Advertisement)</b>	Enviado por un router dando a conocer a un nuevo host, se envía la dirección de multicast.
10	<b>Solicitud de router (Router Solicitation)</b>	Enviado por host o router para pedir que otros router envíen mensajes Router Advertisement
11	<b>Tiempo sobrepasado (Time exceeded)</b>	Enviado por un router para eliminar un paquete IP porque se ha agotado el contador de saltos, o no se completa la fragmentación a tiempo.
12	<b>Problema de parámetros (Parameter problem)</b>	Se usa como respuesta para errores que no tienen un mensaje ICMP específico.
13	<b>Petición de marca de Tiempo (Timestamp Request)</b>	Solicita un mensaje Timestamp Reply.
14	<b>Respuesta de marca de tiempo (Timestamp Reply)</b>	Contiene una marca de tiempo de equipo que lo envía que permite calcular retardos.
17	<b>Petición de máscara de dirección (Address Mask Request)</b>	El router que recibe este mensaje debe responder con un Address Mask Reply
18	<b>Respuesta de máscara de dirección (Address Mask Reply)</b>	Es una respuesta a la petición de tipo 17, informa de la máscara correspondiente

### **Mensaje ICMP de solicitud y mensaje ICMP de error**

Un mensaje ICMP de solicitud, da a conocer un acontecimiento concreto que no es causado por un mensaje de error. Dichos mensajes hacen uso de un mensaje de respuesta Echo Reply que responde a un Echo Request ejecutado por la aplicación “ping”.

Un mensaje ICMP de error dan a conocer situaciones en las que se produce un error en el envío de datagramas en la red como puede ser el campo TTL alcanza el valor 0, una máquina es inaccesible, una fragmentación es requerida pero imposible de realizar etc. Casos que no generan mensajes ICMP de error:

- Un datagrama destinado a una dirección de IP de “Broadcast”.
- Un datagrama enviado como “Broadcast” de la capa de enlace.
- Un datagrama fragmentado que no sea el primero de la secuencia.
- Un fragmento de datagrama recibido fuera de secuencia.

### **Mensajes echo reply y echo request**

Ping es una aplicación que utiliza tanto el mensaje echo reply como echo request, su apoyo es directamente sobre el protocolo ip, no tiene ninguna relación con el protocolo de transporte TCP o UDP, su función consiste en comunicarse con otra máquina y que nos devuelva lo que le decimos como un “echo” [37].

Ping utiliza el mensaje echo request, para enviar de una computadora emisor un datagrama a una computadora receptor, y luego espera un retorno del mensaje echo reply generado por el computador receptor al computador emisor.

La trama del mensaje echo request es igual al mensaje echo reply observe la TABLA XIII, solo existe una diferencia en el campo tipo el valor del mensaje echo reply será 0 y el valor del mensaje request será 8.

**TABLA XIII ENCABEZADO DE MENSAJE ECHO REPLY Y ECHO REQUEST**

<b>Tipo</b>	<b>Código</b>	<b>Checksum</b>
<b>Identificador</b>		<b>Secuencia de número</b>
<b>Datos</b>		

Descripción de campos:

- **Tipo.** El valor dependerá del mensaje echo reply o echo request
- **Código.** Siempre toma el valor de 0.
- **Checksum.** Proporciona un método para la determinación de la integridad del mensaje.
- **Identificador.** Simula el comportamiento de los puertos UDP, aunque de forma mucho más simple sirve para identificar una sesión de mensajes echo.
- **Secuencia de números:** Este campo con ayuda del anterior permite identificar únicamente un mensaje en concreto Echo Request, para que el Echo Reply pueda identificar a qué petición de echo en concreto está respondiendo.
- **Datos:** Los datos que van en este campo no son definidos así que puede introducirse datos distintos [37].

#### 11.6.3. Capa de Transporte

La capa de transporte tiene como objetivo principal establecer una comunicación de extremo a extremo a través de una red. En otras palabras, actuar de interfaz entre los niveles orientados a la aplicación y los niveles orientados a la red de la jerarquía de protocolos.

La capa de transporte debe ofrecer algún mecanismo que permita distinguir de forma única a qué aplicación van dirigidos los datos, este mecanismo se conoce con el nombre de TSAP que vienen hacer los puertos lógicos.

En la capa de transporte se efectúa la comunicación lógica entre procesos ejecutándose en diferentes máquinas, la comunicación se da a través de los protocolos de transporte, permite la segmentación de datos y brinda el control necesario para reensamblar las partes dentro de los distintos canales de comunicación. [38].

##### 11.6.3.1. Protocolo TCP

Protocolo de control de transmisión (Transmission Control Protocol) conocido como TCP es un protocolo orientado a la conexión, fiable en la comunicación entre dos extremos, diseñado para encajar en una jerarquía en capas de protocolos que soportan aplicaciones sobre múltiples redes. TCP garantiza la entrega de las tramas de datos en forma ordenada

a los programas que se ejecutan en los hosts de red. El protocolo sirve como soporte como la mayoría de las aplicaciones de internet tal como los buscadores www, e-mail y transferencia de archivos [39].

TCP cuenta con las siguientes características:

- Una conexión TCP tiene dos extremos, emisor y receptor, garantiza que los datos transferidos serán entregados sin ninguna perdida, duplicación o errores de transmisión.
- Los extremos que participan en una conexión TCP pueden intercambiar datos en ambas direcciones simultáneamente.
- Conexión de inicio confiable, garantiza sincronización entre los dos extremos. Conexión de finalización aceptable, garantiza la entrega de todos los datos antes de la finalización de la conexión.

Una cabecera de TCP sigue a la cabecera de internet observe la TABLA XIV, aportando información específica del protocolo de TCP. Esta división permite la existencia de otros protocolos de la capa de 'host' distintos de TCP.

**TABLA XIV CABECERA TCP**

Puerto Origen		Puerto Destino											
Número de Secuencia													
Número de Acuse de Recibo													
Posición de los datos	Reservado	U R G	A C K	P S H	R S T	S Y N	F I N						
Suma de Control						Puntero Urgente							
Opciones							Relleno						
Datos													

Descripción de los campos:

- **Puerto origen y Puerto destino.** Se especifica los puertos que va a utilizar cada ordenador para comunicar con las aplicaciones e intercambian datos.
- **Número de secuencia.** Indica el número que corresponde en la conexión al primer byte que se envía en el campo datos.
- **Número acuse de recibo.** Si el bit de control ACK está puesto a uno, este campo contiene el valor del siguiente número de secuencia que el emisor del segmento espera recibir. Una vez que una conexión queda establecida, este número se envía siempre [39].
- **Posición de los datos.** El número de palabras de 32 bits que ocupa la cabecera de TCP. Este número indica dónde comienzan los datos
- **Reservado (4 bits):** Bits reservados para uso futuro, serán rellenados por ceros.
- **Bits de control:**
  - **URG:** Hace significativo el campo "Puntero urgente"
  - **ACK:** Hace significativo el campo "Número de acuse de recibo"
  - **PSH:** Función de "Entregar datos inmediatamente" ('push')
  - **RST:** Reiniciar ('Reset') la conexión
  - **SYN:** Sincronizar ('Synchronize') los números de secuencia
  - **FIN:** Últimos datos del emisor
- **Ventana.** Indica la cantidad de bytes que se está dispuesto a aceptar del otro lado en cada momento.
- **Suma de control.** Sirve para detectar errores en el segmento recibido; estos podrían ser debidos a errores de transmisión no detectados, a fallos en los equipos o problemas software.
- **Puerto urgente.** Este campo es interpretado si ACK se establece en 1, su función es apuntar al número de secuencia del octeto al que seguirán los datos urgentes
- **Opciones.** Ocupan un cierto espacio al final de la cabecera TCP, su longitud tiene que ser un múltiplo de 8 bits.
- **Relleno.** Se utiliza para asegurar que la cabecera de TCP ha finalizado, los datos que lleva este campo son ceros.
- **Datos.** Información que envía la aplicación.

#### **11.6.4. Capa de Aplicación**

La capa de aplicación es la capa superior del modelo TCP/IP, en ella se encuentran las aplicaciones y procesos con los que intercambia datos la capa de transporte, además contiene protocolos que soportan servicios de correo, conexión remota y transferencia de archivos [40].

##### **11.6.4.1. Protocolos de la capa de aplicación**

Algunos de los protocolos que se encuentran la capa de aplicación son los siguientes:

- **Sistema Común de Archivos de Internet** (Server Message Block) SMB2. Es un protocolo utilizado para la transmisión de datos entre ordenadores Windows y Linux. Permite al usuario de una aplicación compartir archivos, discos, directorios, impresoras, puertos seriales y mail slots a través de una red, permitiendo de esta forma poder comunicarse con cualquier servidor, siempre y cuando este último se encuentre configurado para recibir una solicitud de un cliente SMB2.
- **Protocolo de terminal de red** (Network Terminal Protocol) Telnet. Permite establecer conexiones con terminales remotas, de tal manera que se puedan ejecutar en ellos comandos de configuración y control.
- **Protocolo de Transferencia de Archivos** (File Transfer Protocol) FTP. Ofrece una gran fiabilidad en el servicio de transferencia de archivos, en gran parte debido a que se basa en el protocolo TCP dentro de la capa de transporte.
- **Protocolo Trivial de Transferencia de Archivos** (Trivial File Transfer Protocol). Funciona más rápido que el protocolo FTP, pero es menos fiable ya que también utiliza mensajes UDP en la capa de transporte.
- **Protocolo simple de transferencia de correo** (Simple Mail Transfer Protocol) SMTP. Permite el funcionamiento del correo electrónico en las redes de ordenadores. SMTP recurre al protocolo de oficina postal
- **Protocolo de transferencia de Hipertexto** (Hypertext Transfer Protocol) HTTP. Permite la transmisión de gran variedad de archivos de texto, gráficos, sonidos e imágenes, regula el proceso mediante el cual navegadores como Netscape, Mozilla o Internet Explorer solicitan información a los servidores web.

## e. MATERIALES Y MÉTODOS

Para realizar el presente trabajo de titulación “**DESARROLLO DE UN PROTOTIPO DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA TÉCNICA DE ESTEGANOGRAFÍA EN LA CAPA DE RED**” se contó con recursos humanos, económicos y tecnológicos como hardware y software necesarios para la culminación del mismo.

### 1. Materiales

En la elaboración del presupuesto del trabajo de titulación se tomo en cuenta los recursos humanos, bienes, servicios e imprevistos.

#### 1.1. Talento Humano

El recurso de talento humano es esencial para realizar el trabajo de titulación, en la TABLA XV se puede observar el personal involucrado.

**TABLA XV TALENTO HUMANO**

Recurso Humano	Cantidad	Horas	V. Unitario	V. Total	Nota
Desarrollador	1	400	8,00	3.200,00	
Coordinador	1	150	10,00	1.500,00	El costo del Coordinador será cancelado por la Universidad Nacional de Loja.
			<b>Subtotal</b>	<b>4.700,00</b>	

#### 1.2. Bienes

El hardware y software que se presentan en la TABLA XVI, representan todos los bienes necesarios que se utilizan para poder llevar a cabo con éxito el trabajo de titulación.

**TABLA XVI BIENES**

<b>Bien</b>	<b>Cantidad</b>	<b>Valor Unitario</b>	<b>Valor Total</b>
<b>Hardware</b>			
<b>Computador portátil ASUS U47A Core i7</b>	1	1200,00	1.200,00
<b>Impresora canon MP190</b>	1	250,00	250,00
<b>Memoria Flash Kingston</b>	1	10,00	10,00
<b>Subtotal</b>			<b>1.460,00</b>
<b>Software</b>			
<b>Scapy</b>	1	0,00	0,00
<b>Wireshark</b>	1	0,00	0,00
<b>OpenSSL</b>	1	0,00	0,00
<b>Windows 7</b>	1	0,00	0,00
<b>Subtotal</b>			<b>0,00</b>

### 1.3. Servicios

En el proceso del trabajo de titulación, será necesario adquirir ciertos servicios, que se describen en la TABLA XVII, estos servicios servirán de complemento para la culminación del trabajo.

**TABLA XVII SERVICIOS**

<b>Servicios</b>	<b>Cantidad</b>	<b>Valor Unitario</b>	<b>Valor Total</b>
<b>Transporte</b>	200 pasajes	0,30	60,00
<b>Copias</b>	500	0,02	5,00
<b>Resma de papel</b>	1	2,00	2,00
<b>Anillados</b>	4	1,00	4,00
<b>Internet</b>	200 horas	0,75	150,00
<b>Cartuchos</b>	2	25,00	50,00
<b>Subtotal</b>			<b>271,00</b>

#### **1.4. Imprevisto**

La tasa que se consideró para los imprevistos es del 10% de la suma de talento humano, bienes y servicios, tal como se presenta en la TABLA XVIII [41].

**TABLA XVIII IMPREVISTO**

<b>Descripción</b>	<b>Valor total</b>
<b>Talento humano – Bienes – Servicios</b>	<b>6.431,00</b>
<b>Imprevistos 10%</b>	<b>643,10</b>

#### **1.5. Total de Recursos**

El total de todos los recursos en la realización del trabajo de titulación, se describen en la TABLA XIX.

**TABLA XIX TOTAL RECURSOS**

<b>Descripción</b>	<b>Valor Total</b>
<b>Talento Humano</b>	<b>4.700,00</b>
<b>Bienes</b>	<b>1.460,00</b>
<b>Servicios</b>	<b>271,00</b>
<b>Imprevisto</b>	<b>643,10</b>
<b>Total</b>	<b>7.074,10</b>

## **2. Métodos y técnicas**

En el proceso del presente trabajo de titulación fue conveniente y necesario la aplicación de diferentes métodos y técnicas que permitieron obtener la información concisa, real y fiable en base a solucionar el problema presente, también se pudo obtener un panorama más claro de cómo será aplicado y orientando el prototipo de seguridad de información en la red.

## **2.1. Métodos**

- **Método Deductivo**

El método deductivo parte desde los aspectos generales hasta llegar a los aspectos específicos, se utilizó para obtener información fundamental que permita plantear el problema que afronta la seguridad de información en la red.

- **Método Inductivo**

El método inductivo procede a partir de primicias específicas a proporcionar conclusiones generales, este método permitió el desarrollo de cada uno de los objetivos específicos para llegar a concluir el objetivo general, así mismo permite comprobar que el prototipo cumpla con todos los requisitos planteados.

- **Método de Revisión Bibliográfica**

En esta sección se hace mención a la revisión bibliográfica efectuada en el presente trabajo, se utiliza la metodología plateada por la Universidad Nacional de Colombia [1], con el propósito de recabar información importante sobre los métodos de criptografía y esteganografía, combinación de técnicas y la aplicación de esteganografía de red en distintos ámbitos. La revisión bibliográfica permite identificar, evaluar e interpretar las investigaciones que se encuentran vigentes para proponer una solución al problema planteado.

## **2.2. Técnicas**

- **Análisis de Información**

Esta técnica permitió seleccionar la información más relevante e importante, con el fin de establecer que métodos de esteganografía y criptografía utilizan los investigadores, para brindar seguridad a la información que se guarda en un equipo informático o se transmite por la red.

- **Encuesta**

Esta técnica ayudo a constatar sobre qué sistema operativo (**Ver Anexo 2**) se puede aplicar el prototipo de seguridad, que medidas de seguridad se utiliza para transmitir información por la red (**Ver ANEXO 4**) y cuál es el grado de conocimiento de los usuarios acera de la técnica de esteganografía (**Ver Anexo 6**) y criptografía (**Ver Anexo 7**), esta encuesta estuvo dirigida al personal que trabaja en la Universidad Nacional de Loja.

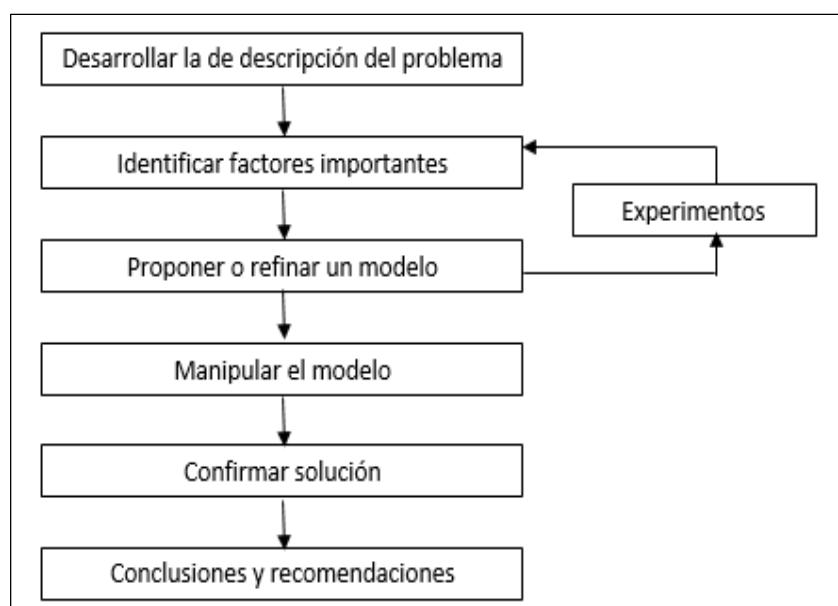
- **Búsqueda de información científica**

Esta técnica se utilizó para argumentar y sustentar el desarrollo del trabajo de titulación, en base a las investigaciones científicas que se han realizado, con el propósito de dar solución a un problema propuesto, adquirir conocimientos y compartir sus casos de éxito.

### **2.3. Metodología de la Ingeniería**

Para el desarrollo de presente trabajo de titulación, se hizo uso de la metodología de ingeniería también conocida como método científico [42], la metodología nos permite tener una estrecha interacción con el problema, proponer un modelo e identificar factores que pueden influir en una solución y además proporciona la experimentación para verificar la adecuación del modelo y la solución propuesta al problema.

En la Fig. 47 se observa los pasos de la metodología de ingeniería para dar solución a un problema.



**Fig. 47** Metodología de la ingeniería [42]

El desarrollo del prototipo se lo realizara a través de siete fases, estas fases tienen como base la metodología de ingeniería, en cada una de las fases se realizará un proceso que permitirá el desarrollo del prototipo de seguridad de información en la red.

**Fase 1. Desarrollar una descripción clara y concisa del problema**

En esta fase se describe uno de los problemas que se presenta cuando se desea transmitir información por la red.

**Fase 2. Identificar, al menos de manera tentativa, los factores importantes que afectan al problema o que puedan jugar un papel en su solución**

En esta fase se mencionará todos los factores, que permitan encontrar una solución al problema, estos factores pueden ser técnicas y métodos.

**Fase 3. Proponer un modelo para el problema, utilizando conocimientos científicos o de la ingeniería del fenómeno de bajo estudio y consignar todas las limitaciones o supuesto del modelo**

Según los factores seleccionados en la Fase 2, se estructurará el modelo del prototipo que combine todos los factores, de manera que se pueda seguir un proceso para minimizar o solucionar el problema.

**Fase 4. Realizar experimentos apropiados y recolectar datos para probar o validar el modelo tentativo o las conclusiones planteadas en la fase 2 y la fase 3.**

En esta fase se tendrá que realizar experimentos, para definir si los factores propuestos contribuyen a la solución del problema, caso contrario se realizará nuevamente un estudio de los factores que aporten una solución al problema en la Fase 2 y refinar el modelo en la Fase 3.

**Fase 5. Manipular el modelo para contribuir a desarrollar una solución del problema.**

La manipulación se basa en la propuesta presentada en la Fig.49, el propósito consiste en establecer un ambiente preciso que integre las herramientas necesarias para la ejecución de las técnicas y métodos.

**Fase 6. Realizar un experimento apropiado para confirmar que la solución propuesta al problema es efectiva y es eficiente.**

Se realiza experimentos considerando la transmisión de archivos de diferente tamaño, teniendo como objetivo determinar el tamaño de archivo óptimo a transmitir por la red.

**Fase 7. Obtener conclusiones y/o recomendaciones con base a la solución propuesta**

En esta fase se concluye los pros que presenta el prototipo y de tal manera se da a conocer recomendaciones para aplicaciones o mejoras futuras.

## f. RESULTADOS

La sección de resultados detalla el proceso seguido en cada fase para el desarrollo del prototipo de seguridad de la información en la red. La metodología de ingeniería es base fundamental para la ejecución de las siete fases, a continuación, se detallará el desarrollo de cada una de ellas.

### Fase 1. Desarrollar una descripción clara y concisa del problema.

En la transmisión de información por una red LAN entre un emisor y un receptor o receptores, una tercera persona que está conectada a la misma red, puede tener acceso a dicha información realizando un ataque pasivo, observe la Fig. 48.

El ataque pasivo consiste en el análisis de flujos de datos, tal como se estudió en la sección D, literal 4.1.1, este ataque se lo realiza de diferentes maneras, una de ellas es utilizando una herramienta que detecta el tráfico de información que se efectúa en una red como es la herramienta Wireshark, este ataque es efectivo y difícil de detectar por sus características solo escucha, no modifica el flujo de datos y detecta patrones de datos cifrados obteniendo la información.

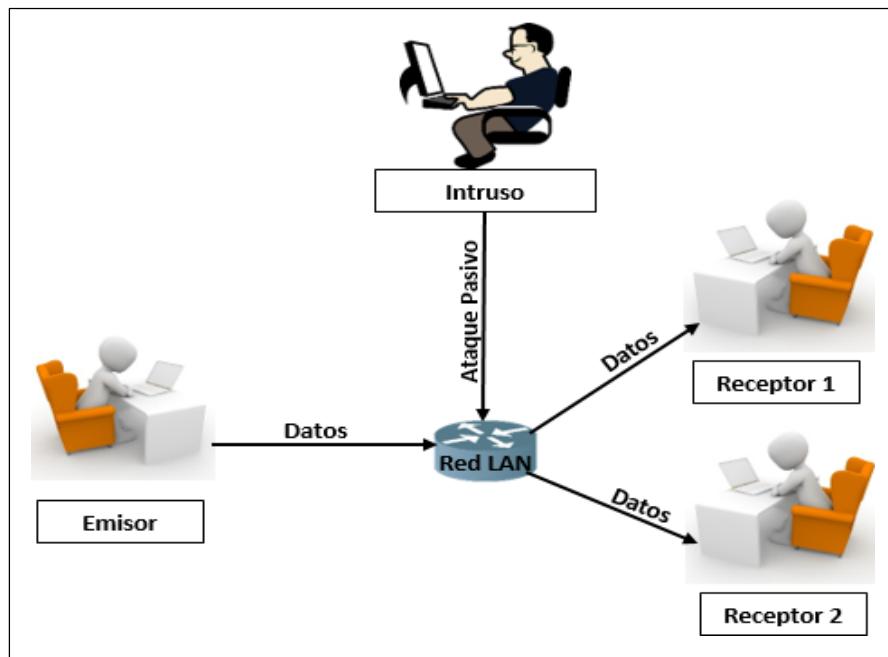


Fig. 48 Descripción grafica del problema en la red [Fuente propia]

## **Fase 2. Identificar, al menos de manera tentativa, los factores importantes que afectan al problema o que puedan jugar un papel en su solución.**

En la revisión bibliográfica de la sección D, se identificó los siguientes factores los cuales consisten en métodos y técnicas propuestos por autores en sus trabajos de investigación, los mismos que permiten cifrar, ocultar y trasmisir información por una red LAN de forma segura, en la TABLA XX se presenta la técnica de criptografía y en la TABLA XXI se presenta la técnica de esteganografía, en cada tabla se describe los métodos de cada técnica con sus respectivas funciones y las herramientas de software que utilizan para su ejecución.

**TABLA XX MÉTODOS DE LA TÉCNICA DE CRIPTOGRAFÍA**

<b>TÉCNICA DE CRIPTOGRAFÍA</b>		
<b>Métodos</b>	<b>Función</b>	<b>Software</b>
<b>Criptografía Simétrica</b>	Permite cifrar la información original a un estado de números y letras, de manera que una tercera persona no pueda tener acceso a su contenido, utiliza claves para el cifrado y descifrado de información.	OpenSSL permite cifrar y descifrar información a través de algoritmos.

**TABLA XXI MÉTODOS DE LA TÉCNICA DE ESTEGANOGRÁFIA**

<b>TÉCNICA DE ESTEGANOGRÁFIA</b>		
<b>Métodos</b>	<b>Función</b>	<b>Software</b>
<b>Flujo Alternativo de Datos (ADS)</b>	Es una característica del sistema de archivos NTFS, permite	Comando del sistema (Command Prompt)

	insertar datos en un fichero principal, dichos datos no modifican el tamaño ni son visibles por un usuario.	CMD permite manipular archivos del Sistema Operativo de Windows.
<b>Compartir archivos en una red LAN</b>	Es una característica de los sistemas operativos de Windows, Linux y Mac-OS, permite transmitir archivos de una computadora a otra, esta característica es utilizada para trasmitir el fichero principal.	Comando del sistema (Command Prompt) CMD permite transmitir archivos por la red en el Sistema Operativo de Windows.
<b>Esteganografía de red</b>	Permite utilizar como portador un protocolo de red, su función es utilizar un campo de su cabecera (canal encubierto) que no sea usado o que al usarlo no modifique la función del protocolo, en este campo se insertar la información.	Scapy es una potente librería de python permite escanear redes, manipulación de paquetes de protocolos de red, envío de datagramas, etc.

### **Fase 3. Proponer un modelo para el problema, utilizando conocimientos científicos o de la ingeniería del fenómeno de bajo estudio consignar todas las limitaciones o supuesto del modelo.**

El modelo del prototipo se basa en combinar dos técnicas que son criptografía y esteganografía conjuntamente con sus métodos, esta combinación permite; ocultar información cifrada, transmitir datos ocultos por la red, enviar la clave de cifrado y descifrado de manera segura utilizando un protocolo de red. En la Fig. 49 se describe de manera gráfica el modelo del prototipo que permite la interacción de los factores que influyen en la solución del problema, el bosquejo del modelo se realizó en la herramienta DIA.

#### **Fase 4. Realizar experimentos apropiados y recolectar datos para probar o validar el modelo tentativo o las conclusiones planteadas en la Fase 2 y la Fase 3.**

Los experimentos se basan en una investigación, estos mismo permiten analizar el modelo propuesto del prototipo, su estructura, sus técnicas y sus métodos; este análisis ayudara a determinar si es viable la ejecución del modelo propuesto para solucionar el problema.

La técnica de criptografía se clasifica en asimétrica y simétrica, en la TABLA XXII se realiza una descripción de características, ventajas y desventajas de cada tipo, se realiza una investigación de cada criptografía basados artículos científicos, luego se analiza los pros y contras y se justifica porque se elige ese tipo de criptografía para aplicarla en el presente modelo del prototipo.

**TABLA XXII DESCRIPCIÓN DE CRIPTOGRAFÍA SIMÉTRICA Y ASIMÉTRICA**

Características	Criptografía Simétrica	Criptografía Asimétrica
<b>Seguridad</b>	Utiliza una sola clave para cifrar y descifrar [22].	Utiliza una clave pública para cifrar y una clave privada para descifrar [22]
<b>Utilidad</b>	Es menos costosa y esta implementada en dispositivos manuales, mecánicos y eléctricos [43].	Actualmente es muy usada en el intercambio de claves privadas y firmas digitales [43]
<b>Eficiencia</b>	Es mucho más rápida	Es más segura porque utiliza claves distintas, pero es más lenta [21].
<b>Capacidad</b>	Cifra grandes cantidades de datos [44].	No cifra grandes cantidades de datos.
<b>Problema</b>	Problema en compartir la clave de forma confidencial [44].	Lenta en realizar una operación de cifrado, consume más recursos [45].

El modelo del prototipo hace uso de la criptografía simétrica por sus características, utilidad, eficiencia y capacidad, la criptografía simétrica cuenta con algunos algoritmos que permiten cifrar como son: AES, RC5, DES, 3DES y muchos más. Se tomó como base la investigación del autor [22] el cual realiza una comparación de los algoritmos DES, AES y 3DES; esta comparación da como resultado que el algoritmo AES es más rápido en software y eficiente en hardware, permite mayor seguridad debido al cifrado por bloques y clave más larga. La criptografía simétrica se aplica en el modelo de prototipo con la finalidad de cifrar archivos que almacenan información (docx, xsl, pdf, ejecutables, multimedia).

La aplicación del flujo alternativos de datos (ADS) en el modelo del prototipo, se da por sus características; permite insertar archivos dentro de un solo fichero principal sin mostrar modificación alguna en su tamaño. El método es utilizado para insertar los archivos cifrados en un solo fichero y trasmítirlo por la red aplicando el método de compartición de archivos en el sistema operativo Microsoft Windows.

La esteganografía de red, se basa en aprovechar un campo de la cabecera de un protocolo de red que no sea utilizado o que al utilizarlo no afecte su función, el objetivo es trasmítir la clave generada en la criptografía simétrica y solventar el problema de compartir la clave de forma confidencial, en la TABLA XXIII se presenta el análisis realizado para determinar el protocolo que se utilizara como portador.

**TABLA XXIII COMPARACIÓN DE PROTOCOLOS DE RED**

Características	IP	ICMP	TCP
<b>Transmisión</b>	Utiliza el método PDU (Unidad de Datos de Protocolo) para modificar los siguientes campos (Ip indetification File, IP fragment offset e IP Options ) e insertar información [17].	Aplica el método PDU (Unidad de Datos de Protocolo) inserta datos en un campo de la cabecera (canal encubierto) del protocolo (Campo DATA) [32].	Utiliza un canal encubierto del protocolo (campo de la cabecera) para trasmítir una señal que de aviso sobre algún tipo de acción al receptor [32].

<b>Comunicación</b>	Proporciona los medios necesarios para la transmisión de datagramas de un nodo origen a nodo destino [35].	Es el encargado de detectar y comunicar errores que se efectúan en un paquete entre un emisor y un receptor [36].	Garantiza la entrega de paquetes de datos, de forma ordenada a los programas que se ejecutan en los hosts de red [39].
<b>Función</b>	Realiza la fragmentación y el ensamblaje de grandes datagramas.	Utiliza la aplicación PING, permite realizar un mensaje de solicitud de una computadora a otra.	Proporciona soporte a la mayoría de aplicaciones de internet buscadores www, e-mail, etc.

El modelo del prototipo aplicara la esteganografía de red en el protocolo ICMP por dos razones, la primera razón es por el análisis de la revisión bibliográfica y la segunda es por sus tres características específicas: transmisión, comunicación y función. La clave se enviará ejecutando la aplicación ping, esta aplicación utilizará el mensaje echo request por parte del emisor enviando un paquete ICMP, el paquete contendrá en su campo DATA de la cabecera la clave, el receptor esperará el mensaje, al recibirla generará un mensaje echo reply que será enviado al emisor confirmado la llegada del paquete.

Existen diferencias en los protocolos de ICMP, en la versión IPV4 e IPV6 la principal radica, en que ICMPv6 introduce simplificaciones en el envío de mensajes, es decir, es de propósito múltiple que engloba funciones que en IPv4 eran facilitadas por diversos protocolos como IGMP o ARP.

El modelo prototipo está orientado y establecido en IPV4, pero de igual manera funciona en IPV6 a pesar que los protocolos son mejorados, existen campos que no cambian, la trasmisión de la clave se realiza utilizando el protocolo ICMv6 insertando la clave en el campo DATA de su cabecera. La trasmisión de un fichero principal se realiza utilizando una dirección de IPV6 aplicando el método de compartición de archivos.

## **Fase 5. Manipular el modelo para contribuir a desarrollar una solución del problema.**

Integrar de manera física el modelo de prototipo, consiste en ejecutar un conjunto de pasos por parte del emisor y por parte de los receptores tal como se observa en la TABLA XXIV, la integración física se realizará en la Universidad Nacional de Loja, Facultad de la Energía, las Industrias y los Recursos Naturales No Renovables, en el Laboratorio de redes y sistemas operativos del bloque 12.

**TABLA XXIV INSTALACIONES DE HERRAMIENTAS DE SOFTWARE**

	<b>Red LAN</b>	<b>Wireshark</b>	<b>Scapy</b>	<b>OpenSSL</b>
<b>Emisor</b>	X		X	X
<b>Receptor 1</b>		X		X
<b>Receptor 2</b>		X		X
<b>Intruso</b>		X		

### **Paso 1. Establecer una red LAN (Red de Área Local)**

El Laboratorio de redes y sistemas operativos del bloque 12, cuenta con una red LAN que da acceso a internet, el motivo por el que no se utiliza una red LAN de la Universidad Nacional de Loja es debido a que se realizara un ataque pasivo con la herramienta Wireshark, por tal razón se trata de minimizar el tráfico de datos, aunque cabe recalcar que el modelo del prototipo funciona de igual manera que una red de la Universidad.

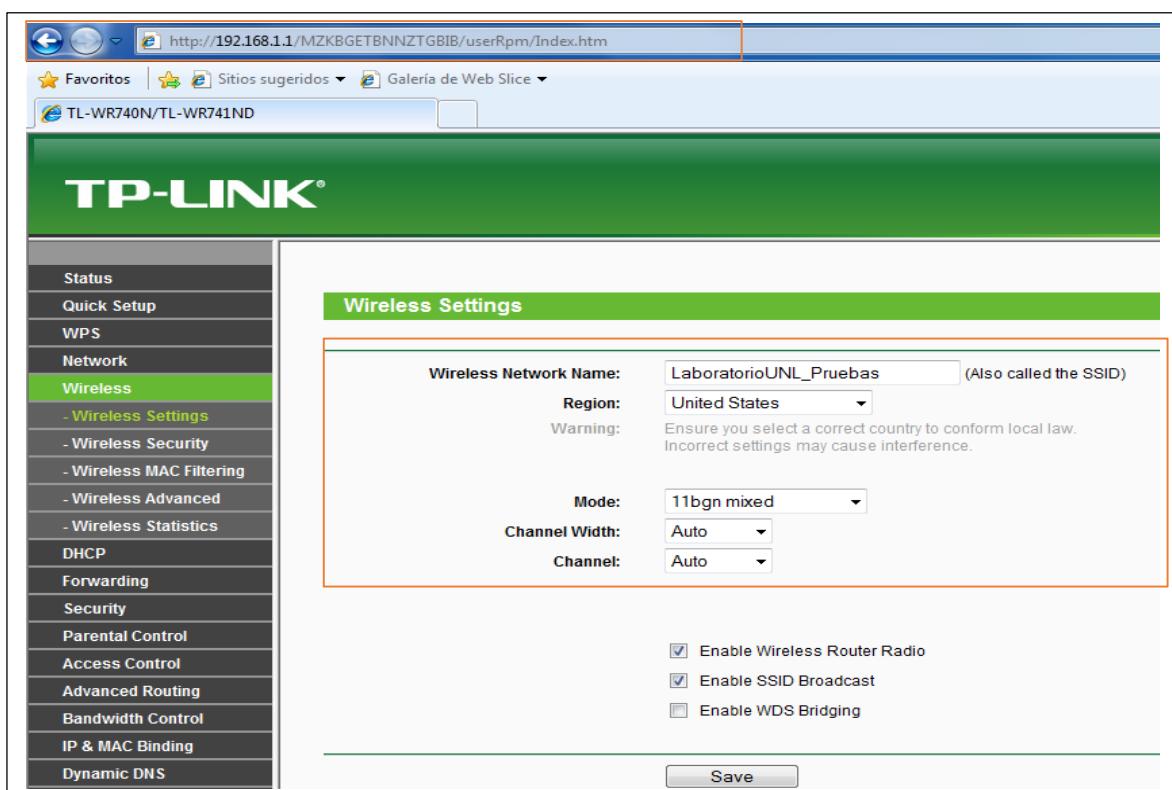
Para establecer la red LAN se necesitó lo siguientes materiales y equipos:

- Router TP-LINK model TL-WR740N-150 Mbps
- Cuatro Cables UTP cat 5 de 2 metros

La configuración del router se realiza de la siguiente manera:

- El router TP-LINK se conecta a un puerto de red (JR45) utilizando cable UTP para acceder a internet, a través de una red de la Universidad Nacional de Loja.
- Se conecta el router al equipo del emisor por medio de un cable UTP.

- Se abre un navegador de internet y se ingresa la ip del Gateway, para acceder al router, observe la Fig.50.
- Dentro del router se ingresa a la pestaña Wireless, para definir un nombre a la red, el nombre asignado es “LaboratorioUNL\_Pruebas” observe la Fig. 50 es importante definir el nombre de la red, debido que algunos de los receptores optaran por conectarse a la red de forma inalámbrica.



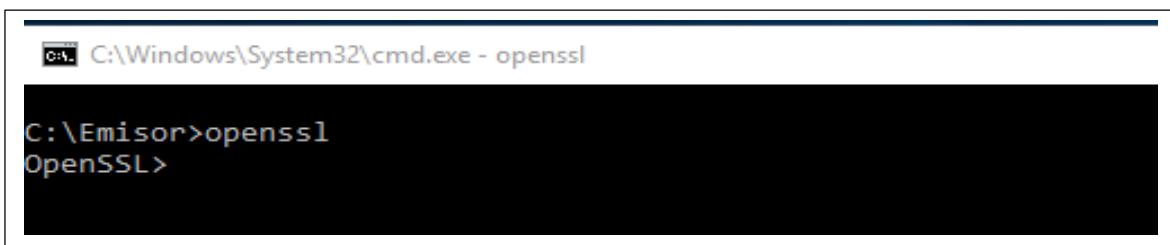
**Fig. 49** Configuración del router “TP-LINK” [Fuente Propia]

## Paso 2. Instalar OpenSSL

OpenSSL es una herramienta libre muy potente, incluye una API criptográfica de propósito general, permite realizar diferentes tipos de cifrado como es criptografía simétrica y criptografía asimétrica. La ejecución de sus comandos se realizan desde cualquier sistema operativo siempre y cuando se encuentre correctamente instalado OpenSSL [24].

La instalación de OpenSSL se realiza de la siguiente manera:

- Descargar OpenSSL de acuerdo al CPU del ordenador (32 bits o 64 bits) de la página oficial o directamente del repositorio (<https://indy.fulgan.com/SSL/>) en este caso el CPU del ordenador es de 64 bits.
- Descomprimir el archivo .rar para obtener la carpeta llamada “**openssl-0.9.8r-x64\_86-win64-rev2**” se recomienda guardar la carpeta en el disco C.
- OpenSSL se debe agregar como variable de entorno, para poder ejecutarlo a través de la consola de comandos del sistema operativo Microsoft Windows se debe realizar los siguiente:
  - Ingresar a equipo
  - Ir a propiedades
  - Seleccionar configuraciones avanzadas
  - Seleccionar variables de entorno
  - Ir a variables del sistema y seleccionar agregar
  - Ingresar al directorio que contiene OpenSSL “**C:\openssl-0.9.8r-x64\_86-win64-rev2**”
  - aplicar y guardar.
- Ya agregada la ruta del directorio “**C:\openssl-0.9.8r-x64\_86-win64-rev2**” al path, openssl se puede ejecutar desde cualquier carpeta ejecutando el comando “**openssl**” desde la consola CMD, tal como se observa en la Fig.51.



The screenshot shows a Windows Command Prompt window titled "C:\Windows\System32\cmd.exe - openssl". The command "openssl" is typed at the prompt, and the response "OpenSSL>" is displayed. The background of the window is black, and the text is white.

Fig. 50 Ejecución de openssl [Fuente Propria]

### Paso 3. Instalar Wireshark

Wireshark es un analizador de protocolos su principal objetivo es el análisis de tráfico de datos, además de ser una excelente aplicación didáctica para el estudio de las comunicaciones y para la resolución de problemas de red. Implementa una amplia gama de filtros que facilitan la definición de criterios de búsqueda para más de 1100 protocolos y

todo ello por medio de una interfaz sencilla e intuitiva que permite desglosar por capas cada uno de los paquetes capturados [46].

La instalación de Wireshark se realiza de la siguiente manera:

- Descargar la última versión de Wireshark desde su página oficial, de acuerdo al CPU del ordenador (32 bits o 64 bits) (<https://www.wireshark.org/download.html>).
- Ejecutar como administrador el archivo Wireshark.exe y esperar su instalación.

#### **Paso 4. Instalar Scapy**

Es un poderoso programa interactivo de manipulación de paquetes. Es capaz de forjar o decodificar paquetes de una gran cantidad de protocolos, enviarlos por distintos medios de red, capturarlos, responder a las solicitudes, etc [47].

La instalación de Scapy se realiza de la siguiente manera:

- Antes de instalar Scapy se debe tener instalado Python, la versión recomendada para que funcione Scapy es Python 2.7.
- Se debe agregar Python27 como una variable de entorno, tal como se hizo con OpenSSL.
- Descargar Scapy de su página oficial (<https://scapy.net/>) o del repositorio github (<https://github.com/secdev/scapy>).
- Descomprimir el archivo .rar para obtener una carpeta llamada “Scapy” esta carpeta se debe agregar en la carpeta Python27.
- Abrir la consola CMD, ir a al directorio donde se encuentra el instalador de Scapy “C: Python27/Scapy”.
- Ejecutar la línea de comandos “**python setup.py install**” y esperar que termine el proceso y Scapy quedara instalado.
- La forma de comprobar que Scapy está instalado correctamente es ejecutarlo, se ingresa al directorio de Scapy y ejecuta “**run\_scapy.exe**” se abrirá una consola tal como se observa en la Fig. 52.

```

C:\WINDOWS\system32\cmd.exe
WARNING: Crypto-related methods disabled for IPsec, Dot11 and TLS layers (needs python-cryptography v1.7+)
WARNING: WinPcap is now deprecated (not maintained). Please use Npcap instead
WARNING: No route found for IPv6 destination :: (no default route?)
INFO: Can't import python-cryptography v1.7+. Disabled WEP decryption/encryption.
INFO: Can't import python-cryptography v1.7+. Disabled IPsec encryption/authentication.
WARNING: IPython not available. Using standard Python shell instead.
AutoCompletion, History are disabled.

          aSPY//YASa
          apyyyyCY/////////Yca
          sY//////YSpCs  scpCY//Pp
ayp ayyyyyySCP//Pp           sy//C
AYAsAYYYYYYYY///Ps           CY//S
          pCCCCY//p      cSSps y//Y
          SPPP///a      pP//AC//Y
          A//A          cy////C
          p///Ac         sC////a
          P///YCpc        A//A
          sCCCCP///pSP///p   p//Y
          sY/////////y caa    S//P
          cayCyayP//Ya    pY/Ya
          sY/PsY///YCc     aC//Yp
          sc  sccaCY//PCypaapyCP//YSs
          spCPY/////YPSPs
          ccaacs

>>> -

```

**Fig. 51 Ejecución de scapy [Fuente Propia]**

### Paso 5. Crear una carpeta compartida

El método de compartir archivos en los sistemas operativos es muy utilizado por los usuarios, cada receptor tendrá que crear una carpeta destino compartida, en esta carpeta se guardara la información o archivos que el emisor trasmite.

La creación de la carpeta se realiza de la siguiente manera:

- Abrir el directorio del disco C.
- Crear una carpeta con el nombre del receptor, en este trabajo de titulación se designó el nombre de “Rceptor\_1” y Receptor\_2 para poder distinguirlos.
- Creado este directorio se hace clic derecho y se selecciona propiedades.
- Seleccionar en la barra de menú la pestaña compartir.
- Clic en la barra despegable, seleccionar todos y clic en agregar.
- Clic en compartir y esperamos el mensaje de confirmación que la carpeta esta compartida.

## **Fase 6. Realizar un experimento apropiado para confirmar que la solución propuesta al problema es efectiva y eficiente**

Los experimentos se basan en transmitir diferentes archivos de distinto tipo y tamaño, el propósito es determinar qué tamaño de archivo es ideal trasmisir por la red, las carpetas con los archivos se estructuran en la TABLA XXV.

**TABLA XXV ARCHIVOS DE EXPERIMENTOS**

Carpetas	Tamaño	Tipo de archivos	Descripción
Documentos_3	83.84 MB	Docx – Pdf - Texto	Documentos de Texto
Documentos_2	57.83 MB	Docx – Pdf - Texto	Documentos de Texto
Documentos_1	12.00 MB	Docx – Pdf - Texto	Documentos de Texto
Archivos_Ejecutable	240.00 MB	Exe	Archivos ejecutables
Archivos_Multimedia	724.45 MB	Mp3 – Avi - Jpg	Archivo multimedia

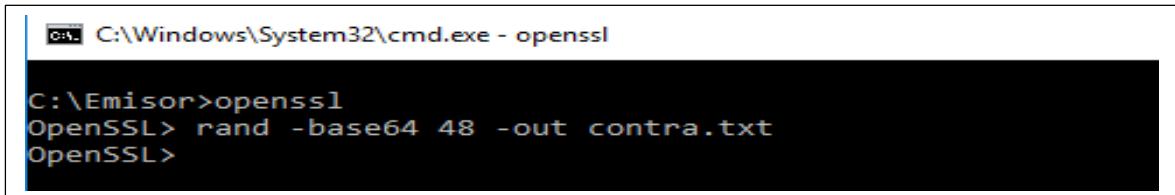
Las tres primeras carpetas contienen archivos que se usan generalmente para almacenar información, por tal motivo cada carpeta contiene archivos de diferente tamaño, pero del mismo tipo (docx, pdf y texto). Las otras dos carpetas contienen archivos multimedia y archivos ejecutables, estos archivos se utilizarán para realizar pruebas de transmisión.

El desarrollo del experimento se basa en ejecutar los procesos establecidos en la Fig. 49, estos procesos son:

### **Proceso 1: Generación de la clave**

La clave es parte fundamental para cifrar los archivos de las cinco carpetas, la generación de la clave se realiza de la siguiente manera:

- Abrir la consola CMD, acceder al directorio Emisor
- Ejecutar “**openssl**”
- Ejecutar la línea de comandos “**rand base64 48 –out contra.txt**” tal como se observa en la Fig. 53, lo que realiza la línea de comandos es generar una clave aleatoria del sistema numérico base 64, dando como salida la clave guardada en un documento de texto llamado “contra.txt”.



```
C:\Windows\System32\cmd.exe - openssl
C:\Emisor>openssl
OpenSSL> rand -base64 48 -out contra.txt
OpenSSL>
```

Fig. 52 Generación de clave aleatoria [Fuente Propia]

La clave generada se deberá copiar en cada una de las cinco carpetas, de tal manera que todos los archivos se cifren utilizando la misma clave.

## Proceso 2. Cifrado de archivos

En este proceso se aplica el método de criptografía simétrica, la forma de cifrar los archivos de cada carpeta se realiza de la siguiente manera:

- Abrir la consola CMD, acceder a cada uno de los directorios
  - C:\Emisor\Documentos\_1
  - C:\Emisor\Documentos\_2
  - C:\Emisor\Documentos\_3
  - C:\Emisor\Archivos\_Ejecutable
  - C:\Emisor\Archivos\_Multimedia
- Ejecutar “**openssl**” en cada uno de los directorios
- Ejecutar la línea de comandos para cada archivo, de cada carpeta “**enc –aes-256-cbc –pass file:contra.txt –in archivo.tipo -out archivo.encrypted**”, observe la Fig. 54, Fig. 55, Fig. 56 , Fig. 57, Fig. 58 lo que realiza la línea de comandos es lo siguiente:
  - **enc – aes-256-cbc:** Especifica el algoritmo que utiliza “AES” y el tipo de cifrado “**Cipher Block Chaining**”, el cbc permite cifrar en la información por bloques.
  - **–pass file:contra.txt:** Utiliza el documento de texto que contiene la clave generada en el Proceso 1 para cifrar los archivos.
  - **–in archivo.tipo:** Especifica el nombre y tipo de archivo a cifrar.
  - **–out archivo.encrypted:** Especifica el nombre del archivo que se obtiene como salida una vez que se cifra la información, el tipo encrypted es determinado para todos los archivos cifrados.

```
C:\Windows\System32\cmd.exe
C:\Emisor\Documentos_1>openssl
OpenSSL> enc -aes-256-cbc -pass file:contra.txt -in esquema.docx -out esquema.encrypted
OpenSSL> enc -aes-256-cbc -pass file:contra.txt -in proyecto.pdf -out proyecto.encrypted
OpenSSL> enc -aes-256-cbc -pass file:contra.txt -in datos.txt -out datos.encrypted
```

**Fig. 53** Cifrado de archivos de la carpeta “Documentos\_1” [Fuente Propia]

```
Símbolo del sistema - openssl
C:\Emisor\Documentos_2>openssl
OpenSSL> enc -aes-256-cbc -pass file:contra.txt -in esquema.docx -out esquema.encrypted
OpenSSL> enc -aes-256-cbc -pass file:contra.txt -in datos.txt -out datos.encrypted
OpenSSL> enc -aes-256-cbc -pass file:contra.txt -in proyecto.pdf -out proyecto.encrypted
```

**Fig. 54** Cifrado de archivos de la carpeta “Documentos\_2” [Fuente Propia]

```
Símbolo del sistema - openssl
C:\Emisor\Documentos_3>openssl
OpenSSL> enc -aes-256-cbc -pass file:contra.txt -in datos.txt -out datos.encrypted
OpenSSL> enc -aes-256-cbc -pass file:contra.txt -in proyecto.pdf -out proyecto.encrypted
OpenSSL> enc -aes-256-cbc -pass file:contra.txt -in esquema.docx -out esquema.encrypted
```

**Fig. 55** Cifrado de archivos de la carpeta “Documentos\_3” [Fuente Propia]

```
C:\Windows\System32\cmd.exe
C:\Emisor\Archivos_Ejecutable>openssl
OpenSSL> enc -aes-256-cbc -pass file:contra.txt -in troyano.exe -out troyano.encrypted
OpenSSL> enc -aes-256-cbc -pass file:contra.txt -in cam.exe -out cam.encrypted
OpenSSL> enc -aes-256-cbc -pass file:contra.txt -inxampp.exe -outxampp.encrypted
```

**Fig. 56** Cifrado de archivos de la carpeta “Archivos\_Ejecutable” [Fuente Propia]

```
C:\Windows\System32\cmd.exe
C:\Emisor\Archivos_Multimedia>openssl
OpenSSL> enc -aes-256-cbc -pass file:contra.txt -in imagen.jpg -out imagen.encrypted
OpenSSL> enc -aes-256-cbc -pass file:contra.txt -in musica.mp3 -out musica.encrypted
OpenSSL> enc -aes-256-cbc -pass file:contra.txt -in video.avi -out video.encrypted
```

**Fig. 57** Cifrado de archivos de la carpeta “Archivos\_Multimedia” [Fuente Propia]

### Proceso 3. Insertar archivos cifrados en un fichero principal

El proceso 3 aplica el método del flujo alternativo de datos (ADS) de la siguiente manera:

- Crear un fichero principal en cada uno de los directorios asignándoles un nombre distintivo, tal como se observa en la TABLA XXVI.

TABLA XXVI CREACIÓN DE FICHEROS PRINCIPALES

Carpetas	Fichero Principal
Documentos_1	Fichero_principal_documentos_1.txt
Documentos_2	Fichero_principal_documentos_2.txt
Documentos_3	Fichero_principal_documentos_3.txt
Archivos_Ejecutable	Fichero_principal_ejecutable.txt
Archivos_Multimedia	Fichero_principal_multimedia.txt

- Los archivos creados tendrán un tamaño de 1 KB, cada uno contiene una descripción de los archivos.
- Abrir la consola CMD, acceder a la ruta de cada uno de los directorios.
- Ejecutar la línea de comandos para cada archivo, de cada carpeta “**type archivo.encrypted > Fichero\_principal\_archivo.txt : ADSarchivo.encrypted**”, lo que realiza la línea de comandos es lo siguiente:
  - **type archivo.encrypted**: Determina el archivo de entrada que va ser insertado en un ADS.
  - **>**: Se utiliza el operador de redirección para definir que se insertara un archivo.
  - **Fichero\_principal\_archivo.txt:ADSarchivo.encrypted**: Hace referencia al nombre del fichero principal y crea el ADS que contendrá el archivo a ocultar, el ADS debe ser del mismo tipo del archivo de entrada en este caso de tipo “encrypted”.
- Utilizar el comando “**dir/r**” para visualizar los archivos insertados en cada fichero principal correspondiente tal como se observa en la Fig.59, Fig.60, Fig.61, Fig.62, Fig.63.

```

C:\Emisor\Documentos_1>type esquema.encrypted > Fichero_principal_documentos_1.txt:ADSesquema.encrypted
C:\Emisor\Documentos_1>type proyecto.encrypted > Fichero_principal_documentos_1.txt:ADSproyecto.encrypted
C:\Emisor\Documentos_1>type datos.encrypted > Fichero_principal_documentos_1.txt:ADSdatos.encrypted

C:\Emisor\Documentos_1>dir/r
El volumen de la unidad C es Windows
El n mero de serie del volumen es: D8A1-D3AC

Directorio de C:\Emisor\Documentos_1

02/07/2018 11:40    <DIR>      .
02/07/2018 11:40    <DIR>      ..
02/07/2018 10:42           65 contra.txt
02/07/2018 11:40           200.096 datos.encrypted
30/06/2018 16:33           200.070 datos.txt
30/06/2018 12:37           3.347.696 esquema.docx
02/07/2018 11:38           3.347.728 esquema.encrypted
02/07/2018 11:42           93 Fichero_principal_documentos_1.txt
                           200.096 Fichero_principal_documentos_1.txt:ADSdatos.encrypted:$DATA
                           3.347.728 Fichero_principal_documentos_1.txt:ADSesquema.encrypted:$DATA
                           9.034.288 Fichero_principal_documentos_1.txt:ADSproyecto.encrypted:$DATA
02/07/2018 11:39           9.034.288 proyecto.encrypted
30/06/2018 13:10           9.034.263 proyecto.pdf
                           8 archivos     25.164.299 bytes
                           2 dirs    739.557.744.640 bytes libres

```

**Fig. 58** Archivos cifrados en el fichero principal "Fichero\_principal\_documentos\_1.txt" [Fuente Propia]

```

C:\Emisor\Documentos_2>type datos.encrypted > Fichero_principal_documentos_2.txt:ADSdatos.encrypted
C:\Emisor\Documentos_2>type esquema.encrypted > Fichero_principal_documentos_2.txt:ADSesquema.encrypted
C:\Emisor\Documentos_2>type proyecto.encrypted > Fichero_principal_documentos_2.txt:ADSproyecto.encrypted

C:\Emisor\Documentos_2>dir/r
El volumen de la unidad C es Windows
El n mero de serie del volumen es: D8A1-D3AC

Directorio de C:\Emisor\Documentos_2

02/07/2018 11:55    <DIR>      .
02/07/2018 11:55    <DIR>      ..
02/07/2018 10:42           65 contra.txt
02/07/2018 11:53           30.230.464 datos.encrypted
01/07/2018 18:51           30.230.445 datos.txt
01/07/2018 18:49           19.869.660 esquema.docx
02/07/2018 11:54           19.869.680 esquema.encrypted
02/07/2018 11:57           93 Fichero_principal_documentos_2.txt
                           30.230.464 Fichero_principal_documentos_2.txt:ADSdatos.encrypted:$DATA
                           19.869.680 Fichero_principal_documentos_2.txt:ADSesquema.encrypted:$DATA
                           10.540.016 Fichero_principal_documentos_2.txt:ADSproyecto.encrypted:$DATA
02/07/2018 11:55           10.540.016 proyecto.encrypted
07/11/2017 21:18           10.539.984 proyecto.pdf
                           8 archivos     121.280.407 bytes
                           2 dirs    739.422.380.032 bytes libres

```

**Fig. 59** Archivos cifrados en el fichero principal "Fichero\_principal\_documentos\_2.txt" [Fuente Propia]

```

C:\Emisor\Documentos_3>type proyecto.encrypted > Fichero_principal_documentos_3.txt:ADSproyecto.encrypted
C:\Emisor\Documentos_3>type esquema.encrypted > Fichero_principal_documentos_3.txt:ADSequema.encrypted
C:\Emisor\Documentos_3>type datos.encrypted > Fichero_principal_documentos_3.txt:ADSdatos.encrypted

C:\Emisor\Documentos_3>dir/r
El volumen de la unidad C es Windows
El n mero de serie del volumen es: D8A1-D3AC

Directorio de C:\Emisor\Documentos_3

02/07/2018 12:09    <DIR>      .
02/07/2018 12:09    <DIR>      ..
02/07/2018 10:42           65 contra.txt
02/07/2018 12:08      529.584 datos.encrypted
30/06/2018 16:42      529.552 datos.txt
30/06/2018 16:25     9.090.745 esquema.docx
02/07/2018 12:09     9.090.768 esquema.encrypted
02/07/2018 12:10           93 Fichero_principal_documentos_3.txt
                           529.584 Fichero_principal_documentos_3.txt:ADSdatos.encrypted:$DATA
                           9.090.768 Fichero_principal_documentos_3.txt:ADSequema.encrypted:$DATA
                           67.811.776 Fichero_principal_documentos_3.txt:ADSproyecto.encrypted:$DATA
02/07/2018 12:07     67.811.776 proyecto.encrypted
14/06/2018 14:40     67.811.755 proyecto.pdf
                     8 archivos   154.864.338 bytes
                     2 dirs   739.282.624.512 bytes libres

```

**Fig. 60** Archivos cifrados en el fichero principal "Fichero\_principal\_documentos\_3.txt" [Fuente Propia]

```

C:\Emisor\Archivos_Ejecutable>type troyano.encrypted > Fichero_principal_ejecutable.txt:ADStroyano.encrypted
C:\Emisor\Archivos_Ejecutable>type cam.encrypted > Fichero_principal_ejecutable.txt:cam.encrypted
C:\Emisor\Archivos_Ejecutable>type xampp.encrypted > Fichero_principal_ejecutable.txt:ADSxampp.encrypted

C:\Emisor\Archivos_Ejecutable>dir/r
El volumen de la unidad C es Windows
El n mero de serie del volumen es: D8A1-D3AC

Directorio de C:\Emisor\Archivos_Ejecutable

02/07/2018 11:03    <DIR>      .
02/07/2018 11:03    <DIR>      ..
02/07/2018 11:02           96.288 cam.encrypted
13/07/2009 20:39      96.256 cam.exe
02/07/2018 10:42           65 contra.txt
02/07/2018 11:07           79 Fichero_principal_ejecutable.txt
                           82.096 Fichero_principal_ejecutable.txt:ADStroyano.encrypted:$DATA
                           118.816 Fichero_principal_ejecutable.txt:ADSxampp.encrypted:$DATA
                           96.288 Fichero_principal_ejecutable.txt:cam.encrypted:$DATA
02/07/2018 11:01     82.096 troyano.encrypted
23/08/2017 22:06     82.064 troyano.exe
02/07/2018 11:03     118.816 xampp.encrypted
30/03/2013 07:29     118.784 xampp.exe
                     8 archivos   594.448 bytes
                     2 dirs   741.104.566.272 bytes libres

```

**Fig. 61** Archivos cifrados en el fichero principal "Fichero\_principal\_ejecutable.txt" [Fuente Propia]

```

C:\Emisor\Archivos_Multimedia>type imagen.encrypted > Fichero_principal_multimedia.txt:ADSimagen.encrypted
C:\Emisor\Archivos_Multimedia>type musica.encrypted > Fichero_principal_multimedia.txt:ADSmusica.encrypted
C:\Emisor\Archivos_Multimedia>type video.encrypted > Fichero_principal_multimedia.txt:ADSvideo.encrypted
C:\Emisor\Archivos_Multimedia>dir/r
El volumen de la unidad C es Windows
El n mero de serie del volumen es: D8A1-D3AC

Directorio de C:\Emisor\Archivos_Multimedia

02/07/2018 11:25    <DIR>          .
02/07/2018 11:25    <DIR>          ..
02/07/2018 10:42              65 contra.txt
02/07/2018 11:11          0 Fichero_principal_multimedia.docx
02/07/2018 11:27          0 Fichero_principal_multimedia.txt
                           226.752 Fichero_principal_multimedia.txt:ADSimagen.encrypted:$DATA
                           25.056.880 Fichero_principal_multimedia.txt:ADSmusica.encrypted:$DATA
                           734.459.936 Fichero_principal_multimedia.txt:ADSvideo.encrypted:$DATA
02/07/2018 11:21          226.752 imagen.encrypted
01/07/2018 18:33          226.725 imagen.jpg
02/07/2018 11:22          25.056.880 musica.encrypted
05/02/2010 05:17          25.056.858 musica.mp3
30/12/2017 09:19          734.459.904 video.avi
02/07/2018 11:23          734.459.936 video.encrypted
                           9 archivos  1.519.487.120 bytes
                           2 dirs   739.586.224.128 bytes libres

```

Fig. 62 Archivos cifrados en el fichero principal "Fichero\_principal\_multimedia.txt" [Fuente Propia]

#### Proceso 4. Transmisi n de archivos por la red LAN

El proceso 4 se divide en dos secciones, la primera secci n utiliza el m todo de compartici n de archivos, para la transmisi n de los ficheros principales que se encuentran en cada carpeta, la segunda secci n aplica el m todo de esteganograf a de red para transmitir la clave generada en el Proceso 1, antes de describir el desarrollo de las secciones se debe obtener las direcciones ip l gicas tanto en la versi n IPV4 e IPV6 de los involucrados, en la Fig. 64 se observa las direcciones del receptor 1, en la Fig. 65 se observa las direcciones del receptor 2 y en la en la Fig. 66 se observa las direcciones del emisor, los receptores deben ejecutar la herramienta Wireshark en todo el proceso de trasmisi n, esta acci n ser  de ayuda para el siguiente proceso.

```

Microsoft Windows [Versi n 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\b-boy>ipconfig

Configuraci n IP de Windows

Adaptador de Ethernet Conexi n de 阿rea local:

Sufijo DNS espec fico para la conexi n . . . . . :
Direcci n IPv6 . . . . . : fdf7:7226:1117:0:20c9:92e:b63b:af00
Direcci n IPv6 temporal . . . . . : fdf7:7226:1117:0:9c92:c5be:dc45:a4eb
V nculo: direcci n IPv6 local . . . . : fe80::20c9:92e:b63b:af00%13
Direcci n IPv4 . . . . . : 192.168.1.20
M scara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 192.168.1.1

```

Fig. 63 Direcciones ip del receptor 1 [Fuente Propia]

```

Microsoft Windows [Versión 6.1.7600]
Copyright <c> 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\daniel>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local:

    Sufijo DNS específico para la conexión. . . .
    Dirección IPv6 . . . . . : fdf7:7226:1117:0:d4f9:a3b1:66bf:7146
    Dirección IPv6 temporal. . . . . : fdf7:7226:1117:0:3198:e64:f5a1:9cab
    Vínculo: dirección IPv6 local. . . . : fe80::d4f9:a3b1:66bf:7146%11
    Dirección IPv4. . . . . : 192.168.1.30
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . : 192.168.1.1

```

Fig. 64 Direcciones ip de receptor 2 [Fuente Propia]

```

Adaptador de LAN inalámbrica Wi-Fi:

    Sufijo DNS específico para la conexión. . . .
    Dirección IPv6 . . . . . : fdf7:7226:1117:0:9531:3aca:874a:5ac1
    Dirección IPv6 temporal. . . . . : fdf7:7226:1117:0:b13e:bbc2:ba6a:827d
    Vínculo: dirección IPv6 local. . . . : fe80::9531:3aca:874a:5ac1%4
    Dirección IPv4. . . . . : 192.168.1.10
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . : 192.168.1.1

```

Fig. 65 Direcciones ip del emisor [Fuente Propia]

## Sección 1. Transmisión de fichero principal

- Abrir la consola CMD, acceder a la ruta de cada uno de los directorios.
- Ejecutar la línea de comandos para cada fichero principal, de cada carpeta “**copy .\Fichero\_principal\_archivo.txt \\"dirección\_ip\nombre\_carpeta receptor"** en la Fig. 67 se observan los archivos transmitidos al Receptor\_1 en la versión IPV4, en la Fig. 68 se observan los archivos transmitidos al Receptor\_1 en la versión IPV6 y en la Fig.69 se observan los archivos trasmitidos al Receptor\_2, lo que realiza la línea de comandos es lo siguiente:

- **copy**: Especifica que se copiara un archivo.
- **.\Fichero\_principal\_archivo.txt**: Hace referencia al nombre del fichero principal que se encuentra en cada carpeta.
- **\dirección\_ip\nombre\_carpeta**: Ingresá la dirección ip de cada receptor, en la versión IPV4 e IPV6 y hace referencia al nombre de la carpeta compartida en la que se guardarán los ficheros.

```

Símbolo del sistema
C:\Emisor>cd Documentos_1
C:\Emisor\Documentos_1>copy .\Fichero_principal_documentos_1.txt \\192.168.1.20\Receptor_1
    1 archivo(s) copiado(s).

C:\Emisor>cd Documentos_2
C:\Emisor\Documentos_2>copy .\Fichero_principal_documentos_2.txt \\192.168.1.20\Receptor_1
    1 archivo(s) copiado(s).

C:\Emisor>cd Documentos_3
C:\Emisor\Documentos_3>copy .\Fichero_principal_documentos_3.txt \\192.168.1.20\Receptor_1
    1 archivo(s) copiado(s).

C:\Emisor>cd Archivos_Ejecutable
C:\Emisor\Archivos_Ejecutable>copy .\Fichero_principal_ejecutable.txt \\192.168.1.20\Receptor_1
    1 archivo(s) copiado(s).

C:\Emisor>cd Archivos_Multimedia
C:\Emisor\Archivos_Multimedia>copy .\Fichero_principal_multimedia.txt \\192.168.1.20\Receptor_1
    1 archivo(s) copiado(s).

```

**Fig. 66** Transmisión de ficheros principales al receptor 1, versión IPV4 [Fuente Propia]

```

Símbolo del sistema
C:\Emisor\Documentos_1>copy .\Fichero_principal_documentos_1.txt \\fdf7:7226:1117:0:20c9:92e:b63b:af00\Receptor_1
    1 archivo(s) copiado(s).

C:\Emisor\Documentos_1>cd C:\Emisor\Documentos_2
C:\Emisor\Documentos_2>copy .\Fichero_principal_documentos_2.txt \\fdf7:7226:1117:0:20c9:92e:b63b:af00\Receptor_1
    1 archivo(s) copiado(s).

C:\Emisor\Documentos_2>cd C:\Emisor\Documentos_3
C:\Emisor\Documentos_3>copy .\Fichero_principal_documentos_3.txt \\fdf7:7226:1117:0:20c9:92e:b63b:af00\Receptor_1
    1 archivo(s) copiado(s).

C:\Emisor\Documentos_3>cd C:\Emisor\Archivos_Ejecutable
C:\Emisor\Archivos_Ejecutable>copy .\Fichero_principal_ejecutable.txt \\fdf7:7226:1117:0:20c9:92e:b63b:af00\Receptor_1
    1 archivo(s) copiado(s).

C:\Emisor\Archivos_Ejecutable>cd C:\Emisor\Archivos_Multimedia
C:\Emisor\Archivos_Multimedia>copy .\Fichero_principal_multimedia.txt \\fdf7:7226:1117:0:20c9:92e:b63b:af00\Receptor_1
    1 archivo(s) copiado(s).

```

**Fig. 67** Transmisión de ficheros principales al receptor 1, versión IPV6 [Fuente Propia]

```

Símbolo del sistema

C:\Emisor>cd Documentos_1
C:\Emisor\Documentos_1>copy .\Fichero_principal_documentos_1.txt \\192.168.1.30\Receptor_2
1 archivo(s) copiado(s).

C:\Emisor>cd Documentos_2
C:\Emisor\Documentos_2>copy .\Fichero_principal_documentos_2.txt \\192.168.1.30\Receptor_2
1 archivo(s) copiado(s).

C:\Emisor>cd Documentos_3
C:\Emisor\Documentos_3>copy .\Fichero_principal_documentos_3.txt \\192.168.1.30\Receptor_2
1 archivo(s) copiado(s).

C:\Emisor>cd Archivos_Ejecutable
C:\Emisor\Archivos_Ejecutable>copy .\Fichero_principal_ejecutable.txt \\192.168.1.30\Receptor_2
1 archivo(s) copiado(s).

C:\Emisor>cd Archivos_Multimedia
C:\Emisor\Archivos_Multimedia>copy .\Fichero_principal_multimedia.txt \\192.168.1.30\Receptor_2
1 archivo(s) copiado(s).

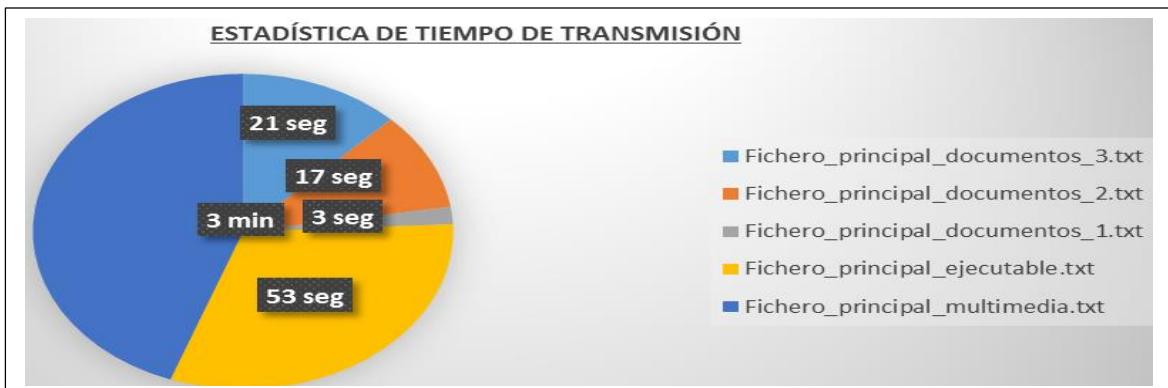
```

**Fig. 68** Transmisión de ficheros principales al receptor 2, versión IPV4 [Fuente Propia]

- Se lleva el control del tiempo de transmisión de cada fichero principal según su tamaño, tal como se observa en la TABLA XXVII y su estadística en la Fig. 70.

**TABLA XXVII TABLA DE TIEMPOS DE CONTROL DE TRANSMISIÓN DE ARCHIVOS**

Ficheros principales	Tamaño	Tiempo	Observaciones
Fichero_principal_documentos_3.txt	83.84 MB	21 segundos	Excelente
Fichero_principal_documentos_2.txt	57.83 MB	17 segundos	Excelente
Fichero_principal_documentos_1.txt	12.00 MB	3 segundos	Excelente
Fichero_principal_ejecutable.txt	240.00 MB	53 segundos	Excelente
Fichero_principal_multimedia.txt	724.45 MB	3 minutos	Problema en red



**Fig. 69** Estadística de tiempos de transmisión [Fuente Propia]

## **Sección 2. Transmisión de la clave**

- Ir al directorio C:\Python27, abrir la carpeta Scripts.
- Ejecutar run\_scapy.exe
- Digitar cada uno de los siguientes comandos en la versión IPV4:
  - **ip = IP ()**: Crea un paquete ip.
  - **ip.dst= “Dirección IPV4”**: Se accede a modificar el campo ip destino, se agrega la dirección ip del receptor.
  - **icmp= ICMP ()**: Crear un paquete icmp.
  - **mensaje= “clave”**: Se inserta la clave generada en el Proceso 1 en la variable mensaje.
  - **icmp.add\_payload(mensaje)**: Se ingresa la variable mensaje en el campo DATA, este campo es el que lleva la información del paquete.
  - **paquete= ip/icmp**: Realiza la composición de capas y combina los paquetes en uno solo.
  - **sr1(paquete)=** Envía el paquete y recibe la respuesta por parte del receptor.
- Digitar cada uno de los siguientes comandos en la versión IPV6:
  - **ip= IPv6()**: Crea un paquete ip.
  - **ip.dst= “Dirección ip IPV6”**: Se accede a modificar el campo ip destino, se agrega la dirección ip del receptor.
  - **mensaje= “clave”**: Se inserta la clave generada en el Proceso 1 en la variable mensaje.
  - **icmp= ICMPv6EchoRequest(data=mensaje)**: Crear un paquete icmp, especificado el tipo de mensaje de solicitud y establecer que la variable DATA será igual a la variable mensaje.
  - **paquete= ip/icmp**: Realiza la composición de capas y combina los paquetes en uno solo.
  - **sr1(paquete)=** Envía el paquete y recibe la respuesta por parte del receptor.
- Al ejecutar los comandos se crean los paquetes (IP - ICMP) y se envían por la red. Se recibe respuesta del destino indicado que el paquete ha llegado correctamente, en la Fig. 71 se observa él envío de la clave al receptor 1 en la versión IPV4, en la Fig. 72 se observa él envío de la clave al receptor 1 en la versión IPV6 y en la Fig. 73 se observa él envío de la clave al receptor 2.

```

>>> ip= IP()
>>> ip.dst= "192.168.1.20"
>>> icmp= ICMP()
>>> mensaje= "ddDS+9kpkT8egJcDD4p+aqb9H5KcySC02jqEyTq2vykaTUY0u3gbschTPiIhhDOJE"
>>> icmp.add_payload(mensaje)
>>> paquete= ip/icmp
>>> sr1(paquete)
Begin emission:
..Finished sending 1 packets.
...

```

**Fig. 70 Transmisión de la clave al receptor 1, versión IPV4 [Fuente Propia]**

```

>>> ipv6=IPv6()
>>> ipv6.dst="fdf7:7226:1117:0:20c9:92e:b63b:af00"
>>> mensaje="ddDS+9kpkT8egJcDD4p+aqb9H5KcySC02jqEyTq2vykaTUY0u3gbschTPiIhhDOJE"
>>> icmpv6=ICMPv6EchoRequest(data=mensaje)
>>> paquete= ipv6/icmpv6
>>> sr1(paquete)
Begin emission:
.WARNINg: Mac address to reach destination not found. Using broadcast.
Finished sending 1 packets.
.....

```

**Fig. 71 Transmisión de la clave al receptor 1, versión IPV6 [Fuente Propia]**

```

>>> ip= IP()
>>> ip.dst="192.168.1.30"
>>> icmp= ICMP()
>>> mensaje= "ddDS+9kpkT8egJcDD4p+aqb9H5KcySC02jqEyTq2vykaTUY0u3gbschTPiIhhDOJE"
>>> icmp.add_payload(mensaje)
>>> paquete= ip/icmp
>>> sr1(paquete)
Begin emission:
..Finished sending 1 packets.
...

```

**Fig. 72 Transmisión de la clave al receptor 2, versión IPV4 [Fuente Propia]**

## **Proceso 5. Recepción de archivos por la red LAN**

En el proceso 5 inicia la tarea de los receptores, de igual manera el proceso 5 se divide en 2 secciones, la recepción de ficheros principales y la recepción de la clave.

### **Sección 1. Recepción de ficheros principales**

- Abrir la carpeta compartida que creó cada receptor.
- Comprobar si los ficheros principales transmitidos se encuentran en la carpeta compartida, observa la Fig.74 la carpeta compartida del receptor 1 y la Fig.75 la carpeta compartida del receptor 2.

The screenshot shows a Windows File Explorer window with the path 'Equipo > Disco local (C:) > Receptor\_1'. The 'Organizar' menu is open. The table lists the following files:

	Nombre	Fecha de modifica...	Tipo	Tamaño
Favoritos				
Descargas	Fichero_principal_documentos_1	02/07/2018 11:42	Documento de tex...	1 KB
Escritorio	Fichero_principal_documentos_2	04/07/2018 11:07	Documento de tex...	1 KB
Sitios recientes	Fichero_principal_documentos_3	04/07/2018 11:11	Documento de tex...	1 KB
Unidad de CD	Fichero_principal_ejecutable	02/07/2018 11:07	Documento de tex...	1 KB
Tesis	Fichero_principal_multimedia	04/07/2018 11:10	Documento de tex...	1 KB

Fig. 73 Recepción de ficheros principales receptor 1 [Fuente Propia]

The screenshot shows a Windows File Explorer window with the path 'Equipo > Disco local (C:) > Receptor\_2'. The 'Organizar' menu is open. The table lists the following files:

	Nombre	Fecha de modifica...	Tipo	Tamaño
Favoritos				
Bibliotecas	Fichero_principal_documentos_1	02/07/2018 11:42	Documento de tex...	1 KB
Grupo en el hogar	Fichero_principal_documentos_2	04/07/2018 11:07	Documento de tex...	1 KB
	Fichero_principal_documentos_3	04/07/2018 11:11	Documento de tex...	1 KB
	Fichero_principal_ejecutable	02/07/2018 11:07	Documento de tex...	1 KB
	Fichero_principal_multimedia	04/07/2018 11:10	Documento de tex...	1 KB

Fig. 74 Recepción de ficheros principales receptor 2 [Fuente Propia]

- Abrir la consola CMD, acceder al directorio de la carpeta compartida y ejecutar el comando “**dir/r**”, con el fin de comprobar que los archivos cifrados estén en su fichero principal correspondiente, tal como se observa en la Fig. 76 y la Fig. 77.

```
C:\Windows\system32\cmd.exe
C:\Receptor_1>dir/r
El volumen de la unidad C no tiene etiqueta.
El n mero de serie del volumen es: 4C34-2813
Directorio de C:\Receptor_1

04/07/2018 11:19    <DIR>   .
04/07/2018 11:19    <DIR>   .
02/07/2018 11:42            93 Fichero_principal_documentos_1.txt
                           200.096 Fichero_principal_documentos_1.txt:ADSdatos.encrypted:$DATA
                           3.347.728 Fichero_principal_documentos_1.txt:ADSesquema.encrypted:$DATA
                           9.034.288 Fichero_principal_documentos_1.txt:ADSproyecto.encrypted:$DATA
04/07/2018 11:07            93 Fichero_principal_documentos_2.txt
                           30.230.464 Fichero_principal_documentos_2.txt:ADSdatos.encrypted:$DATA
                           19.869.680 Fichero_principal_documentos_2.txt:ADSesquema.encrypted:$DATA
                           10.540.016 Fichero_principal_documentos_2.txt:ADSproyecto.encrypted:$DATA
04/07/2018 11:11            93 Fichero_principal_documentos_3.txt
                           529.584 Fichero_principal_documentos_3.txt:ADSdatos.encrypted:$DATA
                           9.090.768 Fichero_principal_documentos_3.txt:ADSesquema.encrypted:$DATA
                           67.811.772 Fichero_principal_documentos_3.txt:ADSproyecto.encrypted:$DATA
02/07/2018 11:07            79 Fichero_principal_ejecutable.txt
                           82.096 Fichero_principal_ejecutable.txt:ADSstroyano.encrypted:$DATA
                           118.816 Fichero_principal_ejecutable.txt:ADSxampp.encrypted:$DATA
                           96.288 Fichero_principal_ejecutable.txt:cam.encrypted:$DATA
04/07/2018 11:10            82 Fichero_principal_multimedia.txt
                           226.752 Fichero_principal_multimedia.txt:ADSimagen.encrypted:$DATA
                           25.056.880 Fichero_principal_multimedia.txt:ADSmusica.encrypted:$DATA
                           734.459.936 Fichero_principal_multimedia.txt:ADSvideo.encrypted:$DATA
                           5 archivos           440 bytes
                           2 dirs      69.953.843.200 bytes libres

C:\Receptor_1>
```

Fig. 75 Archivos cifrados insertado en los ficheros principales del receptor 1 [Fuente Propia]

```

C:\Windows\system32\cmd.exe

C:\Receptor_2>dir/r
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 4C34-2813

    Directorio de C:\Receptor_2

06/07/2018  16:10      <DIR>
06/07/2018  16:10      <DIR>
02/07/2018  11:42      .
                           93 Fichero_principal_documentos_1.txt
                           200.096 Fichero_principal_documentos_1.txt:ADSdatos.encrypted:$DATA
                           3.347.728 Fichero_principal_documentos_1.txt:ADSEsquema.encrypted:$DATA
                           9.034.288 Fichero_principal_documentos_1.txt:ADSproyecto.encrypted:$DATA
04/07/2018  11:07      .
                           93 Fichero_principal_documentos_2.txt
                           30.230.464 Fichero_principal_documentos_2.txt:ADSdatos.encrypted:$DATA
                           19.869.680 Fichero_principal_documentos_2.txt:ADSEsquema.encrypted:$DATA
                           10.540.016 Fichero_principal_documentos_2.txt:ADSproyecto.encrypted:$DATA
04/07/2018  11:11      .
                           529.584 Fichero_principal_documentos_3.txt:ADSdatos.encrypted:$DATA
                           9.090.768 Fichero_principal_documentos_3.txt:ADSEsquema.encrypted:$DATA
                           67.811.776 Fichero_principal_documentos_3.txt:ADSproyecto.encrypted:$DATA
02/07/2018  11:07      .
                           82.096 Fichero_principal_ejecutable.txt
                           118.816 Fichero_principal_ejecutable.txt:ADSxampp.encrypted:$DATA
                           96.288 Fichero_principal_ejecutable.txt:cam.encrypted:$DATA
04/07/2018  11:10      .
                           82 Fichero_principal_multimedia.txt
                           226.752 Fichero_principal_multimedia.txt:ADSimagen.encrypted:$DATA
                           25.056.880 Fichero_principal_multimedia.txt:ADSmusica.encrypted:$DATA
                           734.459.936 Fichero_principal_multimedia.txt:ADSvideo.encrypted:$DATA
                           440 bytes
                           5 archivos
                           2 dirs   69.013.762.048 bytes libres

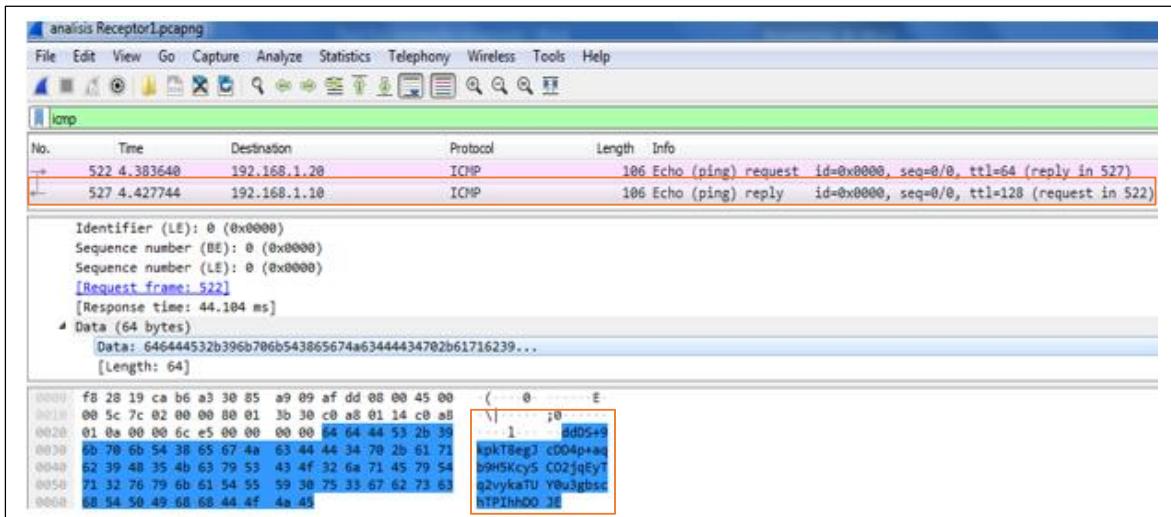
C:\Receptor_2>

```

**Fig. 76** Archivos cifrados insertado en los ficheros principales del receptor 2 [Fuente Propia]

## Sección 2. Recepción de clave

- Realizar un filtro de paquetes ICMP con la herramienta Wireshark.
- Buscar un paquete ICMP generado por la dirección ip del emisor “**192.168.1.10**” en la versión IPV4 y “**fdf7:7226:1117:0:9531:3aca: 874a:5ac1**” en la versión IPV6.
- Acceder a la estructura del paquete ICMP, ir al campo DATA tal como se observa en la Fig. 78 y la Fig. 79 en la versión IPV4 y en la Fig. 80 en la versión IPV6.
- En el campo DATA se encuentra la clave, obtener la clave y guardarla en documento de texto.



**Fig. 77** Filtro de paquetes ICMP por el receptor 1, versión IPV4 [Fuente Propia]

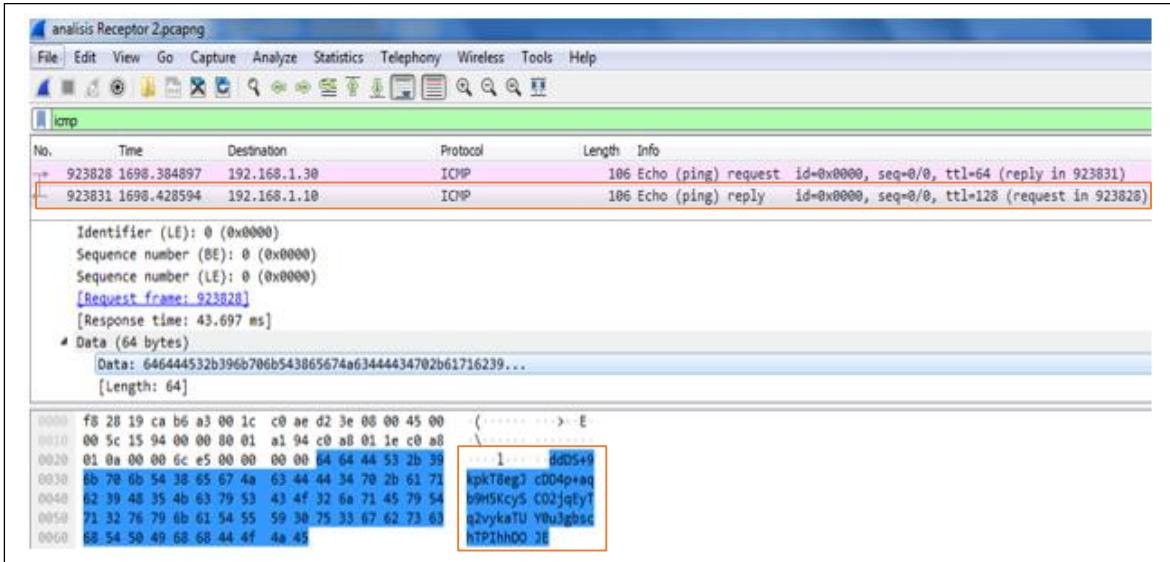


Fig. 78 Filtro de paquetes ICMP por el receptor 2, versión IPV4 [Fuente Propia]

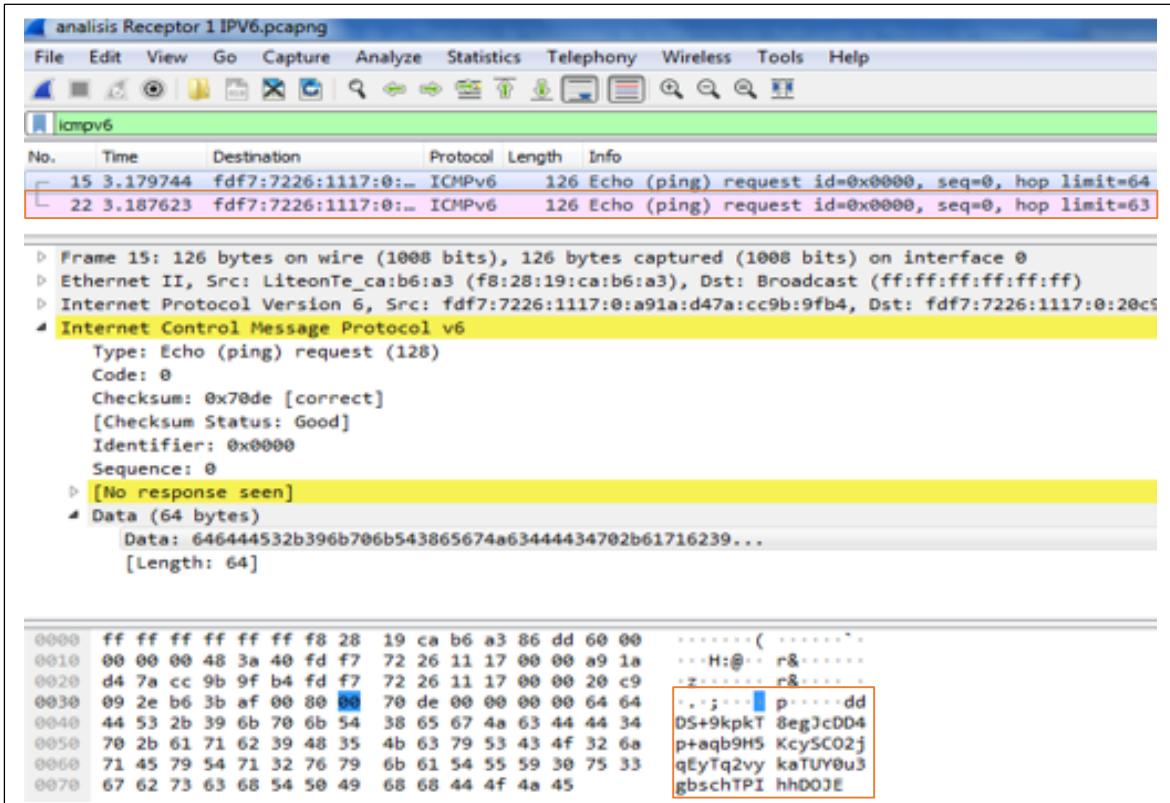
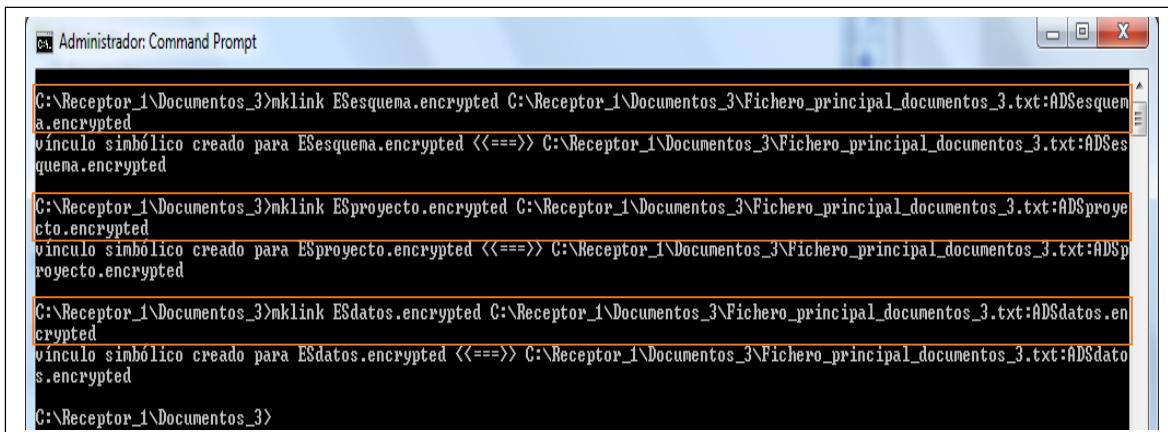


Fig. 79 Filtro de paquetes ICMP por el receptor 1, versión IPV6 [Fuente Propia]

## Proceso 6. Extracción de archivos

El proceso 6 realiza la extracción de archivos cifrados que fueron insertados en los ficheros principales, se debe crear cinco carpetas, guardar cada fichero principal y el documento de texto que contiene la clave, el proceso de extracción en todas las carpetas y en los receptores es igual, de tal forma se realizará la extracción de los archivos de la carpeta "Documentos 3" correspondiente al receptor 1 de la siguiente manera:

- Abrir la consola CMD en modo administrador, acceder a cada uno de los directorios.
- Crear un enlace simbólico para cada archivo insertado en el fichero principal, ejecutando la siguiente línea de comando "**mklink EArchivo.encrypted C:\Receptor\_1\ Fichero\_principal.txt:ADSarchivo.encrypted**", tal como se observa en la Fig. 81, lo que realiza el comando es lo siguiente:
  - **Mklink EArchivo.encrypted:** Crea un acceso directo del archivo cifrado que se encuentra dentro del fichero principal.
  - **C:\Receptor\_1\Fichero\_principal.txt:ADSarchivo.encrypted:** Hace referencia al directorio donde se encuentra el archivo cifrado.



```
C:\Receptor_1\Documentos_3>mklink EEsquema.encrypted C:\Receptor_1\Documentos_3\Fichero_principal_documentos_3.txt:ADSesquema.encrypted
Vínculo simbólico creado para EEsquema.encrypted <<==>> C:\Receptor_1\Documentos_3\Fichero_principal_documentos_3.txt:ADSesquema.encrypted

C:\Receptor_1\Documentos_3>mklink Eprojeto.encrypted C:\Receptor_1\Documentos_3\Fichero_principal_documentos_3.txt:ADSproyecto.encrypted
Vínculo simbólico creado para Eprojeto.encrypted <<==>> C:\Receptor_1\Documentos_3\Fichero_principal_documentos_3.txt:ADSproyecto.encrypted

C:\Receptor_1\Documentos_3>mklink Esdatos.encrypted C:\Receptor_1\Documentos_3\Fichero_principal_documentos_3.txt:ADSdatos.encrypted
Vínculo simbólico creado para Esdatos.encrypted <<==>> C:\Receptor_1\Documentos_3\Fichero_principal_documentos_3.txt:ADSdatos.encrypted

C:\Receptor_1\Documentos_3>
```

**Fig. 80** Creación de accesos directos, de archivos cifrados [Fuente Propia]

- En cada carpeta quedaran archivos de tipo symlink de acceso directo, el acceso directo no muestra sospecha de contener archivos, ya que su tamaño es de 0 KB ante la vista del usuario, tal como se observa en la Fig. 82.

The screenshot shows a Windows File Explorer window with the path "Disco local (C:) > Receptor\_1 > Documentos\_3". The search bar at the top right contains the text "Buscar Documentos\_3". The main area displays a list of files and folders. On the left, there is a sidebar with "Favoritos" containing "Descargas", "Escritorio", "Sitios recientes", "Unidad de CD", and "Tesis". The main list shows the following entries:

	Nombre	Fecha de modifica...	Tipo	Tamaño
	contraseña	02/07/2018 10:42	Documento de tex...	1 KB
	ESdatos	07/07/2018 14:08	.symlink	0 KB
	ESEsquema	07/07/2018 14:07	.symlink	0 KB
	ESproyecto	07/07/2018 14:08	.symlink	0 KB
	Fichero_principal_documentos_3	04/07/2018 11:11	Documento de tex...	1 KB

Fig. 81 Accesos directos creados [Fuente Propia]

- Creado el acceso directo de cada archivo cifrado, se necesita obtener dicho archivo de tipo encrypted, esto se realiza aplicando la siguiente línea de comandos “**type ESArchivo.encrypted > archivo.encrypted** ” observe la Fig. 83 y el resultado de la extracción en la Fig. 84, lo que realiza la línea de comandos es lo siguiente.
  - type ESArchivo.encrypted:** Hace referencia al acceso directo que se creó.
  - >:** Se utiliza el operador de redirección para realizar una copia del archivo que contiene el acceso directo.
  - archivo.encrypted:** Se da un nombre a la copia que se extrae del enlace simbólico, el tipo del archivo tiene que ser encrypted.

The screenshot shows a Command Prompt window titled "Administrador: Command Prompt". The command entered is "type ESEsquema.encrypted > esquema.encrypted". The output shows the command being run and the resulting file "esquema.encrypted" being created. The full command history is as follows:

```

C:\Receptor_1\Documentos_3>type ESEsquema.encrypted > esquema.encrypted
C:\Receptor_1\Documentos_3>type ESproyecto.encrypted > proyecto.encrypted
C:\Receptor_1\Documentos_3>type ESDatos.encrypted > datos.encrypted
C:\Receptor_1\Documentos_3>

```

Fig. 82 Extracción de archivos cifrados de los accesos directos [Fuente Propia]

The screenshot shows a Windows File Explorer window with the path "Disco local (C:) > Receptor\_1 > Documentos\_3". The search bar at the top right contains the text "Buscar Documentos\_3". The main area displays a list of files and folders. On the left, there is a sidebar with "Favoritos" containing "Descargas", "Escritorio", "Sitios recientes", "Unidad de CD", and "Tesis". There is also a section for "Bibliotecas" and "Documentos". The main list shows the following entries:

	Nombre	Fecha de modifica...	Tipo	Tamaño
	contraseña	02/07/2018 10:42	Documento de tex...	1 KB
	datos.encrypted	07/07/2018 14:38	Archivo ENCRYPT...	518 KB
	ESdatos	07/07/2018 14:36	.symlink	0 KB
	ESEsquema	07/07/2018 14:35	.symlink	0 KB
	ESproyecto	07/07/2018 14:35	.symlink	0 KB
	esquema.encrypted	07/07/2018 14:37	Archivo ENCRYPT...	8.878 KB
	Fichero_principal_documentos_3	04/07/2018 11:11	Documento de tex...	1 KB
	proyecto.encrypted	07/07/2018 14:38	Archivo ENCRYPT...	66.223 KB

Fig. 83 Archivos cifrados [Fuente Propia]

## Proceso 7. Descifrar los archivos

En el proceso 7 se lleva a cabo el descifrado de los archivos que contienen la información que fue trasmisita por el emisor, se utilizara la clave que fue guardada junto con el fichero principal en cada carpeta, el proceso de descifrar archivos es igual para todas las carpetas y todos los receptores que realizaron con éxito el Proceso 6, de tal forma se realizará la extracción de los archivos de la carpeta “Documentos 3” correspondiente al receptor 1 de la siguiente manera:

- Abrir la consola CMD, acceder a cada uno de los directorios donde se encuentran los archivos cifrados.
- Ejecutar línea de comandos por cada archivo, de cada carpeta “**enc –aes-256-cbc -d –pass file:clave.txt –in archivo.tipo –out archivo.encrypted**” observe la Fig. 85, lo que realiza la línea de comandos es lo siguiente:
  - **enc – aes-256-cbc:** Especifica el algoritmo que utiliza “AES” y el tipo de cifrado “**Cipher Block Chaining**”, el cbc permite cifrar en la información por bloques.
  - **– d:** Indica que se requiere descifrar la información
  - **–pass file:contra.txt:** Utiliza el documento de texto que contiene la clave aleatoria generada en el Proceso 1 para descifrar los archivos.
  - **–in archivo. encrypted:** Especifica el nombre y tipo del archivo, que se va a descifrar.
  - **–out archivo.tipo:** Especifica el nombre del archivo que da como salida una vez que se descifra, se debe agregar el tipo del archivo original .

```
C:\Receptor_1\Documentos_3>openssl
OpenSSL> enc -aes-256-cbc -d -pass file:contra.txt -in esquema.encrypted -out esquema.docx
OpenSSL> enc -aes-256-cbc -d -pass file:contra.txt -in proyecto.encrypted -out proyecto.pdf
OpenSSL> enc -aes-256-cbc -d -pass file:contra.txt -in datos.encrypted -out datos.txt
OpenSSL>
```

**Fig. 84** Descifrar archivos con openssl [Fuente Propia]

- Ya descifrados los archivos la información podrá ser vista por el receptor utilizando una aplicación acorde al tipo de archivos, observe la Fig. 86.

The screenshot shows a Windows File Explorer window with the following details:

- Path:** Disco local (C:) > Receptor\_1 > Documentos\_3
- Toolbar:** Organizar, Incluir en biblioteca, Compartir con, Grabar, Nueva carpeta.
- Search Bar:** Buscar Documentos\_3
- File List:**

	Nombre	Fecha de modifica...	Tipo	Tamaño
★ Favoritos	proyecto	07/07/2018 15:23	Archivo PDF	66.223 KB
Descargas	proyecto.encrypted	07/07/2018 14:38	Archivo ENCRYPT...	66.223 KB
Escritorio	Fichero_principal_documentos_3	04/07/2018 11:11	Documento de tex...	1 KB
Sitios recientes	esquema.encrypted	07/07/2018 14:37	Archivo ENCRYPT...	8.878 KB
Unidad de CD	esquema	07/07/2018 15:22	Documento de Mi...	8.878 KB
M Tesis	ESprojeto	07/07/2018 14:35	.symlink	0 KB
Bibliotecas	ESesquema	07/07/2018 14:35	.symlink	0 KB
Documentos	ESdatos	07/07/2018 14:36	.symlink	0 KB
Imágenes	datos	07/07/2018 15:24	Documento de tex...	518 KB
Música	datos.encrypted	07/07/2018 14:38	Archivo ENCRYPT...	518 KB
Videos	contra	02/07/2018 10:42	Documento de tex...	1 KB

Fig. 85 Archivos descifrados [Fuente Propia]

## Fase 7. Obtener conclusiones y/o recomendaciones con base a la solución propuesta

- Al trasmisir archivos por una red LAN el tamaño apropiado y recomendado es alrededor de 240,00 MB la transmisión se realiza de forma rápida y efectiva en no más de un minuto.
- Se provoca congestión de la red al trasmisir archivos de 300 MB, ocupa la capacidad del router generando fallos en la red wifi o cableada.
- Un ataque pasivo realizado a una red LAN muestra paquetes SAMBA, estos paquetes se crean al momento de trasmisir los ficheros principales, de tal manera se puede observar su nombre (**Ver Anexo 12**) (**Ver Anexo 13**), pero no su contenido.
- Un receptor puede tener problemas si no configura su red para la transmisión de archivos sin clave o si tiene un antivirus activado.
- La transmisión de la clave por compartición de archivos, no es recomendada porque en un ataque pasivo se podría observar su contenido sin problema alguno.

## **g. DISCUSIÓN**

El presente trabajo de titulación denominado “**DESARROLLO DE UN PROTOTIPO DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA TÉCNICA DE ESTEGANOGRÁFÍA EN LA CAPA DE RED**” se culminó planteando, desarrollando y ejecutado el prototipo de seguridad de la información en la red.

Con la aplicación de métodos, técnicas y la metodología de ingeniería, se pudo concluir en su totalidad con el objetivo general y los objetivos específicos, a continuación, se detallada el cumplimiento de cada uno:

### **Objetivo 1: Analizar las funcionalidades y características de esteganografía en la actualidad, ADS y capa de red**

El desarrollo adecuado de este objetivo se dividió en dos partes, la primera se enfocó en obtener las funcionalidades y características de esteganografía en la actualidad realizando una revisión bibliográfica en la sección (d), literal 2, con el objetivo de encontrar casos de éxito en que se hayan aplicado la esteganografía, así mismo se realizó una demostración en la literal 8 sobre la aplicación de esteganografía en archivos digitales.

En la segunda parte en la sección (d), literal 10 y literal 11 se realizó el estado del arte, del flujo alternativo de datos (ADS) y la capa de red, con el propósito de obtener características y funcionalidades en base a la seguridad de la información.

### **Objetivo 2: Desarrollar el prototipo de esteganografía de red enfocándose en el protocolo ICMP y en los ADS**

Para el desarrollo de este objetivo se plantearon tres factores importes, el primer factor se basa en la sección (d) literal 1, en donde se realiza un estudio de los problemas existentes en la actualidad sobre la seguridad de la información, con el fin de obtener bases para plantear la problemática, en el segundo factor se aplicó la técnica de la encuesta (**Ver Anexo 1**) al personal de la Universidad Nacional de Loja, la encuesta tuvo como objetivo determinar el sistema operativo en el que se aplicara el prototipo de seguridad, obteniendo como resultado el sistema operativo Microsoft Windows (**Ver Anexo 2**) y en el tercer factor se basa en el estudio y la aplicación de la metodología de ingeniería [42] esta metodología

permitió realizar la combinación del método de esteganografía de red aplicada al protocolo ICMP, el método de flujo alternativo de datos (ADS) aplicado a los archivos que contienen información y agrego el método de criptografía simétrica al desarrollo del prototipo logrando un grado de seguridad mayor al que se tenía previsto.

**Objetivo 3: Realizar un plan de pruebas para el prototipo de esteganografía en una red LAN**

El desarrollo de este objetivo se realiza ejecutando la Fase 5 (Realizar un experimento apropiado para confirmar que la solución propuesta al problema es efectiva y eficiente) de la metodología de ingeniería [42]. Esta fase tiene en si un plan de pruebas estructurado en las fases anteriores, lo que se realiza en esta fase es ejecutar los experimentos correspondientes del prototipo en una red LAN, con el único propósito de determinar si el prototipo aporta un grado de seguridad a la información, todo el proceso de experimentos se lo realizó en el laboratorio de redes y sistemas operativos del bloque 12, de la Facultad de Energía, las Industrias y los Recursos Naturales No Renovables, de la Universidad Nacional de Loja (**Ver Anexo 14**).

## **h. CONCLUSIONES**

- Actualmente la información que se trasmite por la red de la Universidad Nacional de Loja, no se le proporciona la seguridad adecuada para proteger la integridad de los datos, el prototipo desarrollado en el presente trabajo de titulación proporciona un cierto grado de seguridad en la transmisión de la información. La esquematización del documento, permitirá a los usuarios utilizar el prototipo para trasmitir información en una red LAN con mayor seguridad.
- La revisión bibliográfica y el uso de la metodología de ingeniería, contribuyo a identificar falencias en el prototipo, por tal razón se adiciono la técnica de criptografía logrando obtener resultados positivos.
- La combinación de técnicas proporciono al prototipo tener mayor seguridad ante un ataque pasivo, cada técnica tuvo un propósito específico, la técnica de criptografía hizo uso de la criptografía simétrica teniendo como finalidad cifrar los datos de los archivos por medio de una clave y la técnica de esteganografía hizo uso de flujo alternativo de datos cuyo propósito fue ocultar los archivos cifrados en un portador.
- El uso de esteganografía de red, solventa la problemática que se genera en la criptografía simétrica, dicha problemática consiste en que una persona ajena al emisor o receptor pueda obtener la clave con la que se cifraron los archivos, por tal motivo la esteganografía de red oculta la clave en un protocolo de la capa de red, de esta manera la clave pasa desapercibida ante una tercera persona.
- La transmisión de la clave y los archivos se efectuó sin problema alguno, evadiendo un ataque pasivo, lo que demuestra que el prototipo desarrollado proporciona un cierto grado de seguridad a la información que se trasmite por la red.
- En base al plan de pruebas establecido se determinó que el tamaño ideal de un archivo para ser trasmitir por la red, de manera rápida y efectiva con un tiempo menor a un minuto es alrededor de 240,00 MB, al sobrepasar este tamaño los archivos de igual manera se trasmitirán, pero en un mayor tiempo trayendo consigo problemas de congestión en la red.

## **i. RECOMENDACIONES**

Al establecer los objetivos de un proyecto no siempre contemplamos lo necesario de tal manera se prestan dificultades o impedimentos para el desarrollo del mismo. A continuación, se detallan algunas recomendaciones que serán de utilidad en futuros trabajos:

- Trasmitir los archivos y la clave a un receptor a la vez, para prevenir congestionamiento de red o que la transmisión sea incompleta.
- Instalar herramientas de software Python 2.7 y Wipcap 4.1.3 en lado del emisor, con el propósito de no presentar problemas al utilizar el método de esteganografía de red en la aplicación de Scapy.
- En trabajos futuros se recomienda, sistematizar el proceso que realiza el prototipo en un lenguaje de programación o aplicación móvil.
- Orientar el prototipo a dar solución a diferentes ataques que se realiza en la red como son: ataque activo, negación de servicio(DOS), *phishing*, etc.
- Realizar un estudio sobre la criptografía asimétrica, de forma que se pueda implementar al prototipo, con la finalidad de lograr obtener mayor robustez en la seguridad de la información.

## **j. BIBLIOGRAFÍA**

- [1] E. Escuela Nacional de Minas (Colombia), D. Universidad Nacional de Colombia. Sede de Medellín. Facultad Nacional de Minas., G. Aponte-Mayor, and L. A. Betancourt-Buitrago, *Dyna.*, vol. 81, no. 184. Universidad Nacional de Colombia, 2014.
- [2] T. Farral, “The attribution problem with information security attacks,” *Netw. Secur.*, vol. 2017, no. 5, pp. 17–19, May 2017.
- [3] Proofpoint, “Q118 Quarterly Threat Report,” pp. 1–16, 2018.
- [4] by Cynerio, “Healthcare Hacking Trends on the Dark Web | Cynerio,” *11 de Junio*, 2018. [Online]. Available: <http://cynerio.co/healthcare-hacking-trends-dark-web/>. [Accessed: 15-Jun-2018].
- [5] Catalin Cimpanu, “Hacker Breaches Syscoin GitHub Account and Poisons Official Client,” *15 the June*, 2018. [Online]. Available: <https://www.bleepingcomputer.com/news/security/hacker-breaches-syscoin-github-account-and-poisons-official-client/>. [Accessed: 15-Jun-2018].
- [6] I. Dragos, “DYMALLOY,” *14 June*, 2018. [Online]. Available: <https://www.dragos.com/blog/20180614Dymalloy.html>. [Accessed: 15-Jun-2018].
- [7] Breaches and Incidents, “HealthEquity hit by data breach affecting 23,000 employees and customers.” [Online]. Available: <https://cyware.com/news/healthequity-hit-by-data-breach-affecting-23000-employees-and-customers-f2b1809a>. [Accessed: 15-Jun-2018].
- [8] A. A. A. El-Latif, B. Abd-El-Atty, M. S. Hossain, S. Elmougy, and A. Ghoneim, “Secure Quantum Steganography Protocol for Fog Cloud Internet of Things,” *IEEE Access*, vol. 6, pp. 10332–10340, 2018.
- [9] R. Das and P. Chatterjee, “Securing Data Transfer in IoT Employing an Integrated Approach of Cryptography & Steganography,” in *Proceedings of the International Conference on High Performance Compilation, Computing and Communications - HP3C-2017*, 2017, pp. 17–22.
- [10] F. Lehner, W. Mazurczyk, J. Keller, and S. Wendzel, “Inter-Protocol Steganography for Real-Time Services and Its Detection Using Traffic Coloring Approach,” in *2017 IEEE 42nd Conference on Local Computer Networks (LCN)*, 2017, pp. 78–85.
- [11] I. Nechta, “Steganography in social networks,” in *2017 Siberian Symposium on Data Science and Engineering (SSDSE)*, 2017, pp. 33–35.
- [12] O. I. Abdullaziz, V. T. Goh, H.-C. Ling, and K. Wong, “AIPISSteg: An active IP identification based steganographic method,” *J. Netw. Comput. Appl.*, vol. 63, pp. 150–158, Mar. 2016.
- [13] M. M. Aljamea, C. S. Iliopoulos, and M. Samiruzzaman, “Detection Of URL In Image Steganography,” in *Proceedings of the International Conference on Internet of things and*

- Cloud Computing - ICC '16*, 2016, pp. 1–6.
- [14] G. Bugar and D. Levicky, “Steganography in data networks based on PDU retransmission,” in *2016 International Symposium ELMAR*, 2016, pp. 127–131.
  - [15] A. Sekhar, M. K. G., and M. A. Rahiman, “A Novel Approach for Hiding Data in Videos Using Network Steganography Methods,” *Procedia Comput. Sci.*, vol. 70, pp. 764–768, Jan. 2015.
  - [16] H. Tian *et al.*, “Optimal matrix embedding for Voice-over-IP steganography,” *Signal Processing*, vol. 117, pp. 33–43, Dec. 2015.
  - [17] S. Bobade and R. Goudar, “Secure Data Communication Using Protocol Steganography in IPv6,” in *2015 International Conference on Computing Communication Control and Automation*, 2015, pp. 275–279.
  - [18] “ISO - International Organization for Standardization.” [Online]. Available: <https://www.iso.org/home.html>. [Accessed: 30-Apr-2018].
  - [19] “ISO 27001 - Software ISO 27001 de Sistemas de Gestión.” [Online]. Available: <https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/>. [Accessed: 01-May-2018].
  - [20] J. Areitio Bertolín, *Seguridad de la información : redes, informática y sistemas de información*. Paraninfo Cengage Learning, 2008.
  - [21] G. G. Paredes, 3150954, and rn, “Introducción a la Criptografía,” *1607 - 6079*, Jul. 2006.
  - [22] M. M. H. A. Median Yuri Tatiana, “Comparación de algoritmos basados en la criptografía simétrica DES, AES y 3DES,” 9th ed., 2015.
  - [23] “Cómo funciona la firma digital | Víctor Iglesias.” [Online]. Available: <https://www.victoriglesias.net/como-funciona-la-firma-digital/>. [Accessed: 05-May-2018].
  - [24] “OpenSSL Cryptography and SSL/TLS Toolkit.” [Online]. Available: <https://www.openssl.org/docs/>. [Accessed: 11-Jul-2018].
  - [25] B. A. M. Navarro Naranjo Victor Adolfo, “Estenografía en contenido multimedia,” 2007.
  - [26] N. Jasper, “História, Técnica e Classificação de Algoritmos Esteganográficos,” 2009.
  - [27] C. Qin, W. Zhou, W. Zhang, and N. Yu, “Ensemble Steganography,” in *2018 IEEE Third International Conference on Data Science in Cyberspace (DSC)*, 2018, pp. 582–587.
  - [28] B. Cristian, C. Daniel, and G. Ignacio, “Booteo con Sistema de Archivos NTFS.”
  - [29] “Introducción a los sistemas de archivos FAT, HPFS y NTFS.” [Online]. Available: <https://support.microsoft.com/es-es/help/100108/overview-of-fat-hpfs-and-ntfs-file-systems>. [Accessed: 15-May-2018].
  - [30] M. Broomfield, “NTFS Alternate Data Streams: focused hacking,” *Netw. Secur.*, vol. 2006,

- no. 8, pp. 7–9, Aug. 2006.
- [31] S. By, R. Mahajan, M. Singh, and S. Miglani, “Design and Development of Improved Stealth Alternate Data Streams,” 2014.
  - [32] R. Rios and J. A. Onieva, “Clasificacion de canales encubiertos. Un nuevo canal: Covert\_DHCP,” *Actas la X Reun. Espa{ñ}ola sobre Criptologia y Segur. la Inf.*, pp. 325–336, 2008.
  - [33] M. H. Gabriel Tolosa and M. K. Powell, “Protocolos y Modelo OSI.”
  - [34] CISCO, “Capa de red.”
  - [35] C. Marina del Rey, “RFC 791 PROTOCOLO INTERNET,” *Information Sciences Institute University of Southern California*. [Online]. Available: <https://www.rfc-es.org/rfc/rfc0791-es.txt>. [Accessed: 06-Jun-2018].
  - [36] J Postel PROTOCOLO DE MENSAJES DE CONTROL INTERNET, “RFC 792.” [Online]. Available: <https://www.rfc-es.org/rfc/rfc0792-es.txt>. [Accessed: 06-Jun-2018].
  - [37] M. U. Y. Valiosa, “CURSO DE TCP / IP : ICMP ( Protocolo de Mensajes de Control de Internet ),” *Control*.
  - [38] E. S. Carlos Caldera, “Módulo II: Redes de datos.,” .
  - [39] C. 90291 Marina del Rey, “RFC 793 Protocolo de Control de Transmisión.” [Online]. Available: <https://www.rfc-es.org/rfc/rfc0793-es.txt>. [Accessed: 11-Jun-2018].
  - [40] CISCO, “Información general de TCP/IP.”
  - [41] L. A. S. I. Y. Los, *Desarrollo de una aplicación web de adopción de mascotas en la ciudad de loja*. 2017.
  - [42] D. C. Montgomery and G. C. Runger, *Probabilidad y estadística aplicadas a la ingeniería*. Limusa-Wiley, 2004.
  - [43] A. Angel, “Criptografía Para Principiantes José de Jesús Angel Angel,” pp. 1–59.
  - [44] A. Pousa, V. M. Sanz, and A. E. De Giusti, “Análisis de rendimiento de un algoritmo de criptografía simétrica sobre arquitecturas multicore,” 2011.
  - [45] H. Corrales Sánchez, “Criptografía y Métodos de Cifrado,” pp. 119–134, 2012.
  - [46] M. F. Borja, “Análisis de tráfico con Wireshark,” p. 52, 2011.
  - [47] “Scapy.” [Online]. Available: <https://scapy.net/>. [Accessed: 04-Aug-2018].

## **k. ANEXOS**

### **Anexo 1: Encuesta a la comunidad que trabaja en la Universidad Nacional de Loja**

#### **DESARROLLO DE UN PROTOTIPO DE SEGURIDAD DE LA INFORMACIÓN APlicando LA TÉCNICA DE ESTEGANOGRÁFÍA EN LA CAPA DE RED**

La siguiente encuesta permitirá obtener información fundamental que ayudará a tener un panorama más claro en la aplicación del prototipo de seguridad de la información en la red.

\*Obligatorio

1. Dirección de correo electrónico \*

---

2. ¿Qué Sistema Operativo utiliza en sus labores diarias?

Marca solo un óvalo.

- Microsoft Windows
- GNU/Linux
- Mac OS
- Otro

3. A utilizado la red de internet para trasmisir información confidencial a través de redes sociales (Facebook, WhatsApp, Twitter), correos o en carpetas compartidas \*

Marca solo un óvalo.

- Sí
- No

4. ¿Qué mecanismo de seguridad posee su sistema informático para proteger la información que transmite por la red de internet? \*

Marca solo un óvalo.

- Sistema de seguridad privado
- Encripta la información
- Aplica esteganografía de red
- Confío en la red
- Ninguno

5. ¿Sería necesario para usted que la información que se transmite a través de la red de internet tenga un mecanismo de seguridad más robusto? \*

Marca solo un óvalo.

- Si
- No

6. Tiene algún conocimiento sobre esteganografía de red \*

Marca solo un óvalo.

- Conocimiento Alto
- Conocimiento Medio
- Ningun Conocimiento

7. Tiene algún conocimiento sobre criptografía \*

Marca solo un óvalo.

- Conocimiento Alto
- Conocimiento Medio
- Ningun Conocimiento

**8. A utilizado el Flujo Alternativo de Datos (ADS) para ocultar información en el Sistema Operativo Windows \***

*Marca solo un óvalo.*

- Si
- No

**9. Tiene algún conocimiento del ataque pasivo (Análisis de tráfico de datos) en la red de internet**

*Marca solo un óvalo.*

- Conocimiento Alto
- Conocimiento Medio
- Ningun conocimiento

**10. A utilizado Opens SSL para encriptar archivos \***

*Marca solo un óvalo.*

- Si
- No

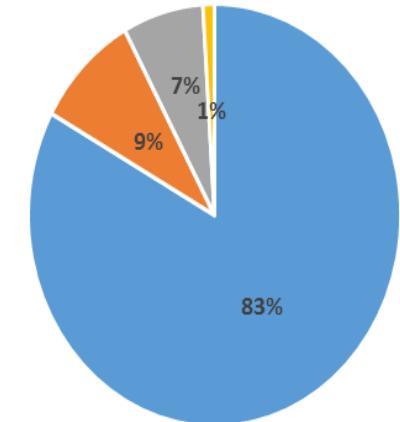
**11. Utilaría un mecanismo que combine criptografía y esteganografía, con el fin de brindar seguridad a lo información que desea enviar por la red \***

*Marca solo un óvalo.*

- Sí
- No
- Tal vez

**Anexo 2: Estadística de la pregunta 1 de la encuesta “¿Qué Sistema Operativo utiliza en sus labores diarias?”**

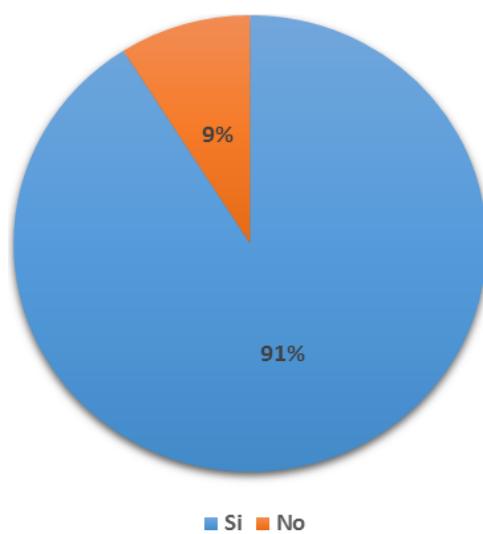
Preguntas 1		
Opciones	Personal	Porcentaje
Microsoft Windows	83	83.8%
GNU/Linux	9	09.1%
Mac OS	7	07.1%
Otro	1	01.0%
<b>TOTAL</b>	<b>100</b>	<b>100%</b>



■ Microsoft Windows ■ GNU/Linux ■ Mac OS ■ Otro

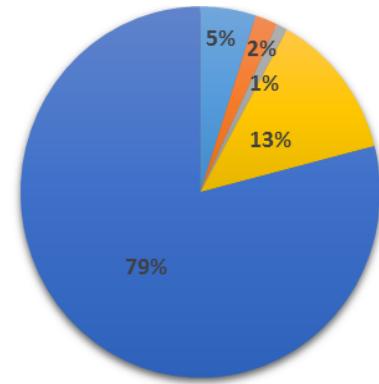
**Anexo 3: Estadística de la pregunta 2 de la encuesta “A utilizado la red de internet para trasmisir información confidencial a través de redes sociales (Facebook, WhatsApp, Twitter), correos o en carpetas compartidas”**

Preguntas 2		
Opciones	Personal	Porcentaje
Si	91	91.0%
No	9	09.0%
<b>TOTAL</b>	<b>100</b>	<b>100%</b>



**Anexo 4: Estadística de la pregunta 3 de la encuesta “¿Qué mecanismo de seguridad posee su sistema informático para proteger la información que transmite por la red de internet?”**

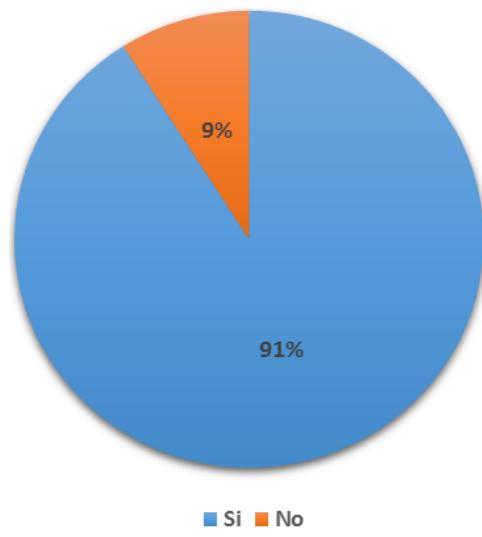
Preguntas 3		
Opciones	Personal	Porcentaje
Sistema de seguridad privado	5	05.0%
Cifra la información	2	02.0%
Aplica esteganografía de red	1	01.0%
Confió en la red	13	13.0%
Ninguno	79	79.0%
<b>TOTAL</b>	100	100%



■ Sistema de seguridad privado    ■ Cifra la información  
■ Aplica esteganografía de red    ■ Confió en la red  
■ Ninguno

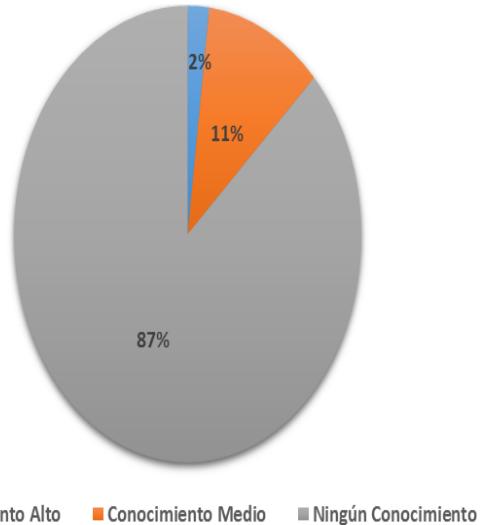
**Anexo 5: Estadística de la pregunta 4 de la encuesta “¿Sería necesario para usted que la información que se transmite a través de la red de internet tenga un mecanismo de seguridad más robusto?”**

Preguntas 4		
Opciones	Personal	Porcentaje
Si	91	91.0%
No	9	09.0%
<b>TOTAL</b>	100	100%



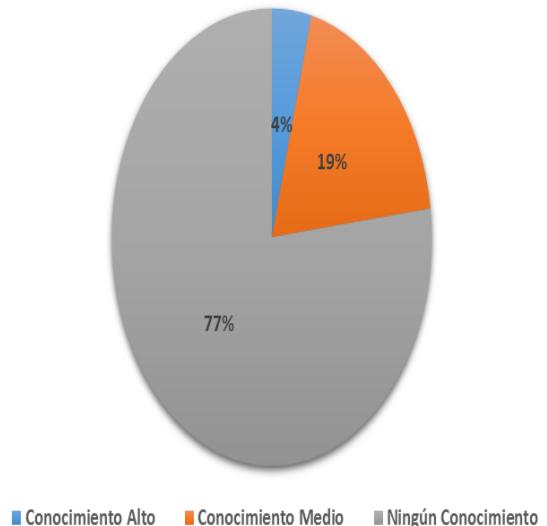
**Anexo 6: Estadística de la pregunta 5 de la encuesta “Tiene algún conocimiento sobre esteganografía de red”**

Preguntas 5		
Opciones	Personal	Porcentaje
Conocimiento Alto	2	02.0%
Conocimiento Medio	11	11.0%
Ningún Conocimiento	87	87.0%
<b>TOTAL</b>	<b>100</b>	<b>100%</b>



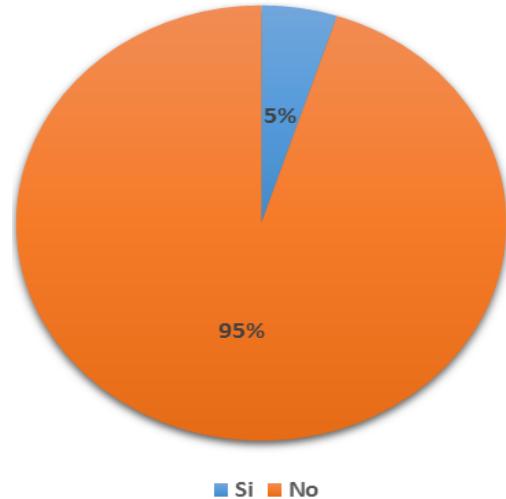
**Anexo 7: Estadística de la pregunta 6 de la encuesta “Tiene algún conocimiento sobre criptografía”**

Preguntas 6		
Opciones	Personal	Porcentaje
Conocimiento Alto	4	04.0%
Conocimiento Medio	19	19.0%
Ningún Conocimiento	77	77.0%
<b>TOTAL</b>	<b>100</b>	<b>100%</b>



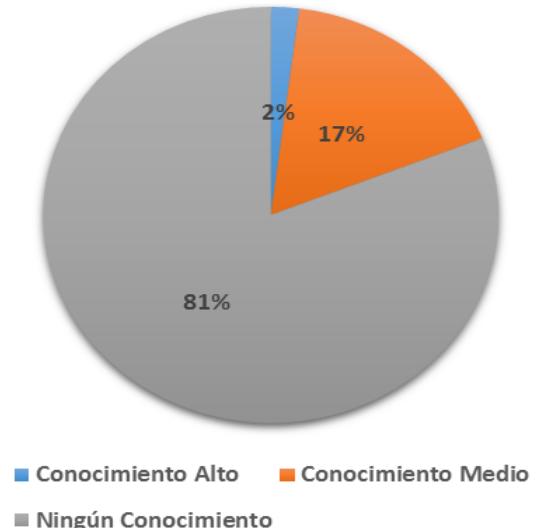
**Anexo 8: Estadística de la pregunta 7 de la encuesta “A utilizado el Flujo Alternativo de Datos (ADS) para ocultar información en el Sistema Operativo Windows”**

Preguntas 7		
Opciones	Personal	Porcentaje
Si	5	05.0%
No	95	95.0%
<b>TOTAL</b>	<b>100</b>	<b>100%</b>



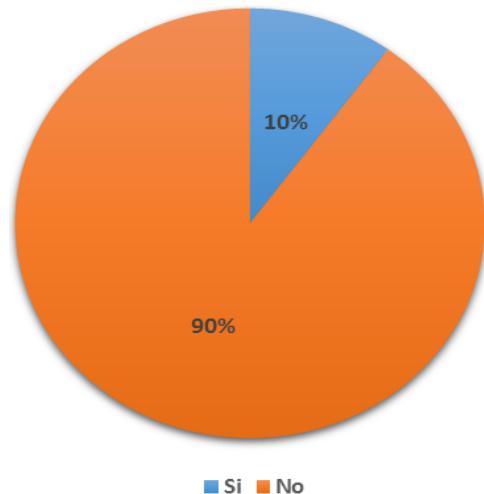
**Anexo 9: Estadística de la pregunta 8 de la encuesta “Tiene algún conocimiento del ataque pasivo (Análisis de tráfico de datos) en la red de internet”**

Preguntas 8		
Opciones	Personal	Porcentaje
Conocimiento Alto	2	02.0%
Conocimiento Medio	17	17.0%
Ningún Conocimiento	81	81.0%
<b>TOTAL</b>	<b>100</b>	<b>100%</b>



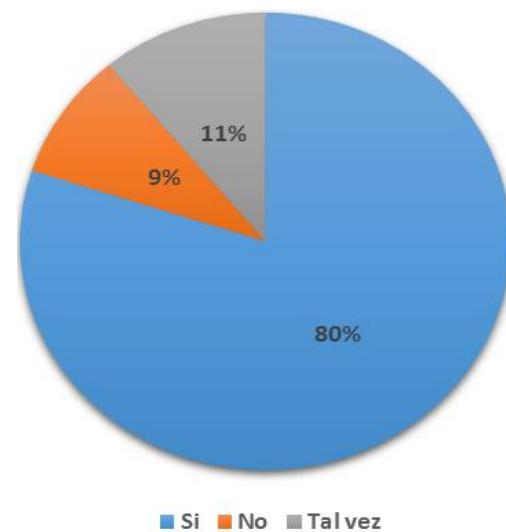
**Anexo 10: Estadística de la pregunta 9 de la encuesta “A utilizado Opens SSL para cifrar archivos”**

Preguntas 9		
Opciones	Personal	Porcentaje
Si	10	10.0%
No	90	90.0%
<b>TOTAL</b>	<b>100</b>	<b>100%</b>



**Anexo 11: Estadística de la pregunta 10 de la encuesta “Utilizaría un mecanismo que combine criptografía y esteganografía, con el fin de brindar seguridad a lo información que desea enviar por la red”**

Preguntas 10		
Opciones	Personal	Porcentaje
Si	80	80.0%
No	9	09.0%
Tal vez	11	11.0%
<b>TOTAL</b>	<b>100</b>	<b>100%</b>



## Anexo 12: Generación de protocolo samba “SMB2” al transmitir ADS en versión IPV4

Destination	Protocol	Length	Info
192.168.1.10	SMB2	386	Create Response File: Fichero_principal_ejecutable.txt
192.168.1.20	SMB2	275	GetInfo Request FS_INFO/FileFsVolumeInformation File: Fichero_principal_ejecutable.txt;GetInfo Request FS_INFO/File...
192.168.1.10	SMB2	250	GetInfo Response;GetInfo Response
192.168.1.20	SMB2	162	SetInfo Request FILE_INFO/SMB2_FILE_ENDOFFILE_INFO File: Fichero_principal_ejecutable.txt
192.168.1.10	SMB2	124	SetInfo Response
192.168.1.20	SMB2	249	Write Request Len:79 Off:0 File: Fichero_principal_ejecutable.txt
192.168.1.10	SMB2	138	Write Response
192.168.1.20	SMB2	330	Create Request File:
192.168.1.10	SMB2	298	Create Response File:
192.168.1.20	SMB2	146	Close Request File:
192.168.1.10	SMB2	182	Close Response
192.168.1.20	SMB2	410	Create Request File: Fichero_principal_ejecutable.txt:ADSdestroyo.encrypted
192.168.1.10	SMB2	298	Create Response File: Fichero_principal_ejecutable.txt:ADSdestroyo.encrypted
192.168.1.20	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: Fichero_principal_ejecutable.txt:ADSdestroyo.encrypted
192.168.1.10	SMB2	186	GetInfo Response
192.168.1.20	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: Fichero_principal_ejecutable.txt:ADSdestroyo.encrypted

## Anexo 13: Generación de protocolo samba “SMB2” al transmitir ADS en versión IPV6

Destination	Protocol	Length	Info
fdf7:7226:1117:0:a91a:d47a:cc9b:9fb4	SMB2	318	Create Response File: Proyecto_Tesis.txt:ADS_Tesis.encrypted
fdf7:7226:1117:0:20c9:92e:b63b:af00	SMB2	182	GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: Proyecto_Tesis.txt:ADS_Tesis.encrypted
fdf7:7226:1117:0:a91a:d47a:cc9b:9fb4	SMB2	206	GetInfo Response
fdf7:7226:1117:0:20c9:92e:b63b:af00	SMB2	182	GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: Proyecto_Tesis.txt:ADS_Tesis.encrypted
fdf7:7226:1117:0:a91a:d47a:cc9b:9fb4	SMB2	206	GetInfo Response
fdf7:7226:1117:0:20c9:92e:b63b:af00	SMB2	182	GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: Proyecto_Tesis.txt:ADS_Tesis.encrypted
fdf7:7226:1117:0:a91a:d47a:cc9b:9fb4	SMB2	206	GetInfo Response
fdf7:7226:1117:0:20c9:92e:b63b:af00	SMB2	182	GetInfo Request FS_INFO/FileFsSizeInformation File: Proyecto_Tesis.txt:ADS_Tesis.encrypted
fdf7:7226:1117:0:a91a:d47a:cc9b:9fb4	SMB2	174	GetInfo Response
fdf7:7226:1117:0:20c9:92e:b63b:af00	SMB2	182	SetInfo Request FILE_INFO/SMB2_FILE_ENDOFFILE_INFO File: Proyecto_Tesis.txt:ADS_Tesis.encrypted
fdf7:7226:1117:0:a91a:d47a:cc9b:9fb4	SMB2	144	SetInfo Response
fdf7:7226:1117:0:20c9:92e:b63b:af00	SMB2	1294	Write Request Len:65536 Off:0 File: Proyecto_Tesis.txt:ADS_Tesis.encrypted [TCP segment of a reassembled PDU]
fdf7:7226:1117:0:a91a:d47a:cc9b:9fb4	SMB2	158	Write Response
fdf7:7226:1117:0:20c9:92e:b63b:af00	SMB2	838	Write Request Len:65536 Off:65536 File: Proyecto_Tesis.txt:ADS_Tesis.encrypted
fdf7:7226:1117:0:a91a:d47a:cc9b:9fb4	SMB2	158	Write Response
fdf7:7226:1117:0:20c9:92e:b63b:af00	SMB2	1066	Write Request Len:65536 Off:131072 File: Proyecto_Tesis.txt:ADS_Tesis.encrypted
fdf7:7226:1117:0:a91a:d47a:cc9b:9fb4	SMB2	158	Write Response
fdf7:7226:1117:0:20c9:92e:b63b:af00	SMB2	1066	Write Request Len:65536 Off:196608 File: Proyecto_Tesis.txt:ADS_Tesis.encrypted
fdf7:7226:1117:0:a91a:d47a:cc9b:9fb4	SMB2	158	Write Response
fdf7:7226:1117:0:20c9:92e:b63b:af00	SMB2	1066	Write Request Len:65536 Off:262144 File: Proyecto_Tesis.txt:ADS_Tesis.encrypted

## Anexo 14: Permiso por parte de la Carrera de Ingeniería en Sistemas para realizar los experimentos del prototipo



## Anexo 15: Artículo