



**FACULTAD DE INGENIERÍA, ARQUITECTURA Y
URBANISMO**

**ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA
DE SISTEMAS**

TESIS

**COMPARACIÓN DE ALGORITMOS DE
ENCRIPCIÓN PARA LA TRANSFERENCIA DE
ARCHIVOS EN MENSAJERIA INSTANTANEA**

**PARA OPTAR EL TÍTULO PROFESIONAL DE
INGENIERO DE SISTEMAS**

Autor:

**Bach. Montenegro Torres Domel
ORCID: <https://orcid.org/0000-0001-6424-474X>**

Asesor:

**Mg. Cachay Maco Junior Eugenio
ORCID: <https://orcid.org/0000-0003-4056-3142>**

Línea de Investigación

Infraestructura, Tecnología y Medio Ambiente

Pimentel – Perú 2020

Comparación de algoritmos de encriptación para la transferencia de archivos en mensajería instantánea

Aprobación del Jurado

Dr. Ramos Moscol Mario Fernando
Presidente del jurado de tesis

Ing. Mejía Cabrera, Heber Ivan
Secretario del jurado de tesis

Bances Saavedra, David Enrique
Vocal del jurado de tesis

DEDICATORIA

A Dios por darme la vida y la salud y a mi familia por su valioso apoyo para seguir contribuyendo en la tarea educativa y lograr las metas trazadas.

AGRADECIMIENTO

En primer lugar agradecer a Dios por darme la oportunidad de llegar hasta este momento que es muy importante en mi vida, y lograr otra meta más que es la culminación de mi carrera.

Agradecer a toda mi familia en especial a mis hijos Jheamy y Fabián que son una de mis fuentes de fortaleza para seguir siempre adelante, Dios los bendiga, los ilumine y los cuide siempre.

Quiero darles gracias a todos los ingenieros de la Universidad Señor de Sipán que hicieron de mí un buen profesional y una mejor persona, sobre todo con sus consejos, su paciencia y opiniones; por su apoyo incondicional en la realización de esta tesis de investigación.

Finalmente agradezco a mis compañeros de grupo, porque la constante comunicación con ellos ha contribuido en gran medida a transformar y mejorar este trabajo de investigación.

RESUMEN

Esta investigación está basada especialmente en la seguridad informática, donde se realiza la comparación de algoritmos de encriptación en la transferencia de mensajería instantánea de un servidor de protocolo seguro de transferencia de archivos (SFTP) a un terminal. Asimismo, está a la vanguardia con las actualizaciones tecnológicas que solicitan las grandes corporaciones empresariales actuales, en constantes ocasiones existe fragilidad en la transmisión de los datos mediante los dispositivos tecnológicos cuando nos conectamos en una red o el internet, ya que tenemos personas que se benefician de la vulnerabilidad con la finalidad de obtener ganancias personales. Por tal razón esta tesis se ha encaminado en desarrollar un análisis de comparación de los algoritmos criptográficos que se usan en los servidores en la transferencia de datos en una red pública, el problema fundamental está en garantizar la seguridad e integridad de los datos al momento de conectamos en una gran red de objetos físicos.

Esta investigación se logró haciendo una selección de algoritmos de encriptación e implementándolo en un servidor SFTP, donde se desarrolló el análisis de encriptación de cada uno de los algoritmos en la transferencia de información con la captura de tráfico entre el servidor y el cliente. De esta manera se observó y analizo cuál de los algoritmos brindaba mayor seguridad e integridad de la información. La metodología utilizada es experimental, se utilizó este método porque permite la manipulación de variables, de esta manera se conoció el tipo de encriptación de cada uno de los algoritmos con respecto al tamaño de paquetes, nivel de encriptación y no encriptación y tiempo de envío. Obteniendo como resultado que el algoritmo Advanced Encryption Standard (AES) fracciona los datos en menor cantidad de paquetes necesitando menos tiempo para remitirlos comparándolos con otros algoritmos. En paquetes encriptados el algoritmo AES muestra mayor cantidad de paquetes encriptados y la cantidad de paquetes no encriptados es menor.

Palabras clave: Análisis, Encriptación, Algoritmos, Vulnerabilidad, Integridad, Seguridad, Transferencia de Archivo y Protocolo.

ABSTRACT

This research is especially based on computer security, where the comparison of encryption algorithms is performed in the transfer of instant messaging from a secure file transfer protocol (SFTP) server to a terminal. Likewise, it is at the forefront with the technological updates requested by the current large business corporations, on constant occasions there is fragility in the transmission of data through technological devices when we connect to a network or the Internet, since we have people who benefit vulnerability in order to obtain personal gain. For this reason this thesis has been aimed at developing a comparison analysis of the cryptographic algorithms that are used on servers in the transfer of data in a public network, the fundamental problem is to guarantee the security and integrity of the data at the time we connect in a large network of physical objects.

This research was achieved by making a selection of encryption algorithms and implementing it on an SFTP server, where the encryption analysis of each of the algorithms in the transfer of information with the capture of traffic between the server and the client was developed. In this way it was observed and analyzed which of the algorithms provided greater security and integrity of the information. The methodology used is experimental, this method was used because it allows the manipulation of variables, in this way the type of encryption of each of the algorithms with respect to the size of packets, level of encryption and non-encryption and time of sending was known. As a result, the Advanced Encryption Standard (AES) algorithm divides the data into fewer packets and takes less time to send them compared to the other algorithms. Regarding the encrypted packets, the AES algorithm has the highest number of encrypted packets and the least number of non-encrypted packets.

Keywords: Analysis, Encryption, Algorithms, Vulnerability, Integrity, Security, File Transfer and Protocol.

ÍNDICE

I. INTRODUCCIÓN	14
1.1 Realidad Problemática	14
1.2 Antecedentes de Estudio	20
1.2.1 A Nivel Mundial	20
1.3 Teorías Relacionadas al Tema.....	22
1.3.1 Norma ISO 27001.....	22
1.3.2 Comunicación Segura	22
1.3.3 Seguridad de la Información	24
1.3.4 Algoritmo.....	24
1.3.5 La Criptografía.....	27
1.3.6 Transferencia de Archivo en Red.....	28
1.3.7 Protocolo Seguro de Transferencia de Archivos (SFTP).....	28
1.3.8 Protocolo Secure SHell (SSH)	29
1.3.9 Software para Configurar el Servidor SFTP.....	31
1.3.10Software para Capturar Tráfico de Red.....	37
1.3.11Software para Conectar Cliente Servidor SFTP	38
1.3.12Software para Conteo de Paquetes Encriptados y no Encriptados	38
1.3.13Firmas Digitales.....	39
1.3.14Ataques Informáticos	40

1.4	Definición de la Terminología	42
1.4.1	Criptografía (Cifrado de datos)	42
1.4.2	Criptoanálisis	42
1.4.3	Encriptado.....	42
1.4.4	Clave Privada.....	42
1.4.5	Clave Publica	42
1.4.6	Protocolo SFTP.....	43
1.4.7	Protocolo SSH.....	43
1.4.8	Transferencia de Archivos en Red	43
1.4.9	Mensajería Instantánea.....	43
1.4.10	Hash	43
1.4.11	Algoritmo de Hash Seguro (SHA)	44
1.4.12	Diffie Hellman	44
1.4.13	Advanced Encryption Standard (AES).....	44
1.4.14	Data Encryption Standard (3DES)	44
1.4.15	Rivest Cypher 4 (RC4).....	44
1.4.16	Internet.....	44
1.5	Formulación del Problema	45
1.6	Justificación e Importancia del Estudio	45
1.7	Hipótesis	45

1.8	Objetivos.....	46
1.8.1	Objetivo General.....	46
1.8.2	Objetivos Específicos.....	46
II.	MATERIAL Y MÉTODO.....	47
2.1	Tipo y Diseño de Investigación.....	47
2.1.1	Tipo de Investigación.....	47
2.1.2	Diseño de la Investigación.....	47
2.2	Población y Muestra.....	48
2.3	Variables, Operacionalización.....	49
2.3.1	Variable Independiente.....	49
2.3.2	Variable Dependiente.....	49
2.3.3	Operacionalización.....	49
2.4	Técnicas e Instrumentos de Recolección de Datos, Validez y Confiabilidad.....	50
2.4.1	Técnicas de Recolección de Datos.....	50
2.4.2	Instrumentos de Recolección de Datos.....	50
2.4.3	Procedimiento Para la Recolección de Datos.....	50
2.5	Procedimiento de Análisis de Datos.....	51
2.6	Criterios Éticos.....	52
2.7	Criterios de Rigor Científico.....	52
III.	RESULTADOS.....	54

3.1	Resultado en Tablas y Figuras.....	54
3.1.1	Evaluación Cuantitativa de los Algoritmos	54
3.1.2	Resume de Evaluación Cuantitativa de los Algoritmos	62
3.2	Discusión de Resultados	63
3.3	Aporte Práctico	65
3.3.1	Selección de Algoritmos Criptográficos para la Transferencia de Archivos en el Mercado Tecnológico.	65
3.3.2	Diseñar un Escenario de Prueba para la Transferencia de Archivos de Forma Segura	66
3.3.3	Construcción del Prototipo de Implementación de Algoritmos de Encriptación.	68
3.3.4	Realización de Pruebas de Funcionamiento de los Algoritmos de Encriptación	71
3.3.5	Comprobación de conectividad entre Host.....	81
3.3.6	Configuración de los Algoritmos en el Servidor SFTP	82
3.3.7	Pruebas de Funcionamiento de los Algoritmos de Encriptación.....	84
IV:	CONCLUSIONES Y RECOMENDACIONES	99
4.1	Conclusiones	99
4.2	Recomendaciones.....	100
	REFERENCIAS	101
	ANEXOS	104

ÍNDICE DE TABLAS

Tabla 1: Características del servidor JSCAPE MFT.....	32
Tabla 2: Diseño de la Investigación	48
Tabla 3: Operacionalización de variables	49
Tabla 4: Evaluación por el tiempo de envío.....	54
Tabla 5: Evaluación por el número de paquetes.....	54
Tabla 6: Evaluación por el número de paquetes no encriptados de la Pc origen (servidor)	56
Tabla 7: Evaluación por el número de paquetes no encriptados de la Pc destino (cliente).....	57
Tabla 8: Evaluación por el número de paquetes encriptados de la Pc origen (servidor)	59
Tabla 9: Evaluación por el número de paquetes encriptados de la Pc destino (destino).....	60
Tabla 10: Algoritmo simetrico de encriptación.....	62
Tabla 11: Resumen de la evaluación de tráfico de datos	65

ÍNDICE DE FIGURAS

Figura 1. Infecciones de malware por países	16
Figura 2. Detecciones de Filecoder en países de LATAM durante el 2017	17
Figura 3. Incidentes de seguridad relacionados con ataques de Ingeniería Social	17
Figura 4. Porcentaje de empresas que no tienen ningún control de seguridad.....	18
Figura 5. Área encargada de la gestión de la seguridad en Latinoamérica	19
Figura 6. Esquema de Comunicación Segura. Se muestra las partes que intervienen para establecer una comunicación segura.	23
Figura 7: Proceso del algoritmo 3DES.....	25
Figura 8. Proceso de encriptamiento y desencriptamiento RC4	26
Figura 9. Proceso del algoritmo AES 128.....	27
Figura 10. Proceso de encriptación	27
Figura 11. Canal de comunicación seguro con el protocolo SFTP	29
Figura 12. Encriptamiento de paquetes con el protocolo SSH.....	30
Figura 13 . Intercambio de llaves	31
Figura 14. Ataque Informático. Un ataque no es más que la realización de una amenaza.	40
Figura 15 . Procesos de Recolección de Datos.....	51
Figura 16. Evaluación por el número de paquetes.	55
Figura 17. Evaluación por el número de paquetes no encriptados de la Pc origen (servidor) ..	56
Figura 18. Evaluación por el número de paquetes no encriptados de la Pc destino (cliente) ...	58
Figura 19. Evaluación por el número de paquetes encriptados de la Pc origen (servidor)	59
Figura 20. Evaluación por el número de paquetes encriptados de la Pc destino (cliente)	61
Figura 21. Diseño de un escenario de prueba.....	66
Figura 22. Prototipo de implementación de algoritmos de encriptación.....	68
Figura 23. Instalación de software JSCAPE MFT Server.....	72
Figura 24. Configuración del usuario y contraseña.....	72
Figura 25. Configuración de memoria que utilizará el servidor SFTP	73
Figura 26. Ingresando al servidor.....	73
Figura 27. Configuración el nombre del servidor	74
Figura 28. Configuración del protocolo y puerto.....	74

Figura 29. Configuración completa del servidor.....	75
Figura 30. Configuración del usuario y contraseña.....	75
Figura 31. Usuario y contraseña configurada.....	76
Figura 32. Configuración de la conexión con el servidor SFTP	76
Figura 33: Configuración del usuario y contraseña, para la conexión con servidor SFTP	77
Figura 34. Conectado con el servidor SFTP.....	77
Figura 35: Conectado con el servidor SFTP	78
Figura 36. Ingresar al panel de control.....	78
Figura 37. Configuración de la extensibilidad de FTP y Servicio FTP	79
Figura 38. Configuración de las herramientas administrativas	79
Figura 39. Configuración del Administrador de Internet Information Services (IIS), sitios y Agregar sitio FTP	80
Figura 40. Configuración de la carpeta raíz de la unidad del sistema en la unidad C y el puerto 21	80
Figura 41. Captura de usuario y contraseña con Wireshark.....	81
Figura 42. Conectividad del servidor SFTP con el host Cliente	81
Figura 43. Conectividad del host Cliente con el servidor FTP	82
Figura 44. Configuración del algoritmo 3DES en SFTP	82
Figura 45. Configuración del algoritmo AES en SFTP.....	83
Figura 46. Configuración del algoritmo RC4 en SFTP.....	83
Figura 47. Archivo a transferir entre un servidor SFTP y un host	84
Figura 48. Visualización del tiempo de la Transferencia de archivo	85
Figura 49. Paquetes encriptados de la Pc origen IP = 10.10.10.12	85
Figura 50. Paquete capturado número 1171 de 1514 bytes con Wireshark	86
Figura 51. Exportando los paquetes capturados de la Pc origen a Excel CSV	86
Figura 52. Visualización de los paquetes capturados de la Pc origen del archivo 3des_origen.csv	87
Figura 53. Convirtiendo archivos de texto excel.csv a excel.xls	87
Figura 54. Filtrando los archivos encriptados y no encriptados de la Pc origen capturados con Wireshark	88

Figura 55. Filtrando los archivos encriptados y no encriptados de la Pc destino capturados con Wireshark	88
Figura 56. Archivo transferido entre un servidor SFTP y un host cliente.....	89
Figura 57. Visualización del tiempo de la Transferencia de archivo	90
Figura 58. Paquetes encriptados de la Pc origen IP = 10.10.10.12	90
Figura 59. Paquete capturado número 644 de 1514 bytes con Wireshark	91
Figura 60. Exportando los paquetes capturados de la Pc origen a excel CSV	91
Figura 61. Visualización de los paquetes capturados de la Pc origen del archivo aes_origen.csv	92
Figura 62. Convirtiendo archivos de texto excel.csv a excel.xls	92
Figura 63. Filtrando los archivos encriptados y no encriptados de la Pc origen capturados con Wireshark	93
Figura 64. Filtrando los archivos encriptados y no encriptados de la Pc destino capturados con Wireshark	93
Figura 65. Archivo a transferir entre un servidor SFTP y un host	94
Figura 66. Visualización del tiempo de la Transferencia de archivo	95
Figura 67. Paquetes encriptados de la Pc origen IP = 10.10.10.12	95
Figura 68: Paquete capturado número 3119 de 12112 bytes con Wireshark	96
Figura 69. Exportando los paquetes capturados de la Pc origen a Excel CSV	96
Figura 70. Visualización de los paquetes capturados de la Pc origen del archivo rc4_origen.csv	97
Figura 71. Convirtiendo archivos de texto excel.csv a excel.xls	97
Figura 72. Filtrando los archivos encriptados y no encriptados de la Pc origen capturados con Wireshark	98
Figura 73. Filtrando los archivos encriptados y no encriptados de la Pc destino capturados con Wireshark	98

I. INTRODUCCIÓN

Esta investigación está referida a la seguridad de la información, en la cual investigué con respecto a la comparación de algoritmos criptográficos en la transferencia de un archivo de 8.55 Mb de un servidor SFTP a un host cliente. Es un tema actual ya que tenemos vulnerabilidad en ataques informáticos dentro y fuera de una organización con equipos tecnológicos muy sofisticados, ya que se tiene hacktivistas que se dedican a interceptar información y luego darle mal uso.

Esta tesis está estructurado en cuatro capítulos: capítulo uno se desarrolló la introducción, acompañada de la problemática que se identificó, los antecedentes de estudio, sustentos teóricos, se justifica el por qué y para qué del problema seleccionado, se plantean los objetivos y las hipótesis con las que se trabajó en esta indagación; en el capítulo dos, se hace referencia a la metodología utilizada para este trabajo, en los que encontramos el tipo y diseño utilizados en esta investigación, también se visualiza la población y muestra, operacionalización de las variables, técnicas e instrumentos de recolección de datos, criterios éticos y de rigor científico; en el capítulo tres, se realizó el análisis de la información y se interpretó los resultados obtenidos, en el cuarto capítulo se presenta las conclusiones a las que arribé en esta investigación, acompañada de las recomendaciones; se culmina con las citas bibliográficas que dan solides a esta investigación.

Esta investigación se orientó en la seguridad de la transferencia de archivos instantáneos, realizándose la comparación de los algoritmos de encriptación 3DES, RC4 y AES, teniendo en cuenta los parámetros de encriptación como: el tiempo de transmisión de archivos encriptados, total paquetes encriptados y no encriptados entre la Pc origen y la Pc destino.

1.1 Realidad Problemática

La red de datos interconectada ha transformado notablemente nuestro quehacer diario. Todos los tipos de empresas en forma general. Utilizan la red informática con la finalidad de recopilar, almacenar, procesar y compartir grandes cantidades de información en forma digital. A medida que se almacena y se transfiere información por internet es

cada día más insegura. Para manejar la información de forma confiable y segura, es a través de la encriptación de los datos, además se debe garantizar la privacidad y la integridad de la información entre los usuarios de la red, gracias a las diversas formas de codificación, autenticación y encriptación. En tal sentido la ciberseguridad, es muy importante en el momento de comenzar una comunicación digital, personalmente se debe proteger su identidad, sus datos y sus dispositivos informáticos. A nivel de corporación se tiene que proteger la reputación, los clientes de la organización y la información. A nivel del estado definitivamente se protegerá la seguridad nacional.

Hoy en día se han desarrollado muchos tipos de algoritmos de encriptación, todos tratan de encriptar una o varias características de la seguridad de la información como la integridad, confidencialidad, la autenticación y el no repudio. Habiendo una difícil evaluación con respecto al cumplimiento de cada uno de los algoritmos, ya que puede tener vulnerabilidad con ataques cibernéticos, la gran mayoría de algoritmos trabajan con diferentes claves de longitudes como por ejemplo envían fotografías falsas haciendo creer que son reales y este tipo de engaño cibernético se le conoce como malware. Es muy fácil que las personas se confíen y acepten este tipo de archivos, descargando así el malware en su dispositivo móvil o computador.

La diferencia del avance tecnológico y la condición de uso de la misma se tiene algunos problemas que pueden resultar de especial interés. Hoy en día se ha puesto de manifiesto la conexión de la comunicación digital y la falta de seguridad que existe en la transferencia de archivos.

La falta de dispositivos de comunicación segura se atribuyen a distintos problemas como: la falta de los recursos en computación en cuanto a la criptografía; dificultades del uso de los dispositivos criptográficos y el desinterés generalizada en cuestiones de la privacidad.

En un estudio que realizo ESET Security Report, (2018) donde recopilaron información a más de 4500 técnicos, gerentes y ejecutivos que son empleados en más de 2500 empresas de 15 países, divididas en pequeñas empresas a menos de 50 trabajadores,

medianas empresas entre 50 y 250 trabajadores, grandes empresas entre 250 y 1000 trabajadores y Enterprise cuya empresa alberga a más de 1000 trabajadores. Con esta información recolectada en el año 2017, se presentó un informe general el 2018, donde detallaban el estado real de la seguridad informática en las empresas de todo Latinoamérica.

De acuerdo a este informe, se puede visualizar al menos tres de cada cinco empresas de la región han sufrido como mínimo un suceso de seguridad informática, estando infectados con códigos maliciosos en un 45%. El 50% de ellos se relacionan al ransomware, esto quiere decir que una de cada cinco empresas que se encuestó en Latinoamérica sufrió secuestro de su información según la figura N°1.

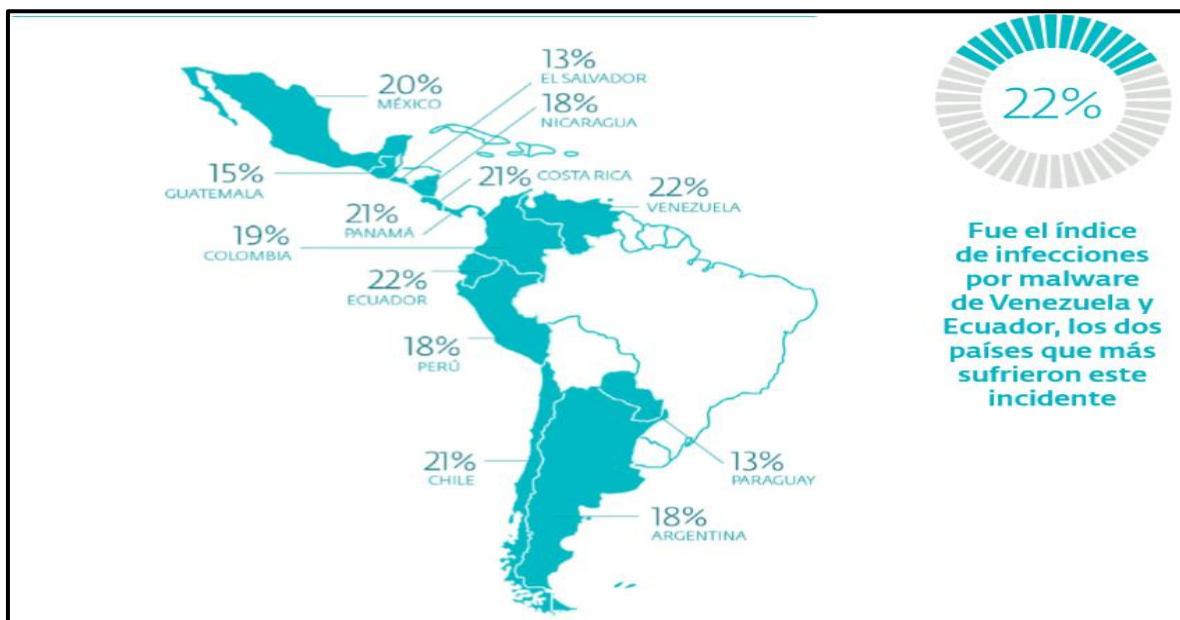


Figura 1. Infecciones de malware por países

Cuando se analizó los códigos negativos de la familia FileCoder, se encontró que la gran mayoría de localizaciones en el año 2017 se obtuvo en territorio peruano, con 25% de la totalidad de países de América Latina. En segundo lugar esta México, con 20%, le sigue Argentina con el 15%, Brasil con el 14% y Colombia con el 10%.

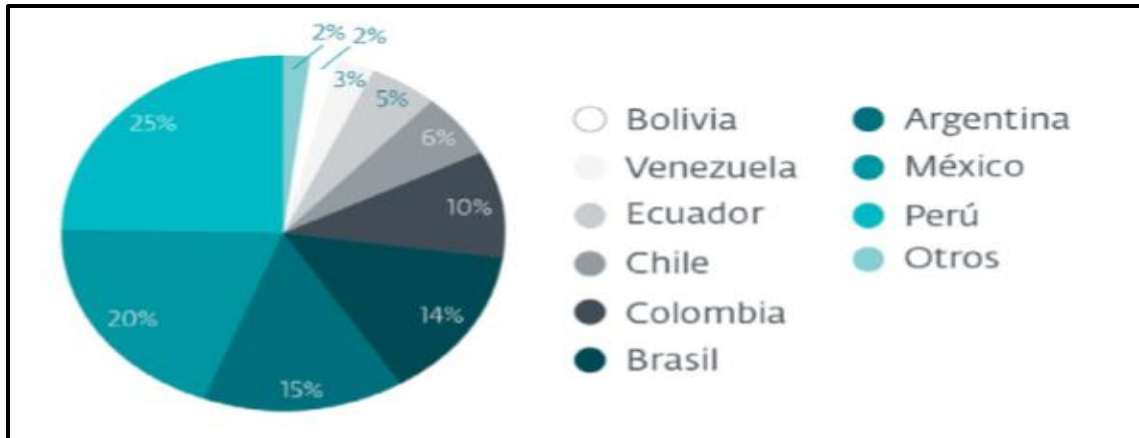


Figura 2. Detecciones de Filecoder en países de LATAM durante el 2017

Con la salvedad que la gran mayoría de códigos no son maliciosos a la hora de discutir de los sucesos de seguridad en las empresas. Detrás de estos, se encontró que una de cada diez empresas encuestadas fue víctima de incidentes que afectó la disponibilidad del servicio crítico. En los últimos años las empresas que dijeron ser víctimas de ataques de ingeniería social en un gran porcentaje han seguido estables, con diferencias pequeñas en el 2017.

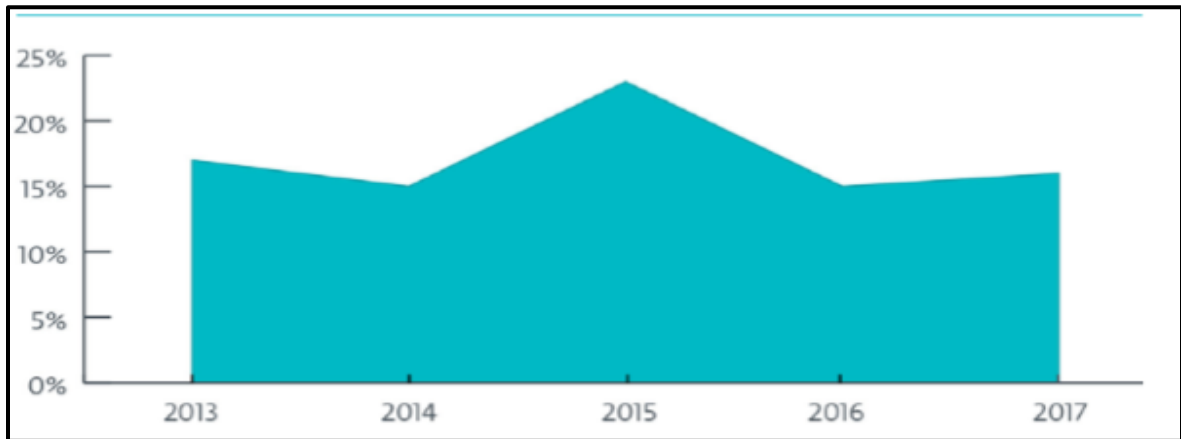


Figura 3. Incidentes de seguridad relacionados con ataques de Ingeniería Social

Esto significativa que, han evolucionado los engaños basados en ingeniería social en estos últimos años, logrando ser más efectivos. En estos tiempos lo hemos visto mutar desde los sitios de phishing, hasta las webs con certificados Secure Sockets Layer (SSL)

que vienen hacer las conexiones seguras que pueden ser falsos o gratuitos y que son desconocidos por las personas; el protocolo Hypertext Transfer Protocol Secure (HTTPS), que en español viene hacer la transferencia de datos seguro de hipertexto, tiene mucha relevancia en la falsificación de marcas de empresas muy reconocidas.

Las empresas de estos tiempos están tomando conciencia de los controles de seguridad, es probable que la gran mayoría de organizaciones piensen en tener alguna solución de protección de sus datos, pero son pocas las empresas que desean implementar políticas de seguridad de la información.

Esta información refleja, que el 1% de las organizaciones empresariales que se encuestaron no cuentan con ninguna tecnología de seguridad, el 25% no tiene ninguna política definida para el aseguramiento de su protección de la información.

Esta diferencia es directa y se relaciona con el tamaño de la empresa; esto quiere decir, que el porcentaje de las pequeñas empresas no tienen protección tecnológica y es mucho más elevado con respecto a lo que registra las organizaciones más grandes.



Figura 4. Porcentaje de empresas que no tienen ningún control de seguridad

Es un proceso integral la gestión de la seguridad, la tecnología y los controles se implementan haciendo un análisis según la necesidad de la empresa. Se tiene que entender que la prioridad es, como está formada el área de seguridad de la empresa en la región. Se

puede observar que al el 10% de las organizaciones empresariales no cuentan con un área de seguridad, exclusivamente, tal como nos muestra la figura N° 5.

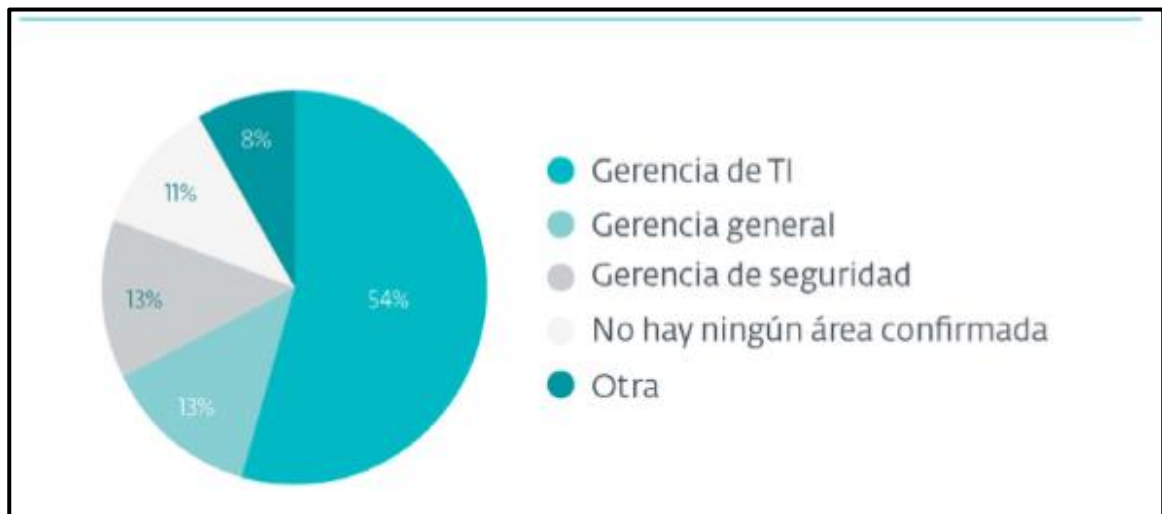


Figura 5. Área encargada de la gestión de la seguridad en Latinoamérica

Se conoce que la mitad de las organizaciones empresariales en Latinoamérica gestionan su propia seguridad desde su área de TI. Ya que esta opción vendría hacer una buena práctica con la finalidad de conformar un grupo independiente, con su propia autonomía y que tenga propiedad de revisión e implementación que se relacione en la gestión de la seguridad.

Los datos sensibles vienen hacer la información que se genera internamente en la institución, la cual está completamente prohibido la divulgación, estos datos se consideran parte fundamental porque permite tener un alto nivel de desarrollo y competitividad, esto quiere decir que el directorio de las empresas ha tratado de implementar sistemas de automatización, con el fin de desarrollar quehaceres rutinarias y mecánicas, es por eso que tienen la necesidad de mantener protegido su información.

Esta indagación está centrada en la parte de la seguridad de la información, ya que se evalúa a los algoritmos criptográficos para la transferencia de archivos en mensajería instantánea, los cuales permiten seguridad en el envío de la información entre los usuarios de forma empresarial o individual.

1.2 Antecedentes de Estudio

1.2.1 A Nivel Mundial

Existen experiencias de investigación mundial con documentación que se relaciona específicamente en los temas de seguridad de algoritmos de encriptación. A continuación hablaremos de los antecedentes que se relaciona con lo que se ha investigado:

Hernández, (2015) En su tesis doctoral "Sistema de detección de intrusos mediante modelado de URI" se orienta en los peligros existentes de las instrucciones en la red, en la seguridad del sistema y de las personas. La gran motivación de esta investigación es ayudar a la minimización de los riesgos a los ataques de los recursos de una red de ordenadores cuyo objetivo principal de esta tesis fue desarrollar las mejoras a un sistema con la detección de intrusos en la red de computadores y se basaba especialmente en el modelado de los mensajes que permiten intercambiar por medio de un protocolo de comunicaciones.

Se denomina a este sistema como SSM (del inglés, Structural Stochastic Model), utiliza el modelo de Markov, representa las cargas más útiles que permiten asociarlas a los protocolos que se basan en el paso de los mensajes. El cual relatan que fue un éxito en la detección de los ataques que se basan en la web, esta información se obtuvo por los resultados por este sistema que el investigador se motivó en la indagación de potenciales modificaciones que se orientan a mejorar sus prestaciones para operar en espacios tales como los servicios de la web en explotación.

Las muchas propuestas mostradas son eficazmente evaluadas y los resultados son cotejados con los que se logran mediante el sistema SSM original, verificándose una mejora en las prestaciones del sistema de descubrimiento de intrusos.

Moya, (2015) En su indagación. Proceso una aplicación para la encriptación de los datos en la transmisión de la información de un aplicativo de mensajes en la web. Cuyo objetivo principal fue desarrollar una aplicación para la encriptación de la información en la web. En esta investigación el escritor en mención ha aplicado las herramientas en su totalidad durante el trabajo desarrollado, utilizo la metodología SCRUM, pues con este

método todos los entregables son más pequeños, pudiéndose revisar habitualmente y permitiendo más efectividad en la identificación de los errores y los cambios. El método Scrum se direcciona específicamente en la transmisión de productos y en menor cantidad en la calidad del código Xtreme Programming (XP); esta metodología no parte de cero, sino que se va adaptando a nuestras preferencias, se utiliza también herramientas existentes de ser necesario. En esta investigación se probó múltiples herramientas como ya es conocido el Dreamweaver, HyperText Markup Language, es decir, Lenguaje de Marcas de Hipertexto (HTML), Hypertext Pre-Processor que significa Lenguaje de Programación Interpretado (PHP), Active Server Pages (ASP), NET, Visual Studio y los gestores de bases de datos como son: Microsoft Lenguaje Estructurado de Consultas (SQL) Server, MySQL, Postgre SQL, que permitió la realización de los cambios, al final lograron su objetivo.

En esta indagación podemos visualizar un claro ejemplo de la vulnerabilidad de los datos en estos tiempos. Esto ha permitido que hoy en día tengan mayor auge en la investigación e implementación de muchos modelos de encriptación de datos, cuya finalidad es asegurar la privacidad cuando se intercambie la información. Esta averiguación aborda la protección de datos y a la vez proporciona información sobre el trabajo de encriptación de algunos algoritmos.

Quizhpe (2011) citado por Capuñay, D. I; Guerrero, A.M & Villegas, J.E (2016) presenta una indagación denominada. “Soluciones de Cifrados a las Seguridades Informáticas en Procesos de Auditaje Organizacional”. Cuyo objetivo principal fue la realización de un estudio comparativo de soluciones de encriptación a la seguridad de los datos con la finalidad de ser utilizada en los métodos de Auditaje Organizacional. Aquí el investigador ha realizado una comparación de soluciones de encriptación a la seguridad de los datos, para que se entienda de una manera más clara esta investigación lo que permite es resguardar los datos utilizando diferentes formas de encriptación que se tiene para cifrar los datos, sobre todo la contraseña del usuario lo que nos permite proteger los equipos, asimismo se realizó esta investigación para que las personas que tengan la intención en este tema experimenten la forma simple y rápida a valorar la importancia que son los datos,

tanto para las pequeñas como para las grandes empresas y sobre todo tener en cuenta los procedimientos de seguridad que permitan alejar las visitas de los hackers.

Es muy fácil la encriptación de nuestras contraseñas, para ello se utiliza softwares gratuitos que se encuentran en internet y debemos tener conocimiento que estas herramientas no son eficaces en la seguridad de los datos.

En este estudio de indagación se aprecia una investigación comparativa de diferentes tipos de algoritmos de encriptación y a la vez se puede determinar cuál es el más eficaz, así poder utilizar en las pequeñas o grandes empresas, se plantea el cifrado con mayor confiabilidad para dar seguridad a los datos de la organización.

1.3 Teorías Relacionadas al Tema

En la información subsiguientes detallo las bases teóricas conceptuales que utilice en este estudio:

1.3.1 Norma ISO 27001.

La ISO/IEC, (2013) refiere una orientación completa a la seguridad de los datos y especifica lo siguiente: “Los activos que requieren resguardo van desde los datos virtuales, la documentación física y activos físicos (computadoras y redes) a los propios saberes de los colaboradores. Los asuntos que se tienen que conocer, tratar van desde el desarrollo de competencias de los colaboradores hasta la protección técnica contra los fraudes informáticos”.

1.3.2 Comunicación Segura

En la transferencia de un archivo electrónico seguro se tiene que tener en cuenta estos aspectos.



Figura 6. Esquema de Comunicación Segura. Se muestra las partes que intervienen para establecer una comunicación segura.

Autenticidad. Lucena (2014), nos dice: La autenticidad es reconocer al generador de la información; radica en la seguridad de los individuos que intervienen en el sistema comunicativo. (p. 23).

Confidencialidad. Peraza, (2012), indica que: la seguridad de la información que posee el manuscrito permanecen confidenciales ante otras personas, durante su recorrido desde un punto A hacia B. En este proceso juega un papel muy importante, el procesamiento que se le brinda a la información cuando han llegado a su destino. Los ataques que pueden surgir, son la captura del manuscrito en el recorrido que realiza de un punto a otro y el mal uso de la información o el inadecuada gestionamiento y acumulación de información por parte de B. Por lo tanto, la confidencialidad se obtiene por los métodos criptográficos.

Integridad. Peraza (2012), menciona: este término hace referencia a la seguridad en los datos de un documento al no someterse a cambios en la transmisión. Lo que se tiene que establecer es que ninguna persona intersecte este documento en el trayecto que realice para llegar a su destino. Para comprobar la integridad se realiza firmas electrónicas, basadas por lo general en funciones Hash. La Autenticidad es condición suficiente para la Integridad, por lo que, si un documento es auténtico, entonces es íntegro, pero no sucede, al contrario.

No Repudio. Lucena (2014), recalca que: no repudio de origen, significa que el remitente no puede hacer una negación de ser el responsable del envío de la información, pues el destinatario tiene prueba del origen de dicho documento, siendo el remitente el autor de esta prueba, por lo que, el destinatario no puede negar la recepción del documento, porque ambos involucrados tienen pruebas tanto de envío como de recepción.

1.3.3 Seguridad de la Información

Para que se haya una correcta la gestión de la seguridad de los datos se tiene que tener en consideración los principios básicos que a continuación detallo:

Confidencialidad. Herrera (2014), define que, es la manera de advertir la propagación de la información a personal o sistemas no facultados. Según la ISO/IEC 17799:2000, “La confidencialidad asegura que a los datos solo acceden las personas autorizadas.

Integridad

Herrera (2014), dice, la integridad es saber cómo los datos se conservan salvos, libres de cambios o transformaciones por personal no autorizado. Según la ISO/IEC 17799:2000, “La integridad es la garantía de la exactitud y completitud de la información y los métodos de su procesamiento”.

Disponibilidad

Herrera (2014), considera que, se tiene que estar dispuesto a solucionar consultas cuando el usuario lo requiera. Según la ISO/IEC (2013), es asegurar que los consumidores autorizados puedan acceder a la información cuando lo crean necesario, sin restricción alguna y el tiempo oportuno.

1.3.4 Algoritmo

Villegas (2009), no dice que, es el modo de cálculo que radica en cumplir con varias instrucciones ordenadas y organizadas que nos conllevan, una vez detallados los datos, a solucionar una situación problemática.

Gembeta (2013), consideró, al concepto de algoritmo como un acumulado de elementos observables (conjunto finito) y precisos que nos direccionan a una solución.

Se puede definir también como la agrupación de manera ordenada y definida de procedimientos que conlleva a la solución de una situación problemática. Concluyendo

entonces que todo algoritmo viene a ser un conjunto de pautas e instrucciones que favorecen en la solución de un problema.

Triple Data Encryption Standard (3DES)

En 1998 International Business Machines (IBM) creó el algoritmo Triple Data Encryption Standard (TDES) que reemplazaría a DES que utilizaba bloques de 128 bits, considerando una clave de igual con amplitud. Con la modificación del algoritmo National Bureau of Standards (NBS), se volvió consistente específicamente en la disminución de la amplitud de la clave y de los bloques, DES encripta bloques de datos de 64 bits, por la sustitución y permutación y usa la clave de 64 bits, 8 son de paridad que consiste en utilizar 56 bits y de esta manera produce 64 bits de cifrado. 3DES está basado en compuertas lógicas booleanas y esta se implementa muy fácilmente, tanto en hardware como en software. Se fundamenta en aplicar el algoritmo de encriptación DES tres ciclos, dependerá de las contraseñas que se utilice, ya sea una longitud de 168 bits como clave, siempre y cuando las tres claves sean diferentes. (Romero & Alvarado, 2016).

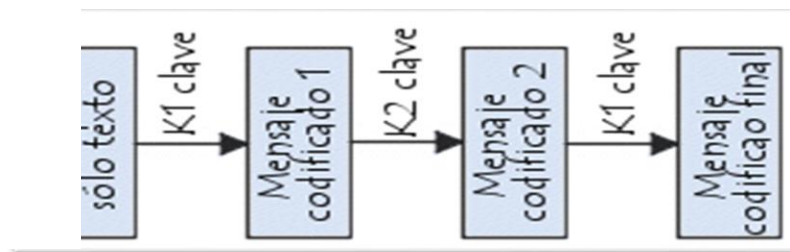


Figura 7: Proceso del algoritmo 3DES

Rivest Cypher 4 (RC4)

Su diseño se le atribuye a Ron Rivest para RSA Security, en 1987. Es el sistema de cifrado de flujo más manipulado en la WEB y se emplea en los protocolos más públicos como TLS/SSL, tiene como finalidad de proteger el tráfico de Internet, dando seguridad en las redes inalámbricas.

Para dar mayor seguridad y evitar repeticiones de la clave RC4 en cada paquete, se concatena un vector de inicialización de 24 bits con la clave WEP de 40 o 104 bits, se

envía el vector de inicialización (IV) en claro junto con el paquete cifrado y se analiza los paquetes con la misma clave (cancelación XOR), trabajan con SSL/TLS y usan un mecanismo similar, pero hacen un hash del IV y la clave WEP para crear la clave RC4. Las repeticiones de las claves son improbables y no hay igualdad y relación entre las claves. (Castanedo, 2007), (Mathur & Kesarwani, 2013).

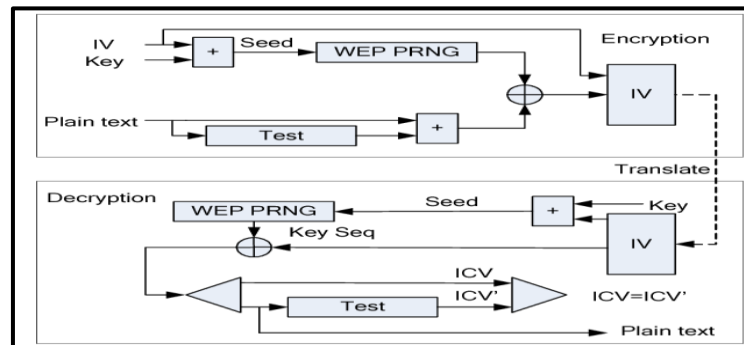


Figura 8. Proceso de encriptamiento y desencriptamiento RC4

Advanced Encryption Standard (AES)

Según (Gutiérrez (2009), el AES, viene a ser el algoritmo de cifrado simétrico. Lo desarrolló, Joan Daeman y Vicent Rijment, los dos de origen belga, bajo el nombre Rijndael.

Este algoritmo de encriptación que más se conoce por los usuarios de routers, ya que Wi-Fi Protected Access (WPA) utiliza AES como metodología de encriptación; esta encriptación puede ser implementada tanto en un sistema de software como en hardware. El sistema de encriptación de AES trabaja con claves y bloques de longitudes variable, existe AES de 256 bits, 192 bits y de 128 bits.

El cifrado intermedio de AES forma una matriz de bytes de cuatro columnas por cuatro filas. A esta misma matriz se le aplica nuevamente una cadena de bucles de encriptación basándose en instrucciones matemáticas. Esta operación consiste en la sustitución no lineal de bytes, desplazando filas de la matriz y realizando la combinación

de columnas por medio de multiplicaciones lógicas y sumas de puertas XOR basándose en claves intermedias.

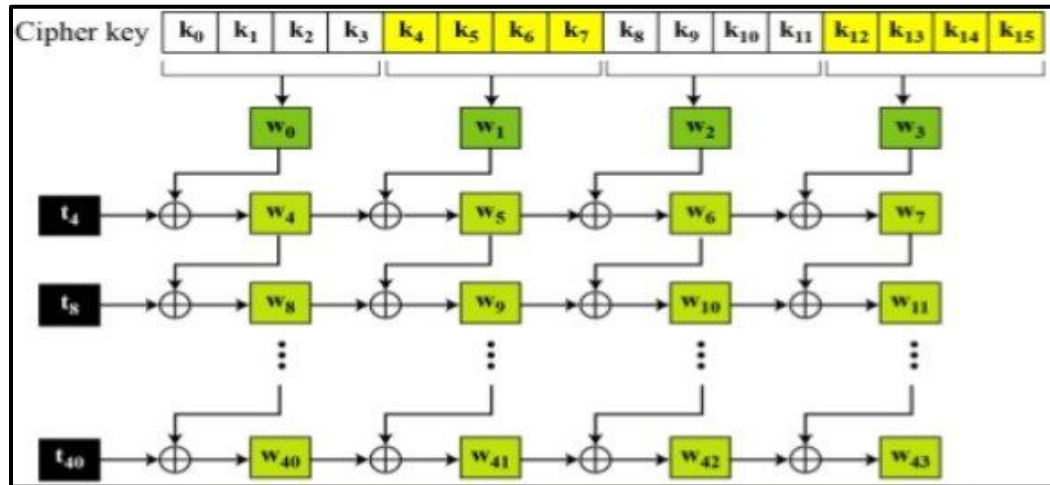


Figura 9. Proceso del algoritmo AES 128

1.3.5 La Criptografía

En un estudio de Silva (2005), da a conocer a la criptografía, como una rama de las matemáticas, encargada del estudio de la evolución clara de la información pudiéndose hacer una lectura directa, pero con un descifrado antes de ser leído.

Encargada de la transposición u ocultamiento del mensaje emitido por el remitente hasta llegar al destinatario siendo descifrado por el receptor. El enunciado criptografía procede de la coalición de términos (oculto) y (escritura), y su axioma es: Habilidad de escribir en código secreto o de manera misteriosa. Se puede precisar a la criptografía como la técnica matemática para cifrar o descifrar información, con la finalidad que no se pueda visualizar los mensajes (Lucena, 2014), (García, 2013)

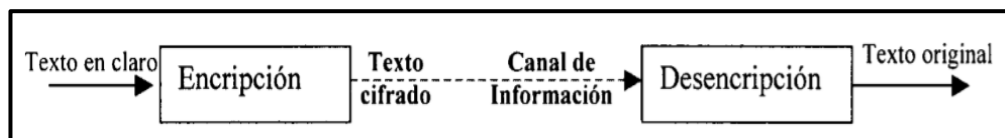


Figura 10. Proceso de encriptación

1.3.6 Transferencia de Archivo en Red

Según Alcantud, (1999). Afirma que, es la transferencia de un archivo del computador a través de canales de comunicación de un sistema a otro. Esta normado esta transmisión de archivos por protocolos establecidos en la comunicación. No olvidemos que existen muchos protocolos de transferencia de archivos elaborados para diversos contextos.

Un protocolo tiene como finalidad comunicar y la diferencia de los protocolos de transferencia de datos es que, no están estructurados para remitir la información en comunicación asíncrona, como sesiones de Telnet. Su objetivo principal es dar la secuencia de bits donde se almacena en una sola unidad del sistema de ficheros de metadatos tales como fecha y la hora, capacidad del archivo y el nombre del archivo.

En Computación, el envío de archivos es un palabra genérica que consiste en la transmisión de ficheros por medio de una red de ordenadores. Si bien es cierto que este término se vincula con el Protocolo de Transferencia de Archivos (FTP), hay muchos métodos de transferir información a través de una red.

Los servidores que permiten la transferencia de información son llamados servidores de archivos.

Niveles en los cuales puede tener lugar

La transferencia de información se da por medio de un sistema de archivos de red, servicios de transferencia de información dedicados tales como File Transfer Protocol (FTP) o Hypertext Transfer Protocol (HTTP), redes punto a punto, sistemas de mensajes sincrónicos, entre ordenadores y dispositivos físicos y en los vínculos directos tales como el módem.

1.3.7 Protocolo Seguro de Transferencia de Archivos (SFTP)

ANYWHERE (2014). Lo define como: “Protocolo del nivel de aplicación que permite el traspaso y manipulación de datos sobre un flujo de información confiable. Es

utilizado con Secure SHell (SSH) para brindar seguridad a los datos y admite ser usado con otros protocolos de seguridad”. (p.72).

1.3.7.1 Descripción y características

El protocolo SFTP reconoce la ejecución de muchas operaciones de archivos remotos, se aplica con más frecuencia en los sistemas operativos Windows y Unix, está creado para que se ejecute como protocolo independiente, la versión 3 es la más utilizada y se ejecuta por el servidor Open Secure Shell (OpenSSH) de SFTP, en la versión 4 su vínculos los redujo con el sistema operativo Unix, es por ello que Windows realiza sus ejecuciones en servidores SFTP, el protocolo SFTP viene utilizando el puerto 22 de TCP y su seguridad en la transmisión de sus datos no lo provee el protocolo SFTP, si no SSH, los archivos que se transfieren se asocian con sus atributos primordiales, como por ejemplo el tiempo que viene hacer una ventaja sobre el FTP, ya que no tiene ningún crédito que permita incluir archivos en la data original.

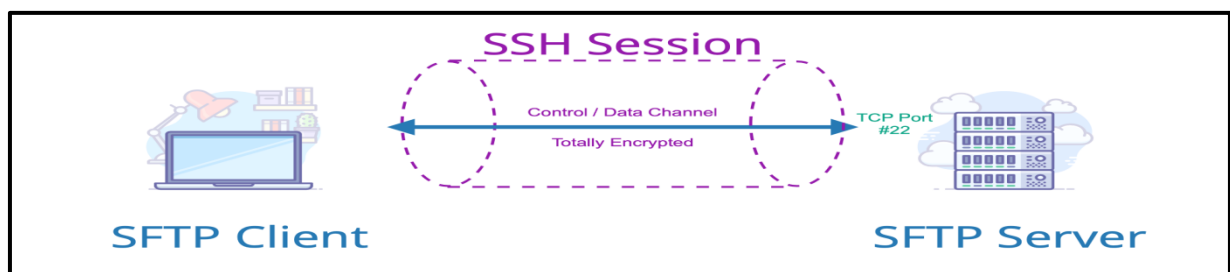


Figura 11. Canal de comunicación seguro con el protocolo SFTP

1.3.8 Protocolo Secure SHell (SSH)

SSH es un protocolo, cuya función principal es permitir el acceso remotamente a un servidor por intermedio de un canal muy seguro en el que los datos está encriptados. Asimismo de la unión a otros terminales, SSH copia información de forma segura, permite gestionar una serie de claves Rivest, Shamir y Adleman (RSA) con la finalidad de no cifrar contraseñas al enlazar a los terminales y pasar la información de una aplicación a

otra por una conducción tunelizado con SSH, asimismo puede dirigir el tráfico y ejecutar remotamente programas gráficos mediante el puerto 22 FTP.

1.3.8.1 Secure SHell Server V2 (SSHv2 Server)

Usar el server SSHv2 nos permite la unión de un host SSH encriptada y segura al enrutador. SSHv2 utiliza una encriptación para la autenticación. El software SSHv2 permite la comunicación con host SSHv2 públicos y comercialmente.

1.3.8.2 Secure SHell Client (SSHv2 Client)

La unión del host o cliente SSHv2 se ejecuta bajo una aplicación sobre el protocolo SSHv2 que permite la autenticación y el la encriptación de la unidad. El Secure SHell Client (SSHv2) hace que el enrutador ejecute una conexión encriptada y segura a cualquier otro terminal que permite la ejecución del servidor SSHv2. Esta unión proporciona un enlace saliente encriptado. Con cifrado y autenticado, el host cliente SSHv2 admite una interconexión segura por medio de una red insegura.

1.3.8.3 Seguridad

SSH trabaja con utilidad de línea de comando tal como lo hace Telecommunication Network (TELNET), con la diferencia que SSH usa métodos de encriptación que hacen que los datos que se trasladan vaya de una forma no legible, evitando que otras personas puedan revelar la contraseña y el usuario y lo que escriben durante toda la comunicación.

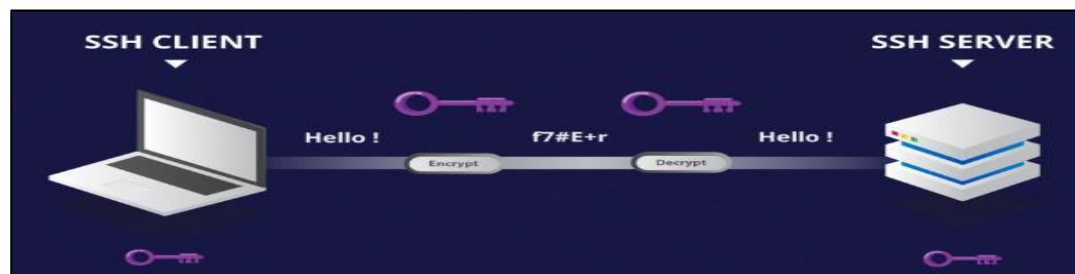


Figura 12. Encriptamiento de paquetes con el protocolo SSH

1.3.8.4 Diffie hellman (DHP)

Es un protocolo de claves entre partes que no tienen relación previa, utilizan un conducto no seguro y de forma no autentica.

Se emplea como medio para asociar claves simétricas en la encriptación de una sesión. Habiendo la no autenticación, es por ello que suministra las plataformas para muchos protocolos autenticados.

Su seguridad está en el extremo peligro, en el cálculo de algoritmos discretos en un cuerpo determinado.

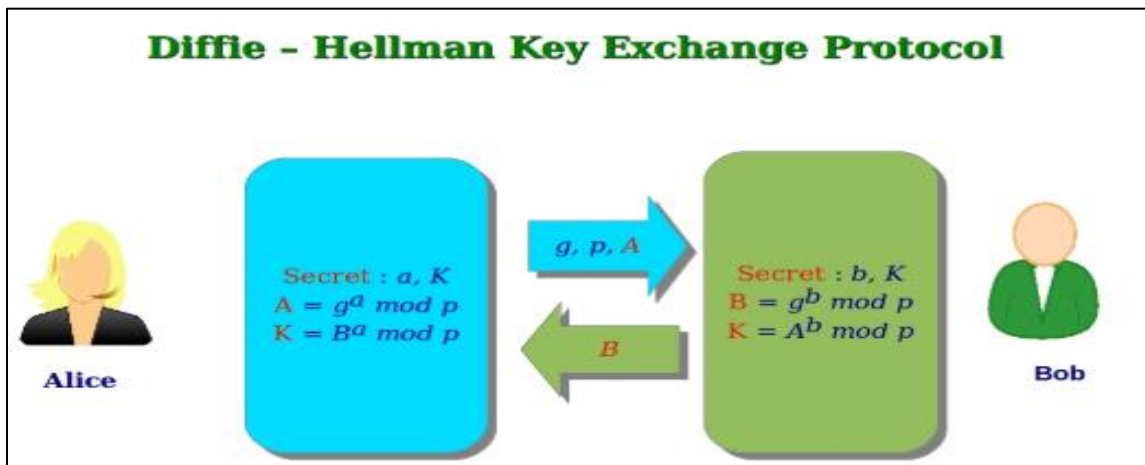


Figura 13 . Intercambio de llaves

1.3.9 Software para Configurar el Servidor SFTP

1.3.9.1 JSCAPE MFT Server

JSCAPE MFT es un servidor de transferencia de archivos administrado independiente de la plataforma que admite AS2 (certificado por Drummond), FTP, File Transfer Protocol Secure (FTPS) (FTP sobre SSL), SFTP (FTP sobre SSH), HyperText Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS), Odette File Transfer Protocol (OFTP) (certificado de Odette), Trivial file transfer Protocol (TFTP), File Transfer Protocol (AFTP) y WebDAV. Protocolos. Las características del servidor JSCAPE MFT visualizadas en la tabla 1:

Tabla 1.

Características del servidor JSCAPE MFT

Característica	Beneficio
Plataforma independiente	El soporte para entornos de Windows, Linux, Solaris y Mac OS X proporciona la flexibilidad de implementación en cualquier lugar dentro de su organización.
Soporte de protocolo múltiple	El soporte para Applicability Statement 2 (AS2) (certificado por Drummond), FTP, FTPS (FTP sobre SSL), SFTP, Secure. Contain. Protect (SCP) (copia segura), TFTP, OFTP (certificado por Odette), AFTP (Protocolo de transferencia de archivos acelerado), HTTP, HTTPS y WebDAV significa que puede Intercambiar datos fácilmente con sus clientes, independientemente de sus requisitos de traspaso de archivos.
Cliente de transferencia de archivos web integrado	El precio de la licencia y el soporte es bastante económico ya que no tenemos que instalar ningún programa cliente. Los host clientes necesitan un navegador web para ejecutar la transmisión de la información, al hacer uso del cliente web integrado, los usuarios no tienen de que preocuparse de las políticas de firewall interno ya que la gran parte de las empresas no limita el tráfico basado en la web.
Transferencia de archivos acelerada	Protocolo de transferencia de archivos acelerado (AFTP) es el protocolo de transferencia de archivos desarrollado por JSCAPE. AFTP está diseñado para activar con rapidez el traspaso de datos por redes de alta velocidad que no pueden utilizar completamente el rendimiento de la red debido a la alta latencia y la pérdida de paquetes. En estas condiciones, AFTP puede acelerar las transferencias de archivos hasta 100 veces más rápido que el FTP y otros protocolos de transferencia de archivos.
Visor de documentos web	El Visor de documentos web de JSCAPE simplifica la distribución de contenido al integrar un visor de documentos en la interfaz web del servidor file transfer management (MFT) de Suppliers Inputs

Característica	Beneficio
	Process Output Customers (JSCAPE). Con soporte para numerosos formatos de documentos, los usuarios pueden ver documentos en el servidor sin tener que descargar o tener instalado software de soporte.
Protección de Datos	Su información confidencial está totalmente protegida durante la transferencia y en reposo cuando se hace uso de las tecnologías de encriptación OpenPGP y SSL de alta categoría. Esto es complejo para muchas organizaciones que ahora viven sujetas a las exigencias de protección de la información de Payment Card Industry Data Security Standard (PCI-DSS), HIPAA y Sarbanes - Oxley.
Prevención de pérdida de datos	Evita la pérdida de información confidencial, para ello utiliza un motor de control Digital Light Processing (DLP) incrustado.
Transferencias de archivos ad-hoc	Realiza la transferencia de datos basados en correo electrónico, permitiendo evitar los problemas que usualmente se advierten con los datos adjuntos de los correos electrónicos de gran dimensión.
Gatillos	Usando los desencadenantes, puede automatizar rápidamente los procesos de negocios basados en eventos y condiciones. Por ejemplo, cuando un cliente recibe un archivo, es posible que desee comprimir automáticamente ese archivo y luego reenviarlo por correo electrónico al representante de la cuenta correspondiente para su posterior procesamiento.
Integración de autenticación	Autentica a los usuarios contra Lightweight Directory Access Protocol (LDAP), es el acrónimo de NT Windows New Technology (NTLM), Active Directory, Privileged account management (PAM), Single Sign On (SSO), Remote Authentication Dial-In User Service (RADIUS) o servidores de bases de datos relacionales existentes. Esto simplifica enormemente el proceso de integración, especialmente en organizaciones con un gran número de usuarios.

Característica	Beneficio
JMS	Publica eventos de servidor suscritos en cualquier cola Java Message Service (JMS) para su posterior procesamiento.
Access Control List (ACL) administrative	Restringe las capacidades de los usuarios administrativos y la visibilidad de los datos mediante roles y etiquetas.
Application Programming Interface (API) de acción	Usando los desencadenantes, puede definir una o más acciones que se ejecutarán en respuesta a eventos coincidentes y condiciones de eventos. Más de 80 acciones integradas le permiten hacer todo, desde comprimir archivos, cifrar archivos OpenPGP, enviar correos electrónicos y más. Si bien esto puede ser suficiente para la mayoría de las organizaciones, Action API es una API basada en Java que le permite definir sus propias acciones en caso de tener necesidades más especializadas. Por ejemplo, supongamos que necesita analizar un documento PDF al cargar y comunicar los datos analizados a otro servidor a través de JMS. Esto se puede lograr fácilmente usando la API de acción.
API REST	La API de Representational State Transfer (REST) está disponible tanto para usuarios administrativos como para clientes. Usando la API REST, los usuarios pueden hacer todo, desde realizar transferencias de archivos hasta administrar el servidor.
Punto de control y soporte de reinicio	La transferencia de datos de gran tamaño a través del Internet, permiten fallas ocasionalmente, esto se debe a problemas que se relaciona con la red. En el caso de una transferencia de datos fallida, el soporte de punto de control y reinicio le permite reiniciar la transferencia desde el último byte de datos transferidos con éxito en lugar de volver a transferir todo el archivo. Esto es fundamental en las organizaciones que transfieren archivos muy grandes o tienen acuerdos de nivel de servicio con los clientes para transferir un archivo dentro de un período de tiempo determinado.
Suma de control de integridad	La verificación de suma de comprobación es un proceso posterior

Característica	Beneficio
	a la transferencia de archivos que verifica la integridad de los archivos transferidos. Esto se logra comparando las sumas de comprobación del archivo en ambos lados, el remitente y el destinatario, lo que garantiza que los archivos se transfieran correctamente.
Notificaciones de Correo Electrónico	Recibe notificaciones por correo electrónico sobre los eventos que son importantes para ti. Por ejemplo, como administrador del sistema, es posible que desee recibir una notificación por correo electrónico si una cuenta de usuario está deshabilitada debido a un número sucesivo de intentos de inicio de sesión no válidos.
Cifrado OpenPGP	Usa el cifrado OpenPGP para asegurarse de que sus datos estén cifrados mientras está en reposo o para descifrar automáticamente los archivos que le envíen los clientes que utilizan el cifrado OpenPGP.
Transferencias automatizadas de archivos	Transfiera automáticamente archivos a / desde el servidor utilizando los protocolos FTP / FTPS / SFTP / Secure Copy Protocol (SCP). Esto es perfecto para usar en situaciones en las que debe transferir archivos de forma programada o en base a otras condiciones de eventos.
Registro de base de datos	Al utilizar las funciones de registro de la base de datos, puede asegurarse de que toda la actividad del servidor se almacene con seguridad en una base de datos remota.
Almacenamiento de red (anteriormente conocido como proxy inverso)	Asigna servicios remotos a directorios virtuales en su servidor. Esto le permite otorgar a los usuarios acceso a servicios remotos utilizando una cuenta de inicio de sesión único. Los usuarios ya no tienen que recordar múltiples nombres de host, nombres de usuario y contraseñas. Esta característica también es muy útil para la transmisión de datos entre un servidor público ubicado en la Demilitarized Zone (DMZ) y un servidor privado ubicado detrás de su firewall. Soporte para FTP / S, SFTP, Amazon S3, Server

Característica	Beneficio
	Message Block (SMB) y otros protocolos.
Reglas de acceso Internet Protocol (IP)	Bloquea su servidor usando reglas de acceso basadas en la dirección IP del cliente.
Sistema de archivos virtual	Define un sistema de archivos virtual, usuarios y permisos sin tener que crear usuarios o permisos a nivel del sistema operativo.
Dominios múltiples	Crea un sin número de servidores virtuales, cada uno con su propio conjunto de usuarios y permisos.
Administración remota	Administra de forma segura su servidor de forma remota desde cualquier parte del mundo.
API de administración de cuentas y servidores	API basadas en Java y REST para integrar funciones de administración de cuentas y servidores dentro de aplicaciones externas.

Nota. Fuente: <https://www.jscape.com/support/documentation>

1.3.9.2 AnyCliente

Es un host cliente de transferencia de información de modo gratuito que permite numerosos protocolos, incluidos: FTP / S, SFTP, Amazon S3 y muchos más. Permite el traspaso de datos desde un computador local a un servidor en Internet.

Escrito en Java, AnyClient es independiente de la plataforma. Siempre y cuando ya tenga un Java Runtime Environment (JRE) adecuado en su computadora, puede usar AnyClient. En este documento, supondremos que ya tiene el JRE y AnyClient instalados y en ejecución.

AnyClient admite los siguientes tipos de conexión: FTP, SFTP / SSH, FTP / SSL implícito, FTP / SSL (AUTH TLS), WebDav, Amazon S3 (HTTP), Amazon S3 (HTTPS), AFTP (TCP), AFTP (UDP). En esta sección, aprenderá cómo conectarse a los servidores utilizando estos tipos de conexión.

1.3.10 Software para Capturar Tráfico de Red

1.3.10.1 Wireshark

Considerado como un programa muy significativo en el escaneo y análisis de protocolos de una red a nivel mundial. Escanea la información microscópica de la red.

Wireshark se mejoró con el tiempo gracias a las contribuciones de los expertos creadores de red en el planeta. Este proyecto muy importante se inició en 1998.

Wireshark posee las siguientes particularidades:

Realiza un examen minucioso de los protocolos de la red que se añaden constantemente, realiza el escaneo y luego hace la captura de datos y protocolos en tiempo real, realizando la investigación externamente sin línea, para ello, utiliza tres paneles exploradores de paquetes, como también multiplataforma como: Windows, OS X, Linux, Solaris, FreeBSD, NetBSD, y otros. Por otra parte, la información que se captura en la red se pueden examinar a través de interfaz gráfica como es el del usuario, de igual forma se puede analizar por medio de la utilización de TTY-mode TShark, utilizando poderosos filtros que permiten la visualización en las empresas y el análisis VoIP Rich, el mismo que ayuda a leer / escribir en muchos formatos de archivo que realizan la captura: Pcap NG, Catapult DCT2000, tcpdump (libpcap), Cisco Secure IDS iplog, Red Sniffer® general (comprimido y sin comprimir), Microsoft Network Monitor, Sniffer® Pro y NetXray®, Redes Visuales Visual UpTime, WildPackets EtherPeek / TokenPeek / AiroPeek y otros.

La información sincrónica es visualizada desde Ethernet, IEEE 802.11, Point to Point Protocol / High Level Data Link Control (PPP / HDLC), Asynchronous Transfer Mode (ATM), Bluetooth, Universal Serial Bus (USB), Token Ring, Frame Relay, Fiber Distributed Data Interface (FDDI), y muchos otros todo depende de la plataforma que se está utilizando. Asimismo, realiza el soporte de descifrado en varios protocolos, entre ellos, IPsec, ISAKMP, Kerberos, SNMPv3, SSL / TLS, WEP y WPA / WPA2; las medidas que utiliza para atenuar son empleadas en la relación de paquetes al realizar el análisis de modo instintivo y rápido y la salida de los paquetes se puede exportar a Extensible Markup Language (XML).

1.3.11 Software para Conectar Cliente Servidor SFTP

1.3.11.1 FileZilla

Es un programa utilizado como cliente de FTP, está desarrollado para el sistema operativo Windows. Esta plataforma funciona como modo Explorador de Windows, señala la ventana local y las carpetas remotas. La transferencia de los datos de una ventana a otra es arrastrando y soltando el mouse. Sus funciones más importantes de FileZilla son:

Permite soportar arrastrar y soltar, es capaz de soportar la continuación de las descargas interrumpidas, tiene una herramienta que permite acumular los parámetros de conexión de sitios de red en FTP, mantiene viva la conexión entre el cliente y el servidor FTP y SFTP, soporta las conexiones de servidores proxy y firewalls, admite conexiones muy seguras en SSL y SFTP, utiliza una cola de cargas y también de descargas. Por otra parte, se encarga de visualizar el tiempo de traslado de los paquetes de los ficheros.

1.3.11.2 Transmisión de Ficheros

La transmisión de ficheros se ejecuta de una manera fácil haciendo uso de mouse, con sólo halar y luego soltar uno o más ficheros desde el Directorio de Archivos Remota al Directorio de datos locales o viceversa.

1.3.12 Software para Conteo de Paquetes Encriptados y no Encriptados

1.3.12.1 Microsoft Excel

Es un programa que permite realizar cálculos y es el más utilizado por los usuarios de todas las profesiones inclusive en el ámbito doméstico, da solución a los problemas matemáticos, estadísticos, físicos y financieros, etc. Permite trabajar con diferentes tablas y hojas y con cualquier tipo de dato numérico y alfanumérico, así como permitimos la creación de gráficos y poder insertar fórmulas, este tipo de información es muy útil en cualquier organización financiera; el trabajo que realiza con Visual Basic lo hace útil a los usuarios quienes codifican formularios grandes y pequeños o utilizan la aplicación con GUIs. y, por lo tanto, sus funciones permiten filtrar y organizar las celdas,

lo realizan perfectamente buscando y comparando datos diferentes. (Users Corporation, 2013)

En Microsoft Excel podemos trabajar con diferentes tablas y hojas, con diferentes tipos de datos alfanuméricos y numéricos, así mismo se puede crear gráficos estadísticos y se puede trabajar con fórmulas, lo que resulta de gran utilidad para cualquier usuario que desarrolla información financiera. Excel está integrado con Visual Basic que permite desarrollar aplicaciones y es de gran utilidad para los que desarrollan códigos en formularios pequeños o aplicaciones con GUIs., su función principal es filtrar y organizar celdas y lo hace perfectamente en la brusquedad y comparación datos diferentes.

Excel trabaja con hojas de cálculo en una forma personalizada, además importa datos de otra bases de y trabaja con tablas, asimismo se puede desarrollar fórmulas complejas, ecuaciones y funciones matemáticas con la única finalidad de ejecutar cálculos.

En Microsoft Excel podemos filtrar valores de las tablas utilizando diferentes criterios y ordena alfabéticamente, crea cualquier gráfico estadístico y trabaja con valores de celdas como gráficos de columnas, barras, dispersión, lineal, áreas y permite la codificación de macros con la única finalidad de la automatización de los trabajos repetidos; a las hoja de cálculo se puede acceder de cualquier maquina siempre y cuando este sincronizado con OneDrive por eso siempre trabaja con la colaboración de diferentes usuarios, permitiendo la edición de los archivo a la vez y es compatible con formatos diferentes, incluidos .xls, .xml y .csv.

1.3.13 Firmas Digitales.

Según Aguirre (2006) . La firma digital es un método criptográfico que vincula la identidad del usuario o de un equipo informático a los datos. En función al tipo de firma, se puede asegurar la integridad del mensaje.

1.3.14 Ataques Informáticos

Mieres (2009) menciona que, un ataque informático reside en utilizar los errores (vulnerabilidad) en el software, hardware, y en las personas los individuos que son parte del contexto informático; con la finalidad de conseguir un beneficio, generalmente financiero, originando efectos negativos en la seguridad de un sistema, que posteriormente repercutirá claramente en los activos de la empresa.

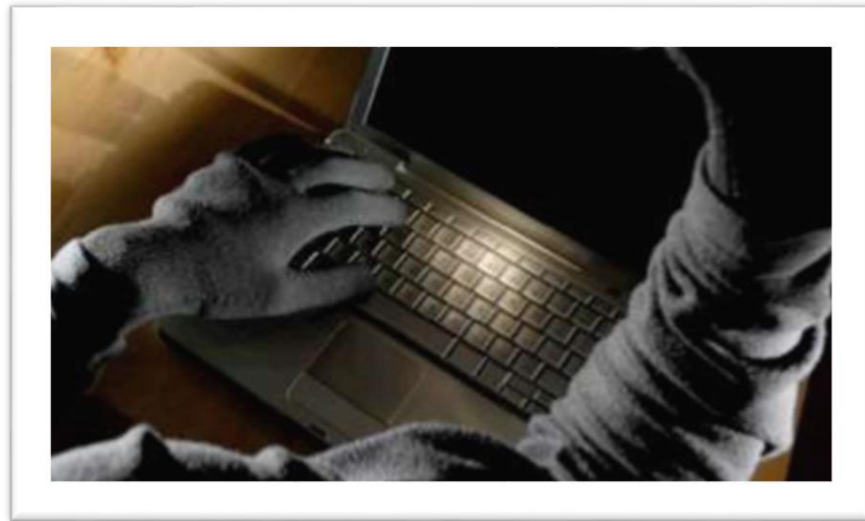


Figura 14. Ataque Informático. Un ataque no es más que la realización de una amenaza.

Las categorías que amenazan o atacan son cuatro:

Interrupción

Esta considerado un ataque del sistema, se refiere a la destrucción y no disponibilidad. García (2011), manifiesta que, un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque es la deshacerse de un elemento de la parte física del computador, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros”.

Intercepción

Según Rodriguez (2011), da a conocer que, una organización o sujeto sin autorización puede acceder a un recurso. Siendo un ataque contra la confidencialidad. Este ataque es el proceso de la obtención de información mediante el uso de softwares conocidos como troyanos, o bien la lectura del código de la cabecera del paquete de datos visualizando la identidad de los usuarios, a través del Spoofing.

Modificación

Garcia (2011) , nos dice que, la entidad no autorizada, tiene acceso a un recurso informático, y también es capaz de manipularlo, siendo un ataque a la integridad. Este ataque se puede visualizar en el cambio de valores en un archivo, transformar un archivo para que no funcione adecuadamente modificando el contenido de la información transferida por la red.

Fabricación

Rodriguez (2011), menciona, la entidad no autorizada implanta objetos adulterados en el sistema, siendo un ataque a la autenticidad. Este ataque consiste en insertar datos erróneos en una red. Estos ataques pueden ser pasivos o activos.

Mensajería Instantánea

Referida a una forma de comunicarse en tiempo real. La información es enviada a través de los aparatos conectados ya sea por internet o en una red, o también datos móviles (3G, 4G, 4G LTE, etc.) sin tener en cuenta el trayecto que hay entre ambos conectores. (Fernández, 2009).

La gran parte hacen uso de redes propietarias y la gran mayoría de programas ofertan este servicio en cada computador. También, tenemos softwares de mensajería que se utiliza para el envío de modo sincrónico, utiliza el protocolo XMPP, con un sin número de servidores descentralizados.

1.4 Definición de la Terminología.

En las consiguientes líneas se detalla los términos utilizados en la presente indagación:

1.4.1 Criptografía (Cifrado de datos)

Oculta la información transferida por el remitente hasta llegar al receptor, siendo inmediatamente decodificada por el receptor. Según la Real Academia, criptografía procede del adiconamiento de términos (oculto) y (escritura), definiéndose como el arte de escribir en clave encriptada. (Lucena, 2014)

1.4.2 Criptoanálisis

Teniendo el conocimiento de las características habituales de los algoritmos de mensajería. Consiste en implicar la seguridad de un criptosistema. Se realiza descifrando la información desconociendo la llave, o bien alcanzando criptogramas empleados en su codificación. (Lucena, 2014, p. 24).

1.4.3 Encriptado

Ejecuta el ocultamiento y la codificación de la información con la finalidad de disuadir su lectura por otras personas y aseverar sobre todo la confidencialidad de las transmisiones.

1.4.4 Clave Privada

Considerado como Cifrado Asimétrico, solo el emisor del mensaje conoce la clave y puede cifrar o descifrar la información.

1.4.5 Clave Publica

La clave pública o public key participa en la encriptación de información y es una de las dos claves principales que utiliza en criptografía asimétrica.

1.4.6 Protocolo SFTP

Es un protocolo que se utiliza en la transferencia de información. Hoy en día se utiliza la versión 3, compuesta por el server SFTP OpenSSH.

1.4.7 Protocolo SSH

Usa métodos de encriptación que permite que los datos al momento de su traslado viaje de una forma no legible, evitando que otros usuarios descubran la contraseña y el usuario de la conexión, a la vez encripta la escritura durante la sesión.

1.4.8 Transferencia de Archivos en Red

Es el traslado de la información de un computador utilizando un medio de comunicación de un host a otro.

1.4.9 Mensajería Instantánea

La mensajería instantánea está basada en la arquitectura cliente-servidor con la finalidad de poder enviar y recibir mensajes de modo síncrono. El host cliente se encuentra instalado en un computador o en un equipo móvil particular de un beneficiario final, lo cual permite el interfaz de comunicación con otros usuarios en tiempo real. Así mismo el servidor es el que maniobra toda la comunicación cliente/servidor, delegando todos los permisos que conciernen. En este modelo, el servidor no necesariamente tiene el compromiso de la transferencia de los mensajes, sino también la fidelidad y autenticación de los beneficiarios. Su característica principal es desarrollar este tipo de comunicación de modo síncrono en la web o por medio de un aplicativo móvil, sobre todo saber si una persona que forma parte de una lista está activo o inactivo y de esa manera poder hacer la comunicación en tiempo simultaneo, propiciando el cambio de datos o chat; transfiriendo archivos y conversando mediante mensajes de texto.

1.4.10 Hash

Función unidireccional que inserta un mensaje de inicio con una longitud arbitraria, produciendo resúmenes con longitud estable. SFTP utiliza tanto Secure Hash Algorithm (SHA) como Message Digest 4 (MD4) en la ejecución de un servidor SFTP.

1.4.11 Algoritmo de Hash Seguro (SHA)

NIST. SHA propuso a Hash unidireccional que está basado en MD4, produciendo 160 bits de digest. SHA promueve 160 bits de digest, resistiendo a los ataques de los hashes de 128 bits, con la única diferencia que es más lento.

1.4.12 Diffie Hellman

Utilizado mayormente como medio para ajustar las claves simétricas que se emplearan en el cifrado de los datos (establecer clave de sesión). Siendo no certificado, pero tiene las bases para muchos protocolos certificados.

1.4.13 Advanced Encryption Standard (AES)

AES está basado en el algoritmo Rijndael, que consiste en la utilización de las claves de 256, 192 y 128 bits de longitud para encriptar bloques de 256, 192 y 128.

1.4.14 Data Encryption Standard (3DES)

Es un algoritmo criptográfico con clave secreta que se basa en el algoritmo Lucifer de la empresa IBM. Al algoritmo 3DES en criptografía se le conoce como el triple cifrado del DES. Así como también como TDES.

1.4.15 Rivest Cypher 4 (RC4)

RC4 es un algoritmo de cifrado de bloque de clave simétrico. Es notable por ser simple, rápido (debido al uso de operaciones de computadora primitivas y consume menos memoria.

1.4.16 Internet

Es la comunicación de redes descentralizadas que están interconectadas, utilizado el protocolo Transmission Control Protocol/Internet Protocol (TCP/IP), lo cual permite garantizar las redes heterogéneas físicas que vienen hacer las redes lógicas de modo único en el alcance mundial.

1.5 Formulación del Problema

¿Cómo mejorar la transferencia de archivos en mensajería instantánea?

1.6 Justificación e Importancia del Estudio

Justificación Tecnológica

Este estudio se realizó en lo tecnológico porque explica una temática que es tendencia en la actualidad y se trata de la comunicación que existe por medio del internet, que es tan inseguro, en especial, al momento de la transferencia de archivos, viene hacer un tema de indagación de mucha importancia debido a los avances tecnológicos actuales.

Justificación Social

Hoy en día la transferencia de archivos por internet es muy utilizada donde se realizan muchas reuniones, acuerdos y convenios constantemente por la red de redes. Este proyecto pretende brindar ayuda social y conseguir herramientas adecuadas y de esta manera garantizar la integridad, seguridad y privacidad.

Justificación Económica

Esta investigación ayuda a disminuir los recursos computacionales en cuanto al tiempo de cifrado y descifrado de la información.

1.7 Hipótesis

Mediante la ejecución de los algoritmos criptográficos, se comprobó la optimización de la transmisión de la información teniendo en cuenta la confidencialidad e integridad de los archivos.

1.8 Objetivos

1.8.1 Objetivo General

Comparar tres algoritmos de encriptación para identificar las mejores características de optimización en la transferencia de archivos en mensajería instantánea.

1.8.2 Objetivos Específicos

- a) Seleccionar los algoritmos de encriptación en el mercado tecnológico.
- b) Diseñar un escenario de prueba para la transferencia de archivos de forma segura en mensajería instantánea.
- c) Construir el prototipo de la implementación de algoritmos de encriptación.
- d) Realizar pruebas de funcionamiento del sistema de algoritmos de encriptación.

II. MATERIAL Y MÉTODO

2.1 Tipo y Diseño de Investigación

2.1.1 Tipo de Investigación

El enfoque utilizado en esta investigación es cuantitativo, de tipo descriptivo-comparativo, porque en gran parte se describe a los algoritmos para la transferencia de datos, objeto de esta investigación se especifican sus características, por otro lado se configuro los algoritmos elegidos con la única finalidad de encriptar la información y enviarlo por medio de la comunicación, que viene hacer una red pública, de esta manera realizar la transferencia de datos. (Hernández Sampieri R. F., 2014)

Comparando con que algoritmos aumenta el nivel de confidencialidad e integridad de los datos.

2.1.2 Diseño de la Investigación

El diseño empleado es de tipo pre – experimental por que se manipulo la variable de estudio demostrando la remisión de información en cantidad de paquetes, encriptado y sin encriptar por una red pública, además se capturó el tráfico en un periodo definido.

El método utilizado en esta indagación fue de tipo deductivo porque, se ha desarrollado de lo general a lo particular, obteniendo conclusiones reales a partir del comportamiento de las variables en estudio. El diagrama en esta tesis es el siguiente (Hernández Sampieri, Fernández Collado , & Baptista Lucio, 2010).



Dónde:

X = Algoritmos de encriptación

Y = Medir la Confidencialidad e integridad

Tabla 2

Diseño de la Investigación

Var. Independiente	Var. Dependiente	Resultado
Algoritmos de encriptación de archivos	Análisis comparativo para medir la integridad y confidencialidad en la transferencia en mensajería instantánea	Con la comparación de algoritmos de encriptación en la transferencia de archivos en una red pública se logró obtener algoritmos de encriptación más seguros.
		Con la comparación de algoritmos de encriptación en una red pública aumento el nivel de integridad y confidencialidad de los datos en la transferencia de archivos.
		Con la comparación de algoritmos de encriptación disminuirémos el tiempo de encriptación de los datos en la transferencia de archivos en una red pública.

Nota. Fuente: Elaboración propia

2.2 Población y Muestra

La población que se utilizó en esta indagación está integrada por algoritmos criptográficos que se utilizan en las empresas y como elemento de análisis a los algoritmos de encriptación conocidos mundialmente como código abierto, siendo la muestra tres algoritmos de encriptación AES, RC4 y 3DES.

2.3 Variables, Operacionalización

2.3.1 Variable Independiente

Algoritmos de encriptación de archivos.

2.3.2 Variable Dependiente

Transferencia de archivos en mensajería instantánea.

2.3.3 Operacionalización

Tabla 3

Operacionalización de variables

Variable dependiente	Dimensiones	Indicadores	Técnicas e instrumentos
Análisis comparativo para medir la integridad y confidencialidad en la transferencia en mensajería instantánea	Archivo	Tamaño de archivo	Algoritmos de encriptación. Software para capturar de información. Reporte de software. Aplicativo para el conteo de paquetes
	Paquete	Numero de paquetes	
	Encriptación	Numero de paquetes encriptados y no encriptados	
	Rendimiento	Tiempo de velocidad en transferencia de archivo	
Variable independiente	Dimensiones	Indicadores	
Algoritmos de encriptación de archivos	Grado de seguridad	Disponibilidad e integridad	

Nota. Fuente: Elaboración propia

2.4 Técnicas e Instrumentos de Recolección de Datos, Validez y Confiabilidad

2.4.1 Técnicas de Recolección de Datos

La observación: Es una técnica que se utiliza para obtener un registro lógico, visual y verificable de lo que se intenta conocer; asimismo nos permite la captación más objetiva de lo que sucede en el mundo entero, ya sea para analizarlo, describirlo o exponerlo desde un aspecto científico; con la discrepancia de lo que sucede en el mundo práctico, en el cual el ser humano utiliza la información observada de una forma práctica con la finalidad de resolver sus necesidades o problemas.

Entrevistas: Entrevisté a profesionales expertos en ciberseguridad, adquiriendo información de manera detallada que tipo de algoritmo de encriptación utilizan los servidores ofreciendo mayor seguridad a los datos.

2.4.2 Instrumentos de Recolección de Datos

Se empleó la técnica de análisis registrado o documentado al resultado obtenido, consiste fundamentalmente en la utilización de instrumentos apropiados con la finalidad de establecer una concordancia entre los hechos reales y la hipótesis, por medio del análisis documentado, asimismo permitió la selección de la información más sobresaliente. Utilizando en la recolección de los datos los siguientes instrumentos.

- a) **Wireshark:** Es una herramienta que nos permite ver lo que sucede en la red de comunicación microscópicamente
- b) **FileZille:** Permite transferir ficheros de un servidor a un cliente.
- c) **AnyClient:** Es un software que trabaja como cliente, permite transferir información en la web es fácil de manipular, siendo compatible con todas las plataformas de sistemas operativos como: Windows, Linux y Mac OS X.
- d) **Excel:** Es un aplicativo que se utiliza como hoja de cálculo, permite filtrar la información de los paquetes encriptados y no encriptados, representándolo gráficamente.

2.4.3 Procedimiento Para la Recolección de Datos

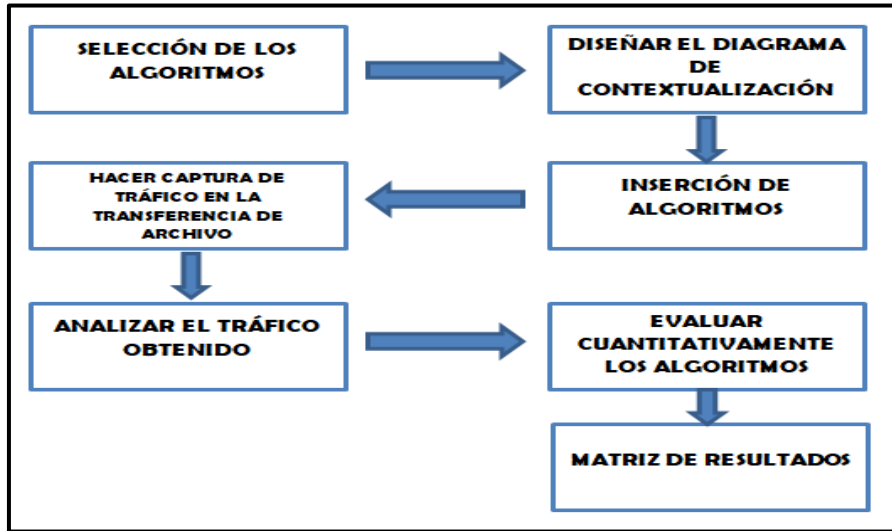


Figura 15 . Procesos de Recolección de Datos.

2.5 Procedimiento de Análisis de Datos

A los datos obtenidos se analizó estadísticamente haciendo uso de las siguientes fórmulas:

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

$$Td = Tf - Ti$$

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

Ti = Tiempo Inicial

Total de paquetes capturados, encriptados y no encriptados Es la suma de los paquetes encriptados y los paquetes no encriptados.

$$TP = Pe + P no e$$

$$Pe = TP - P no d$$

$$P no d = TP - Pe$$

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

P no e = Paquetes no encriptados

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

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

2.6 Criterios Éticos

En esta investigación se tuvo en cuenta lo siguiente:

- a) **Criterio de confiabilidad.** Los datos que se obtuvieron en el presente estudio, son legales y profesionales y no causan perjuicio al usuario involucrado; manifestado en la Ley N° 29733: “Ley de protección de datos personales”, en su título IV: “Obligaciones del titular y del encargado del banco de datos personales” En su artículo 28 señala: “Que recopilar datos personales por medios ilícitos, fraudulentos o desleales está penado por el estado peruano”.
- b) **Criterio de Conformabilidad.** Las afirmaciones y resultados que se obtuvieron en este estudio están validados y confirmados por profesionales especializados en la materia, como se anuncia: El Código Deontológico del Colegio de Ingenieros del Perú en su Capítulo III “Faltas Contra la Ética Profesional y Sanciones”, en su Artículo 105 señala: “Los ingenieros serán objetivos y veraces en sus informes y declaraciones, y expresarán opiniones en temas de ingeniería”.

2.7 Criterios de Rigor Científico

En este estudio los criterios de rigor científico utilizados son: La validez externa e interna.

La validez externa: Consiste en la generalización de los resultados obtenidos de la indagación en otras muestras.

La Validez interna: Es la metodología que permite la evaluación de manera idónea, utilizando mecanismos de control; consiste en la evaluación externa e interna. La

estrategia que nos permite aumentar la validez interna de una investigación, permitiéndonos un diseño de investigación sólida; aun en los argumentos en que esto sea aceptado, es necesario analizar la información con la finalidad de establecer la respectiva validez. De igual modo, se ejecutó la validez interna con la finalidad de evaluar con originalidad e idoneidad la presente tesis, obteniendo la solidez en el esquema de este estudio.

III. RESULTADOS

3.1 Resultado en Tablas y Figuras

3.1.1 Evaluación Cuantitativa de los Algoritmos

Se utilizó el mismo archivo de prueba de 8.55 MB en la transferencia de archivo entre el servidor y el cliente con los tres algoritmos elegidos.

3.1.1.1 Tiempo de envío.

Tabla 4

Evaluación por el tiempo de envío

Algoritmo	Por el tiempo de envío
RC4	00:03:80
3DES	00:03:80
AES	00:03:20

Nota. Fuente: Elaboración propia

El tiempo que necesita el algoritmo AES para enviar el mismo archivo es menor al resto de algoritmos, optimizando los recursos del computador.

3.1.1.2 Número de paquetes

Tabla 5

Evaluación por el número de paquetes

Algoritmo	Por el número de paquetes
RC4	8069
3DES	7951
AES	7943

Nota. Fuente: Elaboración propia

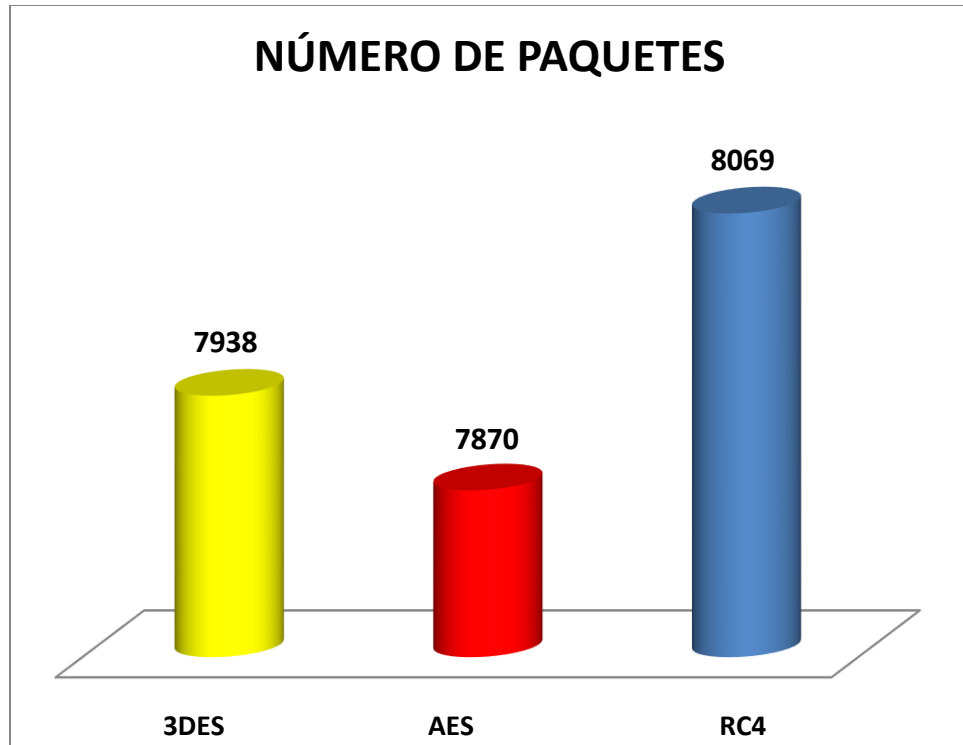


Figura 16. Evaluación por el número de paquetes.

ANÁLISIS E INTERPRETACIÓN DE LA FIGURA N° 16

Como se puede apreciar en la figura N° 16 se compara los algoritmos criptográficos según la fragmentación de paquetes que se obtiene de un archivo de 8.55 MB nos da los siguientes resultados:

- De un archivo de 8.55 MB el algoritmo criptográfico 3DES fragmenta al archivo en 7938 paquetes, el algoritmo AES en 7879 paquetes y el algoritmo RC4 en 8059 paquetes.

3.1.1.3 Paquetes no encriptados de la Pc origen (servidor)

Tabla 6

Evaluación por el número de paquetes no encriptados de la Pc origen (servidor)

Algoritmo	Por el número de paquetes no encriptados – Pc origen
RC4	128
3DES	86
AES	69

Nota. Fuente: Elaboración propia

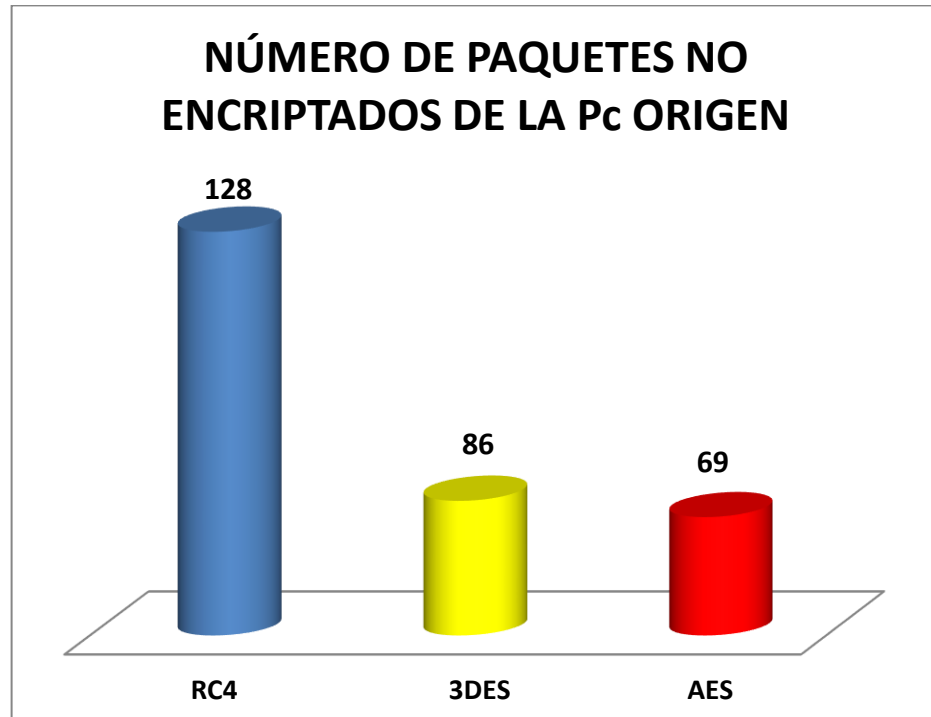


Figura 17. Evaluación por el número de paquetes no encriptados de la Pc origen (servidor)

ANÁLISIS E INTERPRETACIÓN DE LA FIGURA N° 17

Como se puede apreciar en la figura N° 17 se compara los algoritmos criptográficos con respecto al número de paquetes no encriptados de un archivo de 8.55 MB del servidor al cliente nos da los siguientes resultados:

- El algoritmo criptográfico RC4 128 paquetes no encripta, 3DES 86 paquetes y AES 69 paquetes.

3.1.1.4 Paquetes no encriptados de la Pc destino (cliente)

Tabla 7

Evaluación por el número de paquetes no encriptados de la Pc destino (cliente)

Algoritmo	Por el número de paquetes no encriptados – Pc destino
RC4	1293
3DES	1216
AES	1264

Nota. Fuente: Elaboración propia



Figura 18. Evaluación por el número de paquetes no encriptados de la Pc destino (cliente)

ANÁLISIS E INTERPRETACIÓN DE LA FIGURA N° 18

Como se puede apreciar en la figura N° 18 se compara los algoritmos criptográficos con respecto al número de paquetes no encriptados de un archivo de 8.55 MB del cliente al servidor nos da los siguientes resultados:

- El algoritmo criptográfico RC4 1293 paquetes no encripta, 3DES 1216 paquetes y AES 1264 paquetes.

3.1.1.5 Paquetes encriptados de la Pc de origen (servidor)

Tabla 8

Evaluación por el número de paquetes encriptados de la Pc origen (servidor)

Algoritmo	Por el número de paquetes encriptados de la Pc origen
RC4	6196
3DES	6197
AES	6200

Nota. Fuente: Elaboración propia

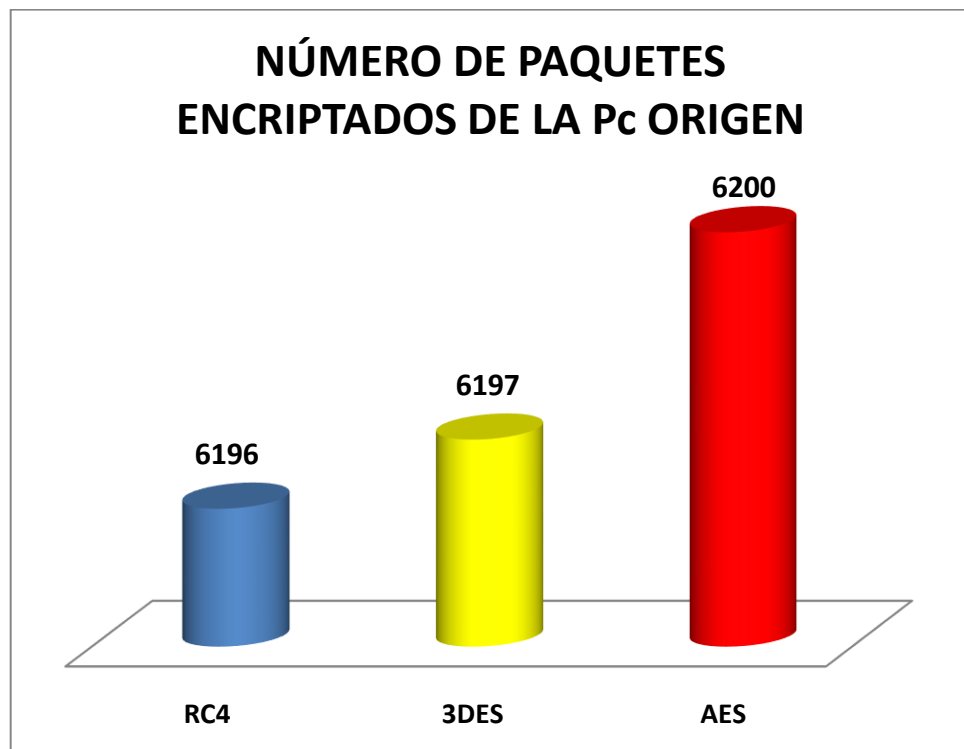


Figura 19. Evaluación por el número de paquetes encriptados de la Pc origen (servidor)

ANÁLISIS E INTERPRETACIÓN DE LA FIGURA N° 19

Como se puede apreciar en la figura N° 19 se compara los algoritmos criptográficos con respecto al número de paquetes encriptados de un archivo de 8.55 MB del servidor al cliente nos da los siguientes resultados:

- El algoritmo criptográfico RC4 6193 paquetes encripta, 3DES 6197 paquetes y AES 6200 paquetes.

3.1.1.6 Paquetes encriptados de la Pc destino (cliente)

Tabla 9

Evaluación por el número de paquetes encriptados de la Pc destino (destino)

Algoritmo	Por el número de paquetes encriptados de la Pc destino
RC4	452
3DES	421
AES	408

Nota. Fuente: Elaboración propia

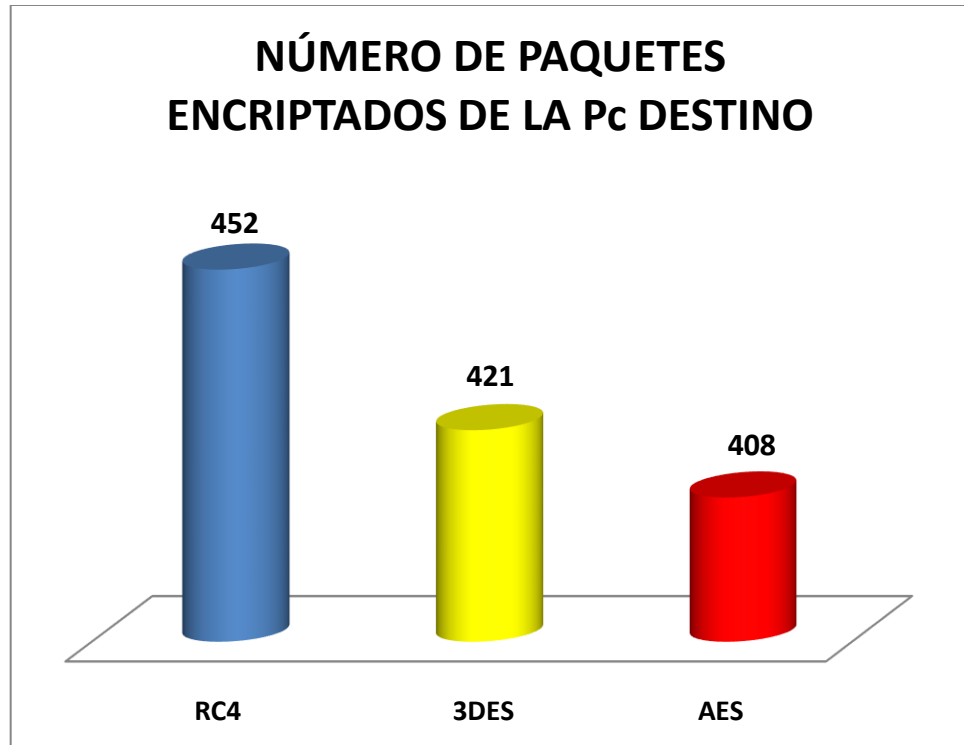


Figura 20. Evaluación por el número de paquetes encriptados de la Pc destino (cliente)

ANÁLISIS E INTERPRETACIÓN DE LA FIGURA N° 20

Como se puede apreciar en la figura N° 20 se compara los algoritmos criptográficos con respecto al número de paquetes encriptados de un archivo de 8.55 MB del cliente al servidor nos da los siguientes resultados:

- El algoritmo criptográfico RC4 462 paquetes encripta, 3DES 421 paquetes y AES 408 paquetes.

3.1.2 Resume de Evaluación Cuantitativa de los Algoritmos

En la Tabla número 11 se muestra el resumen de la evaluación de tráfico de datos.

Tabla 10

Resumen de la evaluación de tráfico de datos

ALGORITMO	RC4	3DES	AES
Tamaño de archivo	8.55 Mb	8.55 Mb	8.55 Mb
Número de paquetes	8069	7951	7943
Tiempo de envió	00:00:03:80	00:00:03:80	00:00:03:20
Número de paquetes no encriptados de la Pc origen (servidor)	128	86	69
Número de paquetes no encriptados de la Pc destino (cliente)	1293	1216	1264
Número de paquetes encriptados de la Pc origen (servidor)	6196	6197	6200
Número de paquetes encriptados de la Pc destino (cliente)	452	421	408

Nota. Fuente: Elaboración propia

En la tabla N° 10 podemos visualizar que en la comparación de los algoritmos criptográficos en la transferencia de un archivo de 8.55 de un servidor SFTP a un host Cliente o viceversa podemos afirmar:

Con respecto al fraccionamiento del archivo. AES tiene 7943 paquetes, 3DES 7951 y RC4 8069 esto quiere decir que AES fracciona a un archivo en menor cantidad de paquetes. Así mismo con respecto al tiempo de envió AES tiene 00:00:03:20, 3 DES 00:00:03:80 y RC4 00:00:03:80 quiere decir que AES ocupa un menor tiempo en el envión de un archivo. Con respecto al número de paquetes no encriptado del servidor al cliente

AES tiene 69, 3DES 86, RC4 128 y con los paquetes no encriptados del cliente al servidor AES tiene 1264, 3DES 1216 y RC4 1293, siendo AES el segundo algoritmo que cumple esta característica con mayor rigurosidad. Así mismo con el número de paquetes encriptados del servidor al cliente AES encripta 6200, 3DES 6197, RC4 6196 y con respecto del host Cliente al servidor AES 408, 3DES, 421 y RC4 452. Siendo AES el que tiene mayor encriptación del servidor al cliente y RC4 de del cliente al servidor

Llegando a la conclusión que el algoritmo AES es el más seguro en la transferencia de archivos en una red pública, teniendo en cuenta su integridad y confidencialidad de la información, además disminuye el tiempo de encriptación de los datos en la transferencia de un servidor a un host cliente o viceversa.

3.2 Discusión de Resultados

En esta tesis se investigó la comparación de algoritmos de encriptación que ofrece cada algoritmo en cuanto al número de paquetes que divide al archivo, número de paquetes que encripta y no encripta y sobre todo el tiempo de velocidad que transfiere el archivo entre el servidor SFTP y el Cliente o viceversa, en mensajería instantánea en la Red Pública del Instituto de Educación Tecnológico Público “Utcubamba”, se hizo una selección de algoritmos criptográficos que mayormente usan las empresas en la actualidad, para ello se recogió información mediante una ficha de expertos e información de artículos científicos, eligiéndose a los algoritmos por longitud de clave, resistencia al criptoanálisis y la seguridad, siendo elegidos los algoritmos: 3DES, AES y RC4. Con base a esto se planteó la hipótesis en la que se desarrolla en esta investigación. El método que se utilizó para el análisis de la información fue descriptivo comparativo porque me permitió describir y comparar los algoritmos de estudio, porque me permitió la manipulación de las variables de estudio, con la finalidad de obtener la información se instaló el servidor SFTP y el host Cliente, configurando el algoritmo diffie-hellman-group1-sha1 que permitió intercambio de llaves públicas, sobre todo para el envío de mensajes instantáneos, esta clave pública permite cifrar descifrar el paquete cuando se envía del servidor al cliente o viceversa. Así mismo se configuró los algoritmos y por medio del software FileZilla permitió la transmisión de ficheros a tiempo real, con sólo arrastrar y luego soltar uno o más archivos desde el Directorio de Archivos Remota hacia el Directorio de Archivos Local o

viceversa y con el software Wireshark se capturo los paquetes fragmentados e encriptados y no encriptados con su respectivo tiempo de envío.

De acuerdo con los resultados de esta investigación del análisis comparativo de los algoritmos elegidos, se pudo observar que el algoritmo AES al archivo de 8.54 MB lo fragmento en 7943 paquetes, esto quiere decir que cada paquete contiene 1 127 3875160519 bytes y pesa 0.0010751605 Mb de los cuales encripto 6200 paquetes y no encripto 69 paquetes en la comunicación entre el servidor y el cliente. En la comunicación del cliente al servidor encripto 408 paquetes y no encripto 1264. El tiempo utilizado para realizar esta función utilizo un tiempo de 00:00:03:20. El algoritmo RC4 al mismo archivo lo fragmento en 8069 paquetes, esto quiere decir que cada paquete contiene 1 109.78300116111 y pesa 0.0010583715 Mb de los cuales encripto 6196 paquetes y no encripto 128 paquetes en la comunicación entre el servidor y el cliente. En la comunicación del cliente al servidor encripto 452 paquetes y no encripto 1293. El tiempo utilizado para realizar esta función utilizo un tiempo de 00:00:03:80. El algoritmo 3DES al mismo archivo lo fragmento en 7951 paquetes, esto quiere decir que cada paquete tiene 1 126.253180732 Bytes y pesa 0.0010740740787 Mb de los cuales encripto 6197 paquetes y no encripto 86 paquetes en la comunicación entre el servidor y el cliente. En la comunicación del cliente al servidor encripto 421 paquetes y no encripto 1216. El tiempo utilizado para realizar esta función utilizo un tiempo de 00:00:03:80.

Podemos afirmar que el algoritmo criptográfico AES fragmenta el archivo en menor cantidad de paquetes, encripta la mayor cantidad y los envía en el menor tiempo. Por lo tanto se recomienda que las empresas utilicen este algoritmo de encriptación para la protección de su información ya que es la parte más importante de una organización empresarial.

En este estudio de investigación se ha comprobado que la seguridad informática en las redes públicas es muy importante porque permiten que los equipos de cada usuario no sufran ataques informáticos.

Se ha evidenciado que la mayor parte de ataques se producen por las malas prácticas del usuario pues desconocen de la seguridad de los algoritmos de encriptación que utilizan los cifrados de los datos.

Existe en el mercado una gran cantidad de herramientas de protección como son los algoritmos de encriptación, las cuales se pueden utilizar de acuerdo como el usuario lo desee. Siempre se debe estar de acorde con las actualizaciones de la tecnología y poder tener los soportes constantes de cualquier fabricante.

3.3 Aporte Práctico

3.3.1 Selección de Algoritmos Criptográficos para la Transferencia de Archivos en el Mercado Tecnológico.

En este objetivo se seleccionó algoritmos criptográficos que mayormente usan en las empresas, según el recojo de información utilizando la ficha de expertos (Ficha N°01) y la información de los artículos científicos de esta investigación se ha elegido por la longitud de la clave, resistencia al criptoanálisis y la seguridad los siguientes algoritmos: 3DES, AES y RC4.

Tabla 11.

Algoritmo simétrico de encriptación

ALGORITMO	TIPO DE CLAVE	LONGITUD DE LA CLAVE	TAMAÑO DEL BLOQUE UTILIZADO	NO. DE RONDAS UTILIZADAS	RESISTENCIA A CRIPTOANÁLISIS	SEGURIDAD	AÑO DE CREACIÓN	PROTOCOLOS	PESO
3DES	Simple (dividida en tres partes)	(k1, k2, k3) 168 bits, (k1 y k2 son las mismas) 112 bits	128, 192, 256 bits	48	Fuerte contra : criptoanálisis fuerza bruta	Seguro	1997	TLS, S-HTTP	4 de 20
AES	Simple	128, 192, 256 bits	128, 192, 256 bits	10, 12, 14	Fuerte contra: criptoanálisis diferencial, lineal y truncado diferencial	Seguro	2001	SSL(Secure Socket Layer, PCT(Private Communications Technology)	4 de 20
RC4	Simple	128, 192 y 256 bits	32, 64 o 128 bits	18	Resistente a: criptoanálisis diferencial, fuerza bruta	Seguro	1994	SSL(Secure Socket Layer, PCT(Private Communications Technology)	4 de 20
RSA	Simple	128,192,256 bits	128 bits	20	Vulnerable contra: criptoanálisis diferencial, lineal y truncado.	Seguro	1998	SSL(Secure Socket Layer, PCT(Private Communications Technology)	4 de 20
BLOWFISH	Simple	32 – 448 bits	64 bits	16	Fuerte contra : Diferencial, Fuerza bruta	Seguro	1993	SSL	3 de 20
IDEA	Simple	128 bits	64 bits	19	Vulnerable a: Diferencial, Fuerza bruta	Vulnerable	1991	TLS	3 de 20

Nota. Fuente: Elaboración Propia.

3.3.2 Diseñar un Escenario de Prueba para la Transferencia de Archivos de Forma Segura

El escenario de prueba en transferencia de archivos se implementó en equipos reales del laboratorio de computo del Instituto de Educación Superior Tecnológico Público “Utcubamba”.

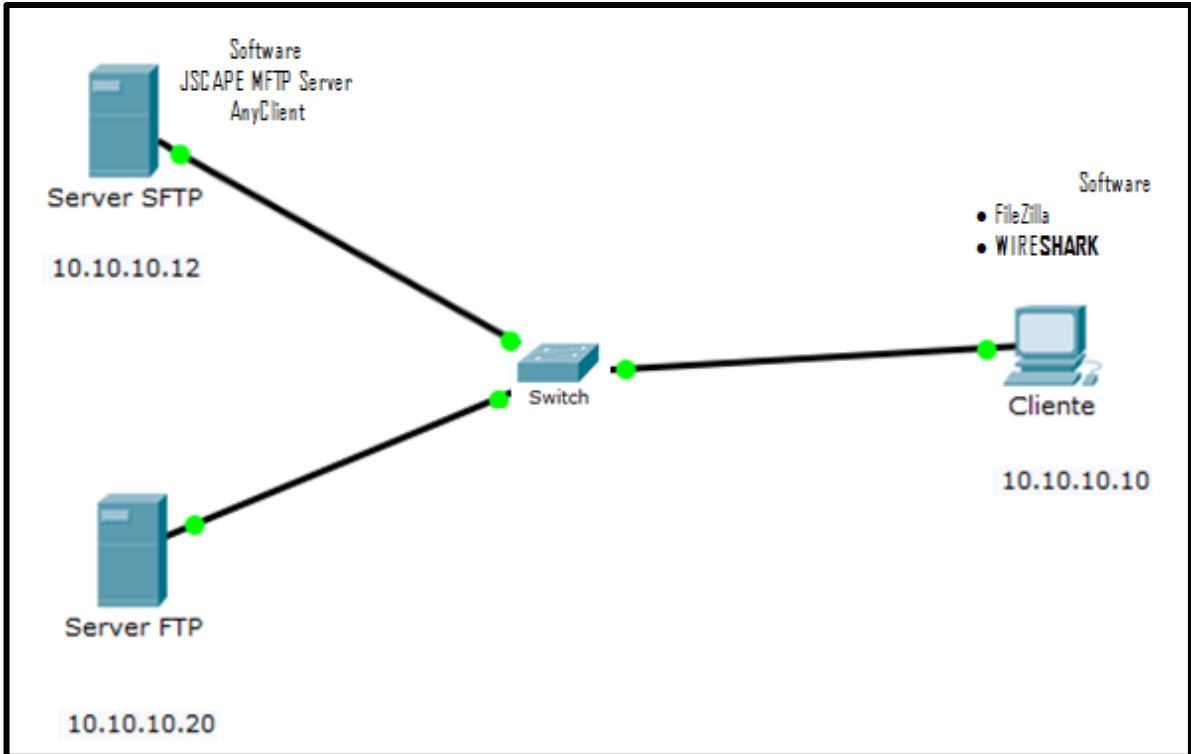


Figura 21. Diseño de un escenario de prueba

3.3.2.1 Servidor SFTP

En el Instituto de Educación Superior Tecnológico Público “Utcubamba” se cuenta con una red pública y con la finalidad de dar seguridad a la red, se decidió por una red de clase A para 254 equipos como máximo.

Se implementó el servidor SFTP (Figura 23 – 31), porque es seguro en la conexión de un servidor y un host cliente en la transferencia de los archivos. Utiliza el protocolo SSH como medio de transmisión seguro. Este servidor cumple con los

algoritmos criptográficos elegidos en nuestra investigación como son: 3DES, AES y RC4.

Este servidor SFTP realiza un cifrado con capas, es por eso que ningún individuo puede visualizar el usuario y contraseña de modo sencillo. Los datos que se trasladan entre el servidor y cliente está encriptado, es por ello que el hacker no puede modificar ni interceptar los datos que se trasladan en una red pública.

Una de las características del servidor implantado en I.E.S.T.P. “Utcubamba” es la accesibilidad de forma local y remota. Los permisos serán controlados de todos los usuarios que tengan acceso al servidor SFTP como escritura, lectura y ejecución. Mediante su usuario y contraseña se verificara la autenticación.

Los softwares utilizados en la instalación y configuración fue el JSCAPE MFTP Server y AnyCliente (figura 23 - 34), este último software me permitió conectarme con el protocolo SFTP remotamente.

3.3.2.2 Servidor FTP

Con la finalidad de poder visualizar la vulnerabilidad que tiene una red pública se configure un servidor FTP en Windows con el IP 10.10.10.20 (figura 36-40) en el laboratorio de redes del I.E.S.T.P. “Utcubamba.

Este servidor me permitió realizar una comunicación rápida entre el servidor y el cliente, en el momento de transferencia de archivos este protocolo FTP utilizo un modelo de capas de red TCP/IP, de igual forma encapsula un password o clave secreta que con la captura del paquete POST con el Wireshark se pudo visualizar el usuario y contraseña tal como se muestra en la figura N°41.

3.3.2.3 Cliente

La máquina cliente se configure con el IP 10.10.10.10 y se instalaron los programas FileZilla (figura 42) que me permitió transferir el archivo en tiempo real, además me mostro el tiempo que demora en encriptar y transferir el archivo entre servidor y cliente, mostrándome además con que algoritmo se está encriptado los

paquetes ya sea con 3DES, AES y RC4, el programa WIRESHARK me permitió capturar los paquetes fraccionados, encriptados y no encriptados del archivo enviado del servidor al cliente y del cliente al servidor.

3.3.2.4 Switch

Se instaló un switch de 12 puertos TPLINK que me permitió conectar los equipos en red, formando una red de área local (LAN). La topología elegida fue estrella.

3.3.2.5 Cable Serial.

Se Utilizó para la transmisión de los datos entre el servidor y el cliente, utilizándose el protocolo de comunicación en serie. La conexión depende del tipo de puerto a utilizar.

3.3.3 Construcción del Prototipo de Implementación de Algoritmos de Encriptación.

Para construir el prototipo de implementación de los algoritmos de encriptación, se diseñó el siguiente escenario.

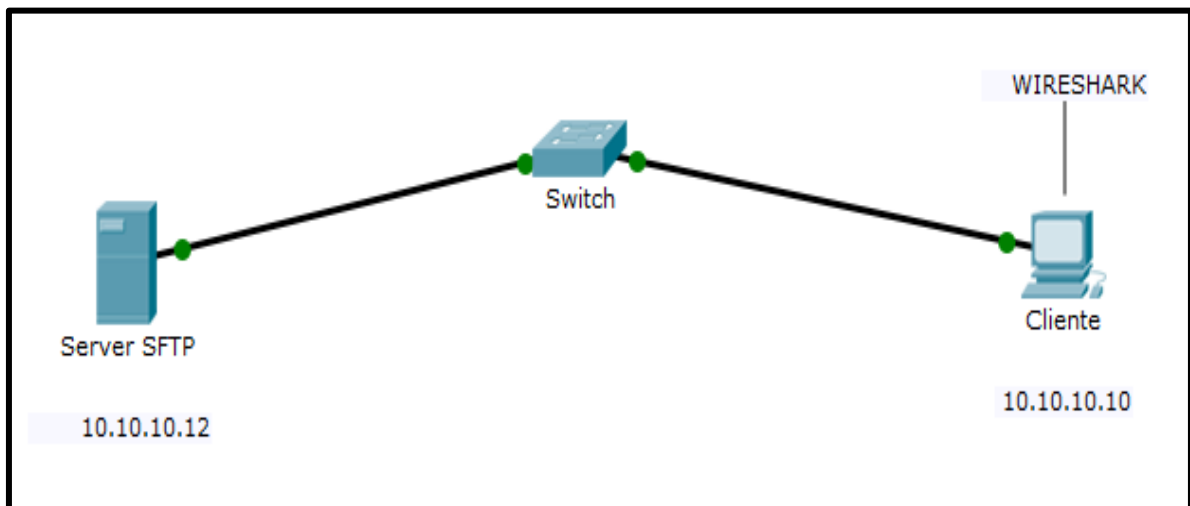


Figura 22. Prototipo de implementación de algoritmos de encriptación.

Sniffer

Es un analizador de paquetes, es un programa que detecta todos los tramas de una red; permitiéndonos la captura del tráfico de información que se traslada en la red.

Wireshark

Es un programa gratis que trabaja en plataformas como Windows, Mac Os, Unix. Se utiliza para escanear los paquetes que viajan en una red, analiza protocolos (packet sniffer). Está combinado por dos elementos principales como, una librería que captura los paquetes y un analizador que permite el análisis de los paquetes.

3.3.3.1 Implementación del Algoritmo 3DES

En la fase 1 se configuró el algoritmo diffie-hellman-group1-sha1 (figura N°44) que permitió intercambio de llaves públicas. Este método criptográfico usa esta llave para el envío de mensajes. La clave pública permite cifrar descifrar el paquete cuando se envía del servidor al cliente o viceversa.

En la fase 2 se configuró el algoritmo 3DES que viene instalado en el software del servidor SFTP como se muestra en (figura N°44).

Su ecuación matemática que utiliza el algoritmo 3DES es:

Formula:

$$C = E^{K3}_{DES}(D^{K2}_{DES}(E^{K1}_{DES}(M)))$$

DONDE:

- Donde M es el mensaje a encriptar
- K3 y K2 y K1 son las claves DES.
- El texto encriptado es C
- E es la clave de Cifrado
- D es la clave de Des Cifrado.
- En la variante 3TDES las tres claves son diferentes; en la variante 2TDES, la primera y tercera clave son iguales.

3.3.3.2 Implementación del Algoritmo AES

En la fase 1 se configuró el algoritmo diffie-hellman-group1-sha1 (figura N°45) que permitió intercambio de llaves públicas. Este método criptográfico usa esta llave para el envío de mensajes. La clave pública permite cifrar descifrar el paquete cuando se envía del servidor al cliente o viceversa.

En la fase 2 se configuro el algoritmo AES que viene instalado en el software de servidor SFTP como se muestra en (figura N°45).

Su ecuación matemática que utiliza el algoritmo AES es:

AES está estructurado para poder trabajar en bytes. Así mismo, se interpreta cada byte como una escritura del polinomio:

$$b_7 x^7 + b_6 x^6 + b_5 x^5 + b_4 x^4 + b_3 x^3 + b_2 x^2 + b_1 x + b_0$$

Donde cada b_i es 0 o 1.

Add Round Key, se cambia en o-exclusiva, donde la multiplicación está definido como polinomio modelo de multiplicación $x^7 + x^4 + x^3 + x + 1$.

SubBytes Routine, En esta práctica, cada byte de esta etapa se reemplaza según la formula siguiente:

Para cada bit i , establezca b_i a b_i O exclusiva $b(i + 4) \bmod 8$ xor $b(i + 5) \bmod$

8 xor $b(i + 6) \bmod 8$ xor $b(i + 7) \bmod 8 + c_i$ donde $c = 63$ hex.

MixColumns, Esta función intercambia la seguridad de la información en cada una de las columna según con las siguiente fórmula:

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

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

Conjunto $s_2, c \oplus s_0, c \oplus s_1, c \oplus s_2, c \oplus s_3$, c

Conjunto $s_3, c \oplus s_0, c \oplus s_1, c \oplus s_2, c \oplus s_3$, c

Rutina AddRoundKey, hace un XOR entre las columnas de cada etapa y un mensaje de 32 bits de la clasificación de llave.

3.3.3.3 Implementación del Algoritmo RC4 (Rivest Cypher 4)

En la fase 1 se configuró el algoritmo diffie-hellman-group1-sha1 (figura N°46) que permitió intercambio de llaves públicas. Este método criptográfico usa esta llave para el envío de mensajes. La clave pública permite cifrar descifrar el paquete cuando se envía del servidor al cliente o viceversa.

En la fase 2 se configuro el algoritmo RC4 que viene instalado en el software de servidor SFTP como se muestra en (figura N°46).

Su ecuación matemática que utiliza el algoritmo RC4 es:

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

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

Donde K_i es la subclave que es usada en i-sima en una ronda y f es la función arbitraria.

3.3.4 Realización de Pruebas de Funcionamiento de los Algoritmos de Encriptación

Para desarrollar este objetivo se configuro el servidor SFTP y todos los host, además se instalaron las herramientas como: Wireshark, AnyCliente y FileZilla para hacer la transferencia de archivos en tiempo real y la captura de datos en los escenarios del prototipo. (Figura 47 – 73)

3.3.4.1 Instalación del Servidor SFTP

3.3.4.1.1 Configuración de un Servidor SFTP

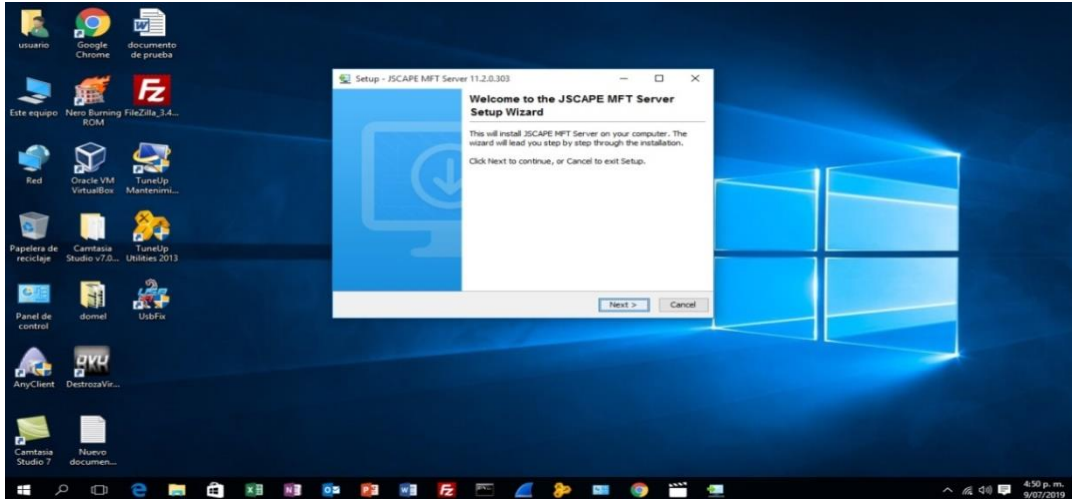


Figura 23. Instalación de software JSCAPE MFT Server

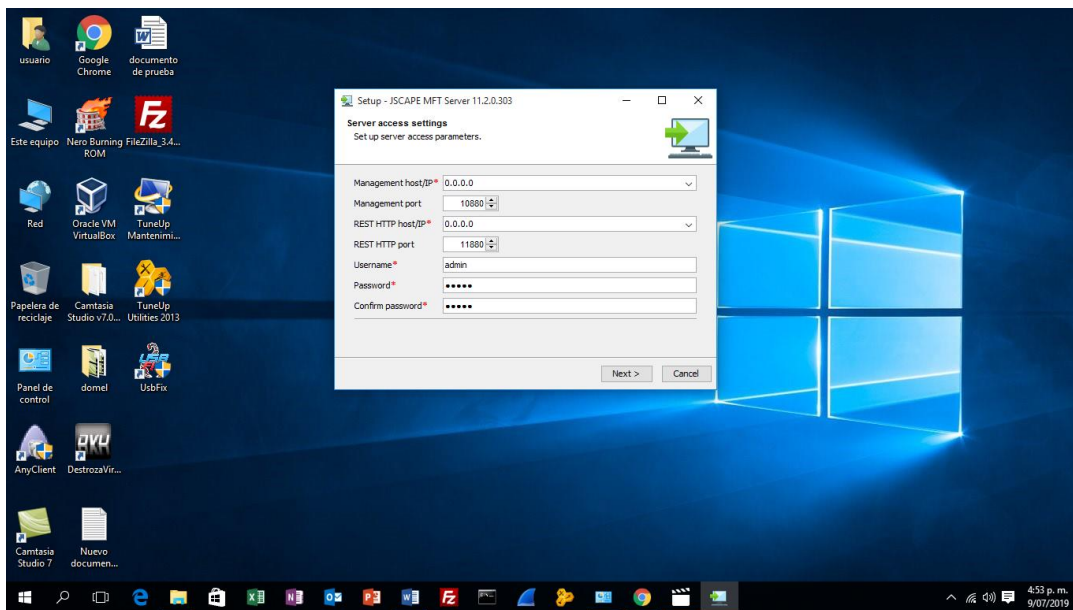


Figura 24. Configuración del usuario y contraseña

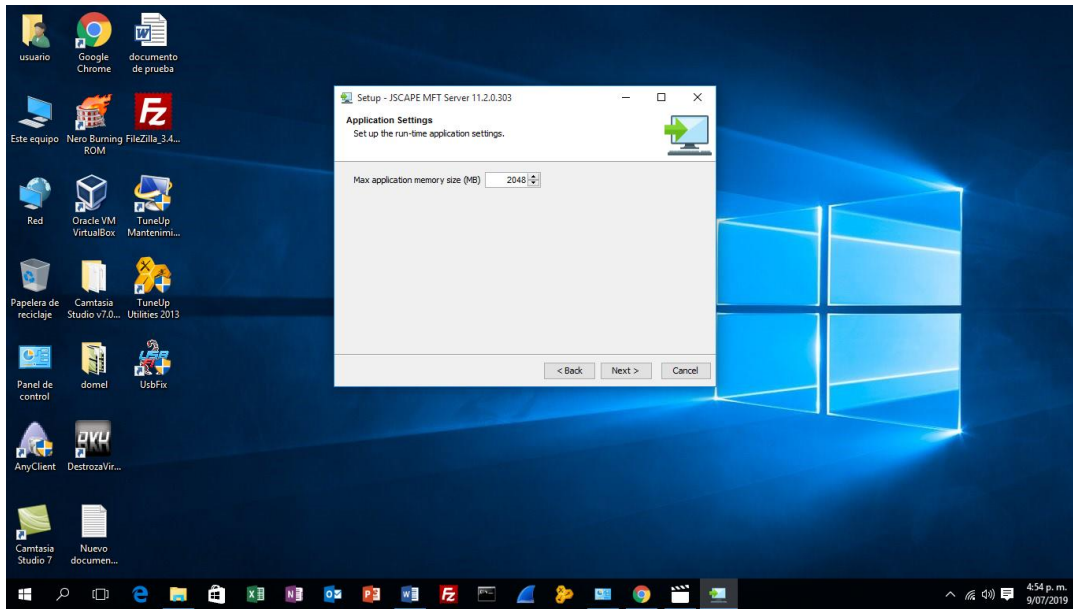


Figura 25. Configuración de memoria que utilizará el servidor SFTP

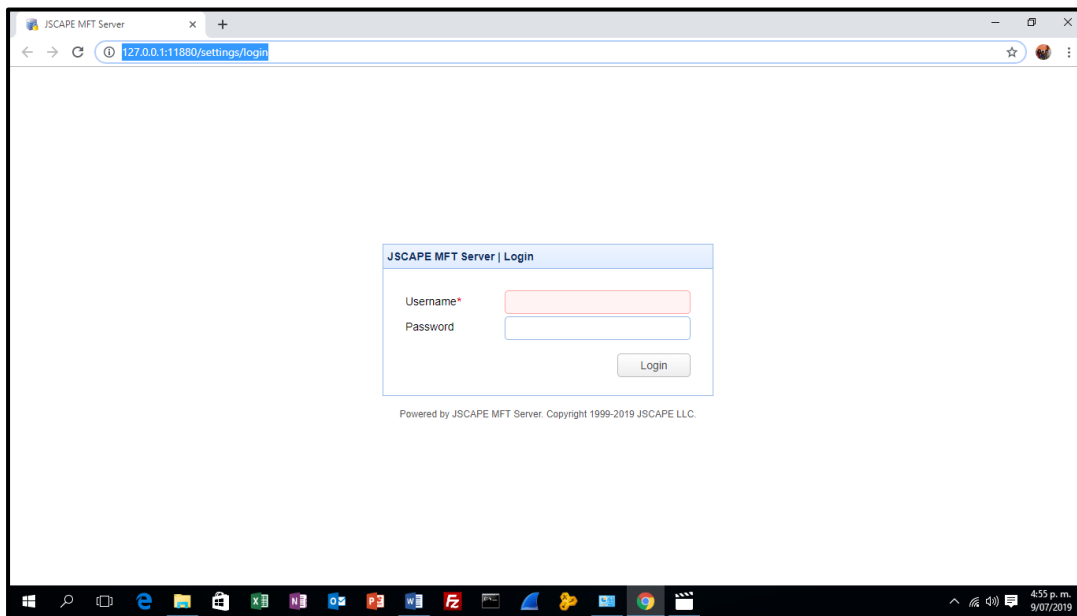


Figura 26. Ingresando al servidor

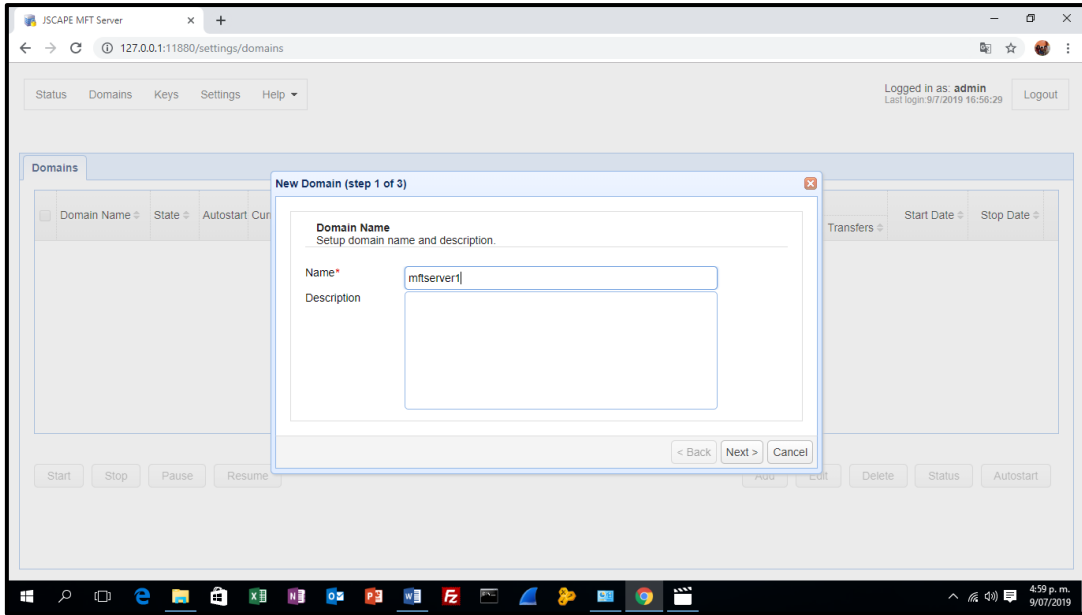


Figura 27. Configuración el nombre del servidor

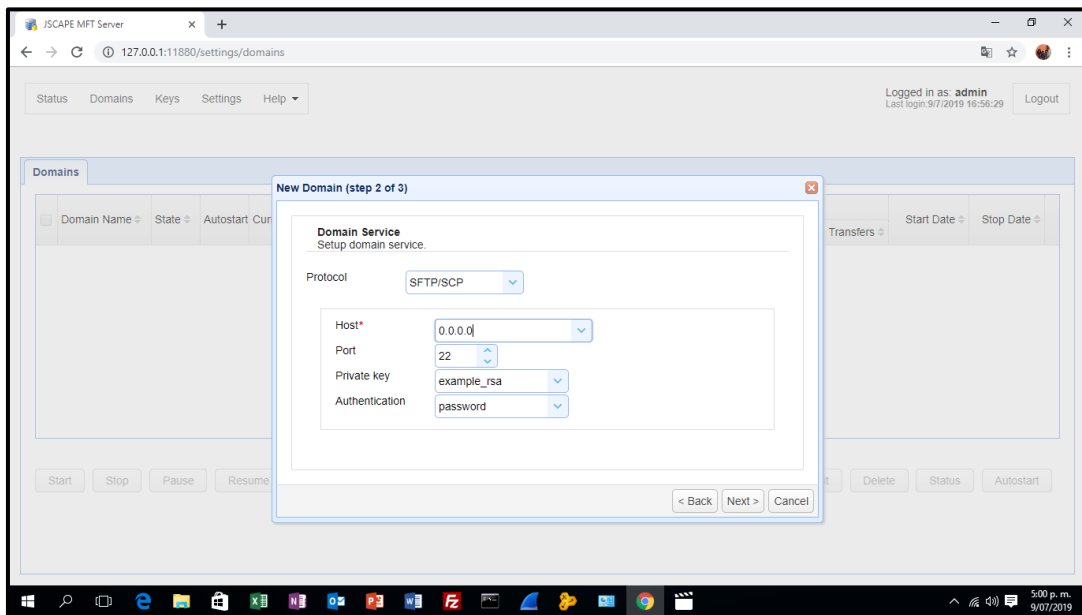


Figura 28. Configuración del protocolo y puerto

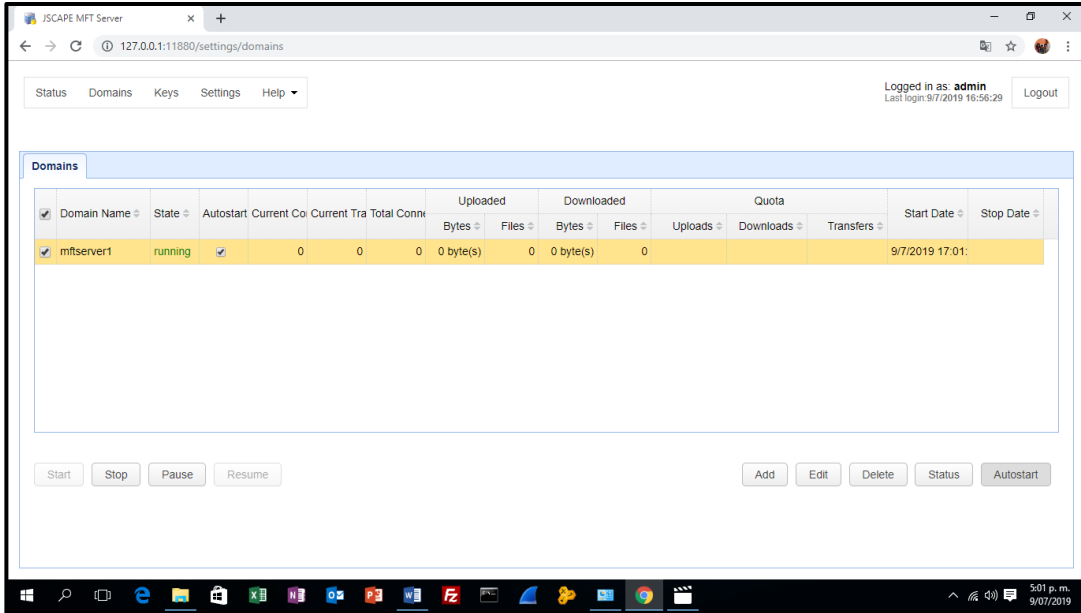


Figura 29. Configuración completa del servidor

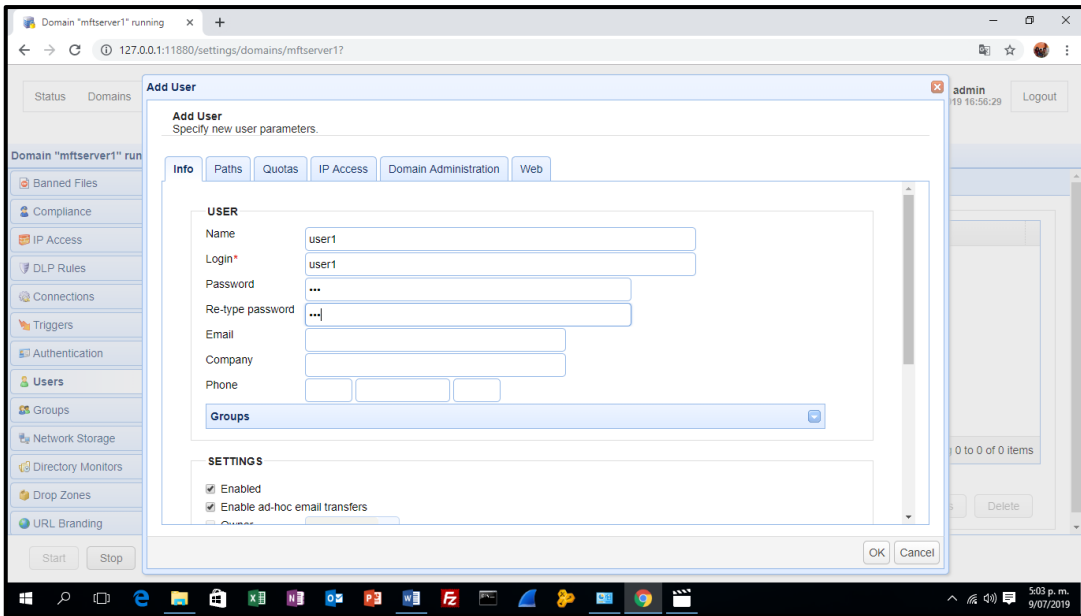


Figura 30. Configuración del usuario y contraseña

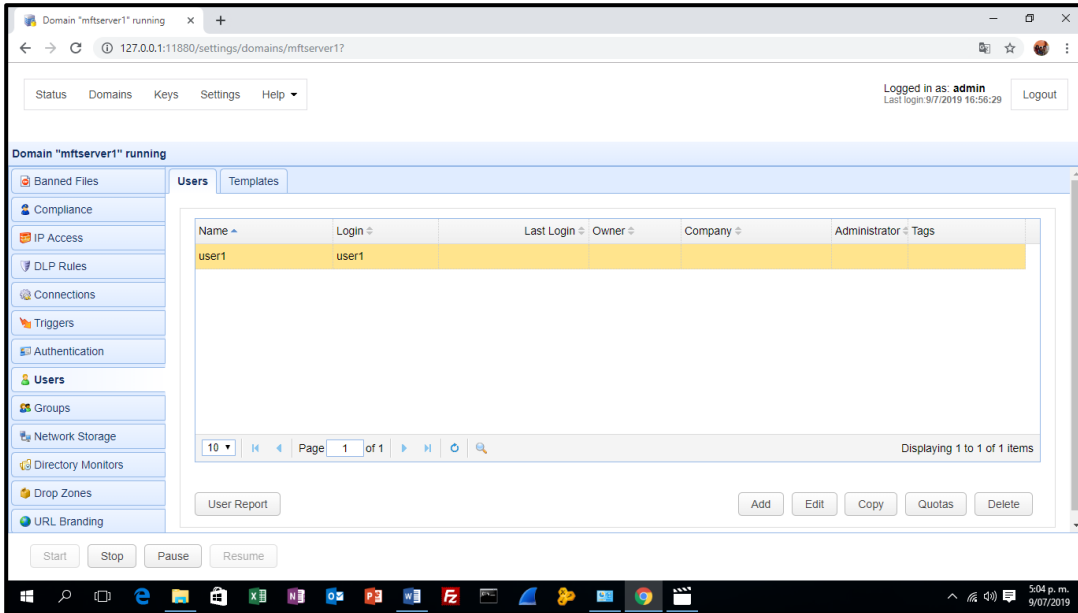


Figura 31. Usuario y contraseña configurada

3.3.4.2 Instalación AnyClient

3.3.4.2.1 Configuración de AnyClient

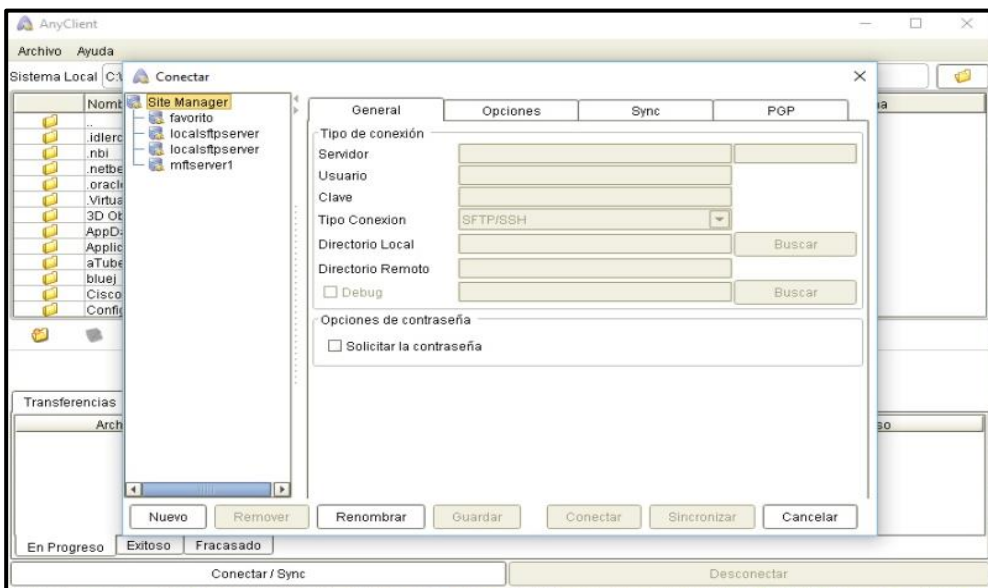


Figura 32. Configuración de la conexión con el servidor SFTP

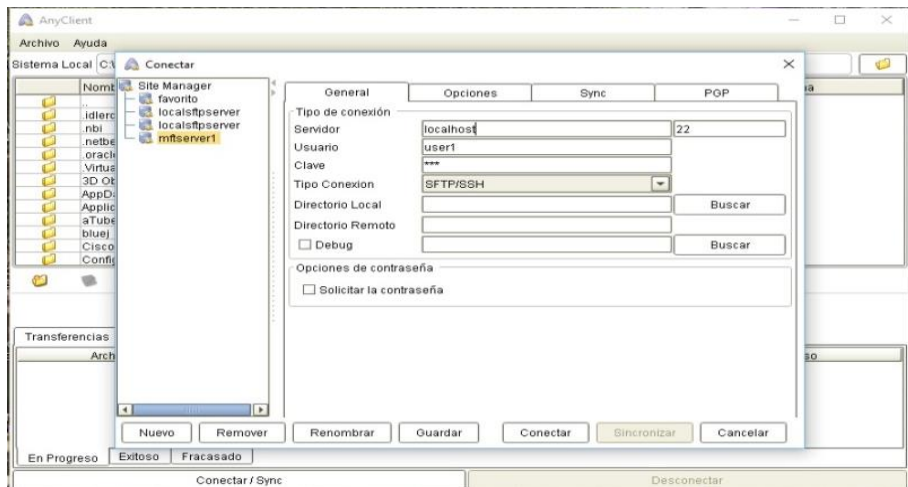


Figura 33: Configuración del usuario y contraseña, para la conexión con servidor SFTP

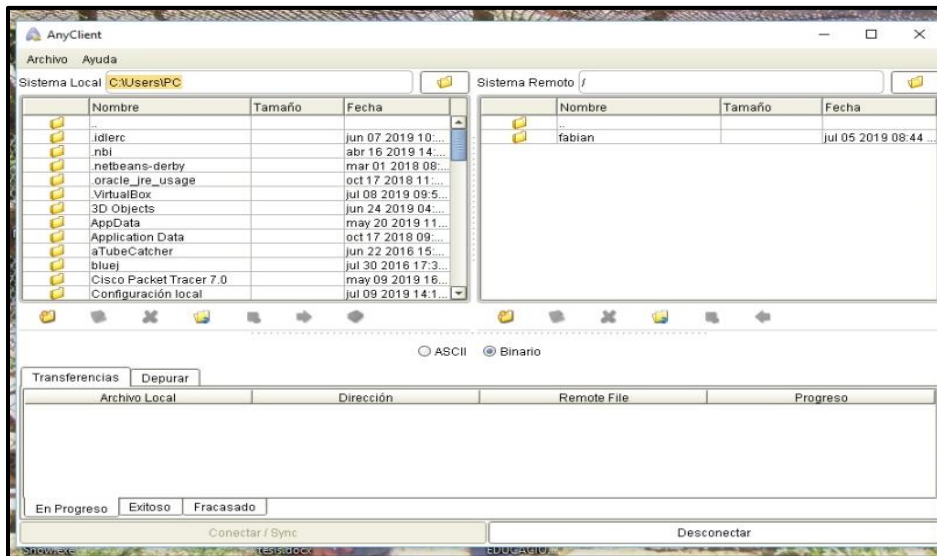


Figura 34. Conectado con el servidor SFTP

3.3.4.3 Instalación FileZilla Client

3.3.4.3.1 Configuración de FileZilla Client

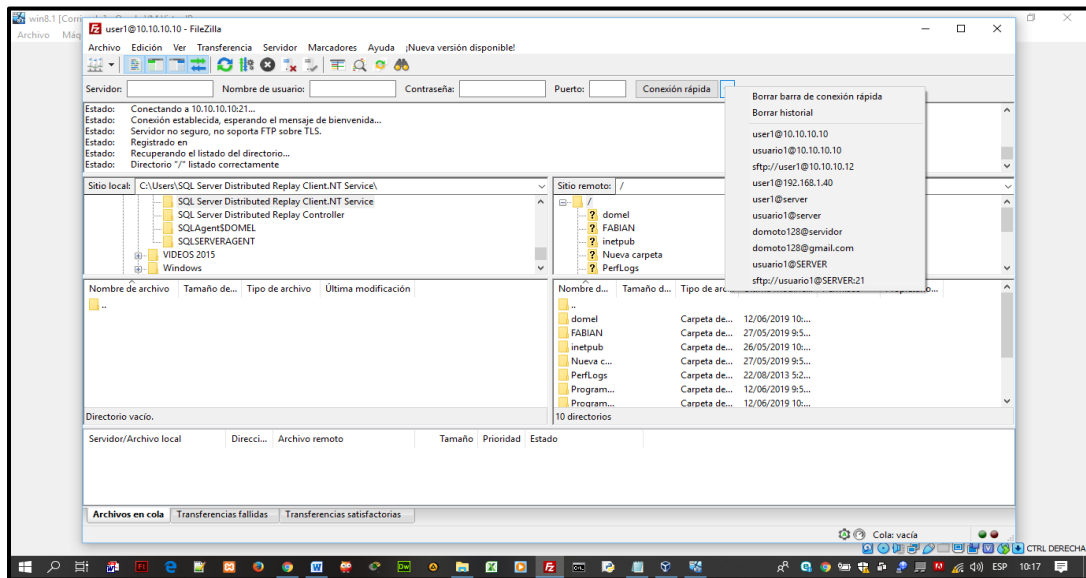


Figura 35: Conectado con el servidor SFTP

3.3.4.4 Configuración de un Servidor File Transfer Protocol (FTP)

FTP es un diseño entre servidor y cliente, utilizando la conexión de control y de los datos separados. Se configuro este servidor con la finalidad de poder visualizar la vulnerabilidad de la información en la transferencia de un archivo en un servidor sin protección criptográfico.

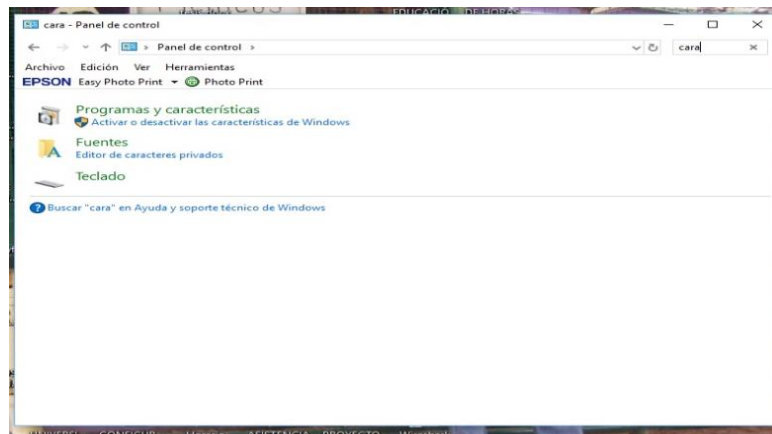


Figura 36. Ingresar al panel de control



Figura 37. Configuración de la extensibilidad de FTP y Servicio FTP

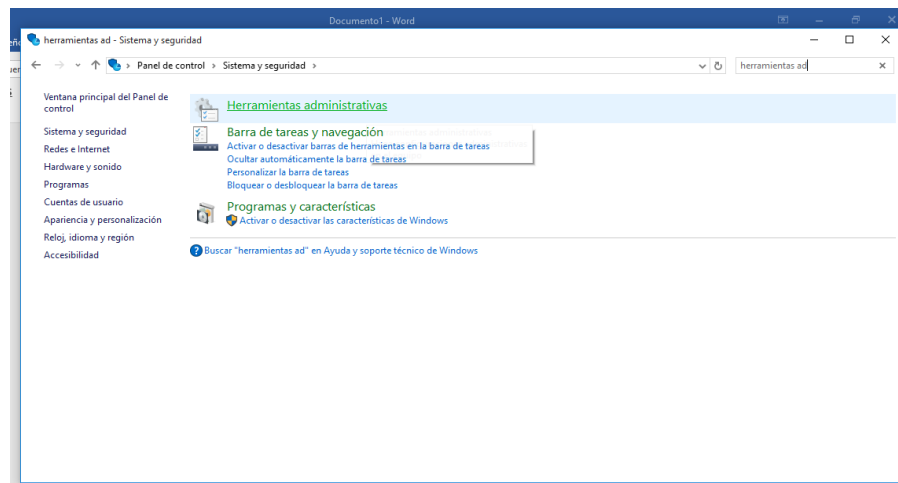


Figura 38. Configuración de las herramientas administrativas

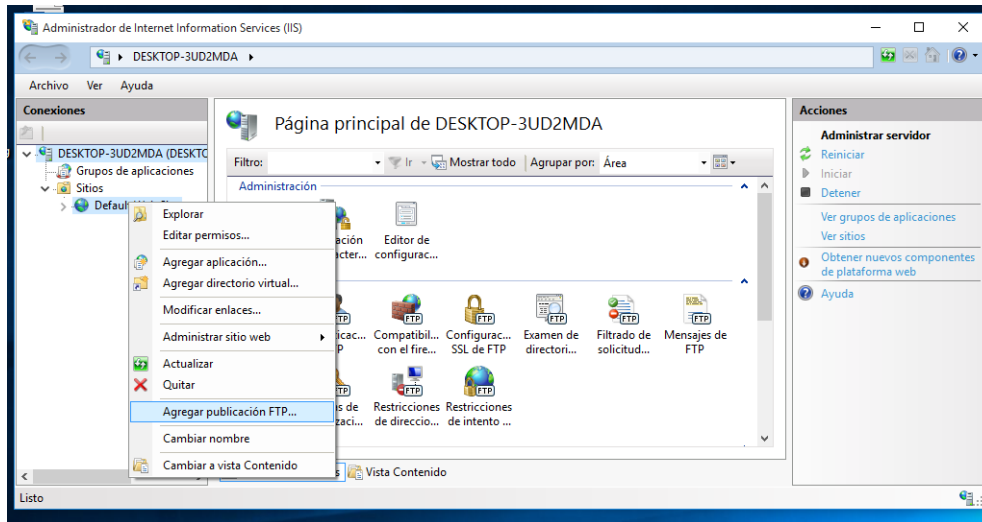


Figura 39. Configuración del Administrador de Internet Information Services (IIS), sitios y Agregar sitio FTP

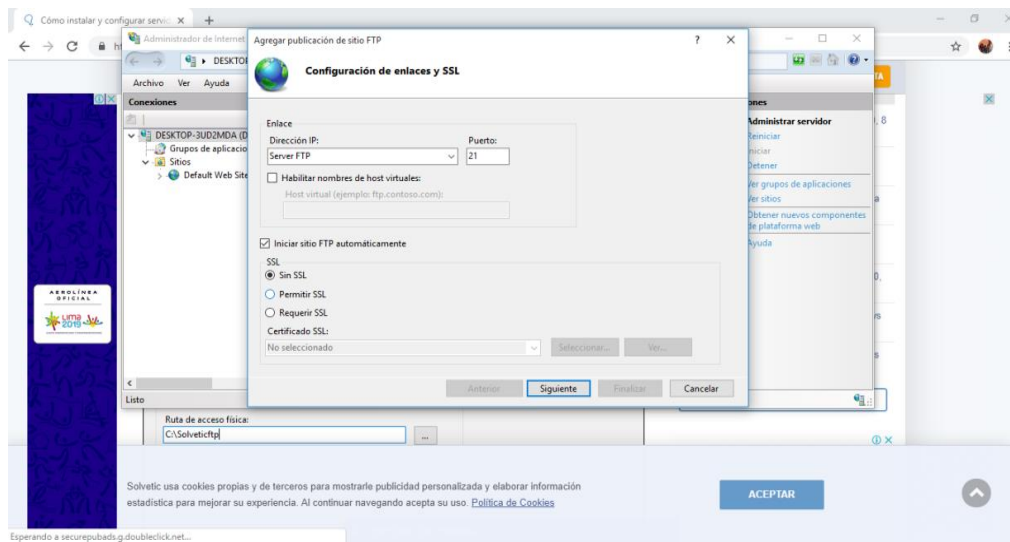


Figura 40. Configuración de la carpeta raíz de la unidad del sistema en la unidad C y el puerto 21

3.3.4.5 Captura de Usuario y Contraseña de un Servidor FTP

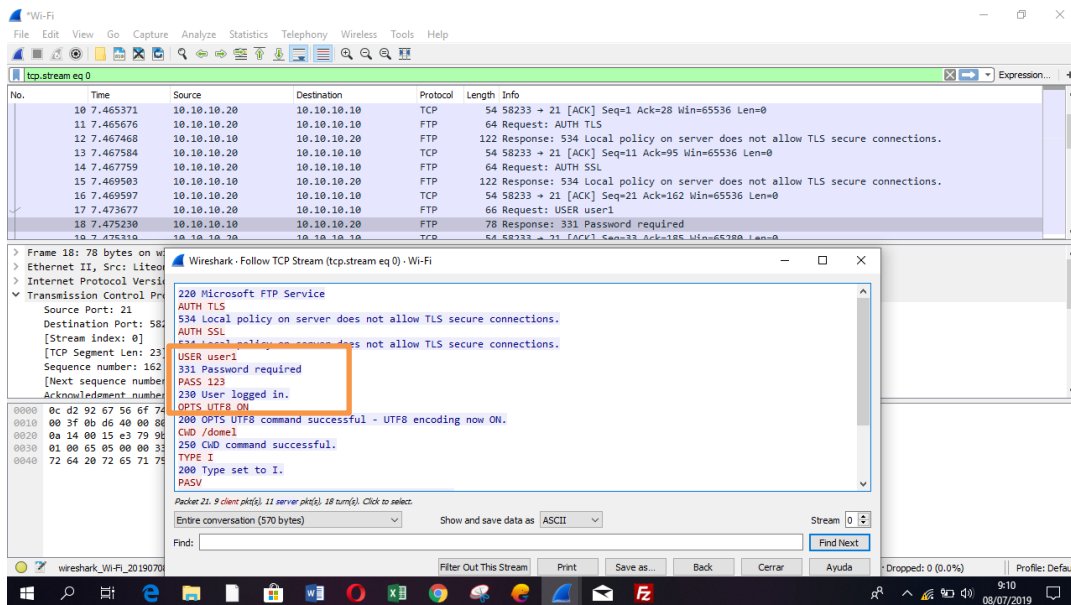


Figura 41. Captura de usuario y contraseña con Wireshark

3.3.5 Comprobación de conectividad entre Host

Para poder comprobar la conexión del servidor FTP, SFTP y Cliente se configuro un ip a cada ordenador con conexión a la red. Para el servidor FTP se le asignó la ip 10.10.10.10, para el servidor SFTP se le asignó la ip 10.10.10.12 y la Pc cliente se le asigno la ip 10.10.10.20, luego se probó la conexión entre los host.

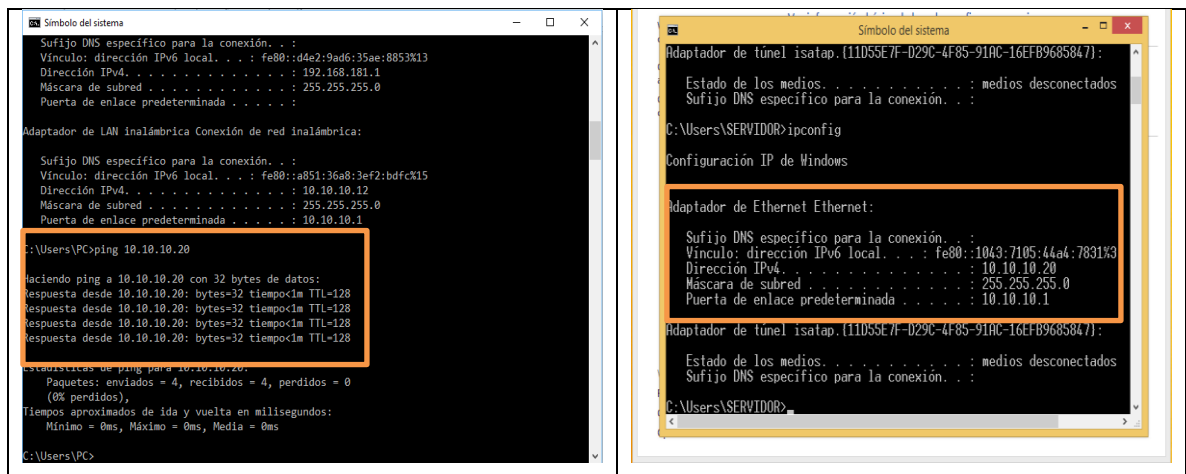


Figura 42. Conectividad del servidor SFTP con el host Cliente

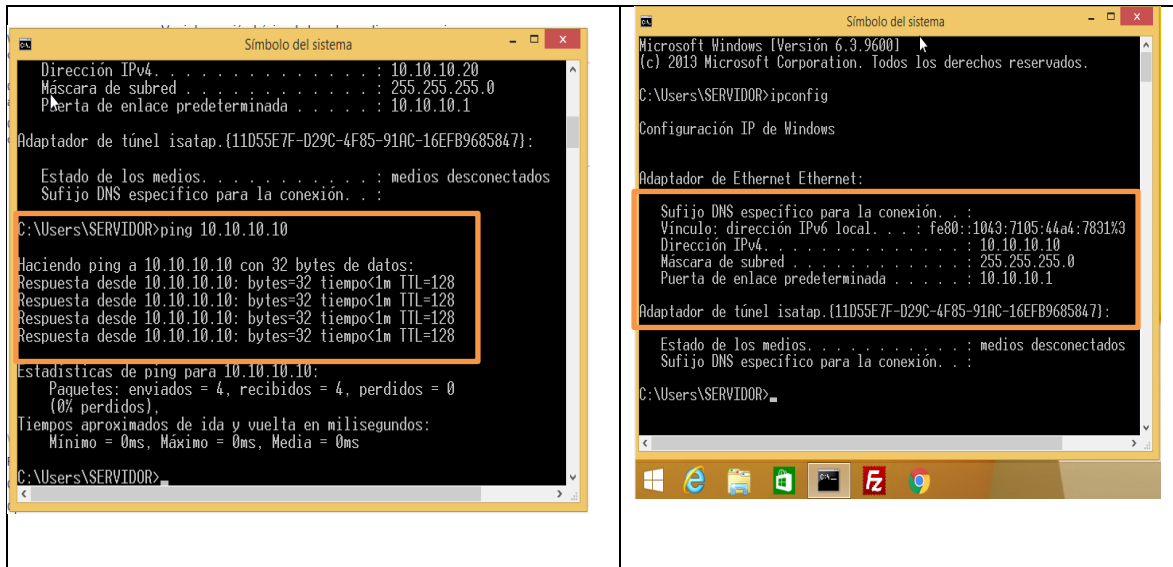


Figura 43. Conectividad del host Cliente con el servidor FTP

3.3.6 Configuración de los Algoritmos en el Servidor SFTP

Para la introducción de los algoritmos de encriptación 3DES, AES y RC4; primero se instaló correctamente el servidor SFTP en la Pc con ip 10.10.10.12.

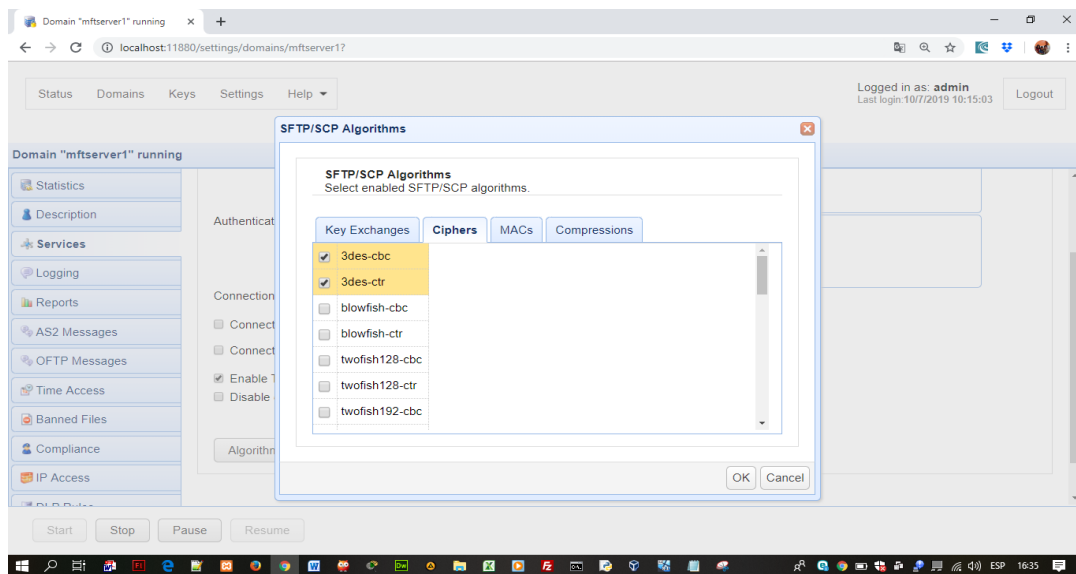


Figura 44. Configuración del algoritmo 3DES en SFTP

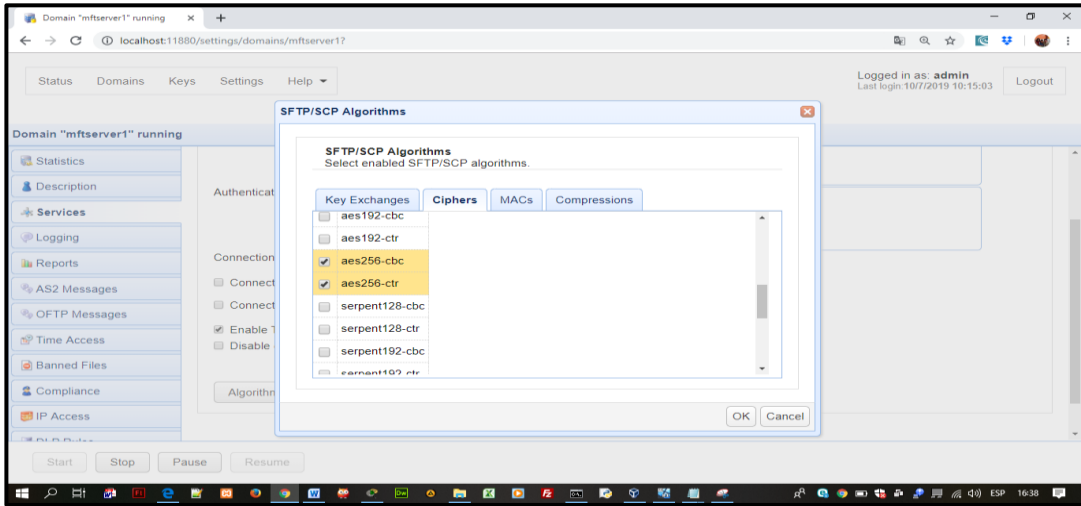


Figura 45. Configuración del algoritmo AES en SFTP

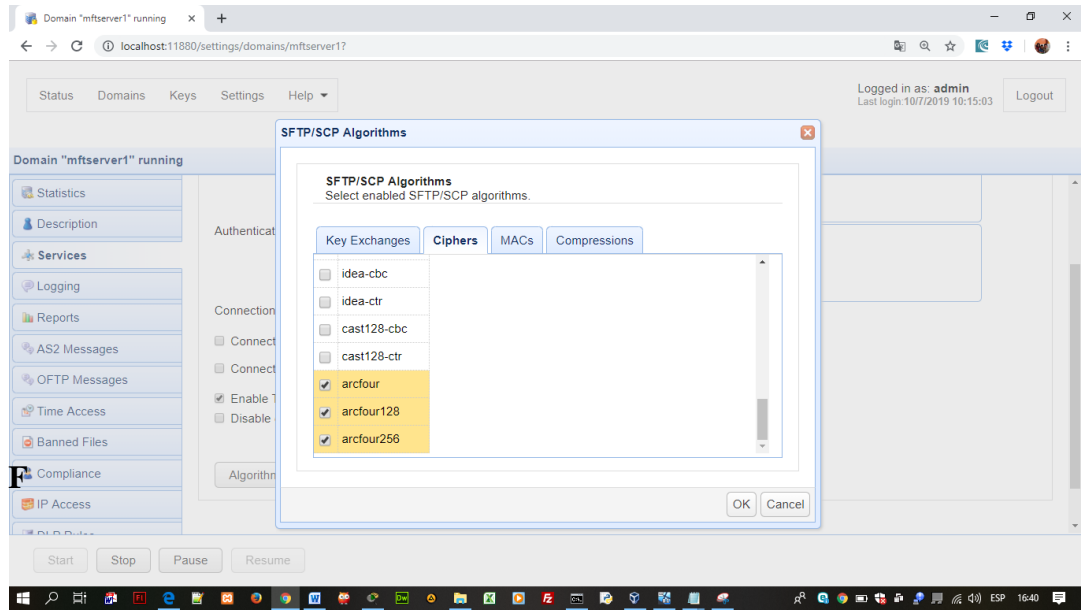


Figura 46. Configuración del algoritmo RC4 en SFTP

3.3.7 Pruebas de Funcionamiento de los Algoritmos de Encriptación

3.3.7.1 Captura de Tráfico de Datos con Wireshark entre SFTP y Cliente Utilizando el Algoritmo 3DES

Para poder capturar el tráfico de paquetes en la transferencia de archivos entre servidor SFTP y el cliente con el algoritmo 3DES, lo primero que se hizo fue conectarnos con el servidor utilizando FileZilla remotamente, enseguida se ubicó el archivo y se transfirió mediante una copia del servidor a la Pc cliente, a la vez se capturo el tráfico con el programa Wireshark.

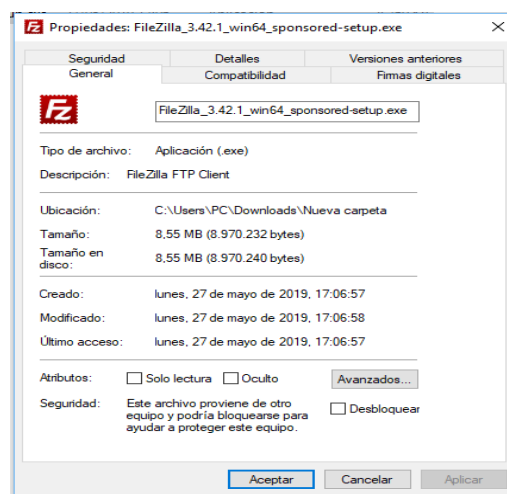


Figura 47. Archivo a transferir entre un servidor SFTP y un host

En la figura 48 se puede visualizar el tiempo que se realizó en la prueba que se ejecutó en la transferencia del archivo del servidor SFTP y la Pc Cliente, con un tiempo de 00:00:03:80

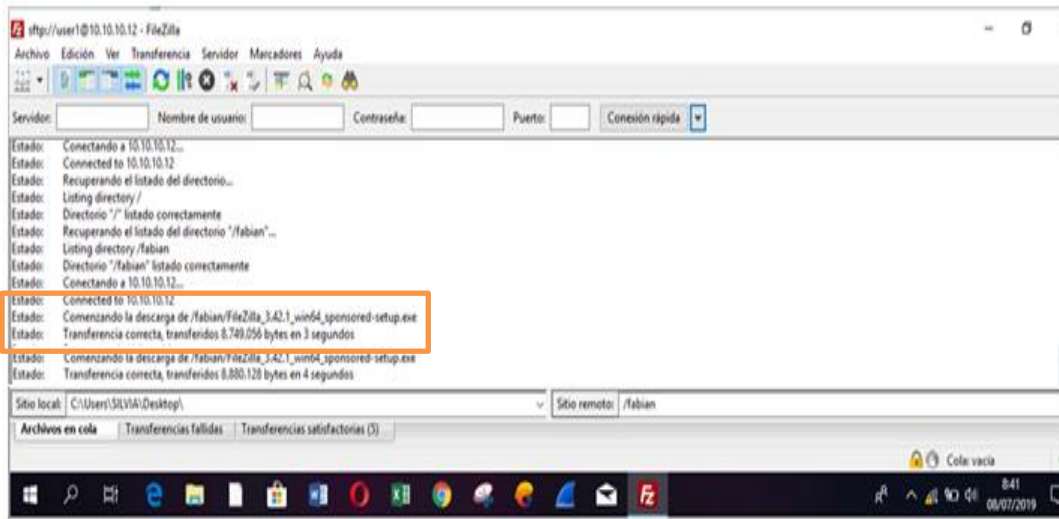


Figura 48. Visualización del tiempo de la Transferencia de archivo

En la figura 49 se capturo los paquetes encriptados de la Pc origen siendo el servidor SFTP y el destino la Pc Cliente haciendo uso del software Wireshark.

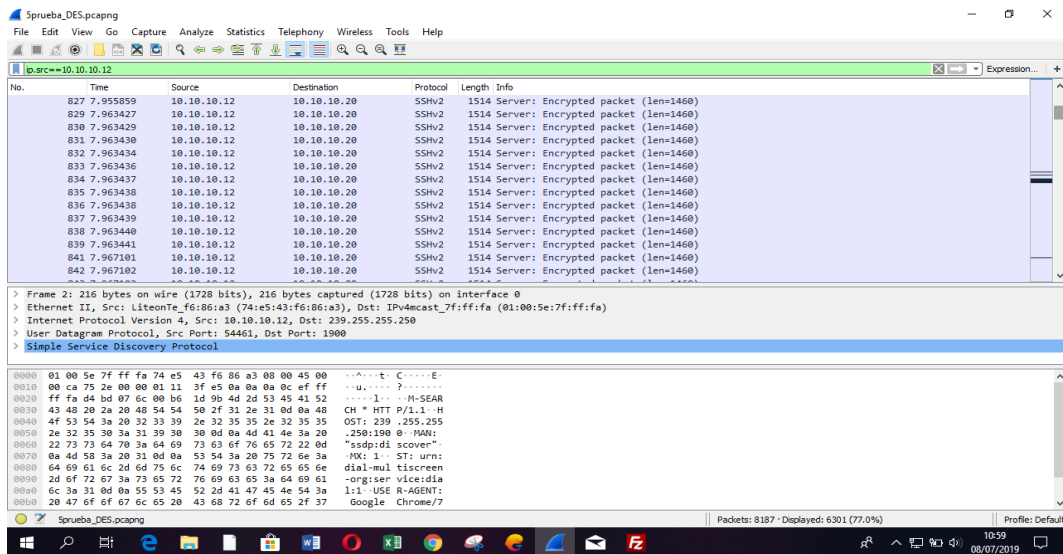


Figura 49. Paquetes encriptados de la Pc origen IP = 10.10.10.12

En la figura 50 se obtuvo uno de los paquetes número 1171 capturados, encapsulados y encriptados con el algoritmo 3DES con 1514 bytes.

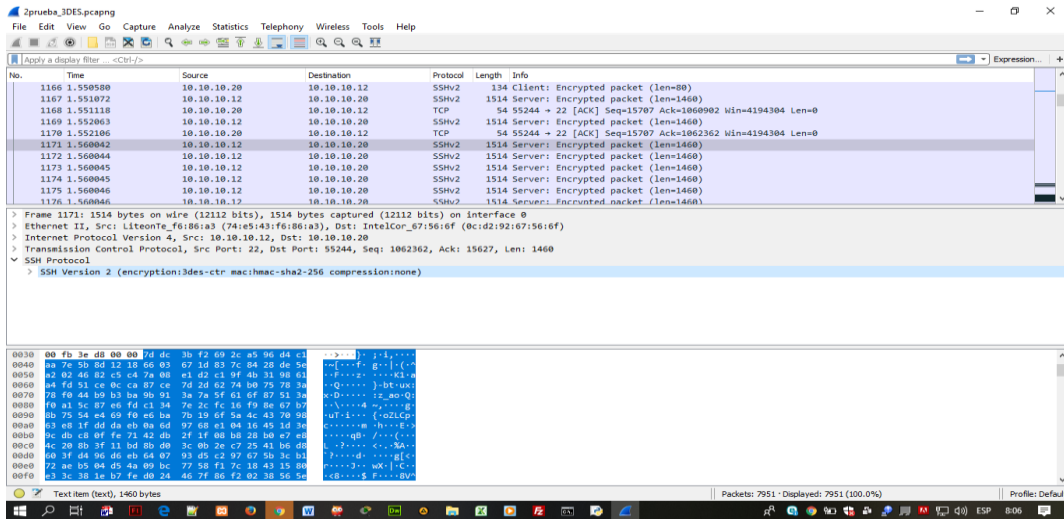


Figura 50. Paquete capturado número 1171 de 1514 bytes con Wireshark

En la figura 51 se exporto los paquetes capturados de la Pc origen a Excel con extensión CSV, para luego guardarlos.

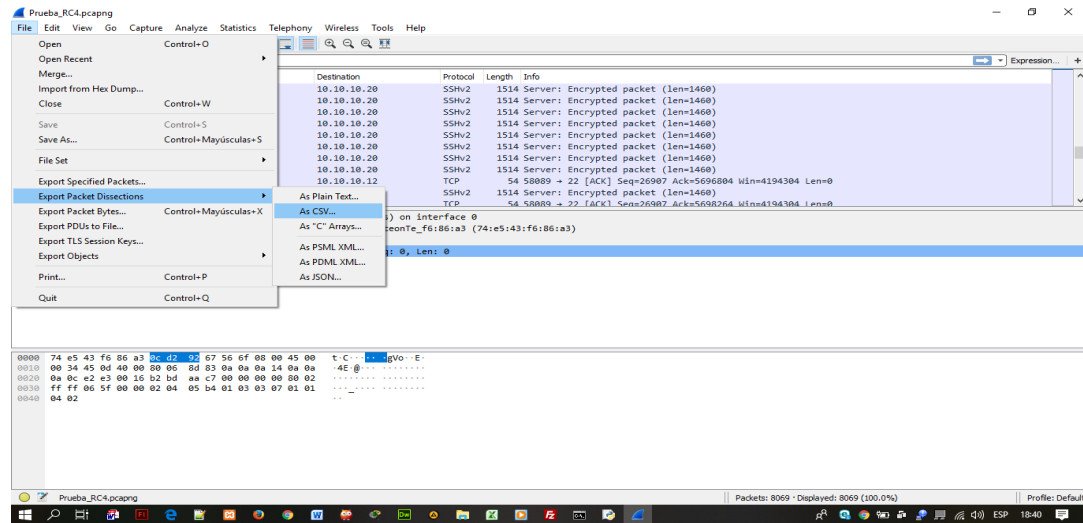


Figura 51. Exportando los paquetes capturados de la Pc origen a Excel CSV

En la figura 52 se visualiza los paquetes exportados de la Pc de origen del archivo 3des_origen.csv.

ID	Source IP	Destination IP	Protocol	Packet Details
6102	7669	4.574.028.10.10.10.12	SSHv2	1514 Server: Encry 7669,"4.574028","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"
6103	7670	4.574.028.10.10.10.12	SSHv2	1514 Server: Encry 7670,"4.574028","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"
6104	7671	4.574.029.10.10.10.12	SSHv2	1514 Server: Encry 7671,"4.574029","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"
6105	7672	4.574.029.10.10.10.12	SSHv2	1514 Server: Encry 7672,"4.574029","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"
6106	7673	4.574.030.10.10.10.12	SSHv2	1514 Server: Encry 7673,"4.574030","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"
6107	7674	4.574.030.10.10.10.12	SSHv2	1514 Server: Encry 7674,"4.574030","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"
6108	7675	4.574.031.10.10.10.12	SSHv2	1514 Server: Encry 7675,"4.574031","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"
6109	7676	4.574.031.10.10.10.12	SSHv2	1514 Server: Encry 7676,"4.574031","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"
6110	7678	4.577.476.10.10.10.12	SSHv2	1514 Server: Encry 7678,"4.577476","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"
6111	7679	4.577.477.10.10.10.12	SSHv2	1514 Server: Encry 7679,"4.577477","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"
6112	7680	4.577.478.10.10.10.12	SSHv2	1514 Server: Encry 7680,"4.577478","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"
6113	7681	4.577.480.10.10.10.12	SSHv2	1514 Server: Encry 7681,"4.577480","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"
6114	7682	4.577.480.10.10.10.12	SSHv2	1514 Server: Encry 7682,"4.577480","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"
6115	7683	4.577.481.10.10.10.12	SSHv2	1514 Server: Encry 7683,"4.577481","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"
6116	7684	4.577.481.10.10.10.12	SSHv2	1514 Server: Encry 7684,"4.577481","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"
6117	7685	4.577.482.10.10.10.12	SSHv2	1514 Server: Encry 7685,"4.577482","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"
6118	7686	4.577.482.10.10.10.12	SSHv2	1514 Server: Encry 7686,"4.577482","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"
6119	7687	4.577.483.10.10.10.12	SSHv2	1514 Server: Encry 7687,"4.577483","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"
6120	7688	4.577.483.10.10.10.12	SSHv2	1514 Server: Encry 7688,"4.577483","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"
6121	7690	4.577.866.10.10.10.12	SSHv2	1514 Server: Encry 7690,"4.577866","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"
6122	7693	4.581.990.10.10.10.12	SSHv2	1514 Server: Encry 7693,"4.581990","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"
6123	7694	4.581.991.10.10.10.12	SSHv2	1514 Server: Encry 7694,"4.581991","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"
6124	7695	4.581.993.10.10.10.12	SSHv2	1514 Server: Encry 7695,"4.581993","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"
6125	7696	4.581.994.10.10.10.12	SSHv2	1514 Server: Encry 7696,"4.581994","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"
6126	7698	4.584.922.10.10.10.12	SSHv2	1514 Server: Encry 7698,"4.584922","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"
6127	7699	4.584.923.10.10.10.12	SSHv2	1514 Server: Encry 7699,"4.584923","10.10.10.12","10.10.10.20","SSHv2","1514","Server: Encrypted packet (len=1460)"

Figura 52. Visualización de los paquetes capturados de la Pc origen del archivo 3des_origen.csv

En la figura 53 convertimos el archivo de texto excel.csv a excel.xls.

Esta pantalla le permite establecer los separadores contenidos en los datos. Se puede ver cómo cambia el texto en la vista previa.

Separadores

- Tabulación
- Punto y coma
- Coma
- Espacio
- Otro: _____

Calificador de texto: [v]

Copiar separadores consecutivos como uno solo

Vista previa de los datos

No.	Time	Source	Destination	Protocol	Length	Info	No.	Time	Source	Destination	Protocol	Length	Info
6102	0.885795	10.10.10.12	10.10.10.20	TCP	66	22	6102	0.885795	10.10.10.12	10.10.10.20	TCP	66	22
6103	0.884159	10.10.10.12	10.10.10.20	SSHv2	454	Server: Key Exchange	6103	0.884159	10.10.10.12	10.10.10.20	SSHv2	454	Server: Key Exchange
6104	0.918930	10.10.10.12	10.10.10.20	TCP	64	22	6104	0.918930	10.10.10.12	10.10.10.20	TCP	64	22

Cancelar < Atrás Siguiente > Finalizar

Figura 53. Convirtiendo archivos de texto excel.csv a excel.xls

En la figura 54 filtramos los archivos encriptados y no encriptados del archivo 3des_origen.xls utilizando la función de Excel =CONTAR.SI(E3:E6284;"SSHV2")

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
6264	7863	4.660.453	10.10.10.12	10.10.10.20	SSHV2	1514	Server: Encrypted packet (len=1460)								
6265	7864	4.660.453	10.10.10.12	10.10.10.20	SSHV2	1514	Server: Encrypted packet (len=1460)								
6266	7865	4.660.454	10.10.10.12	10.10.10.20	SSHV2	1514	Server: Encrypted packet (len=1460)								
6267	7867	4.662.867	10.10.10.12	10.10.10.20	SSHV2	1514	Server: Encrypted packet (len=1460)								
6268	7868	4.662.868	10.10.10.12	10.10.10.20	SSHV2	1514	Server: Encrypted packet (len=1460)								
6269	7869	4.662.869	10.10.10.12	10.10.10.20	SSHV2	1514	Server: Encrypted packet (len=1460)								
6270	7870	4.662.870	10.10.10.12	10.10.10.20	SSHV2	1514	Server: Encrypted packet (len=1460)								
6271	7871	4.662.871	10.10.10.12	10.10.10.20	SSHV2	1514	Server: Encrypted packet (len=1460)								
6272	7874	4.664.717	10.10.10.12	10.10.10.20	SSHV2	1514	Server: Encrypted packet (len=1460)								
6273	7875	4.664.718	10.10.10.12	10.10.10.20	SSHV2	1514	Server: Encrypted packet (len=1460)								
6274	7876	4.664.718	10.10.10.12	10.10.10.20	SSHV2	1514	Server: Encrypted packet (len=1460)								
6275	7877	4.664.720	10.10.10.12	10.10.10.20	SSHV2	1514	Server: Encrypted packet (len=1460)								
6276	7878	4.664.721	10.10.10.12	10.10.10.20	SSHV2	1514	Server: Encrypted packet (len=1460)								
6277	7879	4.664.721	10.10.10.12	10.10.10.20	SSHV2	397	Server: Encrypted packet (len=343)								
6278	7881	4.665.341	10.10.10.12	10.10.10.20	SSHV2	134	Server: Encrypted packet (len=80)								
6279	7883	4.666.847	10.10.10.12	10.10.10.20	SSHV2	134	Server: Encrypted packet (len=80)								
6280	7885	4.668.109	10.10.10.12	10.10.10.20	SSHV2	134	Server: Encrypted packet (len=80)								
6281	7888	4.671.306	10.10.10.12	10.10.10.20	SSHV2	134	Server: Encrypted packet (len=80)								
6282	7949	27.281.387	10.10.10.12	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1								
6283	7951	30.241.743	10.10.10.12	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1								
6284															
6285					PAQUETES NO ENCRIPADOS			86							
6286					PAQUETES ENCRIPADOS			6197							
6287					TOTAL PAQUETES			6283							

Figura 54. Filtrando los archivos encriptados y no encriptados de la Pc origen capturados con Wireshark

En la figura 55 filtramos los archivos encriptados y no encriptados del archivo 3des_destino.xls utilizando la función de Excel =CONTAR.SI(E3:E1639;"SSHV2")

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1619	7919	10.368.100	10.10.10.20	224.0.0.252	LLMNR	69	Standard query 0x881c A retracker								
1620	7921	10.369.013	10.10.10.20	224.0.0.252	LLMNR	69	Standard query 0x4116 AAAA retracker								
1621	7922	10.704.151	10.10.10.20	10.10.10.255	NBNS	92	Name query NB RETRACKER-00>								
1622	7923	10.953.644	10.10.10.20	224.0.0.251	MDNS	75	Standard query 0x0000 A retracker.local, "QM" question								
1623	7925	10.954.990	10.10.10.20	224.0.0.251	MDNS	75	Standard query 0x0000 AAAA retracker.local, "QM" question								
1624	7927	11.455.672	10.10.10.20	10.10.10.255	NBNS	92	Name query NB RETRACKER-00>								
1625	7928	14.971.807	10.10.10.20	10.10.10.255	NBNS	92	Name query NB RETRACKER-00>								
1626	7929	14.972.550	10.10.10.20	224.0.0.251	MDNS	75	Standard query 0x0000 A retracker.local, "QM" question								
1627	7931	14.973.912	10.10.10.20	224.0.0.251	MDNS	75	Standard query 0x0000 AAAA retracker.local, "QM" question								
1628	7934	14.976.108	10.10.10.20	224.0.0.252	LLMNR	69	Standard query 0x8d09 A retracker								
1629	7936	14.977.558	10.10.10.20	224.0.0.252	LLMNR	69	Standard query 0xf60 AAAA retracker								
1630	7938	15.387.361	10.10.10.20	224.0.0.252	LLMNR	69	Standard query 0x8d09 A retracker								
1631	7940	15.388.276	10.10.10.20	224.0.0.252	LLMNR	69	Standard query 0xf60 AAAA retracker								
1632	7941	15.721.683	10.10.10.20	10.10.10.255	NBNS	92	Name query NB RETRACKER-00>								
1633	7942	15.972.727	10.10.10.20	224.0.0.251	MDNS	75	Standard query 0x0000 A retracker.local, "QM" question								
1634	7944	15.973.798	10.10.10.20	224.0.0.251	MDNS	75	Standard query 0x0000 AAAA retracker.local, "QM" question								
1635	7946	16.472.727	10.10.10.20	10.10.10.255	NBNS	92	Name query NB RETRACKER-00>								
1636	7947	17.991.553	10.10.10.20	228.68.29.115	UDP	62	52499 > 1004 Len=20								
1637	7948	21.289.306	10.10.10.20	228.68.29.115	UDP	62	52499 > 1004 Len=20								
1638	7950	27.380.880	10.10.10.20	228.68.29.115	UDP	62	52499 > 1004 Len=20								
1639															
1640					PAQUETES NO ENCRIPADOS			1216							
1641					PAQUETES ENCRIPADOS CLIENTE			421							
1642					TOTAL PAQUETES DESTINO			1637							

Figura 55. Filtrando los archivos encriptados y no encriptados de la Pc destino capturados con Wireshark

3.3.7.2 Captura de Tráfico de Datos con Wireshark entre SFTP y Cliente Utilizando el Algoritmo AES

Para capturar el tráfico de paquetes en la transferencia de archivos entre servidor SFTP y el cliente utilizando AES, nos conectamos con el servidor utilizando FileZilla remotamente, enseguida se ubicó el archivo y se transfirió mediante una copia del servidor a la Pc cliente, a la vez se capturo el tráfico con el programa Wireshark.

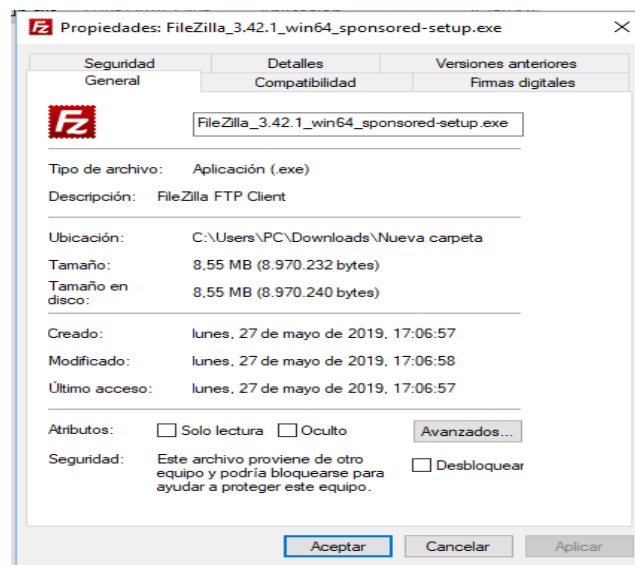


Figura 56. Archivo transferido entre un servidor SFTP y un host cliente

En la figura 57 se puede visualizar el tiempo que se realizó en la prueba que se ejecutó en la transferencia del archivo del servidor SFTP y la Pc Cliente, con un promedio de tiempo de 00:00:03:20

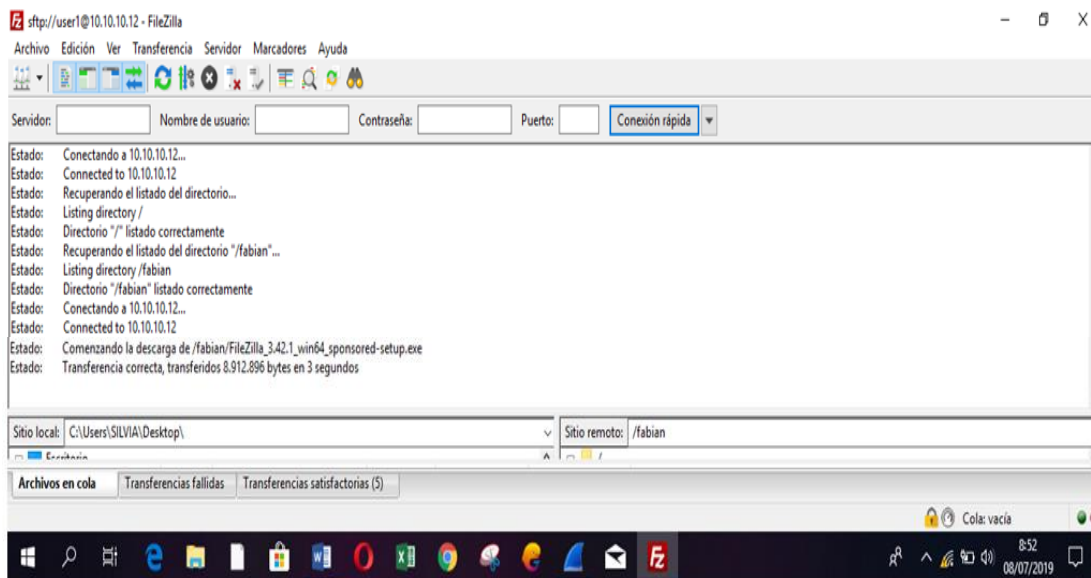


Figura 57. Visualización del tiempo de la Transferencia de archivo

En la figura 58 se capturo los paquetes encriptados de la Pc origen siendo el servidor SFTP y el destino la Pc Cliente haciendo uso del software Wireshark.

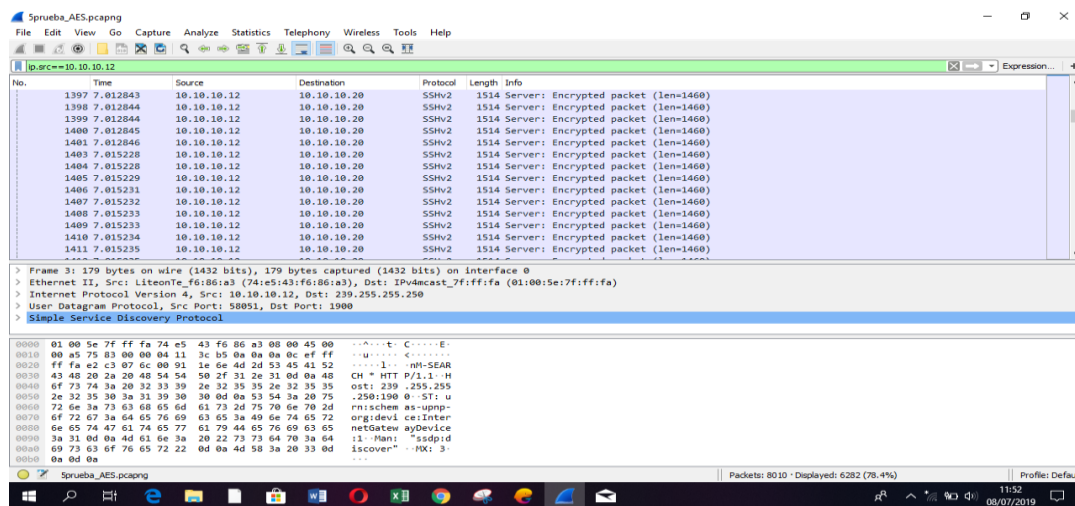


Figura 58. Paquetes encriptados de la Pc origen IP = 10.10.10.12

En la figura 59 se obtuvo el paquete número 644 encriptado con el algoritmo AES con 1514 bytes.

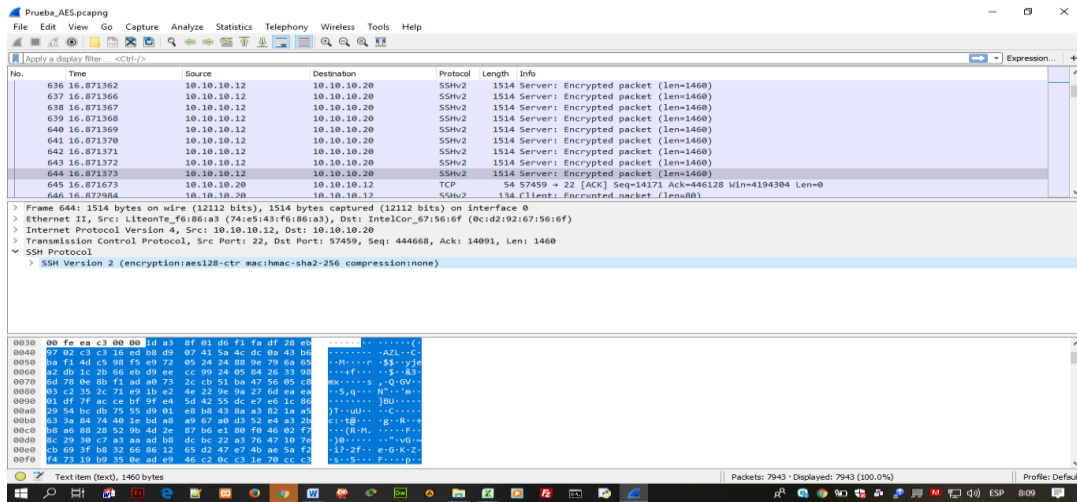


Figura 59. Paquete capturado número 644 de 1514 bytes con Wireshark

En la figura 60 se exporto los paquetes capturados de la Pc origen a Excel con extensión CSV, para luego guardarlos.

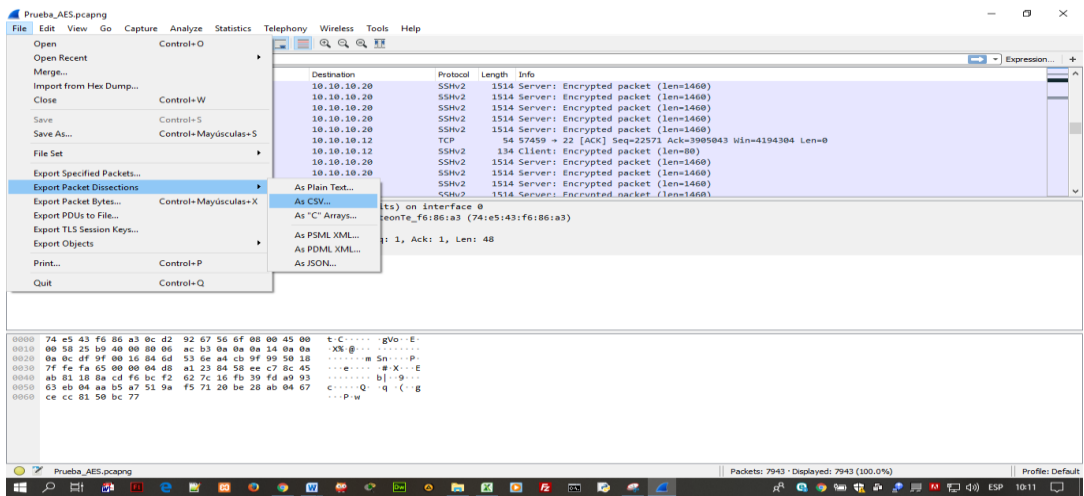


Figura 60. Exportando los paquetes capturados de la Pc origen a excel CSV

En la figura 61 se visualiza los paquetes exportados de la Pc de origen del archivo aes_origen.csv.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
5735	7313	20.225.543	10.10.10.12	10.10.10.20	SSHv2	1514	Server: Encry	7313,"20.225543"	"10.10.10.12","10.10.10.20"	"SSHv2","1514"	"Server: Encrypted packet (len=1460)"				
5736	7314	20.225.543	10.10.10.12	10.10.10.20	SSHv2	1514	Server: Encry	7314,"20.225543"	"10.10.10.12","10.10.10.20"	"SSHv2","1514"	"Server: Encrypted packet (len=1460)"				
5737	7315	20.225.544	10.10.10.12	10.10.10.20	SSHv2	1514	Server: Encry	7315,"20.225544"	"10.10.10.12","10.10.10.20"	"SSHv2","1514"	"Server: Encrypted packet (len=1460)"				

Figura 61. Visualización de los paquetes capturados de la Pc origen del archivo aes_origen.csv

En la figura 62 convertimos el archivo de texto excel.csv a excel.xls.

Asistente para importar texto - paso 1 de 3

El asistente estima que sus datos son Delimitados.

Si esto es correcto, elija lo siguiente, o bien elija el tipo de datos que mejor los describe.

Tipo de los datos originales

Elja el tipo de archivo que describe los datos con mayor precisión:

- Delimitados - Caracteres como comas o tabulaciones separan campos.
- De grncho fijo - Los campos estn alineados en columnas con espacios entre uno y otro.

Conectar a portar en la fila: 1 Origen del archivo: MS-DOS (PC-8)

Vista previa del archivo C:\Users\PC\Desktop\PPPT PROYECTO\lone/pruebas\Nuevo filtro de paquetes\ORIGEN\aes_origen.csv

No.	Time	Source	Destination	Protocol	Length	Info	No.	Time	Source	Destination
1	0.079086	10.10.10.12	10.10.10.20	SSHv2	102	Server: Encrypted packet (len=48); 72, 0, 0, 0				
2	0.078889	10.10.10.12	10.10.10.20	TCP	84	22 87247 [FIN, ACK] Seq=49 Ack=88 Win=23				
3	0.076489	10.10.10.12	10.10.10.20	TCP	84	22 87247 [FIN, ACK] Seq=49 Ack=88 Win=23				

Figura 62. Convirtiendo archivos de texto excel.csv a excel.xls

En la figura 63 filtramos los archivos encriptados y no encriptados del archivo aes_origen.xls utilizando la función de Excel =CONTAR.SI(E2:E6270;"SSHV2").

Paquete	Origen	Destino	Protocolo	Detalle
6250	7916	20.504.399.10.10.10.12	SSHV2	1514 Server: Encrypted packet (len=1460)
6251	7917	20.504.400.10.10.10.12	SSHV2	1514 Server: Encrypted packet (len=1460)
6252	7918	20.504.403.10.10.10.12	SSHV2	1514 Server: Encrypted packet (len=1460)
6253	7919	20.504.404.10.10.10.12	SSHV2	1514 Server: Encrypted packet (len=1460)
6254	7920	20.504.405.10.10.10.12	SSHV2	1514 Server: Encrypted packet (len=1460)
6255	7921	20.504.406.10.10.10.12	SSHV2	1514 Server: Encrypted packet (len=1460)
6256	7922	20.504.407.10.10.10.12	SSHV2	1514 Server: Encrypted packet (len=1460)
6257	7923	20.504.407.10.10.10.12	SSHV2	1514 Server: Encrypted packet (len=1460)
6258	7924	20.504.408.10.10.10.12	SSHV2	1514 Server: Encrypted packet (len=1460)
6259	7925	20.504.409.10.10.10.12	SSHV2	1514 Server: Encrypted packet (len=1460)
6260	7926	20.506.391.10.10.10.12	SSHV2	1514 Server: Encrypted packet (len=1460)
6261	7929	20.506.392.10.10.10.12	SSHV2	1514 Server: Encrypted packet (len=1460)
6262	7930	20.506.393.10.10.10.12	SSHV2	1514 Server: Encrypted packet (len=1460)
6263	7931	20.506.396.10.10.10.12	SSHV2	1514 Server: Encrypted packet (len=1460)
6264	7932	20.506.397.10.10.10.12	SSHV2	1514 Server: Encrypted packet (len=1460)
6265	7933	20.506.397.10.10.10.12	SSHV2	958 Server: Encrypted packet (len=904)
6266	7934	20.506.398.10.10.10.12	SSHV2	134 Server: Encrypted packet (len=80)
6267	7935	20.506.398.10.10.10.12	SSHV2	134 Server: Encrypted packet (len=80)
6268	7937	20.508.680.10.10.10.12	SSHV2	134 Server: Encrypted packet (len=80)
6269	7939	20.509.668.10.10.10.12	SSHV2	134 Server: Encrypted packet (len=80)
6270	7942	20.512.498.10.10.10.12	SSHV2	134 Server: Encrypted packet (len=80)
6271				
6272			PAQUETES NO ENCRYPTADOS	69
6273			PAQUETES ENCRYPTADOS	6200
6274			TOTAL PAQUETES	6269

Figura 63. Filtrando los archivos encriptados y no encriptados de la Pc origen capturados con Wireshark

En la figura 64 filtramos los archivos encriptados y no encriptados del archivo aes_destino.xls utilizando la función de Excel =CONTAR.SI(E2:E1673;"SSHV2")

Paquete	Origen	Destino	Protocolo	Detalle
1655	7854	20.471.255.10.10.10.20	SSHV2	134 Client: Encrypted packet (len=80)
1656	7856	20.472.846.10.10.10.20	TCP	54 57459 > 22 [ACK] Seq=34891 Ack=8940913 Win=4194304 Len=0
1657	7859	20.477.235.10.10.10.20	TCP	54 57459 > 22 [ACK] Seq=34891 Ack=8943833 Win=4194304 Len=0
1658	7871	20.478.504.10.10.10.20	TCP	54 57459 > 22 [ACK] Seq=34891 Ack=8959893 Win=4194304 Len=0
1659	7881	20.480.774.10.10.10.20	TCP	54 57459 > 22 [ACK] Seq=34891 Ack=8973033 Win=4194304 Len=0
1660	7882	20.481.592.10.10.10.20	SSHV2	134 Client: Encrypted packet (len=80)
1661	7891	20.488.758.10.10.10.20	TCP	54 57459 > 22 [ACK] Seq=34971 Ack=8984713 Win=4194304 Len=0
1662	7895	20.489.206.10.10.10.20	TCP	54 57459 > 22 [ACK] Seq=34971 Ack=8989093 Win=4194304 Len=0
1663	7899	20.490.790.10.10.10.20	TCP	54 57459 > 22 [ACK] Seq=34971 Ack=8993473 Win=4194304 Len=0
1664	7901	20.495.751.10.10.10.20	TCP	54 57459 > 22 [ACK] Seq=34971 Ack=8994933 Win=4194304 Len=0
1665	7913	20.500.858.10.10.10.20	TCP	54 57459 > 22 [ACK] Seq=34971 Ack=9010993 Win=4194304 Len=0
1666	7914	20.501.704.10.10.10.20	SSHV2	134 Client: Encrypted packet (len=80)
1667	7926	20.504.699.10.10.10.20	TCP	54 57459 > 22 [ACK] Seq=35051 Ack=9027053 Win=4194304 Len=0
1668	7927	20.505.428.10.10.10.20	SSHV2	134 Client: Encrypted packet (len=80)
1669	7936	20.506.589.10.10.10.20	TCP	54 57459 > 22 [ACK] Seq=35131 Ack=9035417 Win=4194304 Len=0
1670	7938	20.508.793.10.10.10.20	TCP	54 57459 > 22 [ACK] Seq=35131 Ack=9035497 Win=4194176 Len=0
1671	7940	20.509.738.10.10.10.20	TCP	54 57459 > 22 [ACK] Seq=35131 Ack=9035577 Win=4194048 Len=0
1672	7941	20.510.748.10.10.10.20	SSHV2	134 Client: Encrypted packet (len=80)
1673	7943	20.512.602.10.10.10.20	TCP	54 57459 > 22 [ACK] Seq=35211 Ack=9035657 Win=4194048 Len=0
1674				
1675				
1676			PAQUETES NO ENCRYPTADOS	1264
1677			PAQUETES ENCRYPTADOS	408
1678			TOTAL PAQUETES	1672

Figura 64. Filtrando los archivos encriptados y no encriptados de la Pc destino capturados con Wireshark

3.3.7.3 Captura de Tráfico de Datos con Wireshark entre SFTP y Cliente utilizando el algoritmo RC4

Para la captura de tráfico en la transferencia de archivos entre servidor SFTP y el cliente utilizando el algoritmo de encriptación RC4, primero nos conectamos con el servidor utilizando FileZilla remotamente, enseguida se ubicó el archivo y se transfirió desde una copia del servidor a la Pc cliente, a la vez se capturo el tráfico con el programa Wireshark.

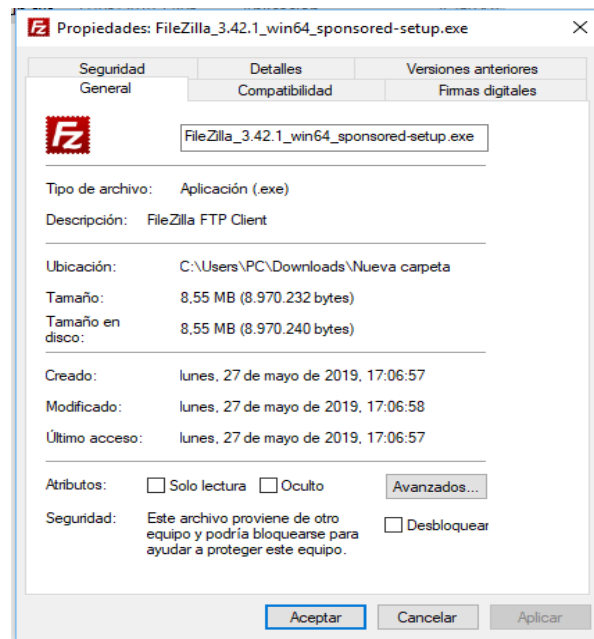


Figura 65. Archivo a transferir entre un servidor SFTP y un host

En la figura 66 se puede visualizar el tiempo que se realizó en la prueba ejecutada en la transferencia del archivo del servidor SFTP y la Pc Cliente, con un promedio de tiempo de 00:00:03:80

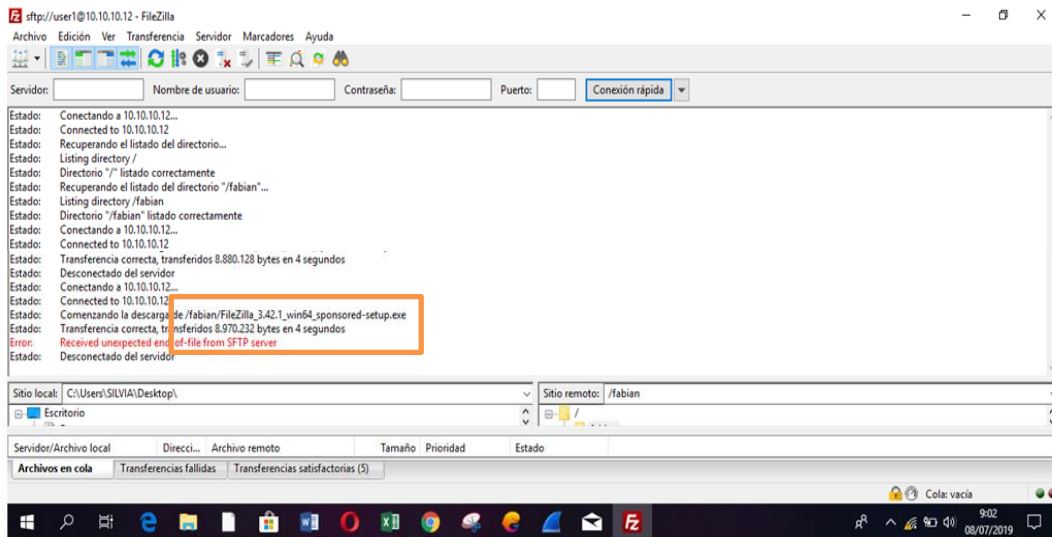


Figura 66. Visualización del tiempo de la Transferencia de archivo

En la figura 67 se capturo los paquetes encriptados de la Pc origen siendo el servidor SFTP y el destino la Pc Cliente haciendo uso del software Wireshark.

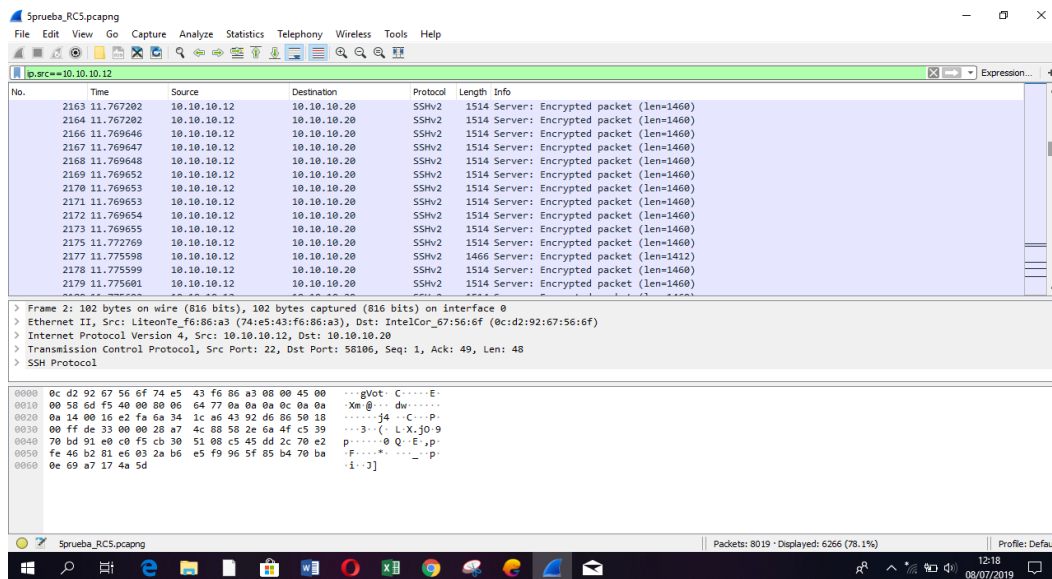


Figura 67. Paquetes encriptados de la Pc origen IP = 10.10.10.12

En la figura 68 se obtuvo uno de los paquetes número 3119 capturados, encriptados con el algoritmo RC4 con 1514 bytes.

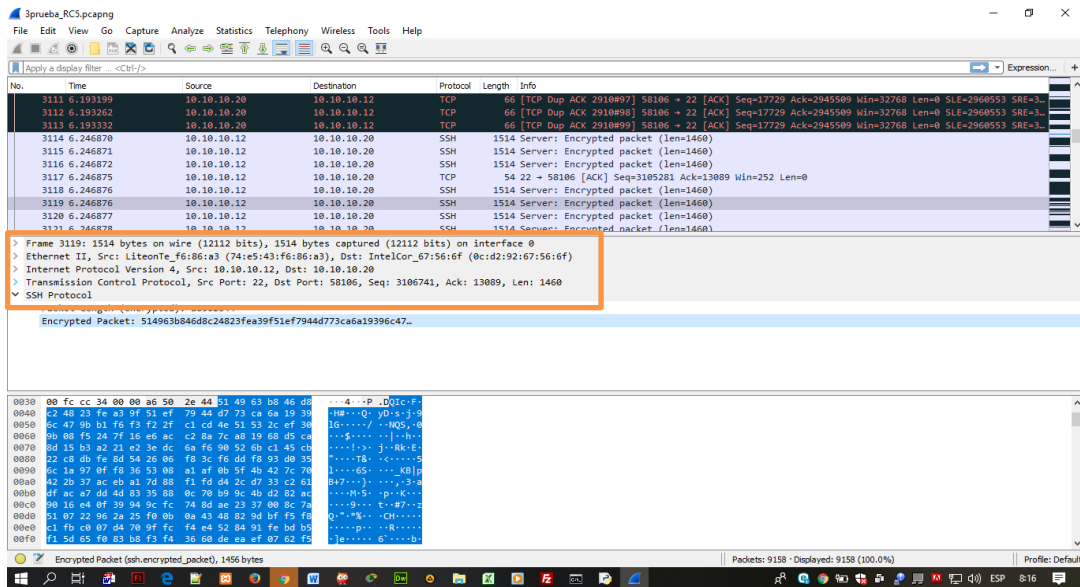


Figura 68: Paquete capturado número 3119 de 12112 bytes con Wireshark

En la figura 70 se exporto los paquetes capturados de la Pc origen a Excel con extensión CSV, para luego guardarlos.

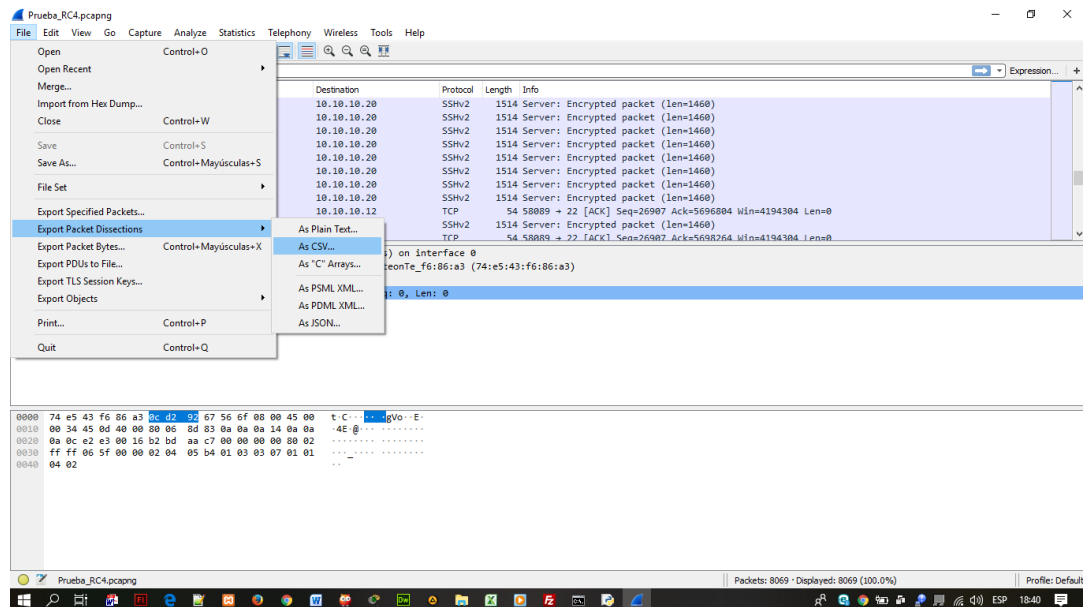


Figura 69. Exportando los paquetes capturados de la Pc origen a Excel CSV

En la figura 70 se visualiza los paquetes exportados de la Pc de origen del archivo rc4_origen.csv.

No.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1018	1457	16.729.696	10.10.10.12	10.10.10.20	SSHv2	1514 Server: Encrypted pac 1457,16.729696,10.10.10.12,10.10.10.20,SSHv2,1514,Server: Encrypted packet (len=1460)							Server: Encrypted packet (len=1460)			
1019	1458	16.729.697	10.10.10.12	10.10.10.20	SSHv2	1514 Server: Encrypted pac 1458,16.729697,10.10.10.12,10.10.10.20,SSHv2,1514,Server: Encrypted packet (len=1460)							Server: Encrypted packet (len=1460)			
1020	1459	16.729.698	10.10.10.12	10.10.10.20	SSHv2	1514 Server: Encrypted pac 1459,16.729698,10.10.10.12,10.10.10.20,SSHv2,1514,Server: Encrypted packet (len=1460)							Server: Encrypted packet (len=1460)			
1021	1460	16.729.699	10.10.10.12	10.10.10.20	SSHv2	1514 Server: Encrypted pac 1460,16.729699,10.10.10.12,10.10.10.20,SSHv2,1514,Server: Encrypted packet (len=1460)							Server: Encrypted packet (len=1460)			
1022	1463	16.732.080	10.10.10.12	10.10.10.20	SSHv2	1514 Server: Encrypted pac 1463,16.732080,10.10.10.12,10.10.10.20,SSHv2,1514,Server: Encrypted packet (len=1460)							Server: Encrypted packet (len=1460)			
1023	1464	16.732.082	10.10.10.12	10.10.10.20	SSHv2	1514 Server: Encrypted pac 1464,16.732082,10.10.10.12,10.10.10.20,SSHv2,1514,Server: Encrypted packet (len=1460)							Server: Encrypted packet (len=1460)			
1024	1465	16.732.083	10.10.10.12	10.10.10.20	SSHv2	1514 Server: Encrypted pac 1465,16.732083,10.10.10.12,10.10.10.20,SSHv2,1514,Server: Encrypted packet (len=1460)							Server: Encrypted packet (len=1460)			
1025	1466	16.732.085	10.10.10.12	10.10.10.20	SSHv2	1514 Server: Encrypted pac 1466,16.732085,10.10.10.12,10.10.10.20,SSHv2,1514,Server: Encrypted packet (len=1460)							Server: Encrypted packet (len=1460)			
1026	1467	16.732.086	10.10.10.12	10.10.10.20	SSHv2	1514 Server: Encrypted pac 1467,16.732086,10.10.10.12,10.10.10.20,SSHv2,1514,Server: Encrypted packet (len=1460)							Server: Encrypted packet (len=1460)			
1027	1468	16.732.087	10.10.10.12	10.10.10.20	SSHv2	1514 Server: Encrypted pac 1468,16.732087,10.10.10.12,10.10.10.20,SSHv2,1514,Server: Encrypted packet (len=1460)							Server: Encrypted packet (len=1460)			
1028	1469	16.732.088	10.10.10.12	10.10.10.20	SSHv2	1514 Server: Encrypted pac 1469,16.732088,10.10.10.12,10.10.10.20,SSHv2,1514,Server: Encrypted packet (len=1460)							Server: Encrypted packet (len=1460)			
1029	1470	16.732.089	10.10.10.12	10.10.10.20	SSHv2	1514 Server: Encrypted pac 1470,16.732089,10.10.10.12,10.10.10.20,SSHv2,1514,Server: Encrypted packet (len=1460)							Server: Encrypted packet (len=1460)			
1030	1471	16.732.090	10.10.10.12	10.10.10.20	SSHv2	1514 Server: Encrypted pac 1471,16.732090,10.10.10.12,10.10.10.20,SSHv2,1514,Server: Encrypted packet (len=1460)							Server: Encrypted packet (len=1460)			
1031	1472	16.732.091	10.10.10.12	10.10.10.20	SSHv2	1514 Server: Encrypted pac 1472,16.732091,10.10.10.12,10.10.10.20,SSHv2,1514,Server: Encrypted packet (len=1460)							Server: Encrypted packet (len=1460)			
1032	1473	16.732.092	10.10.10.12	10.10.10.20	SSHv2	1514 Server: Encrypted pac 1473,16.732092,10.10.10.12,10.10.10.20,SSHv2,1514,Server: Encrypted packet (len=1460)							Server: Encrypted packet (len=1460)			
1033	1475	16.738.129	10.10.10.12	10.10.10.20	SSHv2	1514 Server: Encrypted pac 1475,16.738129,10.10.10.12,10.10.10.20,SSHv2,1514,Server: Encrypted packet (len=1460)							Server: Encrypted packet (len=1460)			
1034	1476	16.738.130	10.10.10.12	10.10.10.20	SSHv2	1514 Server: Encrypted pac 1476,16.738130,10.10.10.12,10.10.10.20,SSHv2,1514,Server: Encrypted packet (len=1460)							Server: Encrypted packet (len=1460)			
1035	1477	16.738.131	10.10.10.12	10.10.10.20	SSHv2	1514 Server: Encrypted pac 1477,16.738131,10.10.10.12,10.10.10.20,SSHv2,1514,Server: Encrypted packet (len=1460)							Server: Encrypted packet (len=1460)			
1036	1478	16.738.134	10.10.10.12	10.10.10.20	SSHv2	1514 Server: Encrypted pac 1478,16.738134,10.10.10.12,10.10.10.20,SSHv2,1514,Server: Encrypted packet (len=1460)							Server: Encrypted packet (len=1460)			
1037	1479	16.738.135	10.10.10.12	10.10.10.20	SSHv2	1514 Server: Encrypted pac 1479,16.738135,10.10.10.12,10.10.10.20,SSHv2,1514,Server: Encrypted packet (len=1460)							Server: Encrypted packet (len=1460)			
1038	1480	16.738.136	10.10.10.12	10.10.10.20	SSHv2	1514 Server: Encrypted pac 1480,16.738136,10.10.10.12,10.10.10.20,SSHv2,1514,Server: Encrypted packet (len=1460)							Server: Encrypted packet (len=1460)			
1039	1481	16.738.137	10.10.10.12	10.10.10.20	SSHv2	1514 Server: Encrypted pac 1481,16.738137,10.10.10.12,10.10.10.20,SSHv2,1514,Server: Encrypted packet (len=1460)							Server: Encrypted packet (len=1460)			
1040	1482	16.738.138	10.10.10.12	10.10.10.20	SSHv2	1514 Server: Encrypted pac 1482,16.738138,10.10.10.12,10.10.10.20,SSHv2,1514,Server: Encrypted packet (len=1460)							Server: Encrypted packet (len=1460)			
1041	1485	16.741.984	10.10.10.12	10.10.10.20	SSHv2	1514 Server: [TCP Previous 1485,16.741984,10.10.10.12,10.10.10.20,SSHv2,1514,Server: [TCP Previous segment not captured], Encrypted pa							Server: Encrypted packet (len=1460)			
1042	1486	16.741.985	10.10.10.12	10.10.10.20	SSHv2	1514 Server: Encrypted pac 1486,16.741985,10.10.10.12,10.10.10.20,SSHv2,1514,Server: Encrypted packet (len=1460)							Server: Encrypted packet (len=1460)			
1043	1487	16.741.985	10.10.10.12	10.10.10.20	SSHv2	1514 Server: Encrypted pac 1487,16.741985,10.10.10.12,10.10.10.20,SSHv2,1514,Server: Encrypted packet (len=1460)							Server: Encrypted packet (len=1460)			

Figura 70. Visualización de los paquetes capturados de la Pc origen del archivo rc4_origen.csv

En la figura 71 convertimos el archivo de texto excel.csv a excel.xls.

Asistente para importar texto - paso 3 de 3

Esta pantalla permite seleccionar cada columna y establecer el formato de los datos.

Formato de los datos en columnas

- General
- Texto
- Fecha: DMY
- No importar columna (saltar)

Avanzadas...

Vista previa de los datos

No.	Time	Source	Destination	Protocol	Length	Info	Raw
1018	00:03:19.10	10.10.10.12	10.10.10.20	TCP	44,23		
1019	00:04:02.10	10.10.10.12	10.10.10.20	SSHv2	701	Server:	
1020	00:04:09.10	10.10.10.12	10.10.10.20	SSHv2	810	Server:	
1021	01:00:22.10	10.10.10.12	10.10.10.20	TCP	44,23		

Cancelar < Atrás Avanzado Fin

Figura 71. Convirtiendo archivos de texto excel.csv a excel.xls

En la figura 72 filtramos los archivos encriptados y no encriptados del archivo rc4_origen.xls utilizando la función de Excel =CONTAR.SI(E2:E6325;"SSHV2")

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
6307	8043	19.777.768	10.10.10.12	10.10.10.20	SSHv2	1514	Server: Encrypted packet (len=1460)									
6308	8044	19.777.768	10.10.10.12	10.10.10.20	SSHv2	1514	Server: Encrypted packet (len=1460)									
6309	8045	19.777.769	10.10.10.12	10.10.10.20	SSHv2	1514	Server: Encrypted packet (len=1460)									
6310	8046	19.777.769	10.10.10.12	10.10.10.20	SSHv2	1514	Server: Encrypted packet (len=1460)									
6311	8047	19.777.770	10.10.10.12	10.10.10.20	SSHv2	1514	Server: Encrypted packet (len=1460)									
6312	8048	19.777.770	10.10.10.12	10.10.10.20	SSHv2	1514	Server: Encrypted packet (len=1460)									
6313	8049	19.777.771	10.10.10.12	10.10.10.20	SSHv2	1514	Server: Encrypted packet (len=1460)									
6314	8050	19.777.771	10.10.10.12	10.10.10.20	SSHv2	1514	Server: Encrypted packet (len=1460)									
6315	8051	19.777.772	10.10.10.12	10.10.10.20	SSHv2	1514	Server: Encrypted packet (len=1460)									
6316	8052	19.777.772	10.10.10.12	10.10.10.20	SSHv2	1514	Server: Encrypted packet (len=1460)									
6317	8054	19.778.402	10.10.10.12	10.10.10.20	SSHv2	1514	Server: Encrypted packet (len=1460)									
6318	8056	19.779.992	10.10.10.12	10.10.10.20	SSHv2	1514	Server: Encrypted packet (len=1460)									
6319	8057	19.779.993	10.10.10.12	10.10.10.20	SSHv2	1514	Server: Encrypted packet (len=1460)									
6320	8058	19.779.996	10.10.10.12	10.10.10.20	SSHv2	1514	Server: Encrypted packet (len=1460)									
6321	8059	19.779.997	10.10.10.12	10.10.10.20	SSHv2	1422	Server: Encrypted packet (len=1368)									
6322	8060	19.779.998	10.10.10.12	10.10.10.20	SSHv2	134	Server: Encrypted packet (len=80)									
6323	8063	19.780.851	10.10.10.12	10.10.10.20	SSHv2	134	Server: Encrypted packet (len=80)									
6324	8065	19.782.959	10.10.10.12	10.10.10.20	SSHv2	134	Server: Encrypted packet (len=80)									
6325	8068	19.785.838	10.10.10.12	10.10.10.20	SSHv2	134	Server: Encrypted packet (len=80)									
6326																
6327					TOTAL PAQUETES NO ENCRYPTADOS		128									
6328					TOTAL PAQUETES ENCRYPTADOS		6196									
6329					TOTAL PAQUETES DE LA PC ORIGEN		6324									
6330																
6331																
6332																

Figura 72. Filtrando los archivos encriptados y no encriptados de la Pc origen capturados con Wireshark

En la figura 73 filtramos los archivos encriptados y no encriptados del archivo rc4_destino.xls utilizando la función de Excel =CONTAR.SI(E2:E1746;"SSHV2")

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1729	7998	19.751.757	10.10.10.20	10.10.10.12	TCP	54	58089 > 22 [ACK] Seq=34827 Ack=8958053 Win=4194304 Len=0									
1730	8000	19.753.681	10.10.10.20	10.10.10.12	TCP	54	58089 > 22 [ACK] Seq=34827 Ack=8959513 Win=4194304 Len=0									
1731	8012	19.758.851	10.10.10.20	10.10.10.12	TCP	54	58089 > 22 [ACK] Seq=34827 Ack=8975573 Win=4194304 Len=0									
1732	8013	19.760.312	10.10.10.20	10.10.10.12	SSHv2	134	Client: Encrypted packet (len=80)									
1733	8025	19.764.219	10.10.10.20	10.10.10.12	TCP	54	58089 > 22 [ACK] Seq=34907 Ack=8991633 Win=4194304 Len=0									
1734	8027	19.764.351	10.10.10.20	10.10.10.12	TCP	54	58089 > 22 [ACK] Seq=34907 Ack=8993093 Win=4194304 Len=0									
1735	8036	19.766.754	10.10.10.20	10.10.10.12	TCP	54	58089 > 22 [ACK] Seq=34907 Ack=9004773 Win=4194304 Len=0									
1736	8038	19.767.936	10.10.10.20	10.10.10.12	TCP	54	58089 > 22 [ACK] Seq=34907 Ack=9006233 Win=4194304 Len=0									
1737	8039	19.768.779	10.10.10.20	10.10.10.12	SSHv2	134	Client: Encrypted packet (len=80)									
1738	8041	19.772.094	10.10.10.20	10.10.10.12	TCP	54	58089 > 22 [ACK] Seq=34987 Ack=9007693 Win=4194304 Len=0									
1739	8053	19.777.917	10.10.10.20	10.10.10.12	TCP	54	58089 > 22 [ACK] Seq=34987 Ack=9023753 Win=4194304 Len=0									
1740	8055	19.778.459	10.10.10.20	10.10.10.12	TCP	54	58089 > 22 [ACK] Seq=34987 Ack=9025213 Win=4194304 Len=0									
1741	8061	19.780.122	10.10.10.20	10.10.10.12	TCP	54	58089 > 22 [ACK] Seq=34987 Ack=9031041 Win=4194304 Len=0									
1742	8062	19.780.734	10.10.10.20	10.10.10.12	SSHv2	134	Client: Encrypted packet (len=80)									
1743	8064	19.780.906	10.10.10.20	10.10.10.12	TCP	54	58089 > 22 [ACK] Seq=35067 Ack=9031121 Win=4194176 Len=0									
1744	8066	19.783.021	10.10.10.20	10.10.10.12	TCP	54	58089 > 22 [ACK] Seq=35067 Ack=9031201 Win=4194048 Len=0									
1745	8067	19.784.188	10.10.10.20	10.10.10.12	SSHv2	126	Client: Encrypted packet (len=72)									
1746	8069	19.785.928	10.10.10.20	10.10.10.12	TCP	54	58089 > 22 [ACK] Seq=35139 Ack=9031281 Win=4194048 Len=0									
1747																
1748					PAQUETES NO ENCRYPTADOS		1293									
1749					PAQUETES ENCRYPTADOS		452									
1750					TOTAL PAQUETES		1745									
1751																
1752																
1753																
1754																

Figura 73. Filtrando los archivos encriptados y no encriptados de la Pc destino capturados con Wireshark

IV: CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- a. Según la información recogida de la ficha técnica de expertos y los artículos científicos de esta investigación se eligió a tres algoritmos de encriptación como el 3DES, AES y RC4, teniendo en cuenta su longitud de clave, resistencia al criptoanálisis y a la seguridad de los datos.
- b. Se implementó y configuró un escenario de prueba para la transferencia de archivos con un servidor SFTP, FTP y un Host Cliente en el Instituto de Educación Superior Tecnológico Público “Utcubamba” - Amazonas.
- c. Se construyó un prototipo de red pública con una topología estrella, teniendo como elementos de conexión a un servidor SFTP donde se configuraron los algoritmos de encriptación (3DES, AES y RC4). Así mismo se configuró el Host Cliente con el sniffer Wireshark que realizaba la captura de los paquetes enviados por el servidor al cliente o viceversa, haciendo uso del programa FileZilla.
- d. Según las pruebas realizadas de la comparación de los tres algoritmos de encriptación, se llegó a la conclusión que AES es el mejor algoritmo en cuanto al tiempo de envío, número de paquetes fraccionados, número de paquetes de encriptación y número menor de paquetes no encriptados, por eso se recomienda a las organizaciones utilizarlo en beneficio de la protección de su información virtual.

4.2 Recomendaciones

- a. Ejecutar la comparación de protocolos con la finalidad de explicar que protocolo brinda mayor integridad, confidencialidad, autenticación y vinculación de la información.
- b. Las empresas deben utilizar servidores SFTP e instalar el algoritmo AES, con la finalidad de dar seguridad e integridad de la información.
- c. Es recomendable la utilización de otras topologías de la red, a la vez implementar más algoritmos de encriptación y protocolos, con la finalidad de tener una evaluación más detallada con respecto a los protocolos que están instalados en un servidores SFTP.
- d. Hacer la captura de los datos de una red inalámbrica, con la finalidad de poder medir el comportamiento de 3DES, AES, y RC4 haciendo uso del protocolo SSL.

REFERENCIAS

- Aguirre, J. (2006). *Seguridad Informática y criptografía*. Obtenido de <http://www.criptored.upm.es/crypt4you/temas/criptografiaclassica/leccion1.html>
- Aidong, F., & Zhiwei, Z. (2018). *Research on Parallel Dynamic Encryption Transmission Algorithm on VoIP*. China: University, Suzhou.
- Alcantud Marín, F. (1999). *Transferencia de Archivos*. España: UAF/CVA.
- ANYWERE. (2014). *Servidores SFTP Seguro/HTTPS/Cliente WEB Correo Seguro*. Obtenido de http://www.att.es/producto/goanywhere/att_archivos/GoAnywhere_Services_Info_General_150310.pdf
- Ashish, K., & Vishal, A. (2015). *Análisis del rendimiento y la seguridad mediante SHA3 en WEP*. India: ICETECH.
- Capuñay Puican, D., Guerrero Millones, A. M., & Villegas Vega, J. E. (Setiembre de 2016). *Análisis Comparativo de Algoritmos Criptográficos para Redes*. Recuperado el 11 de Noviembre de 2019, de <http://revistas.uss.edu.pe/index.php/ING/issue/download/40/1>
- Castanedo, M. (14 de 09 de 2007). Recuperado el 05 de 11 de 2019, de http://bibing.us.es/proyectos/abreproy/11314/fichero/MEMORIA_FIRMA_DIGITAL_XML%252FCap%C3%ADtulo+6+Cifrado.pdf
- Castells, M. (2001). *Internet y la Sociedad Red*. Barcelona: universidad Obrera de Cataluña.
- ESET Security Report. (2018). *Cifrado de la información*. Obtenido de <http://www.eset-la.com/centro-amenazas/descarga/Latinoamerica-2018/>
- ESET Security Report. (06 de 2018). *Cifrado de la información*. Recuperado el 06 de 11 de 2019, de <http://www.eset-la.com/centro-amenazas/descarga/Latinoamerica-2018/>
- Fernández, M. (2009). *Mensajería Instantánea en Internet*. Argentina: Creative Commons.

- García, J. (2011). *Tipos de ataques informáticos*. Obtenido de <http://www.delitosinformaticos.com/seguridad/clasificacion.shtml>.
- García, M. (2013). *Implementación del Algoritmo de cifrado AES para bajo consumo sobre FPGA*. Madrid, España.
- García, J. (05 de 09 de 2011). *Tipos de Ataques informáticos*. Obtenido de <http://www.delitosinformaticos.com/seguridad/clasificacion.shtml>.
- Gembeta. (2013). *Tipos de Criptografía*. Obtenido de <https://www.genbeta.com/>
- Gutiérrez, J. (03 de 07 de 2009). *Grupo Unican*. Recuperado el 20 de 11 de 2019, de <https://grupos.unican.es/amac/articles/aes.pdf>
- Hernández Sampieri, R. F. (2014). *Metodología de la Investigación* (6 ed.). México.
- Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2010). *Metodología de la investigación* (5 ed.). México. Recuperado el 21 de 11 de 2019, de [https://www.esup.edu.pe/descargas/dep_investigacion/Metodologia de la investigación 5ta Edición.pdf](https://www.esup.edu.pe/descargas/dep_investigacion/Metodologia%20de%20la%20investigacion%205ta%20Edici3n.pdf)
- Hernández, R. S. (2015). *Sistema de detección de intrusos mediante modelado de URI*. España: Universidad de Granada.
- Herrera, E. (2014). *Principios fundamentales que se busca proteger con la seguridad - CIA*. Obtenido de <https://informaticaseguraupc.wordpress.com/2014/09/15/principios-fundamentales-de-la-seguridad-de-la-informacion-cia/>
- ISO/IEC. (2013). Obtenido de Seguridad de la Información: <http://www.dnvba.com/cl/certificacion/sistemas-de-gestion.aspx>
- Lucena, M. (2014). *Criptografía y Seguridad en Computadores*. Obtenido de <http://sertel.upc.edu/tdatos/Libros/Lucena.pdf>.
- Mathur, N., & Bansode, R. (2016). *AES Based Text Encryption Using 12 Rounds with dynamic key selection*. *Procedia Computer*, 1036-1043. EE UU.

- Mathur, N., & Kesarwani, A. (2013). *Comparison Between. DES, 3DES, RC4, RC6, Blowfish and DES. Proceeding of National Conference of New Horizons in IT*. EEUU.
- Mieres, J. (2009). *Ataques Informáticos (Debilidades de seguridad)*. Obtenido de https://www.evilmfingers.com/publications/white_AR/01_Atiques_informaticos.pdf.
- Moya, J. (2015). *ECB Cifrado. Desarrollo de una aplicación para encriptar información en la transmisión de datos en un aplicativo web*. Quito, Pichincha, Ecuador: PUCE.
- Peraza, A. (2012). *La Criptografía: "Una guerra de Piratas y Corsarios"*. Obtenido de <http://www.egov.ufsc.br/portal/conteudo/la-criptograf%C3%ADauna-guerra-de-piratas-y-corsarios>.
- Ralph, H., Johanna, A., Olivier, M., Matthias, W., & Mohamed Ali, K. (2016). *TLS en la naturaleza: un análisis de Internet de protocolos basados en TLS para la comunicación electrónica*. Australia: CSIRO.
- Rodriguez, J. (2011). *Tipos de violación a la seguridad informática*. Obtenido de <http://wwwcomputacion95.blogspot.pe/2011/04/tipos-de-violacion-la-seguridad.html>.
- Romero, C., & Alvarado, Y. (24 de Setiembre de 2016). Recuperado el 16 de Julio de 2019, de <http://aaronbernaldezgrande.blogspot.com/2012/09/algoritmo-d-cifrado-3des.html>
- Silva, S. (2005). *Internet y correo electrónico/Internet and Email*. España: Ideas Propias Editorial S:L.
- Users Corporation. (2013). *Excel 2013 Avanzado* (1 ed.). Buenos Aires, Argentina: Fox Andina.
- Vikrant, S., & Meghana, K. (2017). *Implementación de hardware basada en FPGA de algoritmo criptográfico híbrido para cifrado y descifrado*. India: Computer and Optimization Techniques.
- Villegas, R. (2009). *Comparativa de Seguridad de Algoritmos de cifrado Asimétrico*. Obtenido de http://hdl.handle.net/12345_6789/8613.

ANEXOS

ANEXO 1: ENTREVISTA JUICIO DE EXPERTOS

Objetivo: COMPARAR TRES ALGORITMOS DE ENCRIPCIÓN PARA IDENTIFICAR LAS MEJORES CARACTERÍSTICAS DE OPTIMIZACIÓN EN LA TRANSFERENCIA DE ARCHIVOS EN MENSAJERÍA INSTANTÁNEA.

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

Datos Generales:

Nombre y Apellidos:

Profesión u ocupación: Edad:

Institución donde labora:.....

- ¿Ha configura Redes Virtuales con servidor SFTP, describa cuáles?
.....
.....
- ¿Conoce Usted algoritmos de encriptación para Redes Virtuales, menciónelos, y diga porque los usa?
.....
.....
- ¿Al analizar comparativamente cada algoritmo criptográfico cree usted que uno tenga el mayor rendimiento en cuanto a la integridad y la confidencialidad de la información?
.....
.....
- ¿Qué criterios usa para elegir que algoritmo resiste al criptoanálisis en una Red Virtual?
.....
.....
- ¿Cree que se debería tener una evaluación de cada algoritmo que utilizara en una Red Virtual?
.....
.....
- ¿Cree que es necesario utilizar algoritmos para encriptar nuestros datos?
.....
.....
- ¿Si realizamos una comparación de algoritmos criptográficos, los más usados en una Red Virtual le gustaría tener esta información de evaluación?
.....
.....