UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TRABAJO DE INVESTIGACIÓN

ALGORITMOS DE ENCRIPTACIÓN DE ARCHIVOS PARA LA TRANSFERENCIA EN MENSAJERÍA INSTANTÁNEA

PARA OPTAR EL GRADO ACADÉMICO DE BACHILLER EN INGENIERÍA DE SISTEMAS

Autor:

Montenegro Torres Domel

Asesor:

Ing. Junior Eugenio Cachay Maco

Línea de Investigación

Infraestructura, Tecnología y Medio Ambiente

Pimentel – Perú

2020

RESUMEN

Esta investigación se refiere a la seguridad informática, la cual hace la comparación de algoritmos de archivos de encriptación en la transferencia en mensajería instantánea de un servidor protocolo seguro de transferencia de archivos (SFTP) a un host cliente. La presente investigación está de acorde con los avances tecnológicos que demanda la sociedad actual, pues constantemente existe vulnerabilidad en el envío de la información mediante equipos tecnológicos haciendo uso de una red o el internet, ya que poseemos interceptores que se pueden utilizar con la finalidad de interceptar la información y luego darle un mal uso.

Es por ello que, con esta investigación se va a desarrollar un análisis comparativo de los algoritmos de encriptación que se usan en diferentes servidores en la transferencia de archivos en una red pública, siendo el problema principal la seguridad e integridad que tienen los datos al ser conectados con otro dispositivo de manera pretérita, por tal motivo compararemos algoritmos criptográficos implementados en un servidor SFTP, donde se tendrá que realizar los estudios y la captura del tráfico de la información, para no perder de vista y analizar quien nos brinda integridad y seguridad de los datos de manera eficiente.

La metodología seguida para la investigación se desarrolla bajo el enfoque cuantitativo de tipo descriptivo comparativo, porque permite manipular las variables en estudio, de esta manera se llegará a conocer el tipo de encriptación que ofrece cada algoritmo en tiempos, tamaño de los paquetes, el nivel de encriptación y no encriptación del archivo enviado.

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

ABSTRAC

This research refers to computer security, which makes the comparison of encryption file algorithms in instant messaging transfer from a secure file transfer protocol (SFTP) server to a client host. This research is in line with the technological advances demanded by today's society, as there is constantly vulnerability in the sending of information through technological equipment using a network or the Internet, since we have interceptors that can be used for the purpose of intercept the information and then misuse it.

That is why, with this investigation, a comparative analysis of the encryption algorithms that are used on different servers in the transfer of files in a public network will be developed, the main problem being the security and integrity of the data when be connected to another device in a pre-existing way, for this reason we will compare cryptographic algorithms implemented in an SFTP server, where studies and the capture of information traffic will have to be carried out, so as not to lose sight of and analyze who gives us integrity and security Of the data efficiently.

The methodology followed for the investigation is developed under the quantitative approach of comparative descriptive type, because it allows to manipulate the variables under study, in this way the type of encryption offered by each algorithm in time, packet size, level will be known. Encryption and no encryption of the file sent.

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

ÍNDICE

I: INTRODUCCIÒN

1.1 Realidad problemática.

En estos tiempos estamos haciendo uso de las tecnologías con la finalidad de ampliar y desarrollar la capacidad de comunicarnos de manera más segura haciendo uso de una red pública, donde la transferencia de los archivos por internet es insegura. La manera de manejar la información de forma segura y confidencial, se da a partir de la encriptación de los datos, de esta forma se garantiza la confidencialidad y la integridad de la información, gracias a los varios procesos de encriptación, autenticación y codificación. Es por eso que la seguridad hoy en día se ha vuelto muy importante cuando se da la comunicación, desde un inicio surgieron muchas indagaciones en seguridad informática de la red en la administración de contraseñas, autógrafos analógicos y el encriptamiento de la información utilizando algoritmos de encriptación, permitiendo así configurar redes de datos, pues en internet toda información es vulnerable, y de gran facilidad la captura de información por individuos extraños.

En estos últimos años están apareciendo diversos tipos de algoritmos con la finalidad de cifrar los datos, todos intentan encriptar las particularidades de la seguridad (integridad, confidencialidad, autenticación, no repudio). Siendo muy complicado determinar el nivel de desempeño de cada uno de los algoritmos, estos son frágiles, ante diferentes métodos de ataque, asimismo la mayor parte de los algoritmos trabajan con combinaciones de múltiples longitudes.

El desfase del avance tecnológico y los medios de uso de la misma, plantea muchos problemas que resultan de mayor interés. En resumen y de manera reciente se ha puesto énfasis entre la conexión de la comunicación digital y la escasa seguridad en la transferencia de información.

Así, la falta de instrumentos de comunicación con gran seguridad suele atribuirse a muchos problemas: la carencia de recursos computacionales en criptografía; las

dificultades de las herramientas criptográficas y la despreocupación en general por cuestiones de privacidad.

Un estudio realizado por ESET Security Report (2018), donde los encargados de seguridad del Laboratorio de Investigación de Enjoy Safer Technology (ESET) Security Report, recogieron información de más de 4500 gerentes, ejecutivos y técnicos que laboran en 2500 empresas en diferentes regiones, fraccionadas en microempresas (menor a 50 trabajadores), medianas empresas (oscilando en 50 y 250 trabajadores), macroempresas (de 250 y 1000 trabajadores) y Enterprise (más de 1000 trabajadores). A raíz de la información recolectada en el 2017, se presentó un informe el 2018, donde informaron el estado actual de la seguridad informática de las diferentes compañías latinoamericanas.

Según el informe presentado, se visualiza que tres de cada cinco empresas sufrieron un suceso de seguridad, quedando en el top del contagio con caracteres maliciosos (45%). Gran parte de ellos son relacionados al ransomware, esto quiere decir que de cada cinco compañías encuestadas en la zona son víctimas del robo de datos.

Observando y analizando caracteres maliciosos de la familia FileCoder, se encontró una gran cantidad de localizaciones al transcurrir el año 2017, en el Perú, con 25% del total de los países de Latinoamérica. En el puesto dos tenemos a México, con 20% de las localizaciones, siguiéndole Argentina con 15%, Brasil con 14% y Colombia con 10%.

No todos se consideran como caracteres malignos al hablar de ocurrencias en seguridad de una compañía. Tras de ello, encontramos al menos una de cada diez compañías entrevistadas comentó ser víctima de incidentes que perturbaron la disposición del servicio crítico (10%) o de un al acceso clandestino a las bases datos (11%). Asimismo, en estos años, la cantidad de compañías que fueron víctimas de irrupciones cibernéticos han sido constantes, observándose algunas diferencias en el año 2017.

Es muy importante tener conocimiento que, los engaños que se basan en ingeniería social, han avanzado en los últimos años, alcanzando en muchos casos más efectividad. Hoy en día se ve mutar de simples sitios de phishing, hasta webs con certificación Secure Sockets Layer (SSL) que significa, Capa de Conexiones Seguras, las mismas que pueden ser gratuitos o falsos, desconocidas por el usuario; el funcionamiento del protocolo Hypertext Transfer Protocol Secure (HTTPS), en español, Transferencia Segura de Datos de Hipertexto, que pasa por ataques homográficos, que están tomando mucha relevancia en la suplantación de empresas y marcas muy reconocidas.

En la actualidad las empresas están teniendo en cuenta los controles de seguridad de los datos, posiblemente se presenta una gran cantidad de empresarios que piensen en tener una solución de seguridad, pero son pocos los que se plantean de incluir políticas y planes con la finalidad de tramitar la seguridad informática.

Hoy en día se ve reflejado la no inclusión de políticas de seguridad en las empresas pues en el recojo de información a través de encuestas se visualiza que el 25% de las empresas no tienen medidas de protección para proteger la información de su empresa.

Se tiene conocimiento de la diferencia que existe en las empresas según la estructura de su capacidad; o sea, la gran mayoría de micro empresas no utilizan tecnología que garantice la seguridad, mientras las macro empresas cuentan con tecnología de protección a su información.

Se conoce que la gestión de la seguridad de los datos son procesos integrales, el estudio no debe restringirse exclusivamente a lo tecnológico y a los controladores que se adicionen. Hay que entender en primer lugar, la manera de formación en el área de seguridad y protección de la información de las empresas. Se puede observar en la información recolectada que un 10% de las compañías de la región no tiene establecida un espacio que se encargue de proteger la información.

Sin embargo, el 50 % de las empresas latinoamericana gestionan su seguridad desde una PC de TI. Al pensar que esto nace como una buena alternativa, lo ideal sería la conformación de un área independiente dentro de la empresa, con autonomía individual para revisar cualquier implementación relacionadas a la gestión de la seguridad de los datos.

La información es de mucha importancia en toda organización y es muy sensible, la cual no se puede divulgar, es considerada la parte fundamental de una empresa porque con ello se tiene un gran nivel de competencia que posibilita el avance, por ello los Gestores y/o Administradores eligen la implementación de sistemas mecanizados capaces de dar facilidad a tareas rutinarias y mecánicas. Es así que surge la necesidad de proteger la información.

El problema que especifico en este trabajo investigativo, se centraliza especialmente en la sección de defensa y en la seguridad, pues, se tiene que evaluar a los algoritmos de encriptación para la trasferencia de archivos, los mismos que van a proporcionar seguridad al momento de la intercomunicación entre individuos en forma personal o empresarial.

1.2 Antecedentes de estudio.

Hay muchas experiencias de investigaciones y artículos científicos que se relacionan con la seguridad de algoritmos de encriptación. A continuación, se hará una revisión exhaustiva con respecto a los antecedentes relacionados con lo que se está investigando:

Hernández, (2015) Da a conocer lo siguiente, el sistema de localización de intrusos a través del modelado de URI se orienta los riesgos existentes en los procedimientos en la red y/o la seguridad de un sistema y los beneficiarios. Estimulados a favorecer y menguar el riesgo vinculado a las intromisiones o ataques de los recursos de una red de ordenadores plantea en este estudio el objetivo principal, "mejorar un sistema de

detección de intrusos en red basado en el modelado de los mensajes intercambiados por un protocolo de comunicaciones".

El trabajo, se denominó Structural Stochastic Model (SSM), en el que usa el modelo de Markov con la finalidad de dar a conocer las cargas útiles relacionadas a formalidades que se basan en el traspaso de la información. Comprobándose el éxito en la localización de los peligros basados en la web, con consecuencias positivas, donde el protagonista se motivó en la indagación de potenciales modificaciones, orientando en la mejora de sus prestaciones con la finalidad de operar en escenarios reales e inclusive haciendo uso de la web en explotación.

Las diferentes propuestas presentes en esta investigación son evaluadas y la información obtenida se compara con lo que se logra con el sistema SSM original, verificando mejoras en las prestaciones del sistema, desarrollado en la localización de intrusos.

Moya (2015) En su indagación. "Desarrollo de una aplicación para encriptar información en la transmisión de datos en un aplicativo de mensajería web". Presenta como objetivo principal "El desarrollo de un aplicativo para encriptar datos en el sistema web". Esta investigación aplica la gran mayoría de equipos investigados en la ejecución de este proyecto, la metodología que utiliza es conocida como el método de SCRUM, con este método las entregas son pequeñas, fáciles de observar y revisar habitualmente, teniendo más efectividad en la detección de faltas y permutaciones, asimismo Scrum se identifica con el desembolso de los servicios evitando la identificación en la calidad de los códigos, como es Xtreme Programming (XP), este método se adapta a nuestras exigencias, pues su estructura es más completa, además se reutiliza las herramientas que existen 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 este trabajo de investigación se puede visualizar un claro ejemplo de lo que es la vulnerabilidad de los datos que se puede ver hoy en día. Por lo que en estos tiempos se puede ver el avance de muchos estudios con respecto a la ejecución de muchos tipos de encriptación, de esta manera garantizar la confiabilidad cuando se intercambia la información. Esta indagación aborda la protección de los datos sobre la funcionalidad de ciertos algoritmos de encriptación utilizando claves de ocultamiento.

Quizhpe (2011), citado por Capuñay, D. I; Guerrero, A.M & Villegas, J.E (2016) presenta una indagación denominda "Soluciones de Cifrados a las Seguridades Informáticas en Procesos de Auditaje Organizacional". Visualizando como objetivo primordial "Realizar un estudio comparativo de soluciones de cifrados a las seguridades informáticas para ser utilizadas en los procesos de Auditaje Organizacional". En esta investigación el investigador efectuó un trabajo comparativo con la solución del cifrado a la seguridad informática de esta manera busca conocer con claridad y precisión las diversas formas de proteger los datos utilizando los múltiples medios de encriptación que se tiene, sobre todo las contraseñas de los usuarios que son muy valiosas, de esta manera nos sirve para tener protegido nuestros computadores, asimismo se realizó esta investigación con la finalidad que toda persona que esté interesado en este tipo de investigación aprenda rápidamente y de una manera escueta a apreciar la información y su importancia, tanto para las macro y micro compañías, asimismo tener algunos sistemas de protección que permitan alejar a los posibles hackers.

Es de mucha importancia tener en cuenta que es fácil la encriptación de nuestras contraseñas haciendo uso de los softwares que están en el Internet de manera gratuita, lo cual no nos da la seguridad de una herramienta efectiva para conservar seguros los datos.

En esta indagación se aprecia la comparación de las diversas formas de cifrado que existe en el mercado, lo que conlleva a elegir el algoritmo que brinde mayor seguridad, para que se utilicen en las diferentes empresas.

1.3 Sistemas teórico conceptuales.

A continuación se detalla las bases teóricas que se van a usar en este trabajo.

1.3.1 Norma ISO 27001.

Se propone una visión a la seguridad de datos, donde se precisa que, los diligentes que requieren resguardo son información digital, documentación escrita y activos físicos a conocimientos de los colaboradores. Los argumentos que se tratan van desde la evolución de competencias del equipo de trabajo hasta la protección técnica frente a las estafas informáticas. Según La ISO/IEC (2013).

1.3.2 Comunicación Segura.

En la transferencia de archivos electrónicos se van a manejar aspectos y a la vez definen una comunicación muy segura.

Autenticidad. Lucena (2014), da a conocer que: "La autenticidad es identificar al generador de la información; es decir, consiste en la seguridad de que las personas que intervienen en el proceso de comunicación son las que dicen ser" (p. 27).

Confidencialidad. Peraza (2012), indica que: "Se trata de la seguridad de que los datos que contiene el documento permanecen ocultos a los ojos de terceras personas durante su trayecto desde A hacia B" (p. 73). Por ello, se puede evidenciar que en este espacio se trabaja con la criptografía ocultando los datos, y también el camino a seguir con los datos incorporados en su destino. Por lo que podemos mencionar que la Confidencialidad es la captura de la información en su traslado de un punto A hacia un punto B, y la utilidad indebida de la información o la inadecuada gestión y acopio de estos datos por parte de B, radicando aquí la importancia de contar con datos encriptados para garantizar la confidencialidad.

Integridad. Peraza (2012), afirma que: "Consiste en la seguridad de que los datos del documento no sufren modificación a lo largo de su transmisión" (p.29). Por lo que en un

posible ataque a una persona x, puede capturar el documento en el trayecto que emplea para llegar a su destino. Para comprobar la integridad de los datos se realiza a través de firmas electrónicas, habitualmente fundamentadas en funciones Hash. Por otra parte, la legitimidad es posición básica para la integridad, por ello si un manuscrito es legítimo también es integro, mas no al contrario.

No Repudio. Lucena (2014), manifiesta que: "El no repudio de origen, es cuando el emisor no puede negar que envió alguna información porque el destinatario recibe una prueba infalsificable del origen del envío" (p. 38). En esta particularidad, la prueba la diseña el mismo remitente y la recibe el receptor; el no repudio de destino, se refiere a que el que recibe la información no puede negar que acogió el mensaje porque el remitente va a tener evidencia de la entrega. Este servicio facilita al remitente las evidencias de que el destinatario del envío, con certeza la ha recibido, evitando de esta manera la negación posterior del receptor. Por ello se concluye, que las evidencias de envíos las crea el destinatario y la recibe el remitente.

1.3.3 Seguridad de la Información.

Se requiere de un adecuado servicio para garantizar la seguridad de los datos, por ello se debe tener en cuenta los consiguientes principios:

Confidencialidad.

Herrera (2014), da a conocer que, la confidencialidad es la manera de advertir la propagación de los datos informáticos a individuos o sistemas no acreditados. Para ISO/IEC 17799:2000, consiste en asegurar que la comunicación sea asequible para el personal facultado.

Integridad.

Herrera (2014), menciona que: al discutir de la integridad, es estar al tanto de cómo los datos se conservan inmunes, libre de cambios o reemplazos personas no acreditadas. La ISO/IEC 17799:2000, sostiene también que, "la integridad es la garantía

de la exactitud y completitud de la información y los métodos de su procesamiento" (p.5).

Disponibilidad.

Herrera (2014), da a conocer: Se debe estar dispuesto al cliente o un régimen cuando estos requieran realizar una consulta sobre la información.

Según la ISO/IEC (2013), la disponibilidad es asegurar que los interesados acreditados puedan acceder cuando lo crean necesario.

1.3.4 Algoritmo.

Para Villegas (2009), es la manera de realizar cálculos, se fundamenta en efectuar con una sucesión o conjunto organizado y determinado de reglas que conducen, una vez detallados los datos, a la resolución del problema.

Gembeta (2013), sostiene "el concepto de algoritmo como un conjunto finito de procesos a su vez finitos y bien definidos que conducen a un resultado" (p.27).

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.

Advanced Encryption Standard (AES)

Viene a ser el algoritmo de cifrado simétrico. Lo desarrolló, Joan Daeman y Vicent Rijment, ambos de origen belga, bajo el nombre Rijndael. (Gutiérrez, 2009)

El algoritmo AES es conocido por los usuarios de routers, ya que Wi-Fi Protected Access (WPA), en español Acceso Wi-Fi Protegido utiliza este algoritmo a manera de técnica de cifrado automático; este cifrado se implementa en software y en

hardware. AES criptográficamente es el que utiliza bloques y claves de longitudes totalmente diferentes, existen algoritmos AES de 256 bits, de 192 bits y de 128 bits.

El cifrado intermedio establece una matriz de gran cantidad de bytes que se forman cuatro filas y cuatro columnas. Esta matriz aplica una serie de bucles de cifrado automático basándose en fórmulas matemáticas (sustituciones de bytes en forma lineal, de esta manera desplaza filas de la matriz, realizando las mezclas de columnas a partir de la multiplicación lógica y suma XOR en base a claves intermedias). (Mathur & Bansode, 2016).

Triple Data Encryption Standard (3DES)

En 1998 IBM ha desarrollado el algoritmo 3DES o Triple DES (TDES) que sería heredero directo de DES que trabaja sobre dispositivos de 128 bits, teniendo la clave de igual longitud. Después de las innovaciones realizadas por el NBS, que consistía esencialmente en el reajuste de la longitud de la clave y la igual forma de los bloques, DES encripta bloques de 64 bits, a través de la sustitución y permutación utilizando una clave de 64 bits, además 8 son de paridad. 3DES opera bajo la lógica booleana y se implementa fácilmente, tanto en hardware como en software. Se fundamenta en ejecutar el algoritmo 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).

Rivest Cypher 4 (RC4)

Fue creado en 1987 por Ron Rivest para RSA Security. Es el algoritmo de cifrado de flujo que se utiliza en la WEB y se emplea en los protocolos con mayor popularidad como el Transport Layer Security/Secure Socket Layer (TLS/SSL) que viene hacer el manto de unión segura y seguridad de la capa de transporte, tiene como objetivo la protección del tráfico de información en el internet, dando mayor seguridad en redes inalámbricas.

Para dar una mayor seguridad y evitar las repeticiones de clave RC4 en cada paquete, el vector se concatena inicializándose los 24 bits con la clave Wired Equivalent Privacy (WEP) de 40 o 104 bits, de esta manera se envía el vector de inicialización (IV) en claro y junto al paquete cifrado se analiza los datos empaquetados con la misma clave (cancelación XOR), además trabajan con los protocolos SSL/TLS, usan un mecanismo con gran similitud, pero realizan un hash del IV y la clave WEP y de esta manera crear la clave única RC4. Las repeticiones de las claves son improbables y no hay igualdad y relación entre las claves. (Castanedo, 2007), (Mathur & Kesarwani, 2013).

1.3.5 La Criptografía.

Silva (2005), se refiere "Como una rama de las matemáticas que estudia la transformación legible en información que se puede leer directamente, sino que debe descifrarse antes de ser leída" (p.30).

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).

1.3.6 Transferencia de Archivo en Red.

Alcantud M, (1999). Afirma que: la transferencia de archivos en red, viene a ser el traspaso de un registro (archivo) del ordenador desde un puente de comunicación o sea de un sistema a otro usualmente, los traslados de registros se realizan mediante la mediación de una comunicación protocolar. En la historia de la informática, una gran cantidad de protocolos de transferencia de archivos han sido elaborados para diversos entornos.

La divergencia de un protocolo con intención de comunicación, es donde los protocolos de transferencia de archivos no están correctamente elaborados para enviar

datos arbitrarios, facilitando de esta manera la comunicación asíncrona, a manera de las sesiones de Telnet. La finalidad principal es únicamente remitir la cadena de bits almacenados en una unidad en el sistema de ficheros, asimismo de utilizar los métodos que existen, tamaño, nombre, fecha y hora de los archivos.

En la Informática, transferir archivos es un término que se utiliza en forma genérica para referirse a la forma de la transmisión de los ficheros a través de una red de computadores. Si se conoce que el término está ligado al Protocolo de Transferencia de Archivos File Transfer Protocol, (FTP), existen muchas maneras de transferir los archivos a través de una red pública.

Los servidores de archivos proporcionan un servicio de transferencia de datos.

Niveles en los cuales puede tener lugar.

Los diferentes niveles de transferir archivos son los siguientes:

Inicialmente se cuenta con la transferencia de los archivos, que utilizados transparentemente se realiza a través de los sistemas de archivos de red, otra manera es la transferencia de los archivos desde los servicios dedicados, como el FTP o HTTP, también se cuenta con la transferencia de los archivos que se distribuyen entre las redes pico a pico, el traspaso del archivo en el sistema de mensajería instantánea, el traslado de información entre computadores y los dispositivos periféricos y por último consideramos al traspaso de archivos sobre vínculos directos como el módem o serie (null modem), como eXtensible Hyper Text Markup Language (XMODEM, YMODEM y ZMODEM). Sin viñetas es todo corrido como si fuera un solo texto.

1.3.7 Protocolo SFTP.

ANIWERE (2014). Lo define como: “Protocolo del nivel de aplicación que permite la transferencia y manipulación de archivos sobre un flujo de datos fiable. Es utilizado con SSH para proporcionar la seguridad a los datos y permite ser usado con otros protocolos de seguridad” (p.72).

1.3.7.1 Descripción y características.

En esta investigación se va a tener en cuenta las siguientes características:

Permite realizar diferentes operaciones sobre ficheros remotos, es aplicable con mayor frecuencia en las plataformas Unix y Windows, aunque existen hoy en día servidores SFTP en la gran mayoría de plataformas, hay que tener presente que su estructura está diseñada con la finalidad de ser un protocolo independiente, al contar con varias versiones como la versión 3 que es la más utilizada, pues ejecutada por el servidor OpenSSH de SFTP, al desarrollar la versión 4, redujo sus vínculos con Unix, por lo que Windows está basado su implementación en servidores SFTP, el SFTP utiliza por lo general el puerto 22 de Transmission Control Protocol (TCP). La seguridad que se utiliza en la transferencia de la información no la administra directamente el protocolo SFTP, sino Secure SHell (SSH), pues cuando se suben archivos, la transferencia pueden estar asociados con sus respetivos atributos básicos, como el tiempo, ya que es una ventaja sobre el protocolo FTP y no dispone de ningún crédito adicional para adicionar archivos en la fecha única.

1.3.8 Protocolo SSH.

El SSH es la designación de este protocolo y del programa que ejecuta su función primordial, considerado como el camino remoto a un servidor por intermedio de una conexión segura en el que todos los datos están cifrados. Por lo que, el enlace a otros dispositivos físicos, SSH permite la copia de la información de una forma segura, de esta manera se gestiona la clave Rivest Shamir y Adleman (RSA) para no estar escribiendo la clave al conectarse a los dispositivos físicos y transportar la información de cualquiera otra forma utilizando una aplicación por un solo medio que brinde seguridad utilizando SSH, asimismo, logra dirigir el tráfico y a la vez ejecutar los programas de gráficos remotamente. El puerto TCP que se asigna es el 22.

1.3.8.1 SSHv2 Server.

Puede usar el servidor SSHv2 para permitir que un cliente SSH realice una conexión segura y encriptada al enrutador. SSHv2 utiliza un cifrado seguro para la autenticación. El servidor SSHv2 en software puede interactuar con clientes SSHv2 disponibles pública y comercialmente.

1.3.8.2 SSHv2 Client.

La función de cliente SSHv2 es una aplicación que se ejecuta sobre el protocolo SSHv2 para proporcionar autenticación y cifrado del dispositivo. El cliente SSHv2 permite que el enrutador realice una conexión segura y encriptada a cualquier otro dispositivo que ejecute el servidor SSHv2. Esta conexión proporciona una conexión saliente cifrada. Con autenticación y cifrado, el cliente SSHv2 permite una comunicación segura a través de una red insegura.

1.3.9 Seguridad.

SSH, desarrolla un trabajo muy parecido al que se realiza con Telecommunication Network (TELNET). Lo que permite diferenciar es que SSH utiliza procesos de cifrado, permitiendo a los datos que se transporta de un punto a otro sea de una forma ilegible, impidiendo que otros logren revelar el usuario y contraseña del vínculo.

1.3.10 Diffie hellman.

Es un protocolo que permite establecer una clave entre dos o más partes que no se conocen, usando de alguna manera un canal poco seguro y de modo anónimo.

Se utiliza como medio para conectar claves simétricas que va a ser utilizadas en el cifrado de una sesión. Siendo de alguna manera poco fiables, por lo tanto, proporciona los pedestales fundamentales para diversos protocolos legitimados.

La seguridad reside principalmente en el exagerado conflicto del cálculo de los logaritmos discretos en un cuerpo limitado.

SOFTWARE PARA CONFIGURAR EL SERVIDOR SFTP

1.3.11 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 se muestran 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 costo de licencia y soporte se reducen significativamente ya que no hay que instalar ningún software cliente. Sus clientes solo necesitan un navegador web para comenzar a transferir archivos.

Característica	Beneficio
	Además, al usar el cliente web integrado, los usuarios no tienen que preocuparse por las estrictas políticas de firewall interno ya que la mayoría de las organizaciones no restringen 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 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	Sus datos confidenciales están protegidos durante el tránsito y en reposo mediante el uso de tecnologías de cifrado OpenPGP y SSL de alto grado. Esto es crítico para muchas empresas que ahora están sujetas a los requisitos de protección de datos de Payment Card Industry Data Security Standard (PCI-DSS), HIPAA y Sarbanes-Oxley.
Prevención de pérdida de datos	Evita la pérdida de datos confidenciales utilizando un motor de reglas Digital Light Processing (DLP) incrustado.
Transferencias de archivos ad-hoc	Realiza transferencias de archivos basadas en correo electrónico a la vez que evita los problemas que comúnmente se experimentan

Característica	Beneficio
	con la información adjunta de los correos electrónicos de gran magnitud.
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.
JMS	Publica eventos de servidor suscritos en cualquier cola Java Message Service (JMS) para su posterior procesamiento.
Access Control List (ACL) administrativo	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

Característica	Beneficio
	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	Las transferencias de archivos grandes a través de Internet están sujetas a fallas ocasionales debido a problemas relacionados con la red. En el caso de una transferencia de archivos 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 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	Transfiera automáticamente archivos a / desde el servidor utilizando los protocolos FTP / FTPS / SFTP / Secure Copy

Característica	Beneficio
archivos	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 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

1.3.12 AnyCliente.

Es un cliente que permite la transferencia de archivos de modo gratuito que admite un sinnúmero de protocolos, incluidos: FTP / S, SFTP, Amazon S3 y otros. Permite la transferencia de archivos desde una computadora local a un servidor que esté conectado en Internet.

AnyClient es completamente independiente como plataforma. Siempre y cuando posee un Java Runtime Environment (JRE) apropiado en el computador, de esta manera se puede usar AnyClient.

Este software como es AnyClient permite los siguientes tipos de conexión: SFTP / SSH, FTP, FTP / SSL implícito, AFTP (UDP), FTP / SSL (AUTH TLS), Amazon S3 (HTTPS), WebDav, Amazon S3 (HTTP), AFTP (TCP).

SOFTWARE PARA CAPTURAR TRÁFICO DE RED

1.3.13 Wireshark.

Es un software muy significativo que permite analizar protocolos de red en el universo. Busca visualizar lo que sucede en la red en forma microscópica.

Wireshark fue mejorándose con la ayuda de los diferentes aportes de los expertos de creadores de redes en el universo. Referido a la continuidad de un importante proyecto que se inició en 1998.

Wireshark posee un sin número de particularidades y contiene lo siguiente:

Se realiza un examen profundo de muchos protocolos, además los que se añaden constantemente, captura en tiempo real y realiza el análisis estando fuera de 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, los datos que se capturan 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 utilidad 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.

Los datos en tiempo real se pueden visualizar 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, incluyendo IPsec, ISAKMP, Kerberos, SNMPv3, SSL / TLS, WEP y WPA / WPA2; las reglas que utiliza para atenuar se pueden emplear en la relación de paquetes para realizar el análisis de modo instintivo y rápido y la salida de los paquetes se puede exportar a Extensible Markup Language (XML).

SOFTWARE PARA CONECTAR CLIENTE SERVIDOR SFTP

1.3.14 FileZilla.

Es un software que se utiliza como cliente de FTP especialmente está desarrollado para Windows. Esta interfaz es de estilo Explorador de Windows, permite mostrar la ventana local como también las carpetas remotas, el paso de la información de una ventana a otra es simplemente arrastrando y soltando. FileZilla tiene funciones muy importantes en FTP como son:

Permite soportar arrastrar y soltar, es capaz de soportar la continuación de las descargas interrumpidas, tiene una herramienta que permite almacenar 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,

SOFTWARE PARA CONTEO DE PAQUETES ENCRIPTADOS Y NO ENCRIPTADOS

1.3.15 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 permitirnos 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)

El Microsoft Excel, ayuda a crear hojas de cálculo de forma personalizada y también el modo de importar datos desde otras bases de datos y también a insertar tablas con datos numéricos y alfanuméricos, además aplica las fórmulas y las ecuaciones matemáticas con la finalidad de realizar cálculos.

Con el Excel se filtra todos los valores de las respectivas tablas con diferentes criterios y los ordena como lo desea el usuario, genera cualquier tipo de gráfico estadístico y utiliza los valores de las celdas tales como los gráficos de columnas, dispersión, barras, línea y áreas, realiza la codificación de los macros con la finalidad de automatizar las tareas que se realizan en forma repetida; con esta hoja de cálculo se puede acceder a todas las hojas de cálculo desde cualquier computador 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.

1.3.16 Firmas Digitales.

Según (Aguirre, 2006), la rúbrica analógica es un procedimiento criptográfico que agrupa la identidad del individuo o de un sistema de información al correo o instrumento. Respondiendo a la tipología de la rúbrica, puede, cerciorar la validez del mensaje.

1.3.17 Ataques informáticos.

Mieres (2009) manifiesta, que el ataque informático viene se refiere al aprovechamiento de las debilidades o fallas (vulnerabilidad) en el software o hardware, inclusive, en los que intervienen en el entorno informático, a fin de obtener beneficios; generalmente económicos, teniendo como consecuencia fragilidad en la seguridad de los sistemas, repercutiendo claramente en la organización.

Existen cuatro categorías de ataques o amenazas las cuales se mencionan a continuación:

Interrupción.

Referido a la irrupción de la disposición de un recurso del sistema es exterminado dejando de operar. 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 destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros".

Intercepción.

Según Rodríguez (2011), manifiesta que: "Una institución no autorizada obtiene acceso a un medio. Esto es considerado como agravio contra la confidencialidad.

Como referencia tenemos el ataque en obtención de datos a través del uso de troyanos o la copia ilegítima de archivos o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes de datos para develar la identidad de uno o más de los usuarios mediante el Spoofing o engaño implicados en la comunicación intervenida.

Modificación.

García (2011), da a conocer que: "Una entidad no autorizada que no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque es el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red".

Fabricación.

Rodríguez (2011), menciona que: "Una entidad no autorizada inserta objetos falsificados en el sistema. Éste es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes falsos en una red o añadir datos a un archivo. Asimismo, estos ataques se pueden clasificar en términos de ataques pasivos y ataques activos".

1.3.18 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).

Este vocablo se usa esencialmente con la finalidad de generar tecnología que funcione por medio de computadores, sin embargo, varias plataformas poseen una aplicación móvil. La mensajería que surgió a través de aplicaciones móviles, hoy en día se conoce como aplicaciones de mensajería instantánea.

La mensajería instantánea necesita utilizar un cliente que permita realizar la transferencia de archivos.

Actualmente se usa redes propias de diferentes softwares que nos ofrecen este tipo de servicio en cada computador diferente. Asimismo, hay softwares de mensajería instantánea que nos sirve de mucha ayuda, de este modo permite llegar la información de forma instantánea, utiliza el protocolo abierto Extensible Messaging and Presence Protocol (XMPP), con un grupo de servidores descentralizados.

1.4 Definición de la terminología.

A continuación se detalla los vocablos más utilizados en el presente trabajo:

1.4.1 Criptografía (Cifrado de datos).

Según, Lucena (2014) la criptografía consiste en encubrir el contenido de la información emitida por el remitente hasta llegar al receptor final y es descifrado por el usuario indicado. Asimismo, se puede mencionar que el vocablo criptografía procede de la coalición de los vocablos (oculto) y (escritura), y se define como: Habilidad de escribir con códigos secretos o de un modo misterioso.

1.4.2 Criptoanálisis.

Se basa en el discernimiento de los algoritmos cifrados y de las peculiaridades en general de los mensajes. Radica en el compromiso de mantener la seguridad de un criptosistema. El Criptoanálisis se puede hacer interpretando el contenido de los datos sin saber los códigos o claves, o también extrayendo a partir criptogramas la contraseña empleada en su ordenamiento. (Lucena, 2014)

1.4.3 Encriptado.

Es la forma de codificar y ocultar los paquetes de datos con la finalidad de imposibilitar la lectura por otras personas y sobre todo garantizar la confiabilidad de ciertas transacciones.

1.4.4 Clave Privada.

Es el cifrado de los datos con un sistema desigual, considerado como la clave que permite que el remitente del mensaje conozca, con la finalidad de cifrar o descifrar la información emitida.

1.4.5 Clave Pública.

También se le conoce como llave pública por su apelativo en inglés, (public key) es una de dos claves principales que actúan en la codificación de los datos, siempre y cuando se use un procedimiento de cifrado de la forma criptográfica asimétrica.

1.4.6 Protocolo SFTP.

Permite la transferencia de archivos con mayor seguridad. Hoy en día la versión que se utiliza es la 3, se ejecuta por el servidor de SFTP OpenSSH.

1.4.7 Protocolo SSH.

Este protocolo usa métodos de cifrado, permitiendo a la información se traslade por un medio de comunicación de forma poco leíble, evitando de esta manera la visualización y descubrimiento de la contraseña y el usuario de la conexión, ni tampoco la escritura que se realiza en la sesión.

1.4.8 Transferencia de archivos en red.

Es la transferencia de los datos entre un computador a otro a través de un canal de comunicación.

1.4.9 Mensajería instantánea.

Se considera a la manera en la que nos comunicamos en tiempo real.

1.4.10 Hash.

Es una función unidireccional encargada de atrapar el mensaje de ingreso con amplitud arbitraria y causa un extracto con distancia precisa. SFTP usa Secure Hash Algorithm (SHA) y Message Digest 5 (MD5) en la ejecución de servidores SFTP.

1.4.11 Algoritmo de hash seguro (SHA).

Hash unidireccional ha sido propuesto por NIST. SHA se basa especialmente en MD4 y origina un digest de 160 bits, resiste más a los ataques en comparación a los hashes de 128 bits (como el MD5), pero tiene el defecto que es lento.

1.4.12 Diffie hellman.

Es un medio que se utiliza generalmente para concertar claves con simetría que se emplean en el cifrado de una sesión. Permitiendo la no autenticación, y proveyendo las bases para un sin número de protocolos autenticados.

1.4.13 Advanced Encryption Standard (AES).

AES viene a ser un algoritmo criptográfico idóneo que utilizan en el procesamiento de información federal, de esta manera protegen la transferencia de información electrónicamente.

AES está basado en el algoritmo Rijndael, que detalla la utilización de las claves con diferente extensión tales como 256, 192 y 128 bits para el cifrado de bloques de 128, 192 o 256 bits.

1.4.14 Data Encryption Estándar (3DES).

3DES fue publicado por primera vez en 1998, por la oficina nacional de estándares y su cifrado de claves ocultas es un esquema establecido en el algoritmo conocido como Lucifer de IBM.

1.4.15 RC4.

Es un algoritmo de cifrado por bloques de clave proporcionado. Es muy notable por ser muy simple y rápido (esto se debe al uso de diferentes operaciones de computadores y el consumo de memoria es mínima).

1.4.16 Internet.

Conjunto de redes descentralizados que permiten la comunicación de computadoras, utiliza la familia de protocolos Transmission Control Protocol/Internet Protocol (TCP/IP), el mismo que permite garantizar a las redes físicas heterogéneas funcionamiento como una red lógica única, de trayectoria global. (Castells, 2001).

1.5 Formulación del problema.

¿Cómo mejorar la transferencia de archivos en mensajería instantánea?

1.6 Delimitación de la Investigación.

Este trabajo indagativo se va a desarrollar en el Instituto de Educación Superior Tecnológico Público "Utcubamba" ubicado en el Jr. Circulación N° 350 del distrito de Bagua Grande, provincia de Utcubamba, región de Amazonas. Los involucrados en esta investigación son el educando de la escuela académica de ingeniería de sistemas Domel Montenegro Torres y el asesor Ing. Junior Eugenio Cachay Maco; logrando ejecutar este proyecto en un espacio de 6 meses.

1.7 Justificación e importancia de la investigación.

Justificación Tecnológica.

En esta indagación en lo tecnológico la considero relevante pues la temática que afronta es de tendencia tecnológica, teniendo en cuenta que hoy en día nos mantenemos interconectados con el resto del planeta a través del internet, y es tan inseguro el uso de la transferencia de archivos por lo que resulta ser un argumento de investigación en estos tiempos debido a los avances científicos y tecnológicos.

Justificación Social.

En la actualidad la trasferencia de archivos por la web se ha convertido en una temática generalizada, en la que los acuerdos, concordias y reuniones se realizan continuamente vía internet. Por lo tanto, con la presente opción tratamos de apoyar a la población para que siga adquiriendo muy buenos instrumentos que permitan garantizar la integridad, seguridad, y reserva de una reunión que se realice por internet.

Justificación Económica.

Haciendo referencia a la justificación económica la investigación pretende auxiliar a disminuir la utilización de los recursos informáticos ya sea la disminución del tiempo de cifrado y descifrado de los paquetes de un archivo.

1.8 Hipótesis.

La implementación de los algoritmos de encriptación, permitirá la optimización de la transferencia de datos teniendo en cuenta la integridad y confidencialidad de la información.

1.9 Objetivos de la investigación.

1.9.1 Objetivo general.

Comparar algoritmos de encriptación para optimizar la transferencia de datos en la mensajería instantánea.

1.9.2 Objetivos específicos.

a) Seleccionar los algoritmos de encriptación que garanticen la seguridad de la información.
b) Describir los algoritmos de encriptación según el grado de confiabilidad.
c) Comparar los algoritmos de encriptación según sus características para garantizar la seguridad de información.

II: MATERIAL Y MÉTODO

2.1. Tipo y diseño de investigación.

2.1.1 Tipo de investigación.

Este estudio es 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 pretende configurar 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 integridad de los datos

Dónde:

X = Algoritmos de encriptación

Y = Medir la Confidencialidad

2.2.2. Diseño de la investigación.

En esta indagación se pretende demostrar la remisión de información encriptado y sin encriptar por una red pública, además se busca capturar el tráfico en un periodo definido. (Hernández Sampieri, Fernández Collado , & Baptista Lucio, 2010)

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 logrará obtener algoritmos de encriptación más seguros.
		Con la comparación de algoritmos de encriptación en una red pública aumentará el nivel de integridad y confidencialidad de los datos en la transferencia de archivos.
		Con la comparación de algoritmos de encriptación disminuiremos el tiempo de encriptación de los datos en la trasferencia de archivos en una red pública.

Nota. Fuente: Elaboración propia

2.1 Población y muestra.

La población que se va a utilizar en este estudio está formada por los algoritmos de encriptación y como elemento de análisis a los algoritmos de encriptación conocidos mundialmente como código abierto.

Selección de algoritmos criptográficos para la transferencia de archivos en el mercado tecnológico.

En este objetivo comparamos los algoritmos criptográficos que mayormente usan en las empresas, según el recojo de información de comparación de algoritmos en esta investigación se ha elegido por la longitud de la clave, resistencia al criptoanálisis y seguridad los siguientes algoritmos: 3DES, AES y RC4.

Tabla 3

Algoritmos simétricos de encriptación del mercado tecnológico

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	3de20
IDEA	Simple	128 bits	64 bits	19	Vulnerable a: Diferencial, Fuerza bruta	Vulnerable	1991	TLS	3de20

Nota. Fuente: Elaboración Propia.

2.2 Variables.

2.2.1 Variable independiente.

Algoritmos de encriptación de archivos

2.2.2 Variable dependiente.

Transferencia en mensajería instantánea

2.3 Operacionalización.

Tabla 4

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 Abordaje metodológico, técnicas e instrumentos de recolección de datos.

2.4.1 Abordaje metodológico.

El método que se va a utilizar en este estudio en cuanto a la recolección de la información es Experimental.

Se utilizará esta metodología, porque admite maniobrar las variables y a la vez va a permitir recolectar la información que se desea, para ello se tiene que conocer la diversa tipología de encriptación que oferta cada algoritmo.

2.4.2 Técnicas de recolección de datos.

La observación: Es una técnica que permite definir en una forma más sistematizada, lógicamente permite registrar en forma visual y verificable de lo que se desea conocer; de esta manera se captará de un modo más objetivo, lo que sucede en el universo, para analizarlo, detallarlo o exponerlo desde un punto de vista científico; con la gran discrepancia de lo que ocurre en el planeta empírico, donde el hombre utiliza la información observada de una forma práctica con la finalidad de resolver problemas o satisfacer sus propias necesidades.

Entrevistas: se entrevista a expertos en seguridad informática, de esta manera se obtendrá con mayor detalle que algoritmo de encriptación utilizan en servidores, y cuál de ellos ofrece mayor seguridad a la información.

2.4.3 Instrumentos de recolección de datos.

Se aplicará la técnica del análisis documentado a los logros que se obtendrán, a esta técnica se le denomina procedimiento de investigación, el cual consiste en la utilización de instrumentos adecuados, de esta manera poder encontrar la relación entre los hechos reales y la hipótesis, a través del análisis documentado, además va a permitir la selección de los datos más relevantes con la finalidad de expresar su contenido. Se utilizará los siguientes instrumentos de recojo de información.

a) **Wireshark:** Permite observar los sucesos en la red a escala microscópica.

b) **FileZille:** Permite enviar ficheros de un cliente a un host servidor.

c) **AnyClient:** Es un host cliente de transferencia de datos basado en web y es fácil de usar, además es muy compatible con todas las plataformas como: Windows, Mac OS X y Linux.

d) **Excel:** Permite filtrar los datos y/o paquetes encriptados y no encriptados, además permite representar gráficamente.

2.5 Procedimiento para la recolección de datos

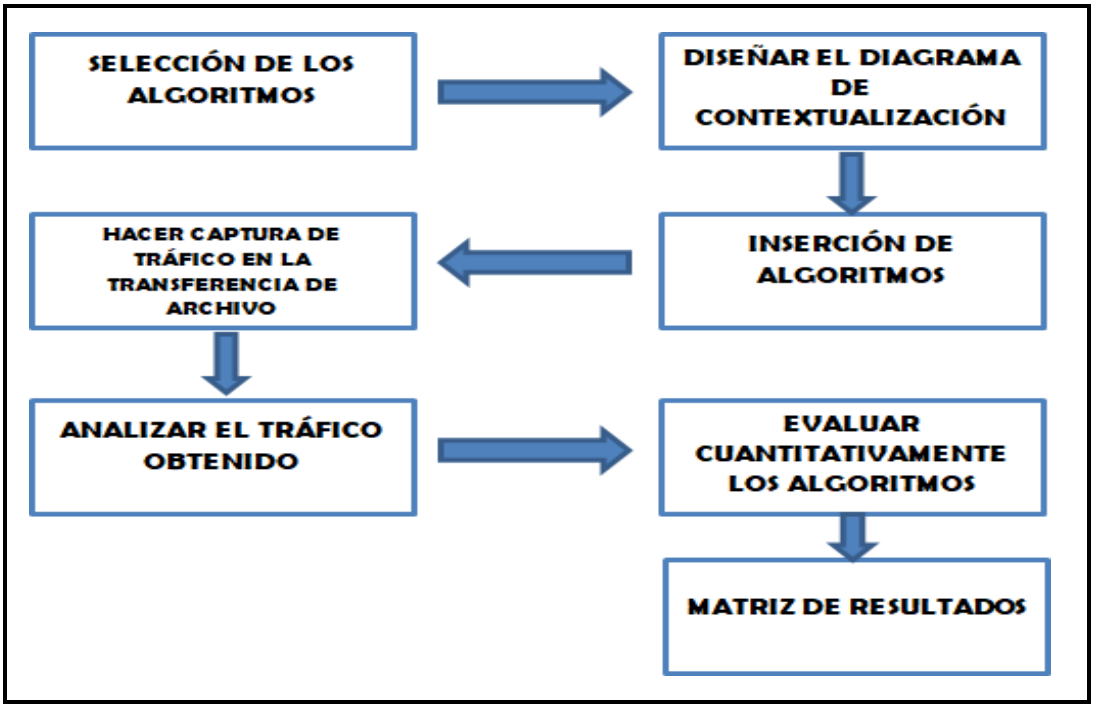

Figura 1. La figura ilustra la forma como es el proceso de la recolección de los datos, de esta manera poder encontrar la relación entre los hechos reales y la hipótesis.

2.6 Análisis estadístico de datos e interpretación de los datos.

A la información que se obtenga se analizará estadísticamente, para ello utilizaremos fórmulas que nos permitirán procesar la información.

Tiempo de demora del envío: Es la diferencia entre el tiempo de Inicio y final. Siendo los segundos o minutos su unidad de medida.

$$Td = Tf - Ti$$

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

$$Ti = Tiempo\ Inicial$$

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

$$TP = Pe + P\ \text{no}\ e$$

$$Pe = TP - P\ \text{no}\ d$$

$$P\ no\ d = TP - Pe$$

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

$$P\ no\ e = Paquetes\ no\ encriptados$$

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

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

2.7 Principios éticos.

Son criterios éticos que se toman en cuenta en este estudio, se relaciona con cualquier suceso en el cual se involucra esta investigación. Aquí podemos mencionar.

a) **Criterio de confiabilidad.** La información que se ha requerido en este estudio se ha obtenido de manera legal con bastante profesionalismo con la finalidad de no causar daños a personas involucradas; tal como está expresado 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 el artículo 28 señala: Que la recopilación de la información por medios fraudulentos, ilícitos o desleales está completamente penado por las leyes peruanas.

b) **Criterio de Conformabilidad.** Las afirmaciones y resultados que se obtendrán como producto de este estudio estarán confirmados y validados por una persona especialista en el tema: El Código Deontológico del Colegio de Ingenieros del Perú en su Capítulo III específica "Las 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".

2.8 Principios de rigor científico.

El presente estudio tendrá los criterios de rigor científico que están dados por: La validez interna y validez externa.

La Validez interna: Este método nos permite evaluar la idoneidad de los elementos de control de la investigación como también del diseño; en forma general consiste en evaluar su validez interna y externa. Siendo la mejor estrategia que permite incrementar la validez interna de una investigación solida; se recomienda primero analizar los datos con la finalidad de establecer las principales características. Por lo tanto, se aplicará la validez interna, porque permite evaluar con plena originalidad e idoneidad el presente estudio de investigación, teniendo en cuenta sobre todo la solidez en el diseño de esta investigación.

La validez externa: Consiste en la posibilidad de generalizar los resultados que se obtendrán de la investigación a otros estudios.

III: CONCLUSIONES

3.1. Conclusiones.

a. 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.

b. Se han seleccionado tres algoritmos de encriptación siendo los más usados los siguientes: Advanced Encryption Estándar (AES), Triple Data Encryption Estándar (3DES) y Rivest Cypher 4 (RC4), porque ellos garantizan la seguridad de la información de los usuarios.

c. 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.

d. 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.

REFERENCIAS BIBLIOGRÁFICAS

Aguirre, J. (2006). *Seguridad Informàtica y criptografia*. Obtenido de http://www.criptored.upm.es/crypt4you/temas/criptografiaclasica/leccion1.html

Aidong, F., & Zhiwei , Z. (2018). *Research on Parallel Dynamic Encryption Transmission Algorithm on VoIP* . China: University, Suzhou.

Alcantud Marìn, 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). *Analisis 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 htpp://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. (06 de 2018). *Cifrado de la informaciòn*. 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.

Garcia, J. (2011). *Tipos de ataques informàticos*. 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.

Garìa, 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

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 conla 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). *Criptografia y Seguridad en Computadores*. Obtenido de http://sertel.upc.edu/tdatos/ Libros/Lucena.pdf.

Mathur, N., & Bansode, R. (2016). *AES Based Text Encription Using 12 Rounds with dinamic key selection.Procedia Computer, 1036-1043*. EE UU.

Mathur, N., & Kesarwani, A. (2013). *Comparison Between. DES, 3DES, RC4, RC6, Blowfish and DES. Proceding ofd National Conference of New Horizons in IT*. EEUU.

Mieres, J. (2009). *Ataques Informàticos (Debilidades de seguridad)*. Obtenido de https://www.evilfingers.com/publications/ white_AR/01_Ataques_informaticos.pdf.

Moya, J. (2015). *ECB Cifrado. Desarrollo de una aplicación para encriptar infromación en la transmisión de datos en un aplicativo web*. Quito, Pichincha, Ecuador: PUCE.

Peraza, A. (2012). *La Criptografia: "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 violaciòn a la seguridad informàtica*. 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 electronico/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 hîbrido para cifrado y descifrado.* India: Computer and Optimization Techniques.

Villegas, R. (2009). *Comparativa de Seguridad de Algoritmos de cifrado Asimétrico*. Obtenido de de http://hdl.handle.net/12345 6789/8613.