UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TÌTULO:
INGENIERO EN TELECOMUNICACIONES CON MENCIÓN EN GESTIÓN EMPRESARIAL

AUTOR (A):
CARLOS FERNANDO FAJARDO CHAMBA

ANÁLISIS DE LA SEGURIDAD EN REDES DE DATOS DE LA U.C.S.G. MEDIANTE CRIPTOGRAFÍA

TUTOR:
ING. EFRAÍN VÉLEZ TACURI

Guayaquil, Ecuador
2014

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por CARLOS FERNANDO FAJARDO CHAMBA, como requerimiento parcial para la obtención del Título de INGENIERIA EN TELECOMUNICACIONES CON MENCIÓN EN GESTIÓN EMPRESARIAL.

TUTOR (A)

_____
Ing. Efraín Vélez Tacuri

DIRECTOR DE LA CARRERA

_____
Ing. Armando Heras Sánchez

Guayaquil, a los 30 del mes de agosto del año 2014

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE EDUCACACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Carlos Fernando Fajardo Chamba**

DECLARO QUE:

El Trabajo de Titulación "**Análisis de la Seguridad en Redes de Datos de la U.C.S.G. Mediante Criptografía"** previa a la obtención del Título **de Ingeniero en Telecomunicaciones con Mención en Gestión Empresarial**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del Trabajo de Titulación referido.

Guayaquil, a los 30 del mes de agosto del año 2014

EL AUTOR (A)

_____
Carlos Fernando Fajardo Chamba

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Carlos Fernando Fajardo Chamba**

Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación en la biblioteca de la institución del Trabajo de Titulación: "**Análisis de la Seguridad en Redes de Datos de la U.C.S.G. Mediante Criptografía"**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 30 del mes de agosto del año 2014

EL (LA) AUTOR(A):

_____
Carlos Fernando Fajardo Chamba

AGRADECIMIENTO

A Dios, por bendecirme con una familia luchadora con sólidos valores morales y éticos, que se ha esforzado tanto para que este proyecto de titulación pueda darse, a mis amigos por siempre contar con su apoyo incondicional.

A nuestros profesores, por transmitir sus conocimientos, experiencias, y esfuerzo, por convertirnos personas profesionales y justos; a las autoridades de la facultad Técnica por la consideración y estimulo que nos han brindado en todo momento, y en especial al Decano, Director de carrera, Coordinador académico y a mi Tutor de Proyecto de Titulación por su ardua y valiosa colaboración, orientación en el desarrollo del presente Proyecto de titulación.

Carlos Fernando Fajardo Chamba

DEDICATORIA

A Dios creador de todo el universo, el que me ha dado resistencia para continuar cuando estado a punto de caer, por ello con toda honestidad que mi corazón puede emanar dedico este proyecto de titulación.

De igual forma, dedico este proyecto de titulación a mis padres que han sido pilares fundamentales a inculcarme valores, lo cual me ayudado a salir adelante en los momentos más difíciles.

A mi hermana que siempre ha estado junto a mí, brindándome su amor y apoyo, sobre todo demostrarme que lo imposible no existe con su lucha y determinación.

Al Ing., Efraín Vélez Tacuri que, como tutor de este proyecto de titulación, me ha guiado y corregido en mi labor con una predilección y entrega que ha superado, con mucho, todas las perspectivas que, como estudiante, deposité en su persona

Carlos Fernando Fajardo Chamba

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA: INGENIERIA EN TELECOMUNICACIONES

CALIFICACIÓN

_____

Ing. Efraín Vélez Tacuri
TUTOR

ÍNDICE GENERAL

ÍNDICE DE FIGURAS.

ÍNDICE DE TABLAS

RESUMEN.

Este proyecto de titulación es parte de un análisis de la seguridad en redes de datos mediante mecanismos criptográficos para los procesos de identificación, de vulnerabilidades entorno a las redes de datos que se utiliza día a día.

El constante desarrollo de nuevos sistemas tecnológicos como son: *hardware*, *software*, ha proporcionado una facilidad entorno al tiempo en lo que se refiere pagos en línea, video conferencias, plataformas de aprendizaje en *online*.

No obstante, esta evolución tecnológica trae consigo sus de riesgos, ya que también sirve como herramienta para causar delitos informáticos los cuales tiene que ver mucho con la manipulación de información que se envía tanto en la red pública como privada.

Se detallara en el capítulo uno el planteamiento del problema como también la metodología que se utiliza, la justificación del proyecto de titulación, el planteamiento de la hipótesis, el objetivo general y específico, tipo de investigación que se debe cumplir al finiquitar el proyecto de titulación.

Se detallara en el capítulo dos el marco teórico que define la historia de la criptografía, proceso de la criptografía, principios de kerckhoffs, criptografía simétrica y asimétrica.

Se detallara en el capítulo tres la autenticación y seguridad de las redes de datos, certificaciones, seguridad IP, seguridad web, seguridad en el correo electrónico, seguridad de los sistemas, detección de la instrucción basada en reglas, software dañino, cortafuegos (*firewalls*).

Se detallara en el capítulo cuatro la metodología, encuesta que se realizó para obtener una muestra, que tan informados están sobre la seguridad web dentro y fuera de la institución, en el capítulo cinco se plantea protocolos de seguridad para las redes de datos, definición de mecanismos: normativas, Recursos, tabla de servicio, Identificación de riesgo y amenazas, Protección de servicios, configuración de la red, control de acceso, salvaguardar la información, solicitación de políticas de seguridad.

Finalmente en el capítulo seis tenemos la conclusión y recomendación del análisis que se realizó en el proceso de la investigación.

Palabras claves: Firewalls, hardware, software, Seguridad IP, Software dañino, seguridad web.

ABSTRACT.

This degree project is part of a safety analysis in data networks using cryptographic mechanisms for identification processes, vulnerabilities environment for data networks used daily.

The constant development of new technological systems such as: hardware, software, has provided a facility environment while as regards payments online, video conferencing, online learning platforms.

However, this technological evolution brings its risks, as it also serves as a tool to cause computer crime which has much to do with the manipulation of information that is sent in both the public and private network.

The exposition of the problem was detailed in the chapter one as also the methodology that is in use, the justification of the project of qualifications, the exposition of the hypothesis, the general and specific aim, type of investigation that must be fulfilled on having concluded the project of qualifications.

It will be detailed in chapter two the theoretical framework that defines the history of cryptography, cryptography process, principles Kerckhoffs, symmetric and asymmetric cryptography.

It will be detailed in chapter three authentication and network security data, certifications, IP security, Web security, security email, security systems, detection of rule-based instruction, malware, firewalls (firewalls).

There was detailed in the chapter four the methodology, survey that was realized to obtain a sample, which so informed they are on the web safety inside and out of

the institution, in chapter five poses security protocols for data networks, definition will be detailed in chapter four mechanisms: Policy, Resources, ironing service, risk and threat identification, protection services, network configuration, access control, safeguard information, solicitation of security policies.

Finally in chapter six we have the conclusion and recommendation of the analysis made in the research process.

Keywords: Firewalls, hardware, software, IP Security, malicious software, web security.

INTRODUCCIÓN.

El estudio de la seguridad de las redes de datos es fundamental para los análisis relacionados con el campo de las telecomunicaciones o informática. La creciente presencia de ataques dentro de las redes de telecomunicaciones en nuestra sociedad, hace ineludible la formación de profesionales en esta área; para los cual se requiere, un conocimiento adecuado de cómo prevenir estos ataques, realizando configuraciones o el mantenimiento de las mismas, es un requisito imprescindible en su preparación.

El mundo a medida que pasa el tiempo va evolucionando drásticamente así como sus tecnologías, se crea nuevos sistemas de conexión los cuales permiten al usuario poder estar en contacto ya sea de manera física o por medio de señales inalámbricas.

Además los últimos años en el ecuador según datos estadísticos generados por la Supertel[1], hace referencia a la conectividad de telefonía fija, telefónica móvil, acceso a internet, cibercafés, televisión pagada etc. Tiene un alcance de 12.116.687 usuarios conectados a la red de datos. No obstante, podemos dar por entendido que toda esta cantidad de usuarios se encuentre exento de algún taque de fuerza bruta.

A medida que se crean nuevas aplicaciones, *website*, incluso plataformas educativas dentro de instituciones universitarias, gubernamentales, se preocupan más

[1] SUPERTEL: La Superintendencia de Telecomunicaciones

del diseño de cómo va a quedar, mas no de cómo se van a proteger los datos de los usuarios que adquieran o estén haciendo uso de dichas aplicaciones o plataformas.

La criptografía hace uso de mecanismos de seguridad que nos permite salvaguardar la información de ciber-delincuentes, pero no por ello se quiere decir que sea totalmente segura ya que dichos mecanismos criptográficos pueden ser rotos.

No obstante, se debe realizar un análisis mediante mecanismos criptográficos, técnicas de detección de intrusos, cortafuegos, seguridad de correo electrónico, etc. con el fin de poder salvaguardar la información.

CAPÍTULO I.

PLANTEAMIENTO DEL PROBLEMA.

1.1 Planteamiento del Problema.

El problema de este proyecto se origina en la necesidad de salvaguardar la seguridad y confidencialidad de la información, para evitar la vulnerabilidad mediante la aplicación de la criptografía y de esta manera prevenir modificaciones dentro de la plataformas que utilizan, con el fin evitar ataques externos e internos.

1.2 Justificación.

Este proyecto de titulación ésta enfocado en proporcionar conocimiento sobre la seguridad de la información mediante mecanismos criptográficos a la comunidad universitaria con el fin de establecer un coloquio de saberes, es decir un conocimiento de distinto mecanismo de protección capaz de eludir los posibles ataques a los equipos informáticos o el medio que esté conectado dentro de alguna institución

En efecto el producto de esta investigación, se puede especular imparcialmente los distintos desarrollos dentro de la criptografía clásica y moderna que hay en la actualidad para mejorar la calidad de servicio de las redes de datos.

1.3 Objetivos.

1.3.1 Objetivo General.

Analizar la influencia de la criptografía en las redes de datos, de forma firme y coherente para reducir las vulnerabilidades de la información.

1.3.2 Objetivos Específicos.

- Identificar las características, tipos de mecanismos, y determinar los diferentes métodos criptográficos en las redes de datos.
- Distinguir los distintos métodos de seguridad de las redes de datos mediante encuestas a los estudiantes UCSG y entrevistas al personal del Departamento de Sistemas de cómputo de la UCSG.
- Promover alternativas de solución, protección y prevención de las redes existentes

1.4 Hipótesis.

Con la elaboración de este trabajo se pretende ampliar los conocimientos en la criptografía moderna empujando el desarrollo de nuevos proyectos y técnicas para el manejo de claves de seguridad, permitiendo saber cuándo aceptar o rechazar una información de dudosa procedencia.

1.5 Tipo de investigación.

Utilizaremos el tipo de investigación explicativa, la cual nos permite tener una relación causal de los procesos o problemas que se enfocan en el análisis de la seguridad de las redes de datos de la universidad católica Santiago de Guayaquil

1.6 Metodología.

El método a utilizar en el presente trabajo de investigación es un análisis con observaciones, bibliografías en enfoque cuantitativo.

1.6.1 Justificación de la selección del método.

Por ser un proyecto de investigación analítica tecnológica se da a conocer el uso de la metodología, que se basa en la hipótesis, estudios realizados, medición de diversas variables.

El enfoque cuantitativo impulsa al proyecto con una realidad veras, con el fin de cumplir con el objetivo de las variables independientes o lograr resultados sostenibles para dicho estudio. En el proceso de este enfoque se deduce que va de lo particular a lo genera y viceversa.

1.6.2 Diseño de la investigación.

Al poder observar que es una investigación cuantitativa lo cual permite medir los resultados que se recogen de encuestas, análisis a lo largo de la investigación de manera concluyente.

1.6.3 Muestra.

La teoría del muestreo permite establecer de una manera efectiva el proyecto de investigación en base al método cuantitativo ya que nos refleja con exactitud los tipos de elementos que conforman.

1.6.3.1 Técnicas e instrumentos de análisis y levantamiento de datos.

El levantamiento de datos es el descriptivo del muestreo realizando a través de las muestras recopiladas en el proyecto de investigación.

El procesamiento analítico de la base de datos recopilada se representa mediante mapas estadísticos, imágenes reales, tablas de contenidos, simulaciones virtuales.

CAPÍTULO II.

MARCO TEÓRICO.

Este capítulo abarca el estudio previo de la criptografía desde sus inicios hasta la actualidad con el fin de poder comprender los procesos de seguridad que se han ido desarrollando durante todo este tiempo.

A medida de que la criptografía tradicional permite comunicaciones seguras entre varias partes, la propuesta hipotética de utilizar la criptografía en la actualidad, podría poner en riesgo algunos sistemas criptográficos más usados como el AES, RSA, entre otros.

2.1. Introducción Histórica.

Hoy en la actualidad, la criptografía está muy presente en nuestro medio. Así, operaciones como transmitir o receptar, por medio de dispositivos móviles, comprar con tarjetas de crédito, retirar dinero del cajero automático, ingresar a una aplicación introduciendo la clave de seguridad etc.

La escritura es, en opinión de muchos, el invento más significativo de la humanidad. La escritura permite dejar constancia de hechos, ideas, etc. Lo cual permite comunicarnos de manera temporal o fija de este modo es como las antiguas civilizaciones han podido dejar rastro de existencia. Por lo tanto mediante el desarrollo de la escritura, se llegó a una conclusión que conlleva su lectura por terceros, con lo cual dio inicio a los primeros sistemas de protección de escritura de texto en claro.

Históricamente las personas han utilizado diversos sistemas con el fin de lograr que un mensaje no llegara a manos de personas no permitidas a leerlo. Esto se remonta al conflicto de Grecia y Persia donde se diseña, hacia el siglo V a. C, el primer método de sistema de cifrado, este consiste en un bastón sobre el que se enrollaba en espiral, fue este método el que salvo a Grecia de ser invadida por el rey Jerjes.

Un griego llamado Demarato exiliado en la ciudad de Persa, tuvo conocimiento de las intenciones de Jerjes rey de reyes para atacar a Grecia, dicho griego al saber esta situación decidió alertar a sus hermanos mediante un mensaje oculto en tablillas de madera el cual estaba recubrir con cera.

La ocultación de cierta información ofrece sin duda un nivel de seguridad, pero padece de una debilidad imprescindible, es decir si se llega a descubrir el texto en claro, el contenido de la comunicación oculta se revela en el instante o por otra parte, interceptar el mensaje compromete toda la seguridad de la información enviada. Es decir, que el producto del desarrollo de la ocultación de la información dio paso a la creación de la criptografía, termino derivado de los vocablos griegos “kyptos” que significa oculto y “graphein” que significa escritura.

El propósito de la criptografía como ya se había mencionado no es de ocultar la existencia de un mensaje, sino ocultar su significado, a este proceso se lo reconoce como cifrado.

La criptografía clásica usa técnicas de permutación y sustitución. En la permutación el texto en claro cambia su patrón de modo de que el texto cifrado aparece en las mismas posiciones pero con sus posiciones permutadas.

Para que esta permutación sea eficaz en su combinación, el texto en claro necesita seguir un sistema muy sencillo y establecido, anticipadamente por el emisor y el receptor. Como por ejemplo se tiene la permutación de "riel" en la que el texto en claro se escribe alterando las letras en dos líneas separadas tenemos como ejemplo:
Criptografía en la UCSG

C-i-t-g-a-í-e-l-u-s

r-p-o-r-f-a-n-a-c-g

Otro sistema de permutación es producido por el primer instrumento criptográfico militar de la historia el Escitalo (siglo V a. C.), se trata de un bastón de madera sobre el cual se enrollaba una tira de cuero tal como se muestra en la (figura 1.).

El desarrollo de este sistema solo podría ser apreciado en una larga lista de letras sin sentido, en ese tiempo para poder cifrar ese mensaje sin sentido se necesitaba un bastón de igual diámetro que el primero, ya que el diámetro de dichos bastones era la clave para poder leer el mensaje del texto en claro.

La opción a la permutación (transposición) es la sustitución. Así, como la transposición es un método más antiguo, la sustitución también lo es. Éste método de cifrado por sustitución emerge en el kamasutra donde la mujer estudia el arte de la escritura secreta con el fin de emparejar las letras del alfabeto y a su vez sustituir cada letra del texto en claro para su pareja, es de esta forma que la escritura secreta se la conoce comúnmente como cifrado de sustitución, dada que cada una de las letras del texto en claro se sustituye por una diferente.

Figura 1. La Escítala lacedemonia.
Fuente: (UGR, s.f.)

La diferencia entre la transposición y sustitución es que la transposición le interesa la posición de las letras que se van a cifrar mientras que en la sustitución hace que el recepto descifre el texto en claro realizando la sustitución inversa que va a variar en el proceso.

No obstante a medida que el tiempo transcurría nos encontramos con un nuevo método es decir el más sonado de la antigüedad clásica, el método de cesar conocido de esa forma por el emperador julio cesar este método consiste en sustituir cada letra del texto en claro sin adulterar el lugar en el mismo para dicha situación se realizó

tres posiciones por delante del alfabeto es decir cambiar todas las AES por DES, todas las BES por ES donde al termino del alfabeto de las letras “X”-“Y”-“Z” se sustituyen por “A”-“B”-“C”.

Estos sistemas de Escítala lacedemonia y de cesar, aclaran los métodos existentes de sustitución y transposición.

Estos métodos en la actualidad son completamente inseguros ya que para poder cifrar la clave se establece la ciencia del criptoanálisis.

Ciertamente, tras la vertiginosa caída del imperio romano y hasta la restauración, la criptografía sólo tuvo progresos significativos en los califatos islámicos, en la capital de Bagdad, en el siglo IX. d. C. donde nace el moderno criptoanálisis a partir de la conjetura de cada lengua tiene una frecuencia característica de cada una de sus letras, de esa forma bastaba para saber cuál era la letra subyacente muy independiente de su forma.

Los sistemas más notorios del renacimiento fueron por Leone Battista Albeti, el inventor del primer artificio cifrado de disco el cual consistía en dos coronas circulares concéntricas una de ellas que se encuentra en el interior lleva grabado el alfabeto cifrado en el exterior llevaba grabado el texto en claro el cual podría girar en su centro. Lo que nos da a entender que el disco superior de texto en claro como el disco inferior de alfabeto cifrado que correspondía a un método polifacético. (Véase la Figura 2)

Figura 2. Leone Battista Alberti Método de disco.
Fuente (Timerime, s.f.)

Así mismo en la era del renacimiento fue creado otro sistema muy popular por Blaise Vigenere en el siglo XVI el cual desarrollo el tema de la criptografía poli-alfabética por lo cual hoy en día se lo denomina “tablero de Vigenére” consiste en una posición de 26 letras que contiene el orden del método de César.

La cifra de Vigenère es la sustitución poli-alfabética solo que, en vez de desplazar cada letra del alfabeto cifrado en un número fijo de posiciones se desplaza varios números fijos para obtener la letra cifrada, su desplazamiento de variable dan paso definitivo a la palabra en clave del texto en claro (Véase la Figura 3.)

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

Figura 3. Blaise Vigenere tablero de Vigenére.
Fuente: (Teknoplof, 2010)

La criptografía sigue avanzando durante la edad moderna y contemporánea pero en el siglo XX las técnicas de cifrado evolucionan dando lugar a nuevas máquinas donde se da a conocer la casi mítica Enigma máquina de cifrado.

Enigma fue una máquina de cifrado patentada por Arthur Scherbius lo cual era una versión eléctrica del disco de cifra de Alberti, la forma inicial del invento de sherbius consiste en tres elementos conectados en cable, un teclado para escribir cada letra de texto en claro, un disco modificador que cifra cada letra del texto en claro correspondiente al texto cifrado, un tablero exterior el cual tiene varias lámparas que indica la letra de texto cifrado.

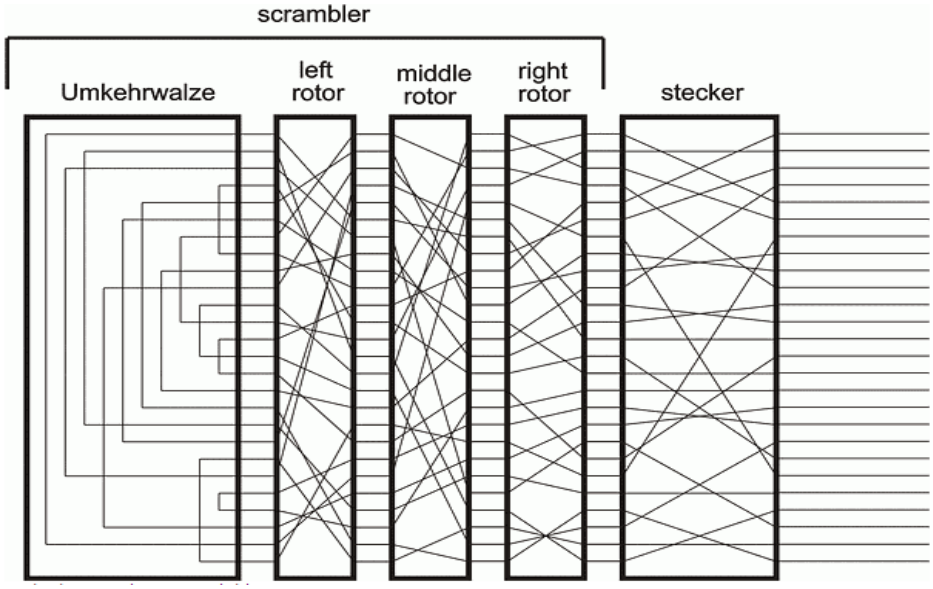


Figura 4. Nonsimple wire diagram (diagrama de alambre Enigma).
Fuente: (IEEE Global History Network., 2011)

Esta máquina para poder cifrar un texto en claro el operador pulsa la letra apropiada en el teclado lo que envía una pulsación eléctrica a través de la unidad modificadora central y llega al tablero, donde se ilumina la correspondiente letra de texto cifrado. El modificador define esencialmente un alfabeto cifrado y la maquina puede ser utilizada tanto para llevar a cabo una cifra de sustitución mono-alfabético simple o poli-alfabético (Véase la figura 4.)

Figura 5. Maquina Enigma.
Fuente: (IEEE Global History Network, 2011)

2.2. Criptografía.

La criptografía es una técnica o más bien un conjunto de técnicas que tratan sobre la seguridad de la información, por otro lado la criptografía es "el estudio de técnicas matemáticas relacionadas con aspectos de la seguridad de la información tales como la integridad, y autenticación de datos. La criptografía no es el único medio de proveer seguridad de la información, sino un conjunto de técnicas" (Menezes, Van Oorschot, & Vanstone, 1996, pág. 15).

Así mismo desde la perspectiva científica y técnica: (Aguirre, 1999)

> Rama inicial de las Matemáticas y en la actualidad de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar y/o proteger un mensaje o archivo por medio de un algoritmo, usando una o más claves. Esto da lugar a diferentes tipos de sistemas de cifra que permiten asegurar estos cuatro aspectos de la seguridad informática: la confidencialidad, la integridad, la disponibilidad y el no repudio de emisor y receptor. (Pág.39).

2.3 Criptoanálisis.

Criptoanálisis es la ciencia que logra descifra los secretos del textos en claro de quienes los protegen. La criptografía y el criptoanálisis son dos herramientas

fundamentales en el marco de la seguridad de la información lo cual la unión de estas dos ciencias dan paso a la criptología[2] en la era moderna.

También podemos definir como criptoanálisis: Al envió delicado de información si un atacante, sin tener algún conocimiento del par de claves de seguridad ya sea (c, f), puede leer el mensaje del texto en claro al crear criptogramas correspondientes en cierto intervalo de tiempo.

El criptoanálisis por medio de los criptosistemas permiten forzar la seguridad, realizando el uso de técnicas matemáticas basadas en conceptos de probabilidad, esta ciencia también atenta a la seguridad de los datos en las redes de la información.

Reducidamente vinculado con el ataque de texto en claro se puede denominar como ataque de palabra probable, si el atacante está trabajando con un texto en general en texto cifrado, podría tener poco conocimiento del contenido del texto en claro. No obstante si va tras una información específica, podría conocer parte del mismo. Tal como se muestra en la (Tabla 1.). Resume los diferentes mecanismos de ataques criptoanalíticos, basados en la cantidad de información que posee el criptoanálista.

[2]Criptología: Es el arte de cifrar y descifrar mediante cálculos matemáticos, aritméticos con el fin de ocultar información para que las personas que estudian este arte puedan descífralos.

Tabla 1. ***Tipos de ataques a mensajes cifrados.***

Tipo de ataque.	Información de criptoanálistas.
Sólo texto cifrado.	• Algoritmo de cifrado. • Texto cifrado que se va a decodificar.
Texto claro conocido.	• Algoritmo de cifrado. • Texto cifrado de cifrado. • Uno o más pares de texto claro-texto cifrado formados con la clave secreta.
Texto claro elegido.	• Algoritmo de cifrado. • Texto de cifrado que se va a decodificar • Mensaje de texto en claro elegido por el criptoanalista junto con su correspondiente texto cifrado generado con la clave secreta • Mensajes de texto en claro elegido por el cifrado generado con la clave secreta
Texto cifrado elegido	• Algoritmo de cifrado. • Texto cifrado que se va a decodificar. • Mensaje de texto claro elegido por el criptoanálista junto con su correspondiente texto claro descifrado generado con la clave secreta.
Texto elegido	• Algoritmo de cifrado. • Texto cifrado que se va a decodificar • Mensaje de texto claro elegido por el criptoanalista junto con su correspondiente texto cifrado generado con la clave secreta. • Texto cifrado intencionado elegido por el criptoanalista, junto con su correspondiente texto claro generado con la clave secreta.

Fuente: (Stallings, 2004, pág. 31)

La única forma que el atacante pueda cifrar la información es que el algoritmo que se ésta utilizado sea sumamente débil y no resista el ataque. Generalmente, un algoritmo es diseñado para resistir estos tipos de ataques de fuerza bruta sobre el texto en claro conocido.

Este tipo de esquemas de cifrado generalmente tiene que cumplir dos esquemas fundamentales el primero el tiempo necesario para romper el cifrado excede el tiempo de vida útil de la información, el segundo el coste de romper el cifrado excede el valor de la información.

El problema radica en la cantidad de esfuerzo que invierte el criptoanálista para descifrar la información. Ya que si no existe alguna debilidad matemática inherentes en el algoritmo, lo que se procede a realizar un ataque de fuerza bruta de esa forma se puede calcular la estimación del costo y tiempo que se empleara para descifrar empleando la fuerza bruta en dicho texto en claro.

El objetivo de la fuerza bruta implica realizar el muestreo cada una de las claves que se obtenga del texto en claro que se desea descifrar. Como referencia se debe de escoger el 50% de las claves aleatorias para conseguir descubrirlas. La (tabla 2.) permite tener una referencia del tiempo necesario para obtener las claves posibles para conseguir descifrarlas.

Tabla 2. ***Tiempo para la búsqueda exhaustiva de claves.***

Tamaño de clave(bits)	Número de claves alternativas	Tiempo necesario a 1 cifrado/µs	Tiempo necesario a 10^6cifrado/µs
32	$2^{32}=4.3x10^9$	2^{31}µs=35.8	2.15milisegundo
56	$2^{56}=7.2x10^6$	2^{55}µs=1.142	10.1 horas
128	$2^{128}=3.4x10^{38}$	2^{127}µs=$5.4x10^{24}$	$5.4x10^{18}$ años
168	$2^{166}=3.7x10^{50}$	2^{167}µs=$5.9x10^{35}$	$5.9x10^{30}$ años
26 caracteres (permutación)	$261=4x10^{26}$	$2x10^{26}$µs=$6.4x10^{12}$	$6.4x10^6$ años

Fuente: (Stallings, 2004, pág. 32).

2.4 Procesos de la criptografía.

2.4.1. Confidencialidad.

Es el mecanismo de protección de datos de la información o también llamada privacidad de la información, hace frente a su divulgación a entidades autorizadas, nadie puede leer los datos a excepción de las entidades autorizadas.

2.4.2. Integridad.

Es el mecanismo del contenido de la información que no permite que sea adulterado, borrada, contra todo tipo de acciones que atente a la integridad de la información que se desea transmitir o guardar.

2.4.3. Autentificación.

Este mecanismo se encarga de garantizar la autenticación de la información mediante las partes o entidades que se va a establecer la comunicación, con el fin de saber si el contenido de dicha información es legítima.

2.4.4. No repudio.

Este mecanismo permite que el emisor o recepto niegue él envió de un mensaje de esta forma cuando se envía un mensaje, el receptor puede comprobar que el supuesto emisor envié el mensaje, además de negar el hecho de haber sido el destinatario de una acción o hecho.

2.5 Fragmentos de un proceso criptología.

Como anteriormente aviamos mencionado que la criptología es el conjunto del criptoanálisis y la criptografía, por consiguiente esta ciencia permite enviar y recibir mensajes de textos en claro, con el fin de poder recibir esos mensajes tenemos los siguientes fragmentos de proceso que tiene la criptología.

- **Receptor**: Es aquel sujeto a quien es enviado el mensaje de texto en claro cifrado.
- **Emisor**: Es aquel sujeto que envía el mensaje de texto en claro encriptado.
- **Sujeto:** Es cualquier persona o cosa que envía, recibe el texto en claro ya sea cifrado o descifrado.
- **Adversario:** Es aquel sujeto que trata de interrumpir, forzar una transmisión o recepción de mensaje de texto en claro que tenga seguridad de esa forma hacer uso de ese mensaje. Dentro de este proceso existen dos tipos de adversarios los cuales son pasivos o activos.
  - ✓ **Adversario Pasivo**: Es aquel sujeto que intercepta la transmisión del texto en claro, más sin embargo la roba ni la modifica solo la lee para uso personal.

- ✓ **Adversario Activo**: Es aquel sujeto que intercepta la transmisión del texto en claro y la roba, modifica con el fin de obtener alguna ganancia ya sea económica o presumir sus habilidades como atacante.

- **Canal**: Es el medio en el cual se envía la información.
- **Canal Seguro**: Es aquel medio que no permite al atacante robar, modificar, algún texto en claro que sea transmitido por ese medio.
- **Canal Inseguro**: Es cualquier canal donde cualquier sujeto puede modificar, leer o borrar cualquier mensaje cifrado.

2.6. Principios de kerckhoffs.

En esta sección se menciona los principios de Kerckhoffs, mencionados en su artículo "La Cryptograhie Militaire" del "Journal des Sciences Militaires" (Kerckhoffs, 1883) En este artículo se menciona 6 requerimientos que un criptógrafo debe tener en cuenta para basar la seguridad de su criptoanálisis. Estos 6 requerimientos los tradujo de manera casi literal.

Menezes et al. (1996) afirma que los principios de Kerckhoffs son:

- El sistema debe ser, sino teóricamente irrompible como irrompible en la partica.
- El comprometer los detalles del sistema no debe disconvenir los correspondientes.
- La llave debe poder ser recordada sin notas y debe ser fácil de cambiarla.
- El criptograma debe poder ser transmitido por telegrama.

- El aparato de encriptación debe poderse portar y debe operarla una sola persona.
- El sistema debe ser fácil, no debe requerir el conocimiento de una larga lista de reglas ni notas mentales. (pág. 14)

El primer requisito nos dice que aunque se conozca un algoritmo. Éste no se puede ejecutar en números muy grandes en tiempo polinomial, sin embargo, si existen algoritmos para factorizar.

El segundo requisito habla de que no debemos basar la seguridad de un criptosistema en la suposición de que el adversario lo único que quiere hacer es encontrar la llave para poder descifrar varios criptogramas con la misma llave, o que quiere encontrar el mensaje asociado a un criptograma.

El tercer requerimiento es claro por ejemplo en el caso de los correos electrónicos, en los cuales se tiene acceso mediante una contraseña, el dueño de cada correo debe leer su correo sin ningún problema, y por ende debe de memorizar su contraseña.

El cuarto requerimiento hay que recordar que el texto original fue escrito en el año 1883 y por tanto se pide ser trasmitido por telegrama una actualización de este requerimiento seria. El criptosistema deben ser transmitido sin dificultad.

El quinto y sexto requerimiento, se enuncia quizá de manera un poco antigua, dos de los objetivos de la programación: la portabilidad y la legibilidad, respectivamente

2.7. Criptografía simétrica.

La criptografía simétrica o también conocida como clave privada es aquel mecanismo de seguridad que utiliza una misma clave para cifrar y descifrar mensajes de texto en claro. En este sentido, las dos partes que se comunican pueden establecer un muto acuerdo de la clave de seguridad que se va a usar. Es decir, que el transmisor y el receptor podrán enviar textos cifrados y a su vez descifrarlos en textos en claro.

La criptografía de cifrado convencional o de clave única era el único mecanismo más utilizado antes que se diera el desarrollo de un nuevo mecanismo de clave asimétrica o clave pública. No obstante, al inicio de los 80 sigue siendo unos de los mecanismos más utilizados en su proceso de cifrado.

Para la criptografía simétrica existen diferentes mecanismos de seguridad uno de estos mecanismo dé cifrado es DES (Data Encryption Standard), fue desarrollada en los Estados Unidos en 1977escogido con un estándar FIPS 46.3 (Revisar anexo).

Referente a la cita textual, (Bermejo & Tlatoani, 2012) señala:

> Desde entonces, el DES se ha revisado cada 5 años aproximadamente, hasta 1998, año en que fue dado de baja como estándar. Una de las razones por las que se dio de baja fue el gran incremento en velocidad de las PC’s, lo que hizo que pudiese romperse inclusive por fuerza bruta. La NIST. Empezó a trabajar en un sustituto al cual llamó AES (Advanced Encription Estándar)

En 1998, Electronic Frontier Foundation gano la competencia RSA, DES Challenge II-2, rompiendo el DES en menos de 3 días. La computadora de la EFF fue llamada DES cracker, la cual fue desarrollada con un presupuesto de $250.000US. Al siguiente año, Net construyó una red de 100.000 computadoras y con un DES cracker, lograron ganar el concurso RSA, DES Challenge III, rompiendo el DES en 22 horas 15 minutos. Se ha logrado romper el DES con un proyecto que costó aproximadamente $1´000.000 US en 3.5 horas. (pág. 13)

Así como este mecanismo de seguridad existe otro como es:

- TDES (triple Data encryption standard)

Más adelante explicaremos detalladamente el estos mecanismos de cifrado Triple DES.

2.7.1. DES (Data Encryption Standard).

El esquema de cifrado más extendido, se basa en el DES adptado en 1977 por el National Bureau of Standarts, ahora el NIST (National Institute of Standard and technology)[3]. DES es un algoritmo de cifra bloques de 64 bits, mediante permutación y sustitución usando la llave de 64 bits donde los

[3] La NIST fue Fundado en 1901, es una agencia federal no reguladora dentro del EE.UU. La misión de NIST es promover la innovación y la competitividad industrial EE.UU. avanzando ciencia de la medición, los estándares y la tecnología en formas que mejoren la seguridad económica y mejorar nuestra calidad de vida.

primeros 8 bits son de precedencia y los 56 bits restantes firmes; de esa forma se obtiene 64bits cifrado.

2.7.2 Cifrado tipo Feistel.

Definición: r es el número de rondas.

C=P= $\{0,1\}^{2t}$

K es el esparció de llaves.

Se puede observar en la siguiente figura como realiza el proceso de cifrado mediante la red de Fesitel.

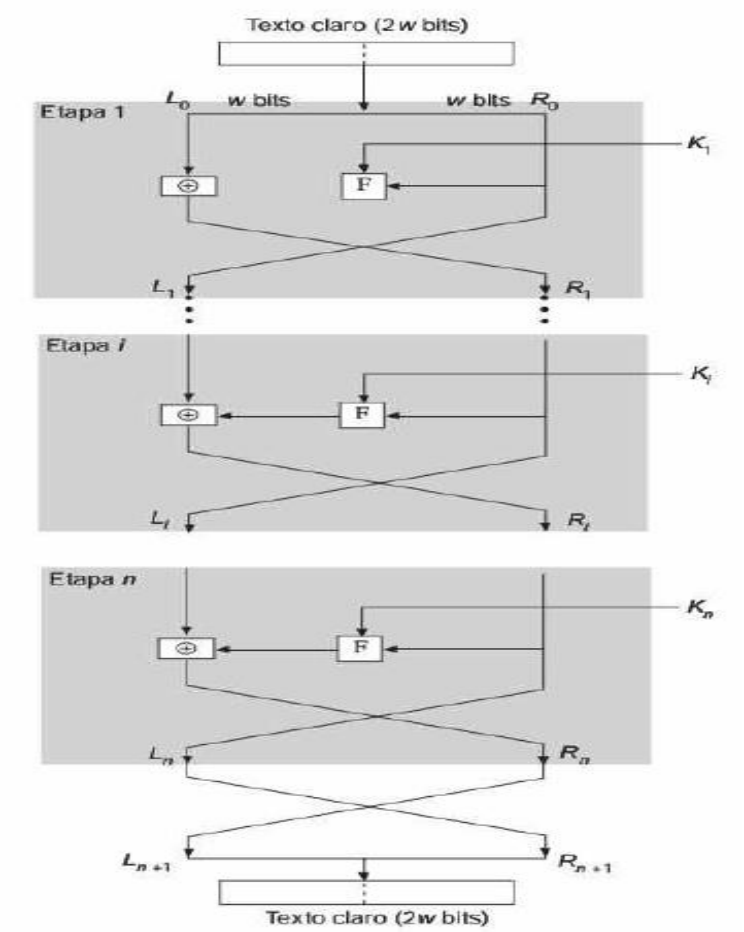


Figura 6. Red clásica de Fesitel.
Fuente: (Stallings, 2004, pág. 33)

2.7.3 Descripción del algoritmo.

El texto en claro tiene una longitud de 64 bits y la clave de 56 bits; No obstante se puede encontrar con una clave de mayor longitud en cual se debe de procesar en el bloque de 64bits. Para este proceso de descifrado DES se pueda realizar mediante red de Feistel (Véase la Figura 6). En la cual podemos entender que existen 16 procesos que generan 16 sub-claves partiendo de la clave original de 56 bits la cual servirá una para cada etapa de cifrado del texto en claro.

El proceso de descifrado del algoritmo de DES es prácticamente el mismo del cifrado, la condición es la siguiente: "usar el texto cifrado como entrada al algoritmo DES, pero las sub-claves K_1 se invierte el proceso. Es decir, en la primera etapa se usa K_{l6}, K_{l5} en la segunda, y así hasta K_1 en la 16^a y última". (Stallings, 2004, pág. 35).

2.7.4 Triple DES.

El triple DES a diferencia del DES tradicional requiere de una llave de 192 bits. Es decir, que tiene mayor longitud; esta clave se divide en 3 partes con la finalidad de tener 3 claves secundarias K_1 K_2 K_3 las cuales se hace uso para cifrar se tomar la clave K_1 y cifra el mensaje de texto en claro M con el DES. No obstante, ejerce una acción para descifrar utilizando la llave K_2 aplicando un algoritmo de cifrado en clave K_3, todo este proceso es análogo al proceso de cifrado. En la siguiente (Figura. 7). Podremos observa cómo es el funcionamiento del algoritmo de TRIPLE DES.

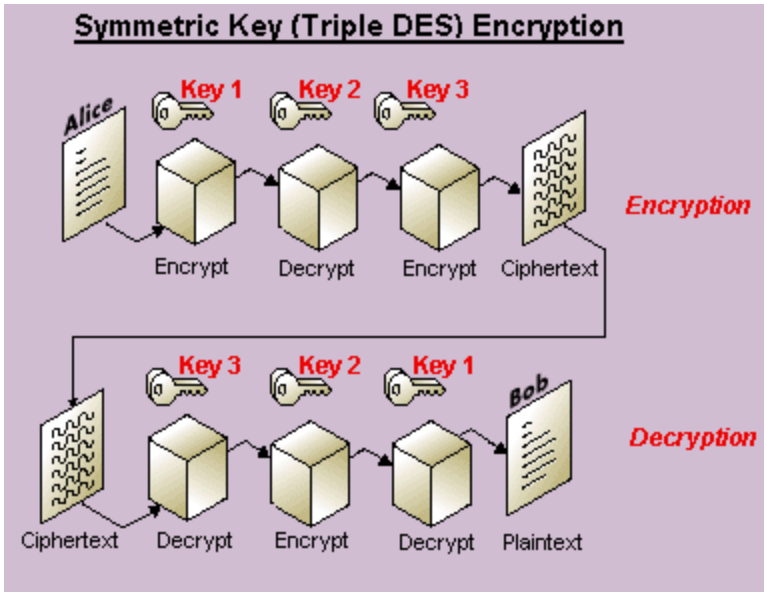


Figura 7. Funcionamiento del algoritmo Triple DES.
Fuente: (El chalé de Gaius Baltar, 2014)

2.7.5 AES.

En 1997 el NIST realizan una nueva propuesta de algoritmo de cifrado del siglo XXI, donde se realizan varias prueba y estándares de protección de datos; AES (Advanced Encryption Standard, Estándar de cifrado Avanzado).

El algoritmo AES cumple con las siguientes funciones:

- Es un algoritmo de dominio público.
- Es un algoritmo de cifrado simétrico por bloques su entrada debe de ser 128 bits.
- Las claves de cifrado podrían optar en 128 bits, 192 bits y 256 bits.

  El algoritmo de cifrado tendrá que implantado tanto en hardware como en software.

El algoritmo de AES fue promovido mediante un concurso que se dio a organizaciones, o instituciones que llevan a cabo el diseño e implementación de nuevos mecanismos de seguridad. En el año 2000 se elige al ganador del mejor

diseño tanto en flexibilidad, velocidad, eficiencia, sobre todo seguridad los ganadores de estos premios fueron dos belgas Joan Daemen y Vincent Rijimen; la publicación oficial de AES se dio bajo las normas FIPS Pub 197 en el año 2001. (Federal Information Processing Standars Publications, 2001).

> Este mecanismo de seguridad AES es el más utilizado en instituciones universitarias, bancarias, gubernamentales, ya que dicho mecanismo de seguridad es más robusto que los mecanismos anteriores expuestos como por ejemplo el algoritmo DES, y el TRIPLE DES.

Por esta razón, el algoritmo de AES es el más utilizado en la actualidad, el funcionamiento de este algoritmo de seguridad AES es el siguiente:

AES tiene una mayor longitud de su clave de seguridad tanto así que su bloque fijo tiene 128 bits con lo cual el tamaño de las llaves pueden llegar a ser de 128, 192, 256 bits. Todos estos cálculos se lo realizan en un estado finito determinado. AES trabaja en una raíz de 4x4 byte la cual utiliza una clave de seguridad de 128, 129 y 256 bits de longitud.

AES tiene una característica valiosa ya que su estructura no es una estructura basada den Feistel[4]. "AES procesa todo el bloque de datos en paralelo durante cada etapa, realizando sustituciones y permutaciones." (Stallings, 2004, pág. 39). En la siguiente figura se mostrara el proceso que realiza este algoritmo de AES para poder cifrar y descifrar textos en claro.

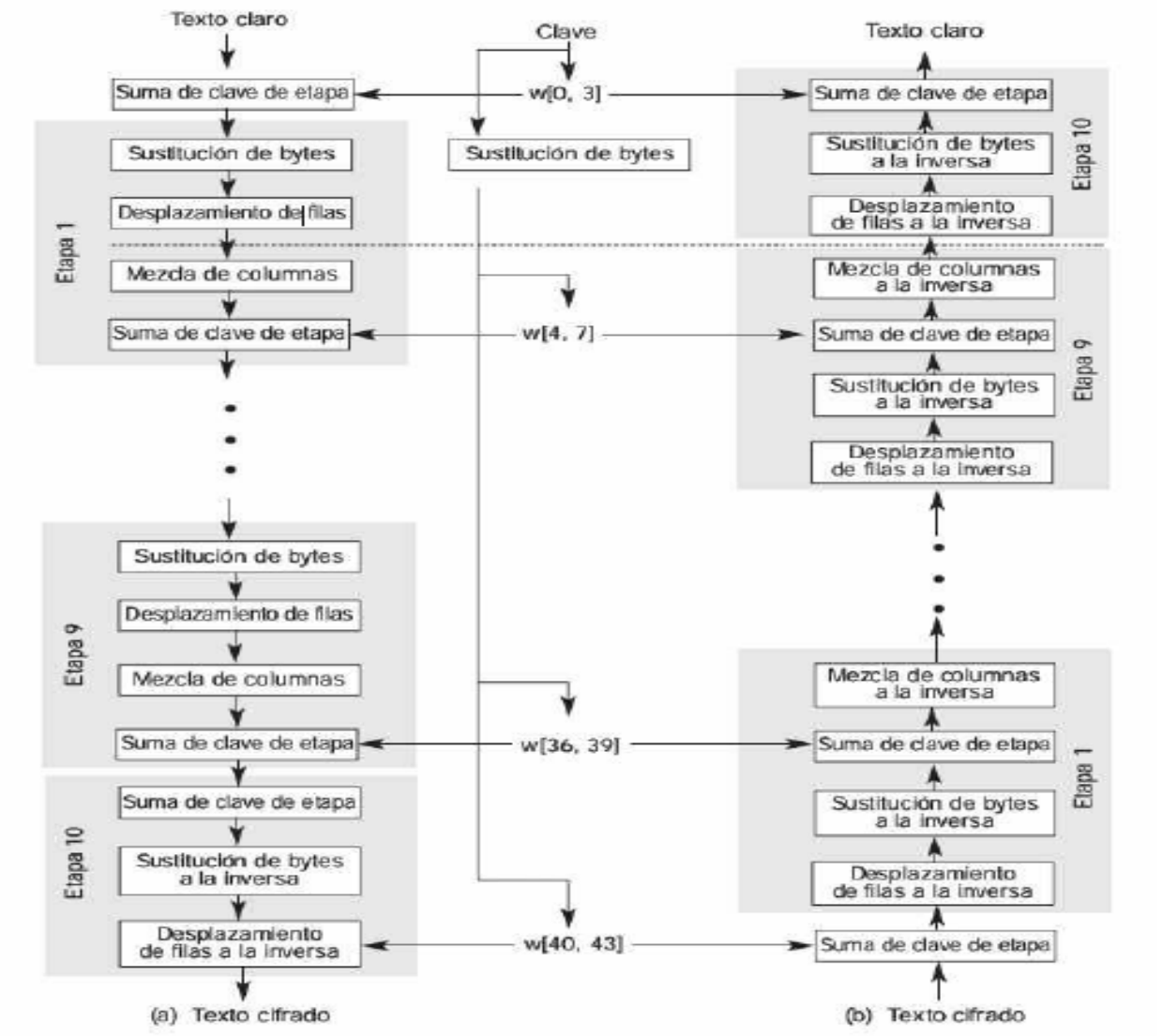


Figura 8. Cifrado y Descifrado de AES.
Fuente: (Stallings, 2004, pág. 40)

[4]Feistel siendo bloque de datos se usaba para modificarla otra mitad, y entonces se intercambiaban entre sí.

2.8 Criptografía asimétrica.

La criptografía asimétrica también llamada clave pública, es un mecanismo de cifrado donde las claves viene en pares. Es decir, donde se cifra el texto en claro, solo la otra persona puede descifrar el texto cifrado.

Pero no necesariamente, las claves son intercambiables, en el sentido de que si la clave A cifra un mensaje, entonces la clave B puede descifrarlo, y si la clave B cifra un mensaje de texto en claro, la clave A puede descifrarlo. No obstante, esta propiedad no es esencial para el cifrado asimétrico. Como ejemplo, podemos decir que si se compra un carro ya sea este nuevo o usado, el usuario que lo ésta adquiriendo tiene una llave adicional a la que el habitualmente la tiene como emergencia por si suscita algún inconveniente, y la primera llave será custodiada por el propietario.

La clave para el uso exitoso de cifrado asimétrico es tener un buen administrador de claves del sistema, el cual implemente varias infraestructura de clave pública. Sin esto, es difícil establecer la fiabilidad de claves públicas, o incluso para encontrar fallos dentro de dichas claves.

El beneficio de este mecanismo de seguridad consiste en la eliminación de la necesidad del envío de la clave de esta forma se apega a un sistema más robusto.

El la dificultad es su lentitud de ejecución, para resolver este inconveniente de cifrado se realizó la unión tanto de la clave pública como privada, de esta forma se da paso a los algoritmos de cifrado asimétrico como son los siguientes:

- RSA. (RIVEST-SHAMIR-ADELMAN).
- DSA. (DIGITAL SIGNATURE ALGORITHM) (Algoritmo de firma digital.).

Así como la clave simétrica, la clave pública consta con los siguientes componentes:

- **Texto en claro**: mensaje legible introducido en el algoritmo como entrada.
- **Algoritmo de cifrado:** Convierte un texto en claro a texto cifrado.
- **Clave pública y privada:** Es el par de claves que se utilizan para cifrar y descifrar dichos algoritmos siempre se proporcionan como entrada.
- **Texto cifrado:** Es aquel mensaje en claro que fue adulterado para no ser leído por otro usuario.
- **Algoritmo de descifrado:** Este algoritmo admite el texto cifrado y la clave proporcionada por el texto en claro.

En la siguiente imagen podemos ver como un texto en claro cifrado y autentificado.

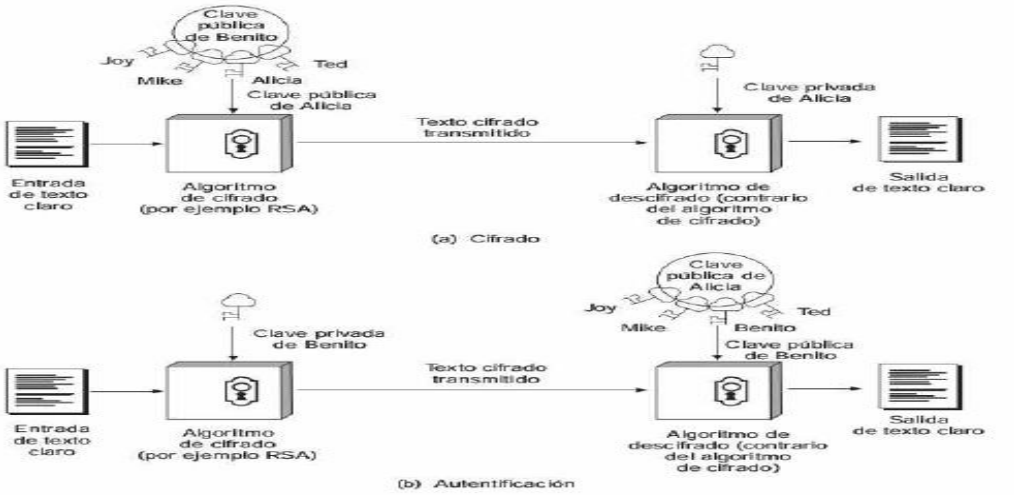


Figura 9. Criptografía De Clave Pública.
Fuente: (Stallings, 2004, pág. 73)

2.8.1 Firma digital.

Una firma digital es básicamente la forma de dar por validado un documento electrónico por ejemplo por medio de e-mail, bancas electrónicas, archivos de texto, etc.

Medina Alvarado & Marca Ludeña (2006) afirma que:

> La validación de identificación de muchos documentos legales, financieros y de otros tipos, se determina por la presencia o ausencia de una firma manuscrita autorizada. Por tanto es necesario que los sistemas computarizados reemplacen el transporte físico de papel y tinta, existen 3 puntos fundamentales.
>
> 1. El receptor pueda verificar la identidad del transmisor.
> 2. El transmisor no pueda repudiar después el contenido del mensaje en claro.
> 3. El receptor no haya podido generar el mensaje por sí mismo. (pág. 16)

Las firmas digitales van más allá de las versiones electrónicas de firmas tradicionales realizando mecanismos criptográficos para tener mayor robustez, flexibilidad, seguridad y validez jurídica.

2.8.1.1. Riesgos.

1. Si el proceso de firma digital no es segura los atacantes pueden crear firmas falsas o mal uso de firmas auténticas.

2. Si no se mantiene la documentación y certificación pertinente para las políticas y prácticas de la gestión de las claves podría resultar en firmas falsas.
3. Algunos proceso de firma digital pueden ser computacionalmente intensivas lo que frena los proceso de negocio y la limitación de su capacidad de escala a una mayor seguridad del documento que se ésta adquiriendo.

2.8.1.2 Beneficios.

- Efectuar firmas digitales robustas con soluciones de alta destitución adecuada para sus procesos más críticos.
- Emplear controles de firmas seguras cumpliendo las normas y estatutos correspondientes.
- Utilizar certificaciones de seguridad internacionales como FIPS 140-2.

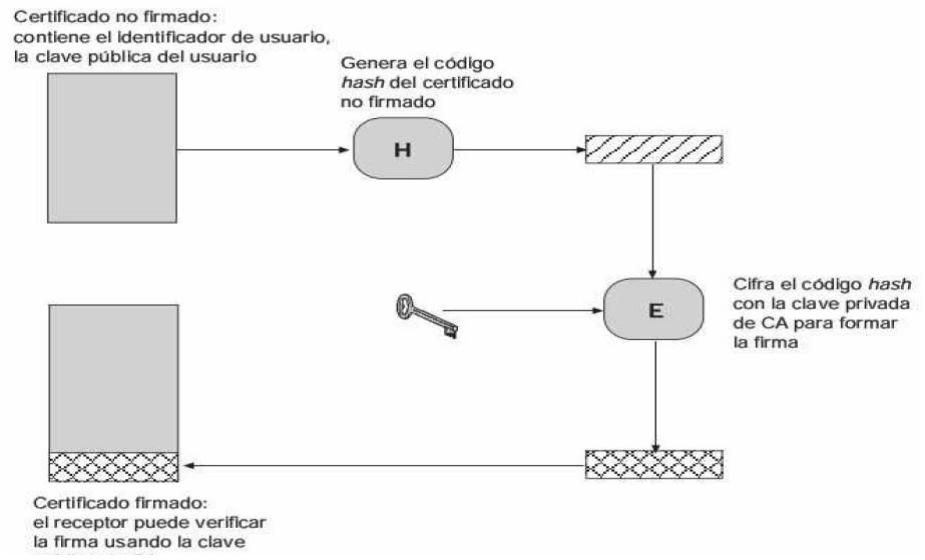


Figura 10. Uso De La Firma Digital Clave Pública.
Fuente*: *(Stallings, 2004, pág. 83)

2.8.2 Algoritmo de cifrado asimétrico.

2.8.2.1. Algoritmo de cifra asimétrica RSA.

Fue diseñado en 1977 por Ron Rivest, Adi Shamair, Len Adleman en el MIT[5], empezaron a discutir como diseñar un sistema de cifrado de llave pública que es sumamente práctico. Rivest acabó teniendo una idea la cual fue sometida a críticas de sus amigos era una cifra de clave pública, tanto para resguardar la información como para firmas digitales, basada en la dificultad de la factorización de números primos grades. Es decir, que el mecanismo de cifrado RSA su mayor ventaja es proporcionada por las propiedades de los números primos cuando se aplican en los problemas matemáticos basadas en la función módulo, emplea la función exponencial discreta para cifrar y descifrar, y cuya inversa, del logaritmo discreto, es muy difícil de calcular.

También podemos decir que para algún bloque de texto M y un bloque cifrado C, el cifrado y el descifrado son de la siguiente forma.

$$C=M^{e} \bmod n$$

$$M=C^{d} \bmod n = (M^{e})^{d} \bmod n = M^{ed} \bmod n$$

Por lo tanto, transmisor como el receptor deben de conocer las variables de n y e, y solo el receptor conoce el valor de d, este mecanismo de cifrado de clave pública cuya llave publica de CU= {e, n} y la llave privada CR= {d, n. Para que este algoritmo de cifrado público debe de cumplir con las siguientes condiciones. (Ver tabla 3).

[5] MIT: Instituto Tecnológico de Massachusetts.

- Que sea posible encontrar el valor de e, d, n talque M^{ed}= M mod n para todo M<n.
- Que sea relativamente fácil calcular M^e y C^d para todos los valores de M<n.
- Que sea imposible determinar d datos e y n.

Tabla 3. ***Algoritmo RSA.***

GENERACIÓN DE CLAVE	
Seleccionar ***p, q***	P y q primos, $p \neq q$
Calcular $n=p \times q$	
Seleccionar entre ***e***	***gcd***(0(n),e)=1; 1<e<0(n).
Calcular ***d***	De mod 0(n)=1
Clave pública ***C U***	***Ku***={e, n}
Clave privada ***C P***	***Kp***={d, n}
CIFRADO	
Texto claro	M< n
Texto cifrado	C= M^e(mod n)
DESCIFRADO	
Texto cifrado	C
Texto claro	M = C^d (mod n)

Fuente: (Stallings, 2004, pág. 76)

2.8.3. Otros algoritmos de clave asimétrica.

2.8.3.1 El algoritmo SHA-1(Secure hash algoritmo-1).

El algoritmo hash seguro (SHA) fue desarrollado por el NFST publicado 1993 como un estándar de seguridad de procesamiento de datos-(FIPS PUB 180); la versión mejoras que da paso en el año 1995 FIPS PUB 180-1 en 1995. (Ver a Anexo)

Este tipo de algoritmo produce una firma de 160 bits, a partir del bloque de 512 bits del texto en claro.

Este mecanismo es idéntico al MD5 (Message-Digest Algorithm 5) en español Algoritmo de resumen de mensaje 5, y se emparejan igual a éste, seguido de una secuencia de uno con sucesivos ceros como es necesario hasta completar 488 bits. Es decir que este algoritmo de seguridad emplea cinco registros de 32 bits en lugar de cuatro.

Tabla 4. ***Funciones HASH seguras*****.**

D5	*SHA-1*	*RIPEMD-160*
128 bits	***160 bits***	***160 bits***
512 bits	***512 bits***	***512 bits***
64(4 etapas de 16)	***80(4 etapas de 20)***	***160(5 etapas de 16)***
Finito	***2^{64}-1 bit***	***finito***
4	***4***	***5***
64	***4***	***9***

Fuente*:(autor del proyecto*)

CAPÍTULO III.

3.1 AUTENTICACIÓN Y SEGURIDAD DE LAS REDES DE DATOS.

3.1.1 Kerberos.

En la mitología griega, Kerberos (en griego Kepbepor; demonio de pozo), kerberos era el perro de Hades, un monstruo de tres cabezas con una cola de serpiente. Así, como kerberos resguarda la entrada, siempre vigilante del inframundo. Se puede decir, que en la seguridad de las redes de datos Kerberos resguarda la entrada de dichas redes: Autentificación, Operaciones, Recursos, Auditoria de las cabeceras.

Kerberos es un servicio que fue diseñado por el MIT para encontrar una solución de seguridad de los datos en las redes de telecomunicaciones o telemática. Es una herramienta de tipo administrativa la cual ofrece seguridad de datos y configuración adecuada de sus puertos tanto de entrada como de salida.

La seguridad e integridad de un sistema de datos ya sea este de instituciones académicas o gubernamentales es muy complicada de salvaguardar ya que son los principales centros de ataques de los ciber-delicuentres en la actualidad.

La protección de estos sistemas puede tener varios administradores para mantener el rastro de cuales están siendo ejecutados. No obstante, si kerberos

es utilizado en la base de datos, con cualquier contraseña no cifrada o kerberizado se encuentra en riesgo de ser vulnerable.

Autenicación: El protocolo de autenticación de kerberos permite identificar por los diferentes mecanismos de criptografía simétrica a los clientes que solicitan el servicio ante el servidor que los ofrece. Por esta razón, cada entidad en la red de datos, sea cliente o servidor comparten la clave secreta sea conocida por el usuario y kerberos.

Podremos observar en la siguiente tabla las abreviaturas más utilizadas.

Tabla 5. ***Tabla De Abreviaturas Utilizadas.***

C	**Cliente que solicita un servicio**
S	Servicio que ofrece dicho servicio
A	Servicio de autenticación
T	Servicio de tickets
K	Clave secreta del cliente
K	Clave secreta del servidor
K	Clave secreta del servidor de tickets
K	Clave de sesión entre el cliente y el servidor de tickets
K	Clave de sesión entre clientes y servidor

Fuente: (Rediris, 2002)

Login: Permite establecer un servicio al cliente "C" para darle acceso a la base de datos por medio de su usuario y clave. Kerberos utiliza ticket que permite la comunicación por medio del servidor de ticket TGS. (Véase la Figura 11.) De esta forma autentifica si el usuario que ésta solicitando dicho ingreso sea el correcto.

Tickets: Para obtener una clave de ingreso tiene que poder acceder al servidor de tickets TGS ya que es necesario realizar el registro de dicho tickets del usuario para ser autentificado por el servicio caso contrario dicho servido TGS no permitirá el acceso a la base de dato que desea acceder.

Petición de servicio: Una vez autentificado el tickets el cliente podrá estar preparado para solicitar el servicio por medio de una credencial que avale su autenticación.

Para este proceso se ilustra la siguiente (figura 11.)

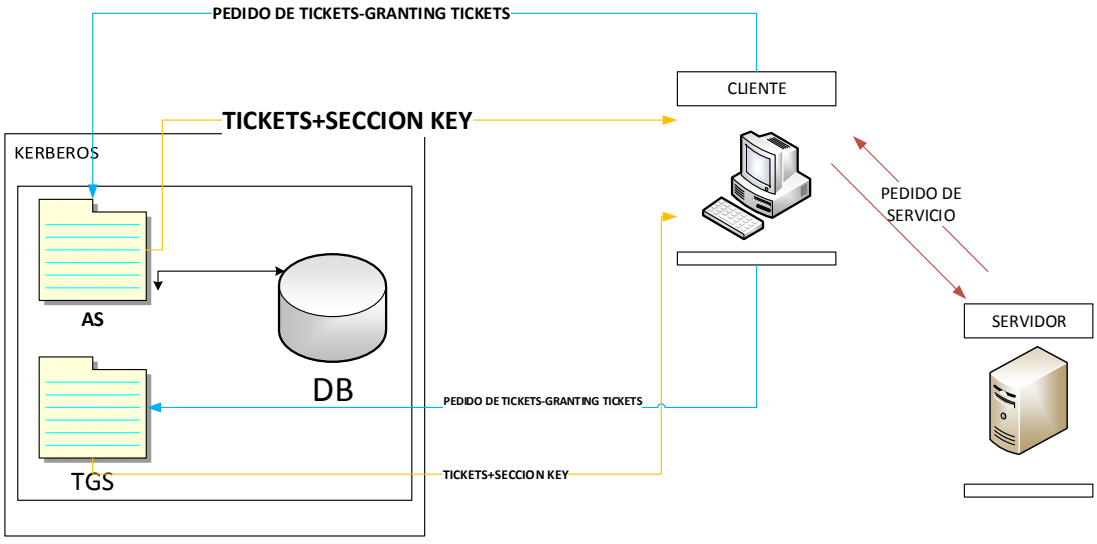


Figura 11. Esquema General De Kerberos.
Fuente: (Autor del proyecto)

3.2 Servicios de Autenticación X.509.

El estándar X.509 que está actualmente en vigencia de la recomendación ITU-T articulo E38895 que hace referencia X.500 la cual define un servicio de directorio. Donde permite saber por medio de la base de datos el estado actual del usuario y direcciones de la red que se encuentra conectada.

Stalling, (2004) afirma que:

> X.509 define un marco para la provisión de servicios de autentificación por parte del Directorio X.500 a sus usuarios. El directorio puede servir como depósito de certificados de clave pública. Cada certificado contiene la clave pública de un usuario y está firmado con la clave privada de una autoridad de certificación confiable. Además, X.509 define protocolos alternativos de autentificación basados en el uso de certificados de clave Pública. (pág. 112)

El X.509 se basa en el mecanismo de criptografía pública y firmas digitales, si tenemos en cuenta se explicó sobre los algoritmos que conforman la criptografía pública como es el caso RSA y para las firmas digitales se basa en la función HASH. (Véase la figura 12.)

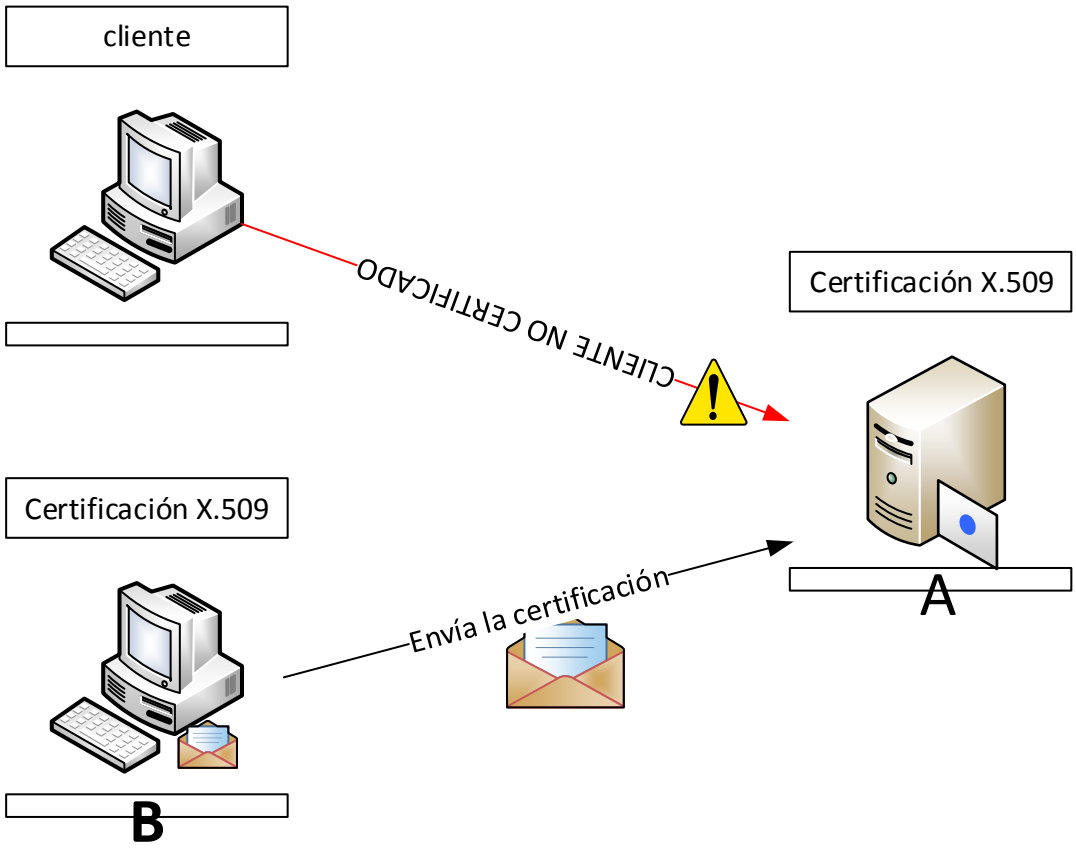


Figura 12. Figura estándar actual de verificación de certificado X.509.
Fuente:(Autor del proyecto).

3.2.1 Certificación.

El estándar x.509 hace referencia al intercambio de claves públicas. Estos certificados x.509 no solo contiene la clave del participante, también contiene información sobres su identidad y tipos de algoritmos que utiliza para la generación de claves y por último la valides misma del certificado de seguridad que el participante ésta operando.

Para RedIRIS - Servicios de certificación. (s. f.)

> Los certificados contienen una firma digital que garantiza la seguridad de sus contenidos, ya sea por la clave privada del mismo participante (**certificados autofirmados**), o por la clave privada de una tercera

parte (**certificado firmado por una C.A**). Este último C.A permite una seguridad más robusta de la certificación.

Datos referentes a un cliente que se encuentra certificando:

- CN: Nombre del cliente.
- E-MAIL: Dirección de correo electrónico.
- O: nombre de su organización
- OU: departamento de la organización
- L: localización de la organización
- SP: Provincia o estado de la organización
- C: País donde se encuentra la organización

Con estas referencias de acuerdo a la estándar de x.509 podemos tener una mejor perspectiva del participante o sujeto que está conectado a la base de datos del servidor con el fin de poder acceder. (Véase la figura 13.)

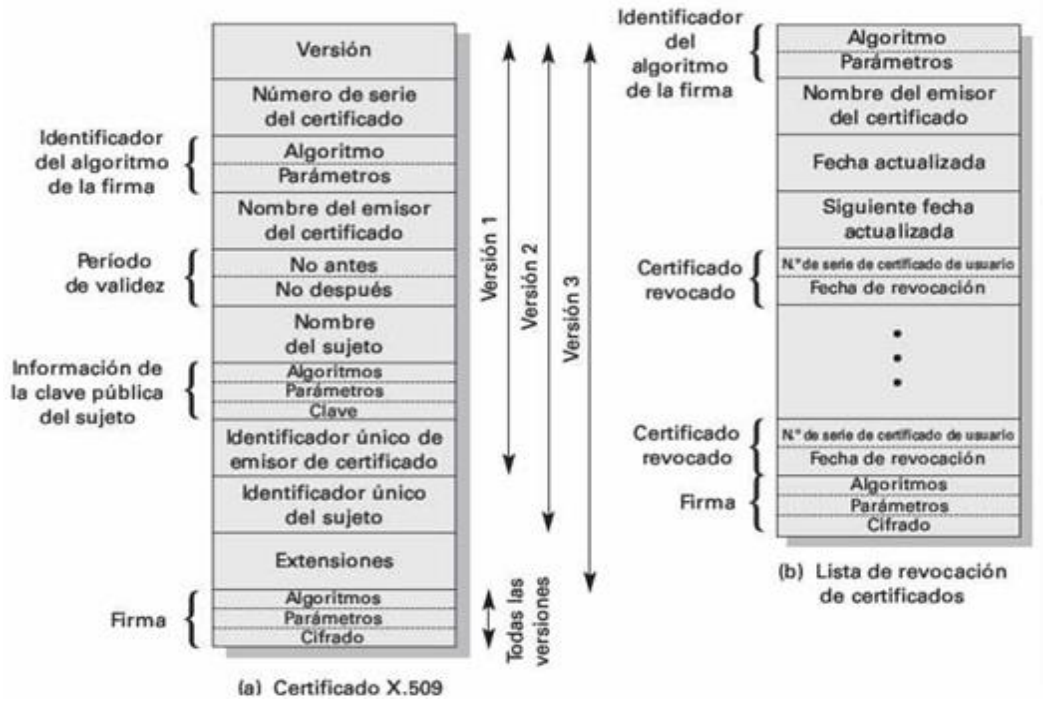


Figura 13. Figura Formato X.509.
Fuente: (Stallings, 2004, pág. 113)

3.3 Autoridades de certificación.

La autoridad de certificación es un ente regulador de las políticas establecida por las certificaciones y algoritmos que se utilizan mediante claves públicas y de firmas digitales. Podemos ver en el siguiente (Ver figura 14.) Cuando el cliente A envía al cliente B su certificación autorizada C.A y esté comprobara su valides de esa misma forma el cliente B enviara su certificado de autorización al cliente A para comprobar su valides.

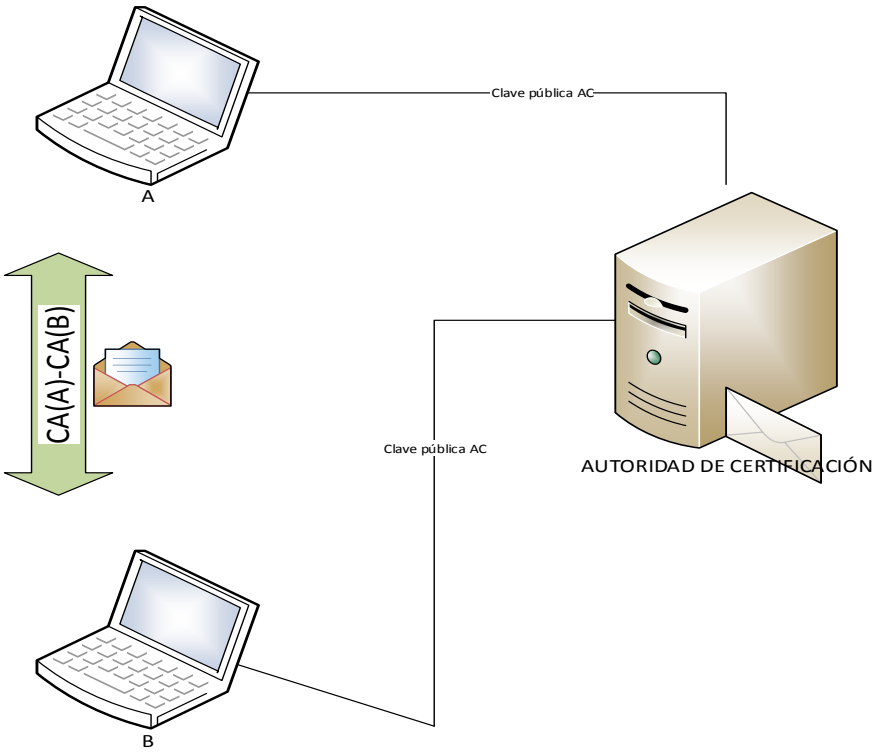


Figura 14. Figura De Autoridades De Certificación
Fuente:(autor del proyecto)

3.4 Seguridad en el correo electrónico.

3.4.1 Pretty good Privacy.

PGP (Pretty Good Privacy) o (Privacidad bastante buena) es un programa que desarrollado por Phil Zimmerman, basado en la criptografía pública, este mecanismo de seguridad tiene un fuerte establecimiento en las páginas web debido a su robustez y seguridad como tal. Para este sistema de seguridad existen dos versiones patentadas la americana e internacional.

PGP proporciona un servicio de autentificación de sus ficheros que se pueden utilizar en su correo electrónico en los siguientes puntos veremos el proceso que tiene este sistema de privacidad.

- Seleccionar como base los diferentes algoritmos criptográficos existentes.
- Integrar algoritmos en una aplicación de propósito, incluido el código fuente del sistema operativo y del procesador, y que se basa en un grupo reducido de comandos fáciles de usar.
- Ofrecer gratuitamente el paquete y sus documentos incluidos el código fuente, por medio del internet, por medio de anuncios o redes sociales.
- Llegar a un acuerdo con una compañía (Viacrypt, network associates) para proporcionar una versión comercial de PGP totalmente compatible y de bajo coste.

Para Stallings (2004) manifiesta el crecimiento del PGP en los siguientes puntos.

- ✓ Está disponible de forma gratuita en versiones que se ejecutan en una gran variedad de plataformas, incluidas Windows, UNIX, Macintosh y muchas más. Además, la versión comercial satisface a los usuarios que quieren un producto con asistencia del fabricante.

- ✓ Se basa en algoritmos que han sobrevivido a revisiones exhaustivas y se consideran sumamente seguros. Concretamente, el paquete incluye RSA, DSS y Diffie-Hellman para cifrado de clave pública; CAST-128, IDEA y 3DES para cifrado simétrico; y SHA-1 para codificación *hash*

- ✓ Tiene un amplio ámbito de aplicabilidad, desde corporaciones que desean seleccionar y reforzar un esquema normalizado para cifrar archivos y mensajes, hasta particulares que desean comunicarse de forma segura con usuarios de todo el mundo por medio de Internet y otras redes de computadores.

- ✓ No fue desarrollado por ninguna organización gubernamental o de estándares, ni lo controlan en la actualidad. Esto hace que PGP sea atractivo para aquellas personas que desconfían instintivamente del sistema.

- ✓ En la actualidad, PGP está propuesto como estándar de Internet (RFC 3156). Sin embargo, todavía lo rodea un aura de resistencia a lo establecido. (pág. 129) (Véase la figura15.)

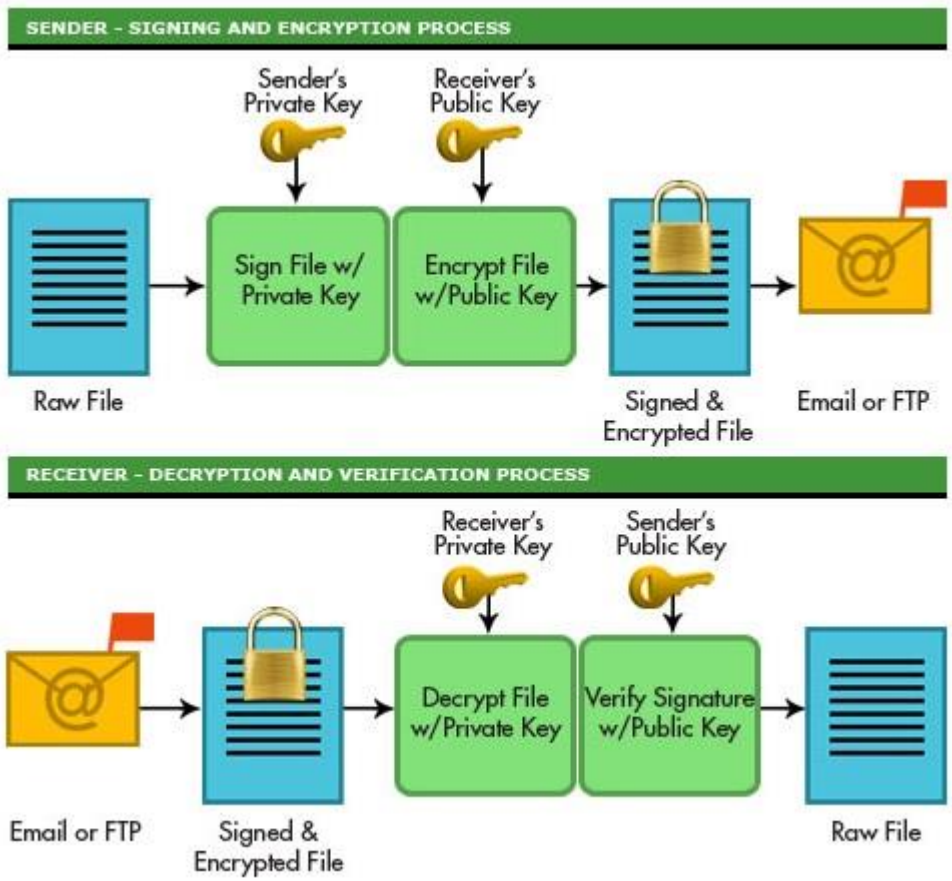


Figura 15. Pretty good Privacy
Fuente: (Go Anywhere, s.f.)

3.4.2 S/MIME.

S/MIME (Secure Multipurpose Intente Mail Extension) es un Sistema de seguridad mejorado para los formatos estándar de envió de correo electrónicos de internet, este sistema de seguridad está basado en criptografía pública con algoritmos como RSA Data Security. No obstante, PGP y SMIME son

especificaciones de la IETF[6]lo cual nos permite convertir estándares industriales para uso de negocios empresariales. SMIME se define como una serie de documentos específicamente en los RFC 2630, 2632, 2633.

3.4.3 Funcionalidad S/MIME.

El funcionamiento de S/MIME es muy equivalente al sistema de PGP (Véase la pág. 49) los dos nos brinda la posibilidad de cifrar un mensaje de texto en claro y/o firma. En los siguientes puntos veremos más detalladamente el funcionamiento del sistema S/MIME

- ✓ Datos empaquetados: Son aquellos datos que están cifrados para uno o más receptores
- ✓ Datos firmados: Lo datos firmados solo pueden ser vistos o leídos por un receptor con capacidad como los es el S/MIME.
- ✓ Datos firmados en claro: Los datos firmados en claro no permiten verificar la firma al receptor pero si puede ver el contenido del mensaje mediante el sistema S/MIME.
- ✓ Datos firmados y empaquetados: Este tipo de datos permiten saber que entidades están firmadas o cifradas, para que estos datos puedan ser firmados es necesario que estén en formato clear-signed (firma clara) y a su vez este permita su cifrado.

A continuación podremos observar en la siguiente tabla los algoritmos utilizados en el S/MIME.

[6]**IEFT**. Siglas en inglés de Internet Engineering Task Force correspondiente a Fuerza de Trabajo de Ingeniería de Internet. Comunidad internacional abierta de diseñadores de redes, operadores, vendedores e investigadores preocupados por la evolución de la arquitectura deInternet y el buen funcionamiento de Internet. Está abierta a cualquier persona interesada. La misión de la IETF está documentada en el RFC 3935

Tabla 6. ***Tabla Algoritmos criptográficos usados SMIME.***

Función	requisito
Crea un resumen de mensaje para crear un firma digital	Debe permitir SHA-1 El receptor DEBERÍA soportar MD5 para tener compatibilidad con versiones anteriores
Cifra un resumen de mensaje para crear una firma digital	Envía y recibir agentes DEBE permitir DDS Envía agentes DEBERÍA permitir cifrado RSA. Recibir agentes DEBERÍA permitir verificación de firma RSA con claves de 512bits a 1024 bits
Cifra de clave de sesión para su transmisión con el mensaje	Enviar y recibir agentes DEBE soportar diffie hellman. Enviar agente DEBERÍA permitir cifrado RSA con claves de 512 bits a 1024 bits Recibir agente DEBERÍA permitir cifrado RSA
Cifra el mensaje para su transmisión con la clave de sesión de un solo uso	Enviar agentes DEBERÍA permitir cifrado con triple DES y RC2/40 Recibir agentes DEBE permitir descifrado usando triple DES y DEBERÍA permitir descifrado con RC2/40.
DEBE: Definición absoluta de la especificación a realizar	DEBERÍA: Puede existir razones válidas como no válidas para sus características o funciones

Fuente: (Stallings, 2004, pág. 158).

3.5 Seguridad IP.

3.5.1 Introducción a la seguridad IP.

En 1994 el comité de arquitectura de internet IBA[7] en unos de sus informes manifiesta la seguridad de la arquitectura en el internet RFC1636 (ver anexo). El informe manifiesta una reforma global del sistema de seguridad en la red de datos de todo el mundo, puesto que han surgido ataques por ciber-delincuentes con el fin de salvaguardar el tráfico de información entre el usuario final utilizando mecanismos de cifrado y firmas de autentificación.

A medida que las direcciones IPv4 estaban al tope de su colisión, surgen una nueva generación de IP, actualmente se la conoce como IPv6 lo cual permite tener una mayor capacidad de flujo de datos y control de tráfico que se esté generando, así mismo una mayor velocidad con una nueva capacidad de IPsec.

3.5.2 Aplicaciones de IPsec.

IPsec permite asegurar las comunicaciones a través de una red LAN como WAN ya sea privada o pública de internet a continuación mostraremos puntos específicos del uso IPsec:

- ✓ Conexión segura a través de internet: Una empresa puede implementar una red virtual privada y segura a través de internet ya sea esta LAN o WAN lo cual permite que dicha empresa poderse conectar a una sola red y no generar

[7] IAB: internet architecture boad)

varios puntos de conexión privados, lo cual realizan una demanda de costo y gestión de la red mediante su tráfico.

- ✓ Acceso remoto seguro a través del internet: Permite al cliente poderse conectar de forma remota a cualquier ordenador red de una manera segura, con tan solo pedirle la clave de acceso y usuario, de esta forma reduce tiempo y costo de producción.
- ✓ Establecimiento de conexión de extranet e intranet: IPsec es utilizada para realizar comunicaciones con otras empresas que sean seguras. Garantizando su autentificación y confidencialidad para proporcionar el intercambio de claves.

3.5.3 Beneficios De IPsec.

MARK97 (citado por Stallings2004) hace referencia a los siguientes puntos como beneficios de la IPsec

- ✓ Cuando IPSec se implementa en un cortafuego o un router, proporciona una gran seguridad que se puede aplicar a todo el tráfico que lo cruza. El tráfico en una compañía o grupo de trabajo no provoca costes adicionales de procesamiento relativo a la seguridad.

- ✓ IPSec es seguro en un cortafuegos si se obliga a que todo el tráfico que proviene del exterior use IP, y el cortafuegos es el único medio de entrada desde Internet a la organización.

- ✓ IPSec está por debajo de la capa de transporte (TCP, UDP) y, por ello, es transparente a las aplicaciones. No es necesario cambiar el software en el sistema de un usuario o de un servidor cuando IPSec se implementa en los cortafuegos o el router. Incluso si IPSec se implementa en sistemas finales, el software de nivel superior, incluyendo aplicaciones y no se ve afectado.

- ✓ IPSec puede ser transparente a usuarios finales. No es necesario entrenar a los usuarios para la utilización de mecanismos de seguridad, ni suministrar material relativo al uso de claves por cada usuario, ni inhabilitar dicho material cuando los usuarios abandonan la organización.

- ✓ IPSec puede proporcionar seguridad a usuarios individuales sí es necesario, lo cual es útil para trabajadores externos y para establecer una subred virtual segura en una organización para las aplicaciones confidenciales. (pág. 180) (Véase la figura.16.)

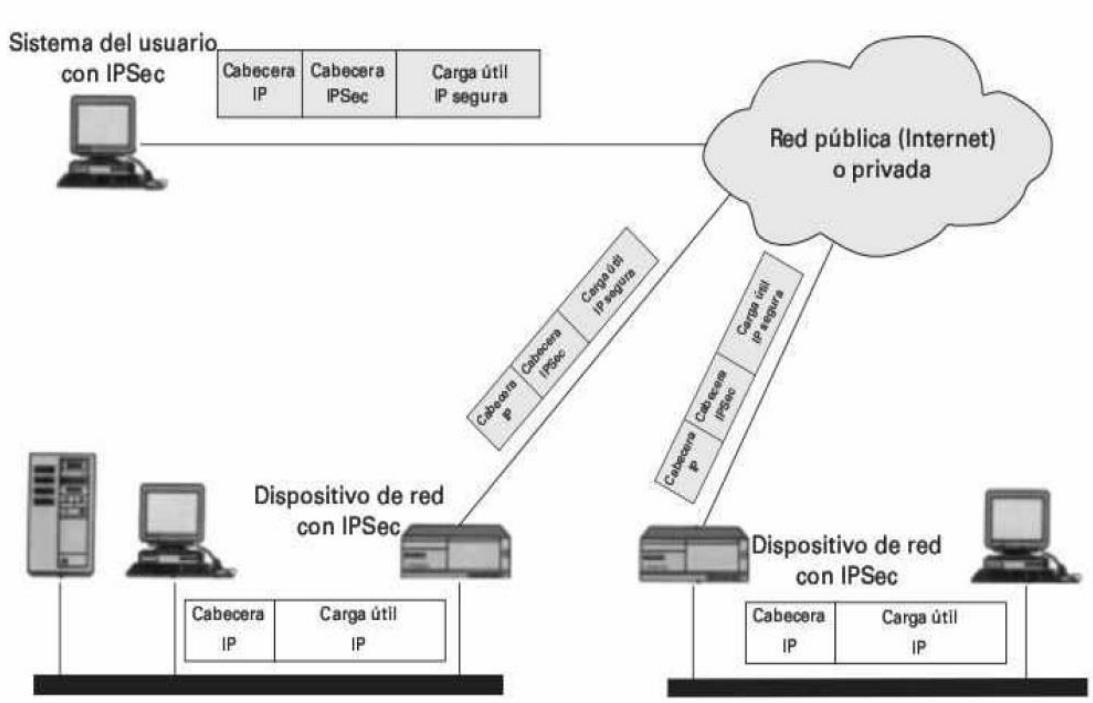


Figura 16. Entorno De La Seguridad IP.
Fuente: (Stallings, 2004, pág. 180)

3.5.4 Aplicaciones de enrutamiento.

A medida que la tecnología va evolucionando las distintas configuraciones de enrutamiento van de la mano para dar soporte a clientes finales y proteger sus datos. IPsec desempeña una función fundamental en la arquitectura de enrutamiento que se necesita para las comunicaciones de las redes. Dentro de este proceso de enrutamiento la IPsec pretende realizar una conexión de router a router autorizados, con el fin de anunciar cuando se encuentra un router vecino y constatar que esté autorizado. No obstante, se envía un mensaje redirigido al router para prevenir que el paquete inicial sea el correcto, de esa formar no se falsifica dichos paquetes.

3.5.5 Arquitectura de seguridad IP.

Para explicar esta arquitectura debemos basarnos en arquitecturas anteriores RFC 2401, RFC 2402, RFC 2406, RFC 2408 (ver anexo). La arquitectura RFC 2401 nos permite por medio de un diagrama de flujo 7 grupos importantes dentro de su jerarquía. Ver el siguiente diagrama de flujo (figura 17.)

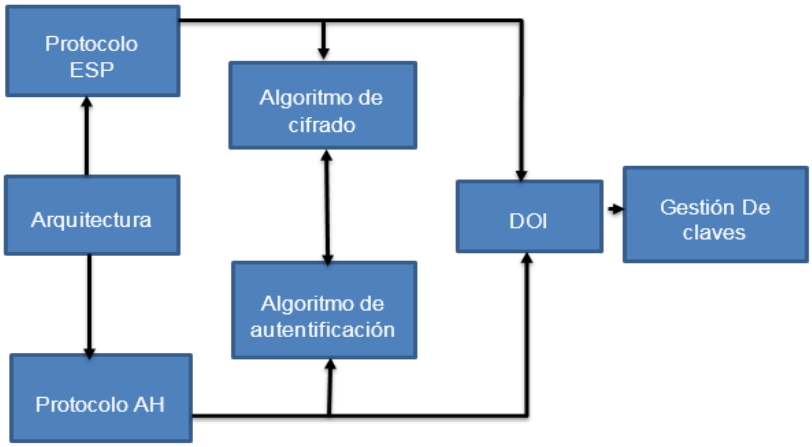


Figura 17. Diagrama Arquitectura de Flujo
Fuente:(Autor)

- ✓ **Arquitectura:** Asigna mecanismos de seguridad conforme a la tecnología IPsec.
- ✓ **Encabezado de carga de seguridad ESP**: resguarda el formato del paquete y aspectos generales de cifrado, de manera opcional para su debida autentificación.
- ✓ **Cabecera de autentificación AH**: resguarda la valides y autentificación de los paquetes.
- ✓ **Algoritmo cifrado**: Es un conjunto de documentos con diferentes algoritmos de cifrados para ESP.
- ✓ **Algoritmo de autentificación**: Es un conjunto de documentos con distintos algoritmos de cifrado para la autentificación de AH y ESP.

- ✓ **Gestión de claves:** Documentos que describen una gestión de claves cifradas.
- ✓ **Dominio de interpretación DOI**: Permite acoger los algoritmos de cifrado para verificación de su valides y autentificación así el tiempo de vida útil

3.5.5.1 Modo transporte de modo túnel.

En modo transporte, nos ayuda a enviar los paquete IP de forma cifrada y/o autenticada. Dicho enrutamiento permanece intacto, ya que no se modifica ni se cifra la cabecera IP; sin embargo, cuando se utiliza la cabecera de autenticación (AH), las direcciones IP no pueden ser traducidas. No obstante, no validaría la función hash. Las dos capas de transporte y aplicación están siempre aseguradas por un hash, de tal forma que no sean adulteradas. El propósito del modo de transporte es dar una comunicación segura punto a punto, entre dos hosts y sobre un canal inseguro.

3.5.6 Cabecera de autentificación.

La cabecera de autentificación permite un transporte para la integridad de datos y la valides de los paquetes IP. Lo cual nos permite tener la seguridad que no se producirá alguna modificación en el contenido del paquete durante la transmisión. Una de las características fundamentales es la autentificación que se realiza al sistema final de envió al momento que filtre el tráfico de información. Hoy en día en internet el algoritmo de AH permite proteger contra los ataques de fuerza bruta.

En la siguiente (figura 18). Vemos la estructura de la cabecera de autentificación.

Figura 18. Cabecera De Autentificación Ipsec.
Fuente: (Stallings, 2004, pág. 188)

- **Cabecera siguiente 8bits:** identifica la cabecera que antes de ésta.
- **Longitud de carga útil 8bits:** longitud de la cabecera de autentificación en palabras de 32 bits menos 2 bits.
- **Reservado 16 bits:** para Uso posterior.
- **Índice de parámetros de seguridad 32bis**: identificar la entidad de seguridad.
- **Numero de secuencia 32bits:** Es un contador que se incrementa monótonamente y se trata después
- **Datos de autentificación (variable):** Un campo de longitud variable depende de números enteros para los paquetes de 32 bits.

3.5.7 Encapsulamiento de la carga útil de seguridad.

El encapsulamiento de carga útil de seguridad proporciona servicio de envíos de paquetes y confidencialidad limitada del flujo de tráfico. En este mecanismo de encapsulamiento de carga útil encontramos los algoritmos ya antes mencionados como son AH y ESP.

Para el sistema de encapsulado ESP es un poco más complicado ya que rodea la carga útil, ESP incluye cabecera y campos para dar mantenimiento a la encriptación y a una autentificación opcional.

A diferencias del algoritmo AH hay una cabecera antes de cada carga útil, lo cual permite que el algoritmo de ESP rodee la carga útil para su protección, en la siguiente figura podemos observar como es el funciona miento del algoritmo ESP. (Véase la Figura 19.)

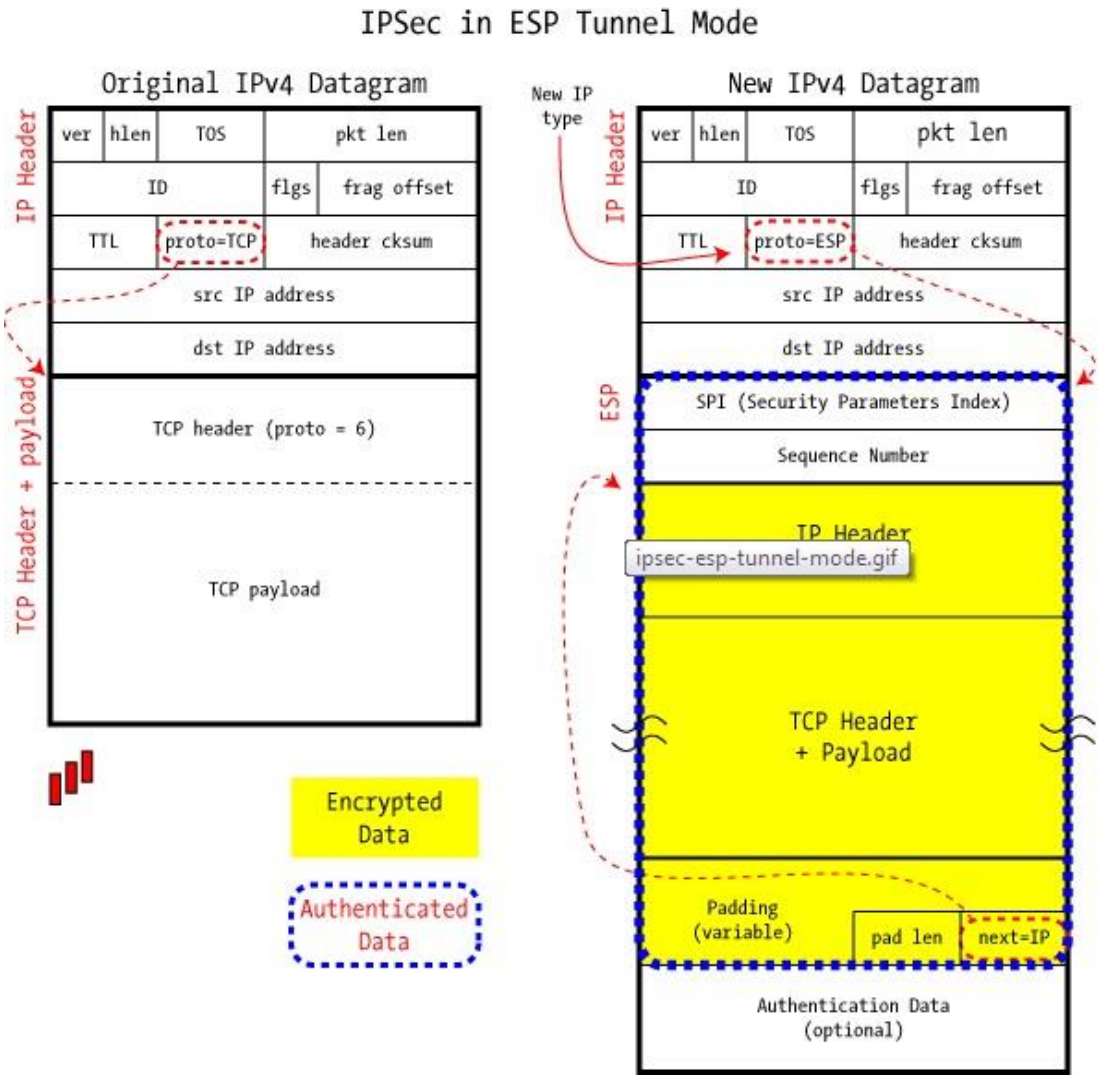


Figura 19. Figura sistemas ESP encapsulamiento.
Fuente: (Universidad Politecnica de Madrid, s.f.)

3.5.7.1 Autentificación más confidencialidad.

La autentificación de un cifrado se puede transportar con mayor confidencialidad en el interior de un paquete IP. Es decir, que dicha confidencialidad y autentificación se encuentra entre dichos terminales que transmiten la información de manera rápida y segura.

3.5.7.2 Combinación básica de asociaciones de seguridad.

Para los proceso de transmisión de datos dentro de la red podemos encontrar diferentes combinaciones que permiten el manejo de asociaciones de seguridad con el fin de que los terminales soporten IPsec en conjunto con *firewall, router,* en la siguiente figura podremos observar los distintos escenarios en los cuales se dan a conocer las combinaciones de seguridad.

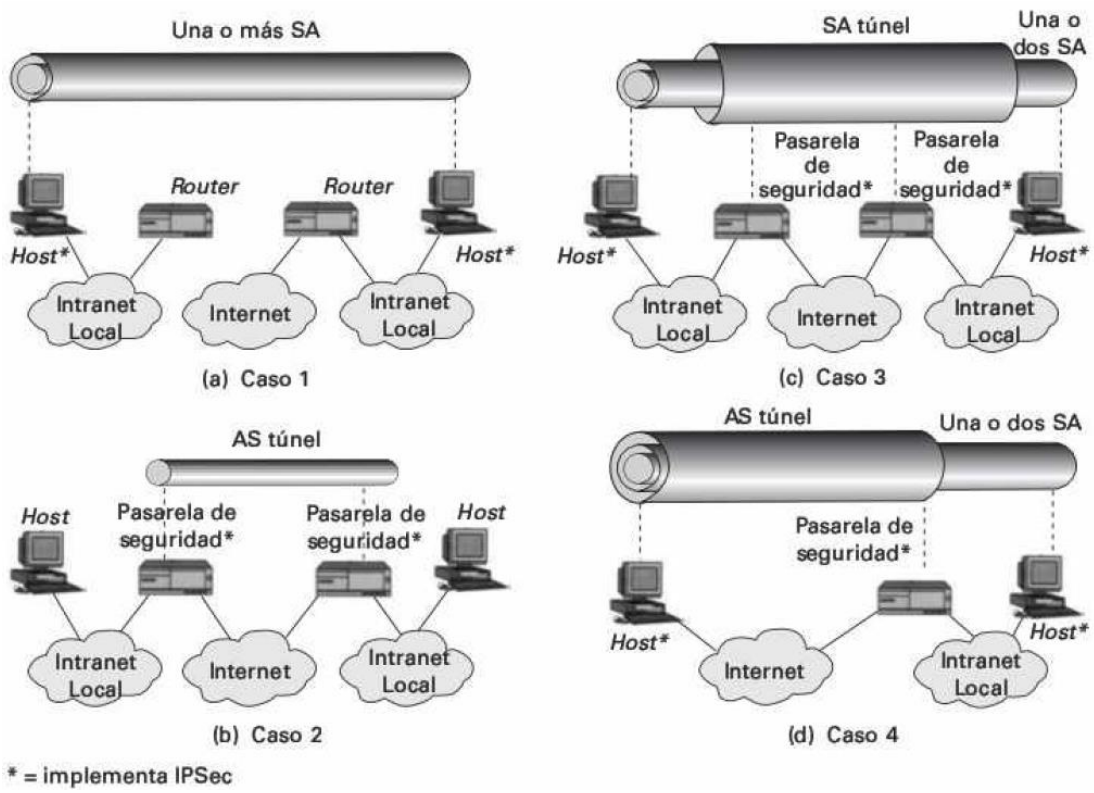


Figura 20. Combinación Básica De Asociaciones De Seguridad.
Fuente: (Stallings, 2004, pág. 200)

Caso 1: El *Host*(A) que se encuentra a su izquierda* envía un paquete por el túnel donde se encuentran una o más SA (asociaciones de seguridad), él envió de estos paquetes es con el fin compartir las claves secretas apropiadas al *host*(B) que se*

encuentra a nuestra derecha, cabe recalcar que estos host implementan IPsec en cada paquete transmitido.

Caso 2: El este caso podemos tener en cuenta que los paquetes que se están transmitiendo el *host (A)* al *host (B)* no implementa IPsec lo cual no da a conocer que esta rede es virtual.

Caso 3: Este caso nos da una combinación del caso 1 y 2 donde el túnel proporciona mayor autentificación y confidencialidad de los paquetes IP los cuales no pueden ser atacados.

Caso 4: Permite que los host se conecten a los cortafuegos para llegar al servidor lo cual nos permite utilizar el host local con host remoto.

3.6 Seguridad Web.

En esta sección nos enfocaremos en temas puntuales sobres la evolución que obtenido la seguridad en la redes de telecomunicaciones, informática. Con la finalidad proveer ítems a discutir sobre los requisitos generales para la seguridad en la web. De tal forma, conocer los esquemas de seguridad como por ejemplo SSL/TLS y SET.

3 6.1 Consideraciones sobre seguridad en la web.

La *World Wide Web* es un esquemas que permite interactuar al cliente con el servidor lo cual se ejecuta en internet y en la interfaces TCP/IP. Considerando que la seguridad en la web hoy en día es uno de los factores más importantes, en la siguiente lista detallaremos los ataques más habituales que sufre la seguridad web.

Ataque Pasivo: Este proceso de ataque analiza el trafico red e intentar conocer la información cifrada, este tipo de proceso es uno de los más difíciles de detectar ya que no podemos saber quién o quienes está fisgoneando la red de transmisión de datos.

Ataque Activo: Este proceso de ataque es el que mayor alcance de penetración hay en los sistemas de seguridad, ya que por medio de estos ataque pretende encontrar fisuras donde permitan la manipulación de los usurarios o servidores. No obstante, estos ataque informáticos son camuflados para persuadir la protección de los servidores que almacenan las claves secretas de los usuarios suscritos. Así mismo, dentro de los ataques activos encontramos a los criptoanálistas los cuales pretenden forzar las claves cifradas y convertirlas en texto en claro.

Ataque de Denegación de servicio: Este tipo de proceso manipula la transmisión de datos enviados por un túnel donde se genera el tráfico de información por lo cual este ataque envía información basura en vez de la información enviada originalmente.

3.6.2 Mecanismos para la seguridad del tráfico en la web.

Hay varios mecanismos que proporcionan la seguridad del tráfico de la web, dentro de este proceso podremos observar que dichos mecanismo de seguridad se encuentran dentro de la pila de protocolos TCP/IP como por ejemplo SSL/TLS y SET a continuación hablaremos brevemente de cada uno de ellos.

3.6.3 SSL (secure socket layer) capa de conexión segura.

Es un protocolo criptográfico que emplea conexiones seguras entre el usuario y el servidor, el protocolo SSL utiliza certificados X.509 el cual es una certificación digital. La función de este protocolo permite una negociación entre usuario y servidor lo cual valida que la conexión entre ambas partes sea segura. No obstante, se obtiene una llave de seguridad preestablecida, para cifrar y descifrar todo lo que se envía hasta que la conexión se cierre.

3.6.4 Arquitectura SSL.

Este protocolo de seguridad está compuesto por dos capas o niveles OSI.

SSL record protocolo: El record protocolo es utilizado para encapsular aquellos protocolos de nivel superior o corporativos.

SSL handshake protocol: Establece la conexión entre el usuario y servido.

SSL change Cipher spec Protocol: Período de recordatorio de los parámetros de cifrado a usar

SSL Alert Protocol: Alerta mensajes de erros que producen en el proceso de validación

HTTP: (Hypertext transfer Protocol) en español Protocolo de transferencia de Hipertexto, protocolo de transacción de la World Wide Web.

TCP: (Transmission Control Protocol) en español Protocolo de transmisión de información. Permite colocar los datagramas que son enviados por el protocolo IP.

IP: (Internet Protocol) en español Protocolo de internet, comunicación de datos dentro de una red. (Véase la figura 21.) Arquitectura el protocolo SSL.

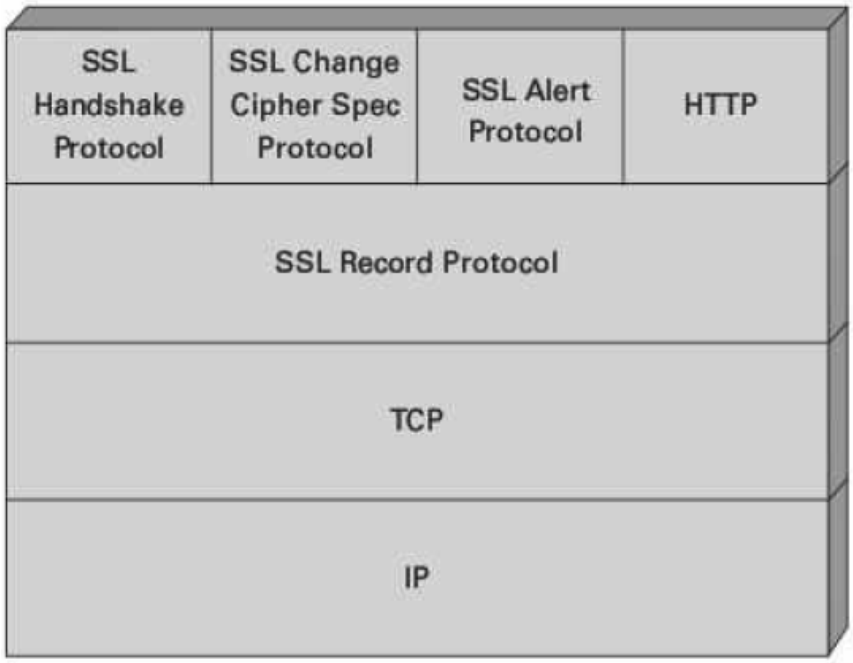


Figura 21. Arquitectura Protocolo SSL.
Fuente: (Stallings, 2004, pág. 228)

3.6.5 TLS (transport layer security).

Este protocolo de seguridad de capa de transporte es el sucesor del SSL cuyo objetivo es una versión estándar de internet (RFC.2246) (ver anexo).

3.6.6 SET (Secure electronic transaction).

Este protocolo está diseñado para la seguridad de transacciones de cuentas bancarias, pagos por tarjetas de crédito. De tal forma, que permite ayudar al protocolo de SSL cuando se encuentra con alguna grita de infiltración, podemos decir que SET cubre los fallos de seguridad que tiene SSL.

3.7 Seguridad de los sistemas.

3.7.1 Intrusos.

Para la seguridad de un sistema informático es imposible no estar expuesto a un ataque por medio de los intrusos ya sea estos los tan denominados hackers o crackers a medida que las nuevas redes de datos van evolucionando es importante tener en cuenta y sobre todo preguntarnos si realmente nos encontramos seguros para Anderson (1980) en uno de sus postulaciones identifica tres clases de intrusos:

- Suplantador: un individuo que no está autorizado a usar el computador y que penetra en un sistemas de control de acceso para explotar una legítima entrada de usuario.
- Usuario fraudulento: un usuario legítimo que accede a datos, programas o recursos a los que no está autorizado, o que está autorizado pero hace mal uso de sus privilegios.
- Usuario clandestino: un individuo que está a cargo del control de supervisión del sistema y utiliza este control para evadir la auditoria y el control de acceso o para suprimir la recopilación de datos auditados.

3.7.2 Técnica de intrusión.

El objetivo de los intrusos es poder penetrar a un sistema o realizar métricas para poder des quebrantar y acceder a dicha información. En la mayoría de los caso, esta información se encuentra cifrada, donde el usuario mantiene la clave y privilegios legítimos. Normalmente un sistema debe mantener un vínculo que

asocie la contraseña con el usuario, en los siguientes puntos detallaremos el proceso de intrusión:

- Cifrado unidireccional: es un sistema que cifra un texto en claro en una sola dirección.
- Control de acceso: Es una contraseña que se encuentra limitada en muy pocas cuentas.

3.7.3 La detección de intrusos.

Para la detección de intrusos no hay hasta el momento un programa que sea lo suficientemente bueno ya que en algún momento este programa será adulterado o manipulado.

En un segundo plano la defensa del sistema contra intrusos ha sigo centro de grandes investigaciones en los últimos años, para esto podemos mencionar los siguientes puntos.

1. Si se detecta un intruso en el interior de un sistema con bastante rapidez, puede ser detectado y expulsado para que no pueda extraer alguna información de la base de datos que estar queriendo manipular.
2. Un sistema de detección efectivo puede servir como elemento convincente para prevenir la intrusión.
3. La detección de dichos intrusos en un sistema permite obtener datos de técnicas de intrusión que se puede usar para reforzar la seguridad.

En la siguiente figura se detalla cómo es el comportamiento del intruso y usuario autorizado. (Véase la figura 22).

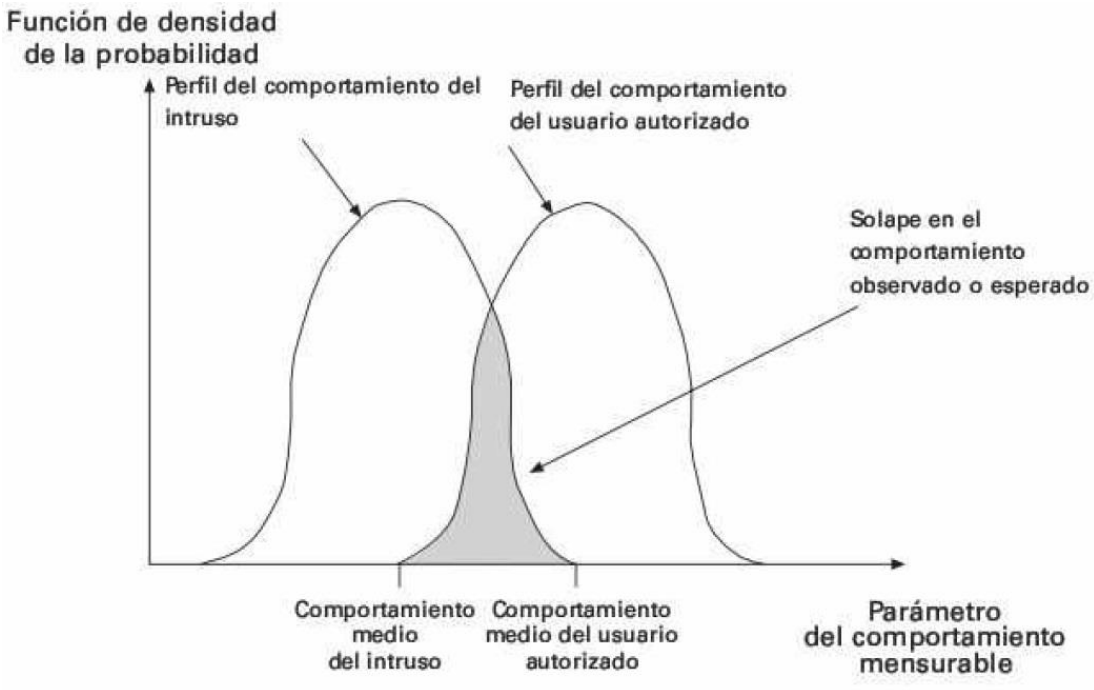


Figura 22. Comparación de intrusos y usuarios autorizados.
Fuente: (Stallings, 2004, pág. 311)

Para Porras (1992) identifica los siguientes tipos de instrucción.

1.- Detección de estadística de anomalías: implica la recopilación de datos relacionados con el comportamiento de los usuarios legítimos en un período de tiempo. Las pruebas estadísticas se aplican a comportamientos observados para determinar con un alto grado de fiabilidad si ese comportamiento no es el de un usuario legítimo.

a) Detección de umbrales: este enfoque trae consigo definir los umbrales, independientes del usuario, para la frecuencia en que se producen distintos acontecimientos.

b) Basado en perfiles: se desarrolla un perfil de la actividad de cada usuario y se utiliza para detectar cambios en el comportamiento de cuentas individuales.

2.- Detección basada en reglas: implica un intento de definir un conjunto de reglas que se pueden usar para determinar si un comportamiento dado es el de un intruso.

a) Detección de anomalías: las reglas se desarrollan para detectar una desviación de los modelos de uso previos.

b) Identificación de la penetración: un enfoque basado en sistemas expertos que busca comportamientos sospechosos. (s/n)

Dentro de estos procesos de detección de intrusos podemos saber los distintos escenarios basados en los perfiles del atacante con el fin de determinar las contramedidas de dichas anomalías que se presentan en el sistema.

3.7.4 Registros de auditoria.

El registró de auditoria es muy importante para la detección de intrusos, estos tipos de auditorías son muy importante que se registren las actividades que realizan el usuario. Con la finalidad de poder saber si realmente el usuario está siendo uso de su verdadero registro para ello tenemos dos puntos muy importantes dentro del registro de auditorías:

1. **Registros de auditoria nativos:** Para el registro de auditoria es fundamental una herramienta de detección de registros que nos permita ver que está realizando el usuario como el servido en tiempo real.
2. **Registros de auditoria específico para la detección:** Para el registro de auditoria específico es necesario tener una herramienta que nos permita ver solo datos del intruso que está queriendo infringir en la red de datos.

3.8. Detección de la intrusión basada en regalas.

Para la detección basada en regalas para la detección de intrusos es muy importa saber que patrón de actividades se está dando dentro de dichos sistemas auditados con la finalidad las anomalías de infiltración para esto, Stallings (2004) manifiesta la siguiente (tabla 7). De detección de intrusos.

Tabla 7. ***Detección de intrusos***

Medias	Modelo	Tipo de intrusión detectada
Actividad de acceso y sección		
Frecuencia de entrada por día y hora	Media y desviación estándar	Es posible que los intrusos entren fuera de las horas punta.
Frecuencia de entrada en diferentes lugares	Media y desviación estándar	Los intrusos pueden acceder desde un lugar que un usuario concreto apenas o nunca use
Tiempo desde la última entrada	Operativa	Irrupción en una cuenta "muerta"
Tiempo trascurrido por sesión	Media y desviación estándar	Desviación significativa podrían indicar un suplantador
Cantidad de salida a la localización	Media y desviación estándar	Excesivas cantidades de datos transmisión a localizaciones remotas podrían significar fuga de datos confidenciales
Utilización de recursos sección	Media y desviación estándar	Procesador inusual o niveles I/O podría intrusión
Fallo en el acceso desde	Operativo	Intento de irrupción por

terminales especificadas		averiguación de contraseña.
Actividad de ejecución de comandos o programas		
Frecuencia de ejecución	Media y desviación estándar	Puede detectar intrusos, que probablemente usen diferentes comandos.
Utilización de recursos de programa	Media y desviación estándar	Un valor anormal podría seguir la inyección de un virus o un troyano.
Negación de ejecución	Modelo operativo	Puede detectar intento de penetración por parte de un usuario individual.
Actividad de acceso a archivos		
Frecuencia de lectura, escritura, de crear, de borrar	Media y desviación estándar	Anomalías para el acceso, eliminación a leer y escribir para usuarios individuales puede significar suplantación u observación.
Registros leídos, escritos	Media y desviación estándar	Una anomalía podría significar un intento de obtener datos confidenciales para inferencia o agregación.
Cuenta de fallos para leer, escribir, crear, borrar	Operativa	Puede detectar usuarios que permanentemente intenta acceder a archivos no autorizados

Fuente: (Stallings, 2004, págs. 316-317)**.**

3.8.1 Detección distribuida de la instrucción.

“elementos que detecta, identifica y responde a actividades no autorizadas o anormales” (Dennig, Neumann, & Parker, 1987, pág. 4), hasta hace poco las redes de telecomunicaciones o telemática han optado por realizar nuevos sistemas de detección contra intrusos con el fin de poder salvaguardar la información de los usuarios.

Porras en los siguientes puntos aclara el diseño de una red de detección de intrusos (Porras, 1992)

- Un sistema distribuido de detección de intrusión puede necesitar tratar con diferentes formatos de registro de auditorías. En un entorno heterogéneo, diferentes sistemas emplearán distintos sistemas nativos de recopilación de información de auditoría y, si usa la detección de intrusión, puede emplear diferentes formatos para los registros de auditoría relacionados con la seguridad.
- Uno o más nodos de la red servirán como puntos de recopilación y análisis de los datos de los sistemas en la red. Así, se deben transmitir por la red datos simples de auditoría o datos de resumen. Por lo tanto, hay un requisito para asegurar la integridad y la confidencialidad de estos datos. La integridad se requiere para evitar que un intruso enmascare sus actividades alterando la información de auditoría transmitida. La confidencialidad se requiere porque la información de auditoria transmitida podría ser valiosa.
- Se podría usar tanto una arquitectura centralizada como descentralizada. Con una arquitectura centralizada hay un solo punto

central de recopilación y análisis de todos los datos de auditoría. Esto facilita la tarea de correlacionar los registros entrantes pero crea un embotellamiento potencial y un solo punto de fisura. Con una arquitectura descentralizada, hay varios centros de análisis, pero éstos deben coordinar sus actividades e intercambiar información. (s/n).

En la siguiente (figura23). Podemos observar la arquitectura de detección de intrusos.

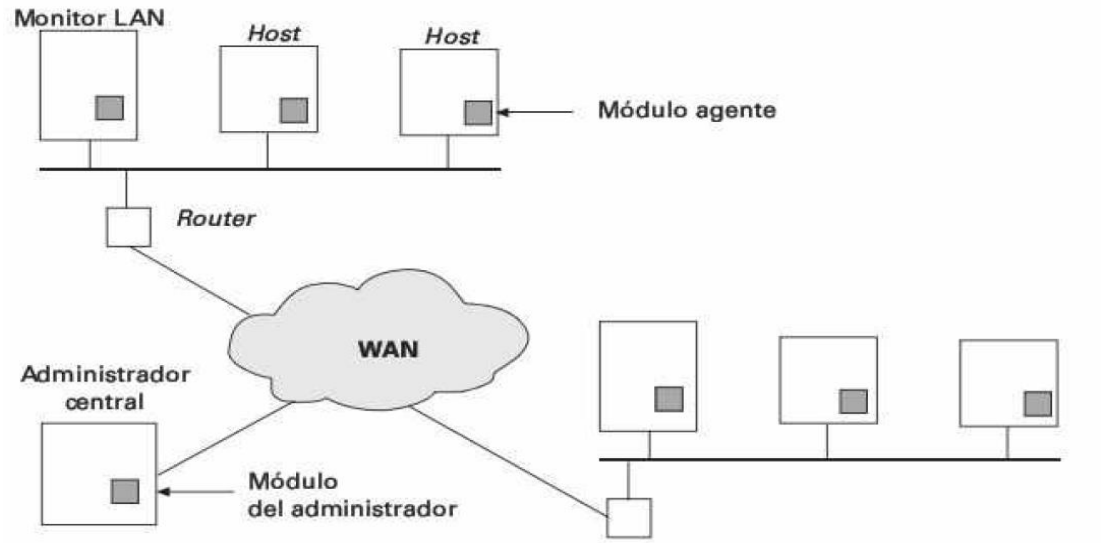


Figura 23. Arquitectura para la detección distribuida de intrusos
Fuente: (Stallings, 2004, pág. 320)

3.8.2 Redes tipo señuelo (honeypots y honeynets).

Honeypor: es un recurso de la red cuyo objetivo es crear áreas virtuales es decir ser el señuelo de ataques informáticos. Con el fin de poder obtener mayor información de los diversos esquemas de ataques de instrucción

Honeynets: nos permite realizar una plataforma con diferentes servidores y aplicaciones vulnerables, donde se realizan ataques de fuerza bruta.

3.9 Software dañino.

En este contexto nos centraremos en aquellos programas que exploran la seguridad del ordenador o a su vez generan cambios en la carpeta raíz de sus directorios como por ejemplo, las bombas lógicas, virus, gusanos, etc.

3.9.1 Virus otras amenazas.

Los tipos de virus o amenazas son aquellos sistemas maliciosos que se implantan directamente en la raíz del alma del sistema operativo con el fin de dañar su funcionamiento y vulnerabilidad.

3.9.2 Programas dañinos.

Estos programas dañinos toman el nombre de software maliciosos y son diseñados para infiltrase en la mayoría de los ordenadores. A continuación hablaremos brevemente de cada uno de ellos.

Bombas lógicas: Estos tipos de programa de infección son ejecutados en un factor de tiempo determinado, cada programador tiene un esquema de ejerces la ejecución de su programa malicioso ya seca por algún tipo de comando o tecla que active dicha bomba lógica

Caballo de Troya: Este tipo de código malicioso se muestra como un programa autentico sin ningún tipo de infección, pero al ejecutarlo puede generar mucho daño al sistema operativo creando una apertura para los *hackers.*

La naturaleza de los virus.

Los virus en un software que tiene la función de propagarse sobre un sistema operativo. Al virus se lo conoce como *malware* este termito se propago en la red ya que tiende a infectar los sistemas informáticos.

Tipos de virus.

Desde que los sistemas de infección (virus) aparecieron por primera vez se generó una guerra informática entre los virus y antivirus con el fin de opacar el impacto de destrucción que se genera dentro de un sistema operativo. Es decir que un virus es auto replicable y puede formar parte de otro virus hasta el punto de transformarse en un virus más letal.

Virus de macro.

Este tipo de virus comúnmente lo encontramos en muchos programas de ejecución es decir los programas como Word, Excel o a su vez en programas de programación como Android, IOS entre otros.

Virus de correo electrónico.

Este tipo de virus por medio del correo electrónico produjo daños colaterales ya que al realizar un envió de dicho programa malicioso en forma de cadena a diferentes ordenadores lograba infectar a un nivel masivo. Uno de esos virus fue el Melissa 1999, que atacaba directamente la carpeta Win 32 que se encuentra en la raíz del sistema operativo.

Gusanos.

Un virus de correo electrónico tiene algunas de las características de un gusano ya que se propagan en un sistema. Sin embargo, estos tipos de gusanos usa la red para extenderse de sistema a sistema, si bien es cierto estos tipos de gusanos se propagan de anfitrión a anfitrión sin necesidad de ejecutarlo tanto así que se puede propagar ya sea por una unidad de almacenamiento extraíble.

Enfoque de antivirus.

La solución ideal para la amenaza de los virus es la prevención, es decir, no permitir que un virus entre en el sistema. Por lo tanto, se crearon programas de protección para dicha infección estos son los antivirus. Hoy en día existen innumerables tipos de antivirus uno mejor que el otro, pero lo que lo hace más eficiente a un antivirus es que este en constante evolución y sobre todo actualizado de los últimos proceso de infección que podría tener un sistema operativo

3.10. Software de bloque de acciones.

Este tipo de software de bloqueo de acción salió en el año 2007 con la plataforma de sistema operativo de vista y fue evolucionando hasta la actualidad en lo que hoy conocemos w8.1 w9, esta plataforma nos advierte por medio de un bloqueo directo del administrador que el software que se esté instalando puede afectar el funcionamiento del sistema es ahí donde se realiza la acción de protección contra un virus, gusano o bomba lógica.

3.11 Cortafuegos (FIREWALLS).

3.11.1 Principios de diseño de cortafuegos.

El diseño de los firewalls es parte del sistema que permite un bloqueo en forma de pared, la cual niega el acceso a personas no autorizadas al sistema con fin de salvaguardar la información. El termino cortafuego (firewalls) es proteger la red. Un cortafuego en otros términos realizar un monitoreo del tráfico de la red de su ordenador lo cual puede filtrar datos de acuerdo a la dirección IP o dominio del protocolo que el mecanismo crea conveniente para su seguridad.

3.11.2 Características de los cortafuegos.

- Permite o bloquea toda dirección proveniente de una dirección específica o de dudosa procedencia.
- Permite o bloquea toda dirección de un dominio específico de dudosa procedencia.
- Dar apertura a puertos específicos o su vez cerrarlos.
- Permitir o bloquear paquetes de datos con algún precedente de cadena específica o de dudosa procedencia.

3.11.3 Configuración de cortafuegos.

A demás del uso de una configuración simple formada por un único sistema, como podría ser un único router de filtrado de paquetes o una única pasarela con esta finalidad se ha realizado los siguientes proceso de configuración los cuales se detallaran en la siguiente (Véase la Figura 24)

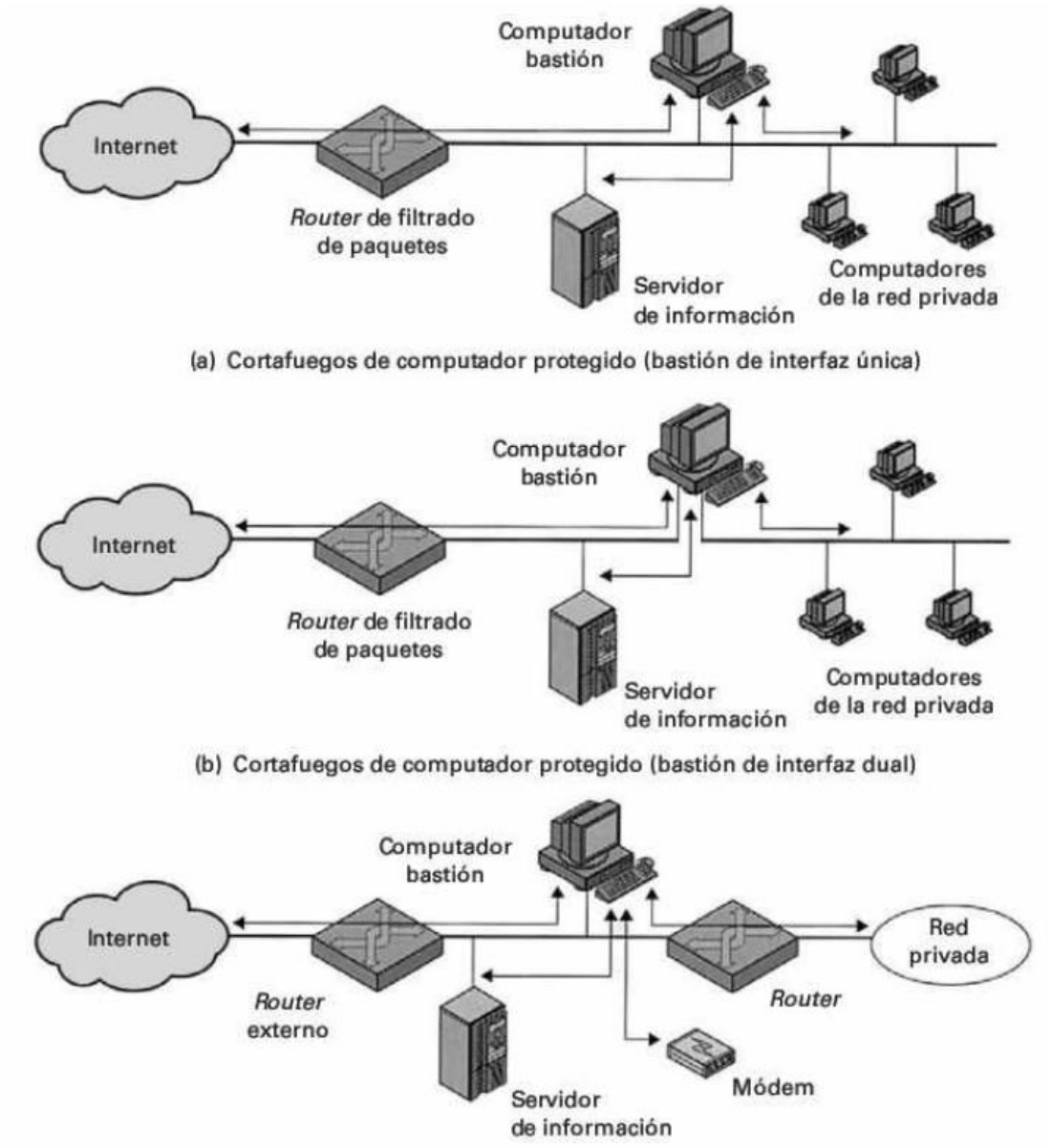


Figura 24. Configuración De Cortafuegos.
Fuente: (Stallings, 2004, pág. 373)

Para la figura (a): Podemos observar que tenemos un router de filtrado de paquetes que conjuntamente esta interactuando con la computador de bastión y dicho computador de bastión está enviando paquetes autorizados al servidor en una interfaz pública.

Para la figura (b): Podemos observar que tenemos un router de filtrado de paquetes la cual se encuentra protegido por una interfaz dual de transmisión de datos hacia el internet.

Para la figura (c): Nos encontramos con una subred que se encuentra protegida por un router que está conectado a la computadora bastión cuyo computador transmite datos a una red privada.

3.11.4 Sistema DMZ (zona desmilitarizada).

Cuando se realiza el diseño de una red tenemos que tener en cuenta que tipos servicios se va a ofrecer al usuario, de tal forma que pueda acceder desde el exterior con cierto nivel de seguridad y confidencialidad del proceso que este ejecutando en la red de datos.

Esta red perimetral tiene servicios como HTTP, DNS, FTP en el siguiente figura observaremos más detalladamente el proceso que realiza la red DMZ

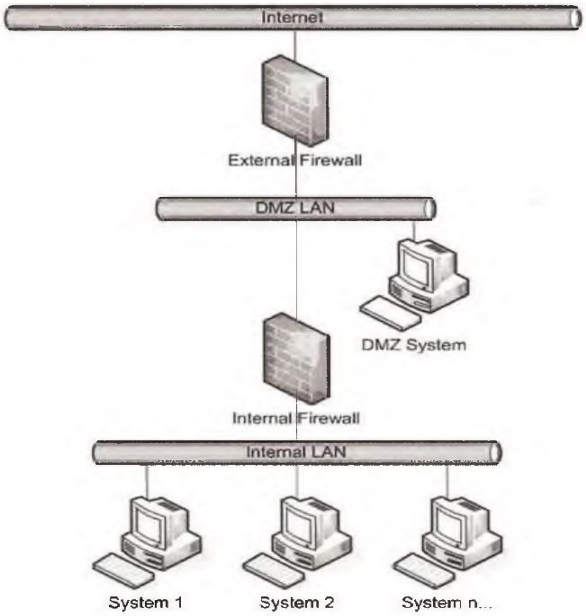


Figura 25. Zona Desmilitarizada o DMZ.
Fuente: (Costa S, 2011, pág. 173)

CAPÍTULO IV.

ANÁLISIS DE RESULTADO DE INTERPRETACIÓN DE DATOS.

4.1 Metodología.

Al realizar este tipo de recolección de información podremos estar al tanto si la comunidad universitaria UCSG, tiene un previo conocimiento de la seguridad de información que nos brindan las redes ya sean estas privadas o públicas. Por lo tanto sea realizado las respetivas encuestas (Alumnos) y entrevistas (Personal del Centro de computo UCSG).

4.2 Encuestas.

Para la encuesta se realizó preguntas de acuerdo al proyecto de titulación planteado, por lo cual se realizó un pequeño encuesta a 382 personas

Unidad primaria de muestreo: Estudiantes empadronados en la Universidad Católica de Santiago de Guayaquil en el año 2014.

Formulación infinita: 9.580 estudiantes

Significancia: 95%

Error: 5%

D**efinición muestra:** $$n = \frac{Z^2\ pq\ N}{e^2(N-1)+Z^2pq}$$

N= 9.580

Z= 1,96 $$n = \frac{1.96^2*0.5*0.5*9580}{0.05^2(9580-1)+1.96^2*0.5*0.5}$$

p= 0,5

q= 0,5

e= 0,05

n=382 $n = 382$

n: tamaño de la muestra, nos permitirá obtener el número de elementos de la muestra que estamos entrevistando para el desarrollo de la recopilación de datos.

N: Es el tamaño de los estudiantes inscritos en el periodo A 2014 de la universidad católica de Santiago de Guayaquil.

Z: Es valor de los datos que corresponden a la distribución Gaussiana, la cual conforma el proyecto de titulación en este presente trabajo, con el fin tener un nivel de confiabilidad 95% valor elegido ya que es el más común, podemos dirigirnos al (Anexo) donde se mostrar la tabla Z.

E: Es el error admitido que puede tener una investigación. Valor de referencia 0,05.

Variabilidad positiva (p): Es la variabilidad de éxito que sirve para determinar el tamaño de la muestra, siendo éste su valor 0.50.

Variabilidad negativa (q): (1-p), es la variabilidad de rechazo que tiene el proyecto de titulación. Siento este su valor 0.50

Población (N): Es la cantidad de estudiantes empadronados en el periodo A 2014 en la Universidad Católica de Santiago de Guayaquil equivalente a 9.580 estudiantes.

Tabla 8. Sexo de las personas encuestadas

Variable	*Cantidad*	*Porcentaje*
Masculino	***232***	***61%***
Femenino	***150***	***39%***
TOTAL	*382*	*100%*

Fuente:(Autor del proyecto)

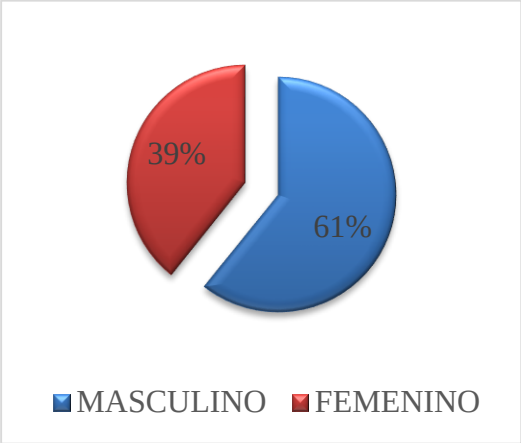


Figura 26. Sexo de las personas encentradas
Fuente:(Autor del proyecto)

Tabla 9. ***Edades de las personas encuestadas***

Variable	*Cantidad*	*Porcentaje*
17-25	***180***	***47%***
26-35	***120***	***31%***
35-50	***82***	***21%***
TOTAL	***382***	***100%***

Fuente: (Autor del proyecto)

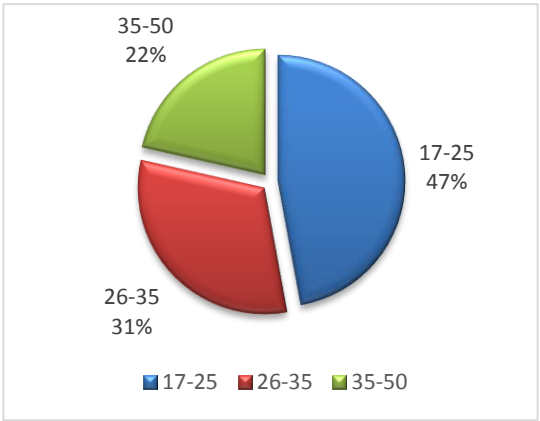


Figura 27. Edades de las personas encuestadas
Fuente:(Autor del proyecto)

1. ¿Cuál de los siguientes servicios de Internet usted utiliza en la institución universitaria?

Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

Tabla 10. Servicios de internet

N	*Variable*	*cantidad*	*porcentaje*
1	***Página Web***	***100***	***26%***
2	***Correo Electrónico***	***152***	***40%***
3	***Banca Electrónica***	***50***	***13%***
4	***Comercio electrónico***	***80***	***21%***
	TOTAL	*382*	*100%*

Fuente:(Autor del proyecto)

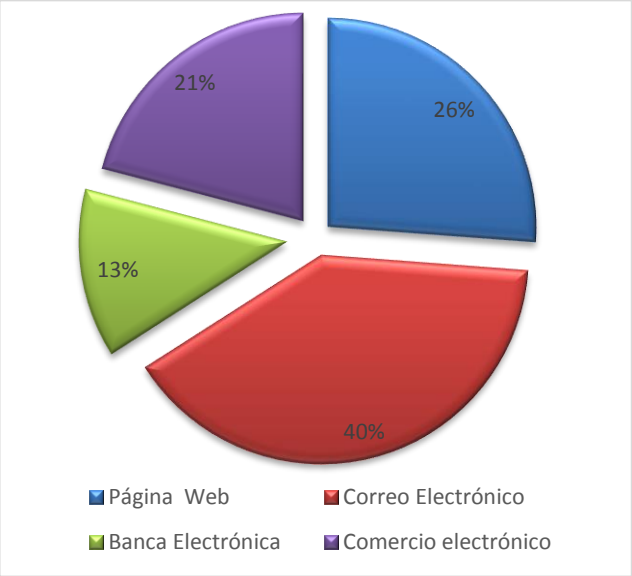


Figura 28.servicio de internet.
Fuente:(Autor del proyecto)

Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.

Preparación: Carlos Fajado.

En la primera pregunta a partir de los datos recolectados los estudiantes de la U.C.S.G. Podemos constatar que 40% de los estudiantes utilizan el correo electrónico de la institución; 26% página web institución; 21% comercio electrónico institución; 13% banca electrónica de la institución. Por ello, según los datos recolectados podemos observar que 13% referente a la banca electrónica tiene un

porcentaje muy bajo debido a que no están seguros de utilizar es medio para realizar sus pagos por cuestión de ser robados.

2. Acerca de los portales web que utiliza su institución educativa.

A) Tipo de servicio?

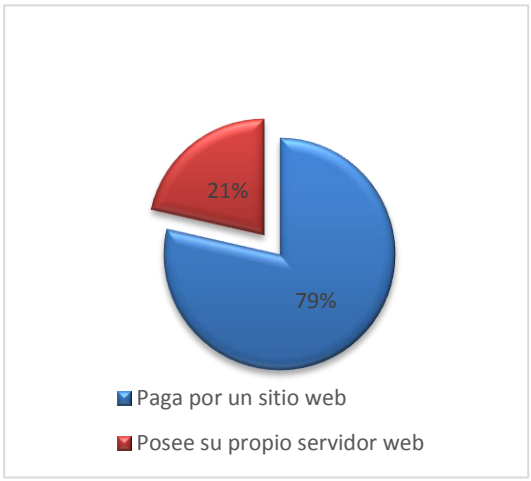
Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

Tabla 11. Tipo de servicio.

N	*VARIABLE*	*CANTIDAD*	*PORCENTAJE*
1	***Paga por un sitio web***	***300***	***78,5%***
2	***Posee su propio servidor web***	***82***	***21,5%***
	TOTAL	***382***	***100,0%***

Fuente:(Autor del proyecto)
Figura 29. Tipo de servicio
Fuente:(Autor del proyecto)

Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.



En la segunda pregunta literal (A) que hace referencia al portal web de la institución donde 79% de los estudiantes tiene conocimiento que se paga por un servicio, y el 21% posee su propio servidor web.

B) ¿Qué operaciones realizan en su sitio web de su institución?.
Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

Tabla 12. ***Sitios web***

N	*VARIABLE*	*CANTIDAD*	*PORCENTAJE*
1	***Solamente como fuente de trabajo***	***182***	***47,6%***
2	***Programas en línea***	***150***	***39,3%***
3	***Ambos***	***50***	***13,1%***
	TOTAL	***382***	***100,0%***

Fuente:(Autor del proyecto**)**

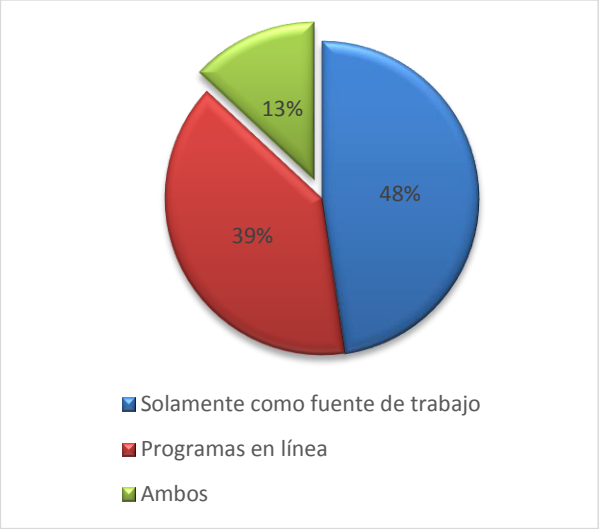


Figura 30. Sitios Web
Fuente:(Autor del proyecto)

Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

En la segunda pregunta literal (B) podemos observar 48% de los estudiantes utiliza la plataforma de la institución como fuente de trabajo, mientras que el 39% lo utiliza para programas en línea (juegos). No obstante, 13% utiliza este servicio para realizar ambas actividad.

C) ¿Considera necesaria la seguridad en este servicio?
Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

Tabla 13. ***Seguridad de servicios***

N	*VARIABLE*	*CANTIDAD*	*PORCENTAJE*
1	***Sí.***	***300***	***78,5%***
2	***No.***	***70***	***18,3%***
3	***Le es indiferente.***	***12***	***3,1%***
	TOTAL	***382***	***100,0%***

Fuente:(Autor del proyecto**)**

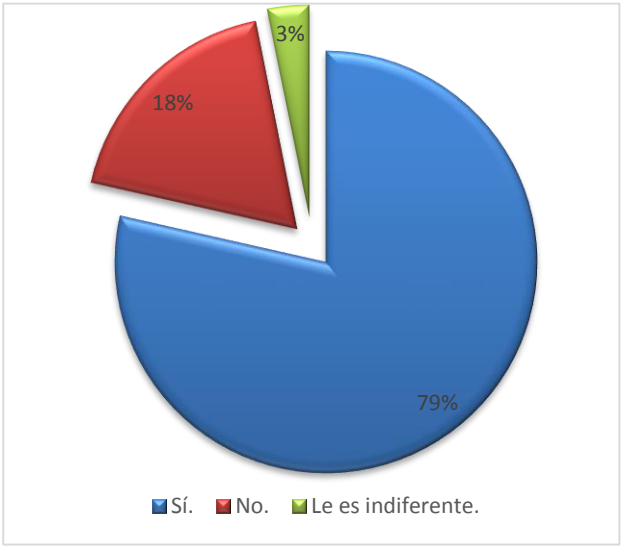


Figura 31. Seguridad de servicios.
Fuente:(Autor del proyecto)

Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

En la segunda pregunta literal (C) hace referencia a las dos preguntas anteriores para lo cual nos permite saber que el 79% considera necesario la seguridad de los servicios en la red de datos, 18% no considera que sea necesario y el 3% le es indiferente.

3.- Acerca del correo electrónico que utiliza la institución.
Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

A) ¿Qué tipo de servicio posee?

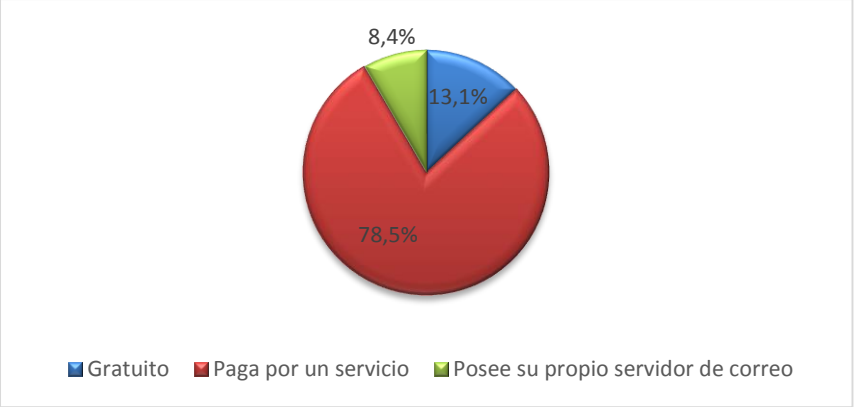
Tabla 14. ***Correo electrónico***

N	*VARIABLE*	*CANTIDAD*	*PORCENTAJE*
1	***Gratuito***	***50***	***13,1%***
2	***Paga por un servicio***	***300***	***78,5%***
3	***Posee su propio servidor de correo***	***32***	***8,4%***
	TOTAL	***382***	***100,0%***

Fuente:(Autor del proyecto**)**

Figura 32. Correo Electrónico.
Fuente:(Autor del proyecto)

Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.



En la tercera pregunta literal (A) el 13% manifiesta que es gratuito el servicio de correo electrónico dentro de la institución, 78.5% paga por un servicio y el 8.4% paga por un propio servidor de correo electrónico.

B) ¿Considera necesaria la seguridad en este servicio?
Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

Tabla 15. ***Seguridad de servicios.***

N	*VARIABLE*	*CANTIDAD*	*PORCENTAJE*
1	***Sí***	***280***	***73,3%***
2	***No***	***72***	***18,8%***
3	***Le es indiferente***	***30***	***7,9%***
	TOTAL	***382***	***100,0%***

Fuente:(Autor del proyecto)

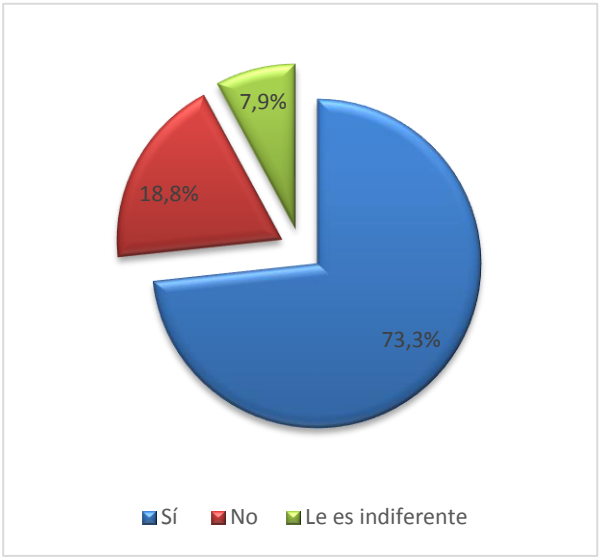


Figura 33. Seguridad de Servicios.
Fuente:(Autor del proyecto)

Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

Para la tercera pregunta literal (B), referente a la seguridad del correo electrónico 73.3% considera que es necesario la seguridad del servicio, 18.8% no es necesario y al 7.9% le es indiferente la seguridad que pueda tener el servicio de correo electrónico.

4.-Acerca de la Banca Electrónica dentro de la instrucción educativa.
Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

Si su institución utiliza Banca Electrónica.
A) ¿Cuáles de las siguientes transacciones realiza?

Tabla 16. ***Banca electrónica***

N	*VARIABLE*	*CANTIDAD*	*PORCENTAJE*
1	***Pago de planilla.***	***50***	***13,1%***
2	***Pago a proveedores.***	***98***	***25,7%***
3	***Recepción de pagos de clientes.***	***56***	***14,7%***
4	***Pago de servicios Consulta de cuentas.***	***20***	***5,2%***
5	***Transferencia de fondos.***	***89***	***23,3%***
6	***Otros.***	***69***	***18,1%***
	TOTAL	***382***	***100,0%***

Fuente:(Autor del proyecto**)**

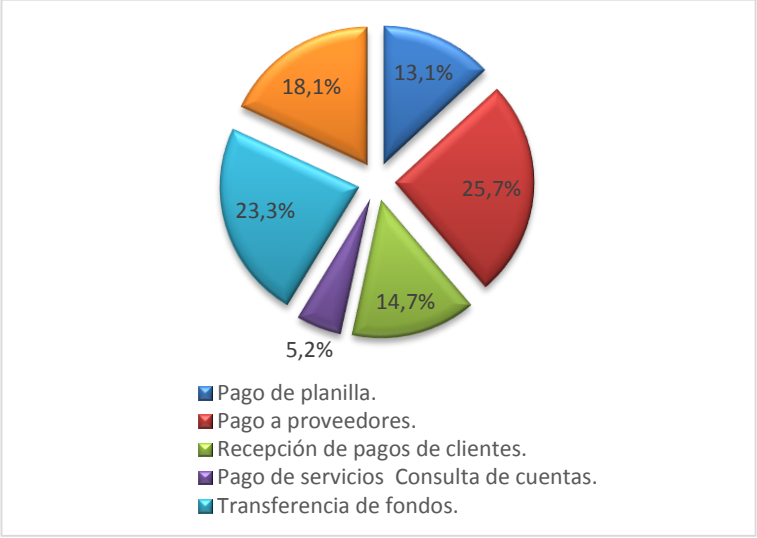


Figura 34. Banca Electrónica
Fuente:(Autor del proyecto)
Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

Para la cuarta pregunta podremos observar que 25.7% realizan pagos a proveedores, 23% realizan transferencias de fondos, 18,1% otras actividades, 14.7% realiza recepción de pagos de clientes, 13% realiza pagos de planillas.

B. ¿Considera necesaria la seguridad en este servicio?
Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.
Tabla 17. Seguridad servicio

N	*VARIABLE*	*CANTIDAD*	*PORCENTAJE*
1	***Sí.***	***300***	***78,5%***
2	***No.***	***40***	***10,5%***
3	***Le es indiferente.***	***42***	***11,0%***
	TOTAL	***382***	***100,0%***

Fuente:(Autor del proyecto)

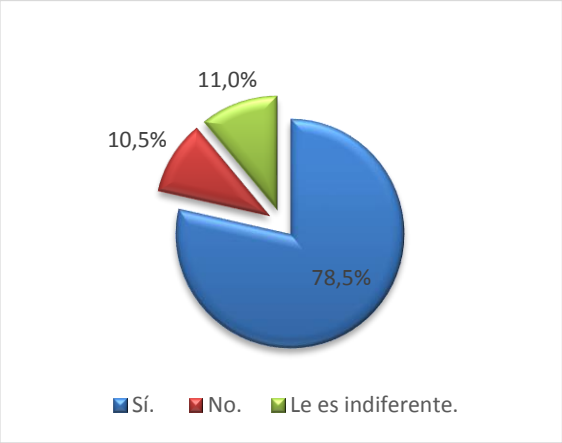


Figura 35. Seguridad de servicios.
Fuente:(Autor del proyecto)

Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

Para la cuarta pregunta literal (B) se hace referencia a la seguridad 78,5% manifiesta que sí, el 10.5% no es necesaria la seguridad, mientras que el 11,0% le es indiferente.

5¿Qué mecanismo de seguridad utiliza?
Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

Tabla 18. ***Mecanismo de seguridad.***

N	*VARIABLE*	*CANTIDAD*	*PORCENTAJE*
1	***Certificados Digitales.***	***10***	***2,6%***
2	***Firma Digitales.***	***100***	***26,2%***
3	***Tarjeta electrónica.***	***100***	***26,2%***
4	***Cifrado de datos.***	***20***	***5,2%***
5	***VPN's.***	***83***	***21,7%***
6	***Ninguno.***	***69***	***18,1%***
	TOTAL	***382***	***100,0%***

Fuente:(Autor del proyecto)

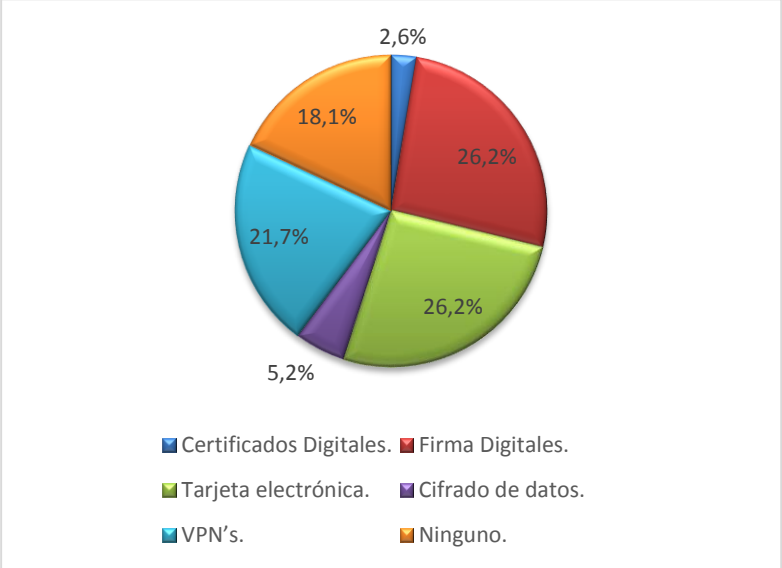


Figura 36. Mecanismos de seguridad.
Fuente:(Autor del proyecto)

Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

Para la quinta pregunta relacionada a los mecanismos de seguridad tenemos los siguientes porcentajes 26.2% está de acuerdo de tener firmas digitales como tarjetas electrónicas, el 21.7% VPN´s (red privada virtual segura), 5,2% cifrados de datos, 2,6% certificado digital, mientras que 18,1% ninguno.

6. ¿Quién autoriza o provee la seguridad?
Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

Tabla 19. ***Autorización y proveedor de seguridad.***

N	*VARIABLE*	*CANTIDAD*	*PORCENTAJE*
1	***Autoridad.***	***262***	***68,6%***
2	***Certificadora Regional.***	***80***	***20,9%***
3	***Autoridad Certificadora.***	***30***	***7,9%***
4	***Extranjera.***	***0***	***0,0%***
5	***Otros.***	***10***	***2,6%***
	TOTAL	***382***	***100,0%***

Fuente:(Autor del proyecto)

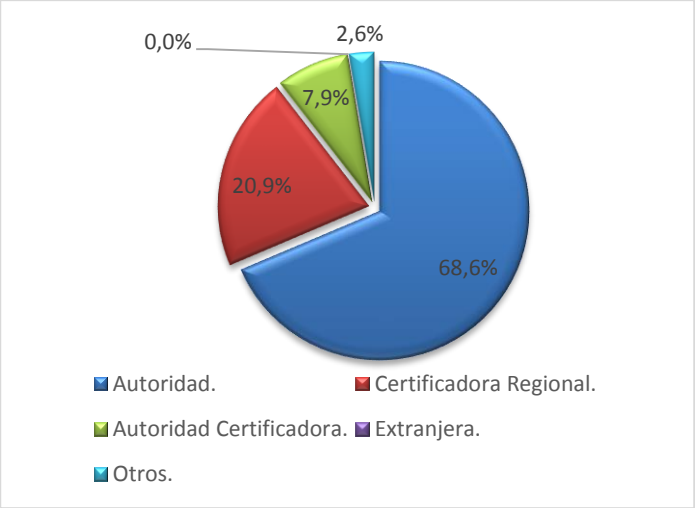


Figura 37. Autorización y Proveedor de seguridad.
Fuente:(Autor del proyecto)

Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

Para sexta pregunta referente a los proveedores de seguridad y autorizaciones el 68,6% Autoridad, 20,9% Certificadora regional, 7,9% Autoridad Certificadora, 2.6% otros, 0.0% extranjera.

7. ¿Cómo considera la inversión de la seguridad dentro de su institución?
Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

Tabla 20. ***Inversión de seguridad.***

N	*VARIABLE*	*CANTIDAD*	*PORCENTAJE*
1	***Baja.***	***12***	***3,1%***
2	***Media.***	***80***	***20,9%***
3	***Alta.***	***280***	***73,3%***
4	***Muy alta.***	***10***	***2,6%***
	TOTAL	***382***	***100,0%***

Fuente:(Autor del proyecto**)**

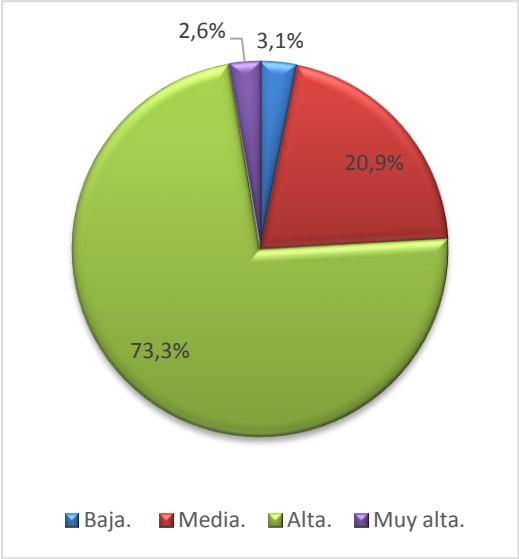


Figura 38. Inversión de Seguridad.
Fuente:(Autor del proyecto)

Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

La séptima pregunta inversión de seguridad institucional 73.3% considera la seguridad que es muy alta, 20,9% media, 3,1% baja, 2,6% muy alta.

8. ¿Tiene conocimiento de los métodos criptográficos de seguridad que existen en su institución?
Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

Tabla 21. Métodos Criptográficos.

N	*VARIABLE*	*CANTIDAD*	*PORCENTAJE*
1	***Sí.***	***2***	***0,5%***
2	***No.***	***380***	***99,5%***
	TOTAL	***382***	***100,0%***

Fuente:(Autor del proyecto)

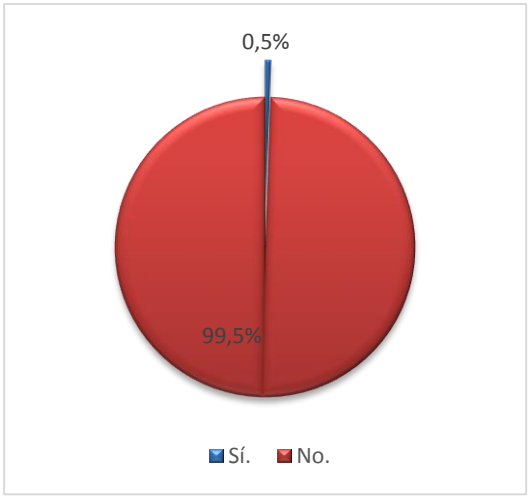


Figura 39. Métodos Criptográficos.
Fuente:(Autor del proyecto)

Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

Para la octava pregunta Métodos criptográficos de seguridad el 99,5% desconocen de estos métodos de seguridad, 0,5% han escuchado sobres los Métodos criptográficos.

9. ¿Tiene conocimiento de lo que es la Criptografía?
Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.
Tabla 22. Criptografía.

N	*VARIABLE*	*CANTIDAD*	*PORCENTAJE*
1	***Sí.***	***82***	***21,5%***
2	***No.***	***300***	***78,5%***
	TOTAL	***382***	***100,0%***

Fuente:(Autor del proyecto)

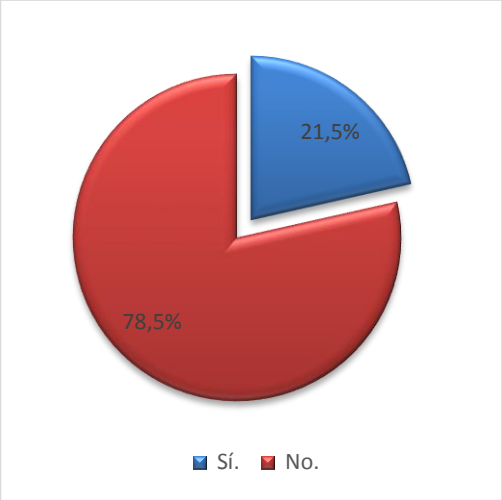


Figura 40. Criptografía.
Fuente:(Autor del proyecto)

Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

Para la novena pregunta relacionada al conocimiento de lo que es la criptografía 21,5% si tiene conocimiento de que es criptografía, el 78,5% no.

10. ¿Cree que le afectaría mucho a su institución si la seguridad actual fuera rota fácilmente y como les afectaría usted?
Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.
Tabla 23. Seguridad.

N	*VARIABLE*	*CANTIDAD*	*PORCENTAJE*
1	***Sí.***	***300***	***78,5%***
2	***No.***	***82***	***21,5%***
	TOTAL	***382***	***100,0%***

Fuente:(Autor del proyecto)

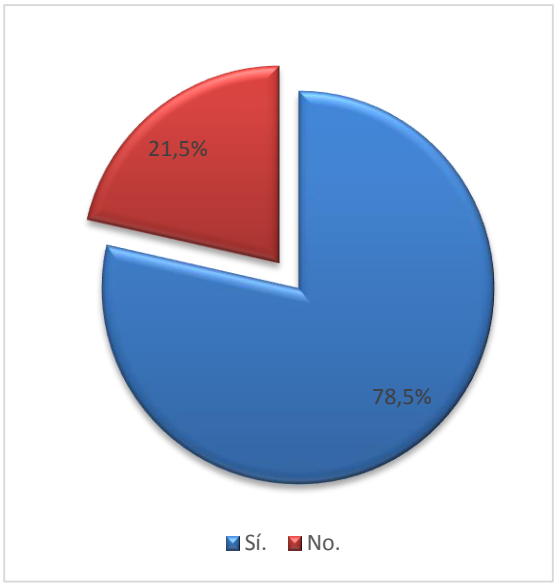


Figura 41. Seguridad.
Fuente:(Autor del proyecto)

Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

Para la décima pregunta 78,5% manifiesta que si afectaría la seguridad de la información si fuera violentada, y el 21,5% no afectaría la seguridad.

A). Si su respuesta fue si, en cuál de estas opciones le afectaría:
Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

Tabla 24. Opciones.

N	*VARIABLE*	*CANTIDAD*	*PORCENTAJE*
1	***Confidencialidad.***	***150***	***39,3%***
2	***Autentificación.***	***50***	***13,1%***
3	***Integridad de la información.***	***82***	***21,5%***
4	***Banca electrónica de la institución.***	***100***	***26,2%***
	TOTAL	***382***	***100,0%***

Fuente:(Autor del proyecto)

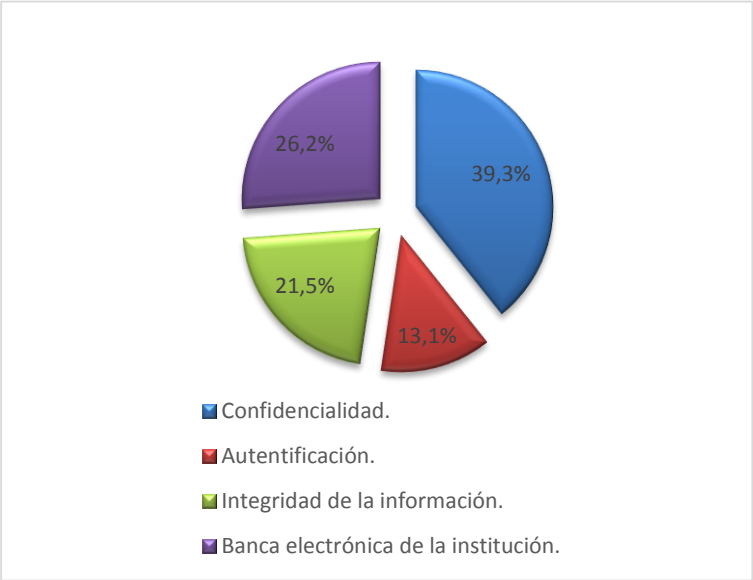


Figura 42. Opciones.
Fuente:(Autor del proyecto)

Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

Para el ítem de la décima pregunta si la respuesta fuera si los entrevistados manifiestan que le afectaría 39,3% la confidencialidad de sus datos, 26,3% la banca electrónica de la institución, 21,5% integridad de información, y el 13,1% Autentificación.

11.- ¿Cuál de las siguientes opciones usted identifica que es una web segura?
Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

Tabla 25. Web seguras.

N	VARIABLE	CANTIDAD	PORCENTAJE
1	**HTTP**	**200**	**52,4%**
2	**HTTP`S**	**150**	**39,3%**
3	**HTTPS**	**32**	**8,4%**
	TOTAL	**382**	**100,0%**

Fuente:(Autor del proyecto)

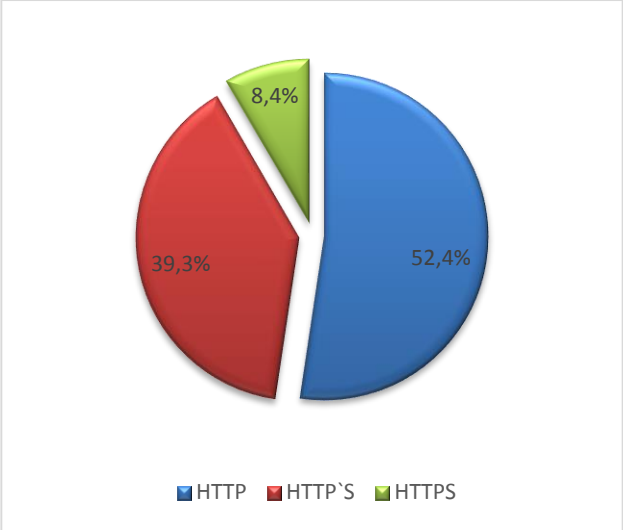


Figura 43. Web seguras.
Fuente:(Autor del proyecto)

Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

Para la décima primera pregunta se da tres opciones para saber si tiene conocimiento cuando se conecta a los website y visualizan su seguridad el 52.4% de los encuestados identificaron que una red segura HTTP, mientas que el 39,3 manifestó que la seguridad HTTP´s, y solo el 8,4%HTTPS tenían conocimiento de una web segura.

12.- ¿Cree usted que la red inalámbrica de la institución es segura?
Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.
Preparación: Carlos Fajado.

Tabla 26. Seguridad inalámbrica.

N	*VARIABLE*	*CANTIDAD*	*PORCENTAJE*
1	***Si***	***200***	***52,4%***
2	***No***	***100***	***26,2%***
3	***Les es indiferente***	***82***	***21,5%***
	TOTAL	***382***	***100,0%***

Fuente:(Autor del proyecto)

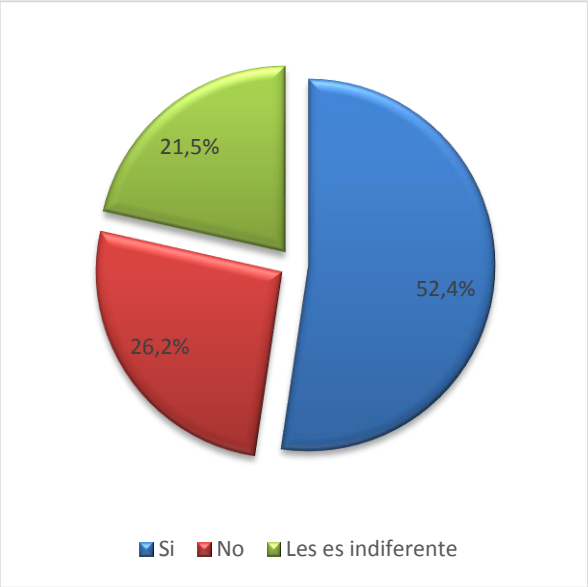


Figura 44. Seguridad inalámbrica.
Fuente:(Autor del proyecto)

Fuente en cuesta: Universidad Católica de Santiago de Guayaquil.

Preparación: Carlos Fajado.

Para la décima segunda pregunta con referente a la red inalámbrica de la institución y su seguridad 52.4% si es segura, 26,2% no es segura, 21,5% le es indiferente

La elaboración de esta encuesta nos permite tener un mayor conocimiento y análisis de las falencias que puede tener el usuario al conectarse a una red sin tener un conocimiento previo sobre seguridad.

Entrevista

La entrevista fue realizada al jefe de producción del centro de cómputo de la U.C.S.G, con el propósito de obtener información general sobre las seguridades implantadas en las redes de datos de la UCSG.

1.- ¿Podría enumerar algunos mecanismos de seguridad para evitar la fuga de información?

- Firewall bloquea el acceso de personas no autorizadas al sistema de la base de datos.
- Cifrado de datos para transportar información segura y confiable.
- VPN para accesos remotos anónimos.
- Antivirus actualizado en cada ordenador y servidores.
- Proxy asignadas a cada facultada.
- Lectores biométricos para el ingreso de empleados en cada facultad.

2.- ¿Esos mecanismos son software libre o licencias pagadas?

- Los mecanismos que se utilizan para la entrada o salida de la información son de carácter confidencial. No obstante, la universidad garantiza la seguridad de datos que se genera entre facultades no por eso garantizamos la seguridad pública como son las redes inalámbricas.

3.- ¿Cuáles son primordiales entornos para determinar la utilización del mecanismos de seguridad por sobre otros gratuitos?

- La mayor parte de instituciones no pondrían en riesgo la información que tienen almacenadas en sus bases de datos con software gratuitos. Por más que, sean seguros no dan una garantía, por ello se opta en realizar variables de costo, beneficio y sobre todo calidad de sistemas vigentes y garantizados.

4.- ¿Quiénes toman estas resoluciones? ¿Existe algún ente regulador o experto en telecomunicaciones, telemática?

- Las resoluciones la toman los directivos y decanos de cada facultad. Siempre se cuenta con el respaldo de grandes profesionales para bridan apoyo con el tema en cuestión.

5.- ¿Existe casos de manipulación de información que se haya generado en los 3 últimos años?

- No existe caso reportados de manipulación o fuga de información. Si bien en cierto muchos trabajadores pueden transportar información ya sea por pendrive, discos externos, para ello existen normas contractuales que sancionan el uso de la mala información.
- ¿Existen métodos de contingencia para bloquear dicha manipulación?
  - ✓ Hay principios que reglamentos éticos y morales que el empleado debe mantener.

6.- ¿Se realiza algún tipo de rastreo para localizar información vulnerada, manipulada en el interior de las redes de datos?

- El software que utilizamos para realizar el análisis es confidencia. No obstante, si hay alguna anomalía dicho software bloquea directamente los puertos de entra y salida.

CAPÍTULO V

5. PROTOCOLOS DE SEGURIDAD PARA LAS REDES DE DATOS.

El crecimiento actual de los grupos activistas denominados *hackers* o *crackers* en todos los sectores empresarial, gubernamental, instituciones educativas, así como el crecimiento de la información global que se maneja en la *web,* nos permite visualizar el manejo de información, la transmisión en línea y las malas prácticas de seguridad dentro de las redes de telecomunicaciones e informática.

De las encuestas y entrevista realizadas a la comunidad de estudiantes de la universidad UCSG podemos acotar que no está exenta de algún ataque de fuerza bruta a las conexiones de las redes inalámbricas de las distintas facultades.

Esto es muy importante establecer mecanismos de protección ya que muchas de las veces el estudiante como docente se conectan a redes inalámbricas que existen en las distintas facultades del campus, cabe destacar que se maneja información en los móviles, Tablet etc., y la mayor parte de estos equipos se encuentran sincronizados con el correo de la institución donde se maneja mayor parte del proceso administrativo que puede ser critica para la institución.

Por lo cual se debe realizar una serie de restricciones imponentes y la parte académica se requiere un buen servicio de conexión. No obstante, los recursos de las redes deben estar unidad físicamente, siguiendo esta medida tan significativa se va a

desarrollar un protocolo para salvaguarda la confidencialidad de las redes de datos de la UCSG.

5.1 Definición de Mecanismos.

5.1.1 Normativas:

Para la prevención de futuros ataques se debe seleccionar un sistema de gestión de la seguridad de la información, se recomienda utilizar la norma ISO/ICE 27001:2005 ya que es un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento de los sistemas de seguridad, orientado a procesos, enfocados activos de la información y sobre todo basado en la gestión de riego.

La institución debe revisar los servicios que se presta tanto a nivel académico como administrativo. Algunos de estos servicios que facilitan a los estudiantes son: website, matrícula en línea, consulta de notas en línea, correo universitario, inscripciones de materias en línea, y en la parte administrativa: servicio de terminales virtuales, pagos en línea, etc. Se debe realizar un esquema donde se pueda verificar el uso que está teniendo de la información, y verificar los posibles riegos con punto de controles.

5.1.2 Recursos (Hardware, software, y comunicaciones):

La institución debe de realizar una auditoría de los recursos tecnológicos a nivel de software, hardware, y de comunicación. A nivel de hardware podemos considerar los servidores, routers, switches, entre otros. A nivel de software: Aplicaciones de seguridad criptografía, llaves de acceso a ordenadores por medio de dispositivos externos. A nivel de comunicación: Firewall, antivirus, seguridad biométrica.

5.1.3 Tabla de servicio:

Por medio de esta tabla tendremos en cuenta los servicios que presta la institución.

Tabla 27 ***Tabla de servicio***

CONTROL			
Servicios	Consulta de notas	Consulta de pensiones	Compara de línea.
Causa	Permite realizar el ingreso de notas por parte del docente posteriormente ser consultadas por el estudiante	Permite realizar la consulta y pago del respectivo mes	Comprar en línea por medio inalámbrico
Periodo	Por semestre	Por mes	Variable
Nivel de seguridad	Alta	Alta	Baja
Usuario	Docente, estudiante	Estudiante	Estudiante, docente, público en general
Riesgos	Modificación de notas	Desvió o manipulación de fondos	Manipulación, modificación, suplantación
Punto de control	Proxy/firewall	Teclado biométrico	Por definir
Responsabilidad	Personal de sistema	Personal de sistema financiero	Ninguna a nivel institucional.

Fuente: *(Autor del proyecto)*

En esta tabla podemos saber la importancia de lo que representa la información hoy en día, y tener claro el que?, el cómo?, a qué hora?, identificar alguna amenaza futura.

5.1.4 Identificar riesgo, amenazas y modificaciones:

Se debe realizar un proceso de seguridad o metodología para prevenir futuras amenazas dentro o fuera de la institución, se recomienda realizar un test de penetración, o a su vez hacking ético, como podemos ver en la siguiente (Véase la Figura 45-46)

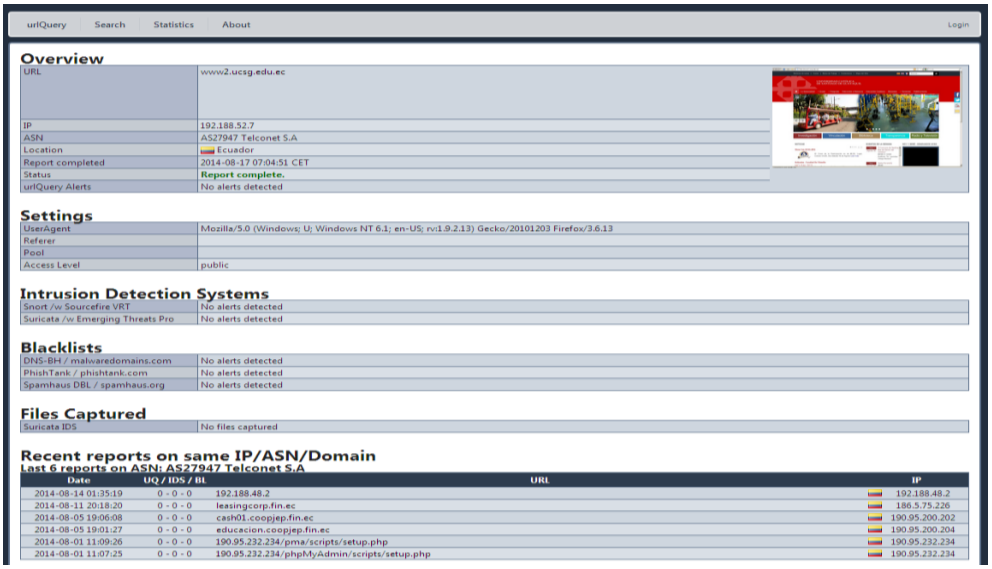


Figura 45. Escaneo de seguridad.
Fuente: (UrlQuery, 2014)

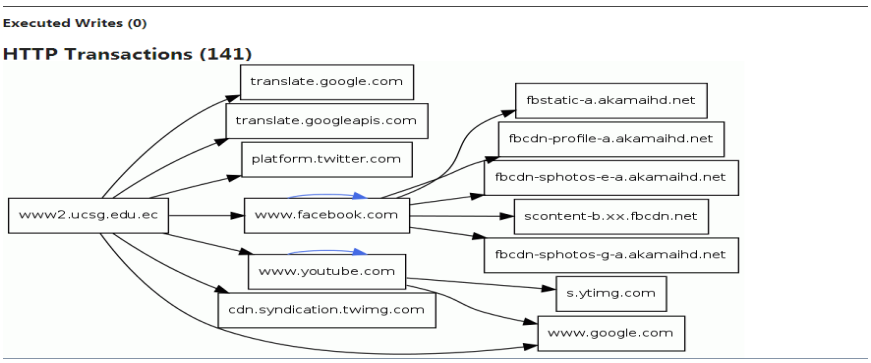


Figura 46. HTTP transacción.
Fuente: (UrlQuery, 2014)

5.1.5 Protección de servicios.

Se debe tomar en cuenta los resultados anteriores, Pero es muy importante proteger las redes de datos, los servicios ofrecidos por la institución y ordenadores de uso administrativo y estudiantil.

- Actualización del software: Se deberá realizar las actualizaciones de las distintas versiones de sistemas operativos que utiliza la institución periódicamente y configuraciones de dichos dispositivos.
- Configuración de firewall: Es importante tener configura el firewall para evitar ataques internos o externos.
- Evitar correos (spam): tener filtros de seguridad y capacitar al usuario del tema
- Utilizar software original: prohibir a los usuarios instalar software de dudosa procedencia para evitar futuros ataques, o pérdida de información.
- Navegación con seguridad: Instalar parches o proxy y capacitar al personal con el fin que puedan identificar una red segura.

5.1.6 Configuración de red.

Para la configuración de la red es importante utilizar los métodos criptográficos ya antes mencionados como por ejemplo los mecanismos de seguridad de clave privada, pública.

Redes inalámbricas: Es muy importante poder tener una seguridad con respecto a las redes inalámbricas con los diferentes métodos criptográficos de seguridad

- ocultar el identificador de redes inalámbricas SSID
- Cifrado WEB 16 bits, WEB 128 bits, WPA-PSK, WAP2 PSK/WAP-PSK.
- Se debe realizar bloqueos de acceso a la red ya sea por RADIUS o autenticación de MAC.
- Establecer un firewall a nivel de la red y a su vez dividir las redes por VLANS.

5.1.7 Control de Acceso.

Para el control de acceso de los docentes o estudiantes es importante cumplir con las siguientes características.

- No poner en la clave la fecha de nacimiento del usuario o número de cedula.
- Realizar una clave que contenga mino 8 caracteres.
- Combinar la clave con símbolos, letras mayúsculas o minúsculas y números.
- Realizar cambio de clave cada 4 meses
- Lo más importante no grabar la clave en los buscadores web ya que se alojan en los llamados cookies.

5.1.8 Salvaguardar la información.

Para salvaguardar la información mediante software criptográfico es muy importante seguir el siguiente paso:

- Cifrar datos confidenciales con algoritmos AES, MD5 entre otros.
- Establecer permiso: como certificaciones, firmas digitales.

5.1.9 Solicitación de políticas de seguridad:

De deber realizar una directiva o asociación para crear políticas de seguridad de la información.

CAPÍTULO VI.

6.1 Conclusiones.

- Por medio del desarrollo de este proyecto de titulación se ha podido indicar que no existe seguridad en las redes inalámbricas ya que cada facultad tiene más de dos punto de redes inalámbricas dentro de la institución.
- Así mismo se identificó que es de gran importancia el desarrollo de normas y sobretodo impartir charlas de seguridad a los estudiantes y docentes de la institución con el fin de que puedan estar alerta alguna amenaza con respecto a la información que manejen.
- Para el desarrollo de este proyecto fue necesario entender el funcionamiento y mecanismos de seguridad que emplean en el centro de cómputo de la institución. Cabe recalcar que por seguridad solo se habla de aspectos generales.
- Para la base de diagnóstico del proyecto de la seguridad de las redes de datos se estableció prioridades para identificar las falencias internas como externas.
- Se cumplen los objetivos de analizar las redes de datos mediante criptografía, para mejorar los protocolos de seguridad de las redes externas de acuerdo a los distintos mecanismos para la necesidad de los docentes o estudiantes que requieran la protección y privacidad de su información.

6.2 Recomendaciones.

- Identificar las website seguras, verificar si el URL es correcto al tener el candado en la parte superior esquina izquierda https, revisar la gramática de la web, verificar el dominio de la página web, verificar leyendas de otros usuarios con respecto a la página que está visitando y por ultimo confía en tu sentido común.
- Identificar nuevas certificaciones y firmas digitales para constatar que no está siendo objetivo de ataque de algún otro usuario.
- No escoger ficheros de descarga de dudosa procedencia ya que podría contener algún troyano que pueda infectar su equipo o robar la información que contiene.
- Realizar un análisis y gestión de riesgo para prevenir ataques de fuerza bruta, cifrar la información con mecanismos criptográficos como AES, DES, configurar routers y swichs.
- No aceptes unidades o memorias externas de extraños, ya que los estudios realizados, se verifica que hay unidades que pueden adulterar el firewall de su ordenador.

Bibliografía

Aguirre, J. R. (1999). *Aplicaciones criptográficas: libro guía de la asignatura seguridad informática* (segunda ed.). Madrid. Obtenido de http://books.google.es/books?id=NOasAAAACAAJ&dq=Libro+electr%C3%B3nico+%E2%80%9CSeguridad+Inform%C3%A1tica%E2%80%9D+cuarta+edici%C3%B3n++versi%C3%B3n+v32+de+Jorge+Rami%C3%B3+Aguirre.+Universidad+Polit%C3%A9cnica+de+Madrid&hl=es&sa=X&ei=9BfbU8jpFoaGyASA14D

Anderson, J. P. (1980). *Computer Security Threat Monitoring And Surveillance.* washintong. Recuperado el 30 de 07 de 2014, de https://archive.org/details/ComputerSecurityThreatMonitoringAndSurveillance

Bermejo, R., & Tlatoani, D. J. (2012). *Estudio y Aplicaciones de Esquemas Criptograficos.* Recuperado el 10 de 08 de 2014, de http://scholar.google.es/scholar?hl=es&as_sdt=0,5&q=Estudio+y+Aplicaciones+de+Esquemas+Criptogr%C3%A1ficos>

Costa S, j. (2011). *Seguridad Y Alta Disponibilidad.* (RA-MA, Ed.) Obtenido de http://books.google.es/books?id=mqyHtgAACAAJ&dq=seguridad+y+alta+disponibilidad&hl=es-419&sa=X&ei=yn36U72DI8i-sQTZ7YGACA&ved=0CCIQ6AEwAA

Dennig, D. E., Neumann, P. G., & Parker, D. B. (09 de 1987). *Social Apecto of computer security.* Recuperado el 05 de 08 de 2014, de Pro. 10th National Computer Security Conference: http://faculty.nps.edu/dedennin/

El chalé de Gaius Baltar. (11 de 08 de 2014). *Aerilon*. Obtenido de http://aerilon.wordpress.com/2011/05/05/introduccion-a-la-criptografia/

Federal Information Processing Standars Publications. (26 de NOVEMBER de 2001). *ADVANCED ENCRYPTION STANDARD.* Obtenido de http://techheap.packetizer.com/cryptography/encryption/fips-197.pdf

FIPS, 4.-3. (1999). *Data Encrytion Standard.* FEDERAL INFROMATION PROCESSING STANDARDS PUBLICATIO. Recuperado el 10 de 08 de 2014

Go Anywhere. (s.f.). *Open PGP*. Recuperado el 05 de 08 de 2014, de goanywheremft: http://www.goanywheremft.com/products/director/encryption/open-pgp

IEEE Global History Network. (s.f de 12 de 2011). *The encryption war of WWII: the Enigma encryption machine*. Recuperado el 21 de 05 de 2014, de IEEE: http://www.ieeeghn.org/wiki/index.php/File:Enigma00.jpg

IEEE Global History Network. (s.f de 12 de 2011). *Nomsimple wire diagram.* Recuperado el 21 de 05 de 2014, de IEEE: http://www.ieeeghn.org/wiki/index.php/File:Nonsimple_wire_diagram.gif

Instituto Nacional de Estadística y Censos . (2012). *Tecnologías de la Información y Comunicaciones (TIC´S) 2012*. Recuperado el 21 de Febrero de 2014, de http://www.inec.gob.e

Kerckhoffs, A. (1883). *The information hiding homepage*. Recuperado el 10 de 08 de 2014, de http://www.petitcolas.net/fabien/kerckhoffs;

Medina Alvarado, F., & Marca Ludeña, V. M. (2006). *Uso de criptografía en la seguridad de la información en internte.* cuenca: tesis. Recuperado el 12 de 08 de 2014, de http://www.dspace.ups.edu.ec/bitstream/123456789/216/2/Capitulo%201.pdf

Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook Of Applied Cryptography* (Primera ed.). CRC Press. Obtenido de http://books.google.es/books?hl=es&lr=&id=nSzoG72E93MC&oi=fnd&pg=PA1&dq=MENEZES,+Alfred,+P.+van+Oorschot,+S.+Vanstone.+Handbook+of+Applied+Cryptography.+CRC+Press,+1996.&ots=MwyiDbmQcH&sig=MrBi3MMmHD-WcbF45AHzZEtR9Do#v=onepage&q=MENEZES%2C%20Alfred%2C%20P

Porras, P. S. (1992). *A State Tansition Analysis Tool For Intrusion Detecction.* Califonia. Obtenido de http://books.google.com.ec/books/about/STAT_a_State_Transition_Analysis_Tool_fo.html?id=TL-iHAAACAAJ&redir_esc=y

Rediris. (1997-2014). *Rediris*. Recuperado el 25 de 07 de 2014, de http://www.rediris.es/difusion/publicaciones/boletin/41-42/ponencia3.html

Rediris. (15 de 07 de 2002). *kerberos*. Recuperado el 10 de 06 de 2014, de Rediris: http://www.rediris.es/cert/doc/unixsec/node27.html

Segu.Info. (2000). *Tipos de Firewall-Filtrado de Paquetes.* Recuperado el 10 de 08 de 2014, de Segu.Info.: http://www.segu-info.com.ar/firewall/filtradopaquetes.htm

Stallings, W. (2004). *Fundamentos de Seguridad en Redes Aplicaciones y Estandares* (segunda ed.). Madrid: Pearson Eduaccion, S.A. Obtenido de http://books.google.es/books?id=cjsHVSwbHwoC&pg=PA2&dq=fundamentos+de+la+seguridad+de+la+informacion+y+estandares&hl=es-419&sa=X&ei=E7veU8ztJsagyASA14K4DA&ved=0CDoQ6AEwAA#v=onepage&q&f=false

Teknoplof. (5 de 07 de 2010). *La necesidad de ocultar: desde la escítala a la criptografía cuántica*. Recuperado el 21 de 05 de 2014, de telnoPlof: http://www.teknoplof.com/tag/vigenere/

Timerime. (s.f.). *TimeRime.com - Historia de la Criptografía Linea de tiempo*. Recuperado el 2014 de 05 de 20, de http://timerime.com/es/evento/2782374/Cifrado+de+Alberti/

UGR. (s.f.). *www.ugr.es*. Recuperado el 2014 de 05 de 20, de http://www.ugr.es/~anillos/textos/pdf/2010/EXPO-1.Criptografia/02a22.htm

Universidad Politecnica de Madrid. (s.f.). *Protocolo IPsec [Sistemas Operativos]*. Recuperado el 09 de 08 de 2014, de Facultad de Informática (UPM): http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec

UrlQuery. (19 de 08 de 2014). *www2.ucsg.edu.ec*. Obtenido de file:///C:/Users/RENACER/Dropbox/scaneo%20de%20la%20red%20UCSG/urlquery.net%20-%20Free%20url%20scanner.htmfile:///C:/Users/RENACER/Dropbox/scaneo%20de%20la%20red%20UCSG/urlquery.net%20-%20Free%20url%20scanner.htm

ANEXOS

Updated by: 4634, 6234 INFORMATIONAL
Errata Exist
Network Working Group
Request for Comments: 3174
Category: Informational

D. Eastlake, 3rd
Motorola
P. Jones
Cisco Systems

September 2001

US Secure Hash Algorithm 1 (SHA1)

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Abstract

The purpose of this document is to make the SHA-1 (Secure Hash Algorithm 1) hash algorithm conveniently available to the Internet community. The United States of America has adopted the SHA-1 hash algorithm described herein as a Federal Information Processing Standard. Most of the text herein was taken by the authors from FIPS 180-1. Only the C code implementation is "original".

Acknowledgements

Most of the text herein was taken from [FIPS 180-1]. Only the C code implementation is "original" but its style is similar to the previously published MD4 and MD5 RFCs [RFCs 1320, 1321].

The SHA-1 is based on principles similar to those used by Professor Ronald L. Rivest of MIT when designing the MD4 message digest algorithm [MD4] and is modeled after that algorithm [RFC 1320].

Useful comments from the following, which have been incorporated herein, are gratefully acknowledged:

Tony Hansen
Garrett Wollman

Network Working Group
Request for Comments: 2420
Category: Standards Track

H. Kummert
Nentec GmbH

September 1998

The PPP Triple-DES Encryption Protocol (3DESE)

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Abstract

The Point-to-Point Protocol (PPP) [1] provides a standard method for transporting multi-protocol datagrams over point-to-point links.

The PPP Encryption Control Protocol (ECP) [2] provides a method to negotiate and utilize encryption protocols over PPP encapsulated links.

This document provides specific details for the use of the Triple-DES standard (3DES) [6] for encrypting PPP encapsulated packets.

Table of Contents

Network Working Group
Request for Comments: 1636
Category: Informational

R. Braden
ISI
D. Clark
MIT Laboratory for Computer Science
S. Crocker
Trusted Information Systems, Inc.
C. Huitema
INRIA, IAB Chair

June 1994

Report of IAB Workshop on

Security in the Internet Architecture

February 8-10, 1994

Status of this Memo

This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Abstract

This document is a report on an Internet architecture workshop, initiated by the IAB and held at USC Information Sciences Institute on February 8-10, 1994. This workshop generally focused on security issues in the Internet architecture.

This document should be regarded as a set of working notes containing ideas about security that were developed by Internet experts in a broad spectrum of areas, including routing, mobility, realtime service, and provider requirements, as well as security. It contains some significant diversity of opinions on some important issues. This memo is offered as one input in the process of developing viable security mechanisms and procedures for the Internet.

this mode while another protocol is using the Record Protocol as a transport for negotiating security parameters.

The TLS Record Protocol is used for encapsulation of various higher level protocols. One such encapsulated protocol, the TLS Handshake Protocol, allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. The TLS Handshake Protocol provides connection security that has three basic properties:

- The peer's identity can be authenticated using asymmetric, or public key, cryptography (e.g., RSA [RSA], DSS [DSS], etc.). This authentication can be made optional, but is generally required for at least one of the peers.

- The negotiation of a shared secret is secure: the negotiated secret is unavailable to eavesdroppers, and for any authenticated connection the secret cannot be obtained, even by an attacker who can place himself in the middle of the connection.

- The negotiation is reliable: no attacker can modify the negotiation communication without being detected by the parties to the communication.

One advantage of TLS is that it is application protocol independent. Higher level protocols can layer on top of the TLS Protocol transparently. The TLS standard, however, does not specify how protocols add security with TLS; the decisions on how to initiate TLS handshaking and how to interpret the authentication certificates exchanged are left up to the judgment of the designers and implementors of protocols which run on top of TLS.

z	0	0.01	0.02	0.03	0.04	0.05	0.06	0.07	0.08	0.09
0.0	0.5000	0.5040	0.5080	0.5120	0.5160	0.5199	0.5239	0.5279	0.5319	0.5359
0.1	0.5398	0.5438	0.5478	0.5517	0.5557	0.5596	0.5636	0.5675	0.5714	0.5753
0.2	0.5793	0.5832	0.5871	0.5910	0.5948	0.5987	0.6026	0.6064	0.6103	0.6141
0.3	0.6179	0.6217	0.6255	0.6293	0.6331	0.6368	0.6406	0.6443	0.6480	0.6517
0.4	0.6554	0.6591	0.6628	0.6664	0.6700	0.6736	0.6772	0.6808	0.6844	0.6879
0.5	0.6915	0.6950	0.6985	0.7019	0.7054	0.7088	0.7123	0.7157	0.7190	0.7224
0.6	0.7257	0.7291	0.7324	0.7357	0.7389	0.7422	0.7454	0.7486	0.7517	0.7549
0.7	0.7580	0.7611	0.7642	0.7673	0.7704	0.7734	0.7764	0.7794	0.7823	0.7852
0.8	0.7881	0.7910	0.7939	0.7967	0.7995	0.8023	0.8051	0.8078	0.8106	0.8133
0.9	0.8159	0.8186	0.8212	0.8238	0.8264	0.8289	0.8315	0.8340	0.8365	0.8389
1	0.8413	0.8438	0.8461	0.8485	0.8508	0.8531	0.8554	0.8577	0.8599	0.8621
1.1	0.8643	0.8665	0.8686	0.8708	0.8729	0.8749	0.8770	0.8790	0.8810	0.8830
1.2	0.8849	0.8869	0.8888	0.8907	0.8925	0.8944	0.8962	0.8980	0.8997	0.9015
1.3	0.9032	0.9049	0.9066	0.9082	0.9099	0.9115	0.9131	0.9147	0.9162	0.9177
1.4	0.9192	0.9207	0.9222	0.9236	0.9251	0.9265	0.9279	0.9292	0.9306	0.9319
1.5	0.9332	0.9345	0.9357	0.9370	0.9382	0.9394	0.9406	0.9418	0.9429	0.9441
1.6	0.9452	0.9463	0.9474	0.9484	0.9495	0.9505	0.9515	0.9525	0.9535	0.9545
1.7	0.9554	0.9564	0.9573	0.9582	0.9591	0.9599	0.9608	0.9616	0.9625	0.9633
1.8	0.9641	0.9649	0.9656	0.9664	0.9671	0.9678	0.9686	0.9693	0.9699	0.9706
1.9	0.9713	0.9719	0.9726	0.9732	0.9738	0.9744	0.9750	0.9756	0.9761	0.9767
2	0.9772	0.9778	0.9783	0.9788	0.9793	0.9798	0.9803	0.9808	0.9812	0.9817
2.1	0.9821	0.9826	0.9830	0.9834	0.9838	0.9842	0.9846	0.9850	0.9854	0.9857
2.2	0.9861	0.9864	0.9868	0.9871	0.9875	0.9878	0.9881	0.9884	0.9887	0.9890
2.3	0.9893	0.9896	0.9898	0.9901	0.9904	0.9906	0.9909	0.9911	0.9913	0.9916
2.4	0.9918	0.9920	0.9922	0.9925	0.9927	0.9929	0.9931	0.9932	0.9934	0.9936
2.5	0.9938	0.9940	0.9941	0.9943	0.9945	0.9946	0.9948	0.9949	0.9951	0.9952
2.6	0.9953	0.9955	0.9956	0.9957	0.9959	0.9960	0.9961	0.9962	0.9963	0.9964
2.7	0.9965	0.9966	0.9967	0.9968	0.9969	0.9970	0.9971	0.9972	0.9973	0.9974
2.8	0.9974	0.9975	0.9976	0.9977	0.9977	0.9978	0.9979	0.9979	0.9980	0.9981
2.9	0.9981	0.9982	0.9982	0.9983	0.9984	0.9984	0.9985	0.9985	0.9986	0.9986
3	0.9987	0.9990	0.9993	0.9995	0.9997	0.9998	0.9998	0.9999	0.9999	1.0000

RSIDAD CATÓLICA
IAGO DE GUAYAQUIL

CC-PI-0880-2014

UNIVERSIDAD CATÓLICA SANTIAGO DE GUAYAQUIL
FACULTAD TECNICA
RECIBIDO
2014
Marlene Chóez López
ASISTENTE DE DECANATO

Guayaquil, 5 de agosto de 2014

Ingeniero
Manuel Romero
Decano(e)
Facultad Técnica

ING.
FRSIN VÉLEZ
6/08/2014

De mis consideraciones:

En atención al oficio DFT-0165-2014 en el cual solicita información de la seguridad de la red de datos de la UCSG para una tésis de grado, cumplo en informarle que, por razones de seguridad es posible darle exclusivamente información de tipo general de las seguridades implantadas en la red de datos, por lo que se sugiere una reunión con el Ing. Ronald Ramírez Piza, Jefe de Producción, para hablar de los temas indicados, el miércoles 13 de agosto a las 17h30, con el personal de la tesis, en la sala de Sesiones del Centro de Cómputo.

Particular que informo a ud, para los fines pertinentes.

Atentamente,

Ing. Vicente Gallardo
Director del Centro de Cómputo

C.C: **Archivo**
RRP

9-01-4671
2206951
– Ecuador