UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

TESIS DE GRADO

TEMA:

"IMPLEMENTACIÓN DE SEGURIDADES MEDIANTE CRIPTOGRAFÍA PARA SERVIDORES BASADOS EN SOFTWARE LIBRE, PARA EL LABORATORIO DE REDES DE LA CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES, DURANTE EL PERÍODO 2013".

TESIS PRESENTADA PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

Autor:

Anchatipán Navas Danilo Fernando

Director:

Ing. Galo Alfredo Flores Lagla

Asesor:

Dr. Telmo Edwin Vaca Cerda

Latacunga – Ecuador

Mayo 2015

FORMULARIO DE LA APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de Miembros del Tribunal de Grado, aprueban el presente Informe de Investigación de acuerdo a las disposiciones reglamentarias emitidas por la Universidad Técnica de Cotopaxi y por la Unidad Académica de Ciencias de la Ingeniería y Aplicadas; por cuanto, el postulante:

- Danilo Fernando Anchatipán Navas

Con la tesis, cuyo título es:

"IMPLEMENTACIÓN DE SEGURIDADES MEDIANTE CRIPTOGRAFÍA PARA SERVIDORES BASADOS EN SOFTWARE LIBRE, PARA EL LABORATORIO DE REDES DE LA CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES, DURANTE EL PERÍODO 2013".

Ha considerado las recomendaciones emitidas oportunamente y reúne los méritos suficientes para ser sometido al **Acto de Defensa de Tesis** en la fecha y hora señalada.

Por lo antes expuesto, se autoriza realizar los empastados correspondientes, según la normativa institucional.

Latacunga, mayo de 2015

Para constancia firman:

_____	_____
Ing. Segundo Corrales	*Dra. Anita Chancusi*
PRESIDENTE	**MIEMBRO**
_____	_____
Ing. Mario Banda	*Ing. Galo Flores*
OPOSITOR	**TUTOR (DIRECTOR)**

AUTORÍA

Los criterios emitidos en el presente trabajo de investigación **"IMPLEMENTACIÓN DE SEGURIDADES MEDIANTE CRIPTOGRAFÍA PARA SERVIDORES BASADOS EN SOFTWARE LIBRE, PARA EL LABORATORIO DE REDES DE LA CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES, DURANTE EL PERÍODO 2013"**, son de exclusiva responsabilidad del autor.

…….……..

Anchatipán Navas Danilo Fernando

0502601974

AVAL DEL DIRECTOR DE TESIS

En calidad de Director del Trabajo de Investigación sobre el tema:

"IMPLEMENTACIÓN DE SEGURIDADES MEDIANTE CRIPTOGRAFÍA PARA SERVIDORES BASADOS EN SOFTWARE LIBRE, PARA EL LABORATORIO DE REDES DE LA CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES, DURANTE EL PERÍODO 2013"

Del señor estudiante; Anchatipán Navas Danilo Fernando, postulante de la Carrera de Ingeniería en Informática y Sistemas Computacionales.

CERTIFICO QUE:

Una vez revisado el documento entregado a mi persona, considero que dicho informe investigativo cumple con los requerimientos metodológicos y aportes científicos - técnicos necesarios para ser sometidos a la **Evaluación del Tribunal de Validación de Tesis,** que el Honorable Consejo Académico de la Unidad de Ciencias de la Ingeniería y Aplicadas de la Universidad Técnica de Cotopaxi designe para su correspondiente estudio y calificación.

Latacunga, mayo de 2015

EL DIRECTOR

……..

Ing. Galo Alfredo Flores Lagla

DIRECTOR DE TESIS

AVAL DEL ASESOR METODOLÓGICO

En calidad de **Asesor Metodológico** del Trabajo de Investigación sobre el tema:

"IMPLEMENTACIÓN DE SEGURIDADES MEDIANTE CRIPTOGRAFÍA PARA SERVIDORES BASADOS EN SOFTWARE LIBRE, PARA EL LABORATORIO DE REDES DE LA CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES, DURANTE EL PERÍODO 2013"

Del señor estudiante; Anchatipán Navas Danilo Fernando, postulante de la Carrera de Ingeniería en Informática y Sistemas Computacionales.

CERTIFICO QUE:

Una vez revisado el documento entregado a mi persona, considero que dicho informe investigativo cumple con los requerimientos metodológicos y aportes científicos - técnicos necesarios para ser sometidos a la **Evaluación del Tribunal de Validación de Tesis,** que el Honorable Consejo Académico de la Unidad de Ciencias de la Ingeniería y Aplicadas de la Universidad Técnica de Cotopaxi designe para su correspondiente estudio y calificación.

Latacunga, mayo de 2015

……..

Dr. Edwin Vaca Cerda

ASESOR METODOLÓGICO

CERTIFICADO

Mediante la presente certificación pongo a su consideración que Danilo Fernando Anchatipán Navas, con cédula de identidad No. 050260197-4, egresado de la Unidad Académica de Ciencias de la Ingeniería y Aplicadas ha implementado y desarrollado su Tesis de Grado en el Laboratorio de Redes de la Universidad Técnica de Cotopaxi con el tema: **"IMPLEMENTACIÓN DE SEGURIDADES MEDIANTE CRIPTOGRAFÍA PARA SERVIDORES BASADOS EN SOFTWARE LIBRE, PARA EL LABORATORIO DE REDES DE LA CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES, DURANTE EL PERIODO 2013"**, implementación que se ha desarrollado en forma correcta.

Es todo cuanto puedo certificar, permitiendo hacer uso del presente certificado para los fines legales pertinentes.

Latacunga, mayo del 2015

Atentamente,

…….

Ing. Segundo Corrales

DIRECTOR DE LA CARRERA

AGRADECIMIENTO

A mi familia, especialmente a mi esposa Susana Bastidas, que ha sido un pilar fundamental en la culminación de este proyecto de titulación, en tan prestigiosa institución de educación superior, Alama Mater de la provincia "Universidad Técnica de Cotopaxi".

Danilo A.

DEDICATORIA

A mis hijos, Ethan y Daniela; quienes en su inocencia permitieron que durante el desarrollo de este trabajo, les despojara del poco tiempo que tengo para disfrutar de sus travesuras y ocurrencias.

ÍNDICE DE CONTENIDOS

CAPÍTULO II

ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS DE LAS ENCUESTAS DIRIGIDAS A ESTUDIANTES Y DOCENTES, PARA APLICAR SEGURIDADES EN CORREO ELECTRÓNICO MEDIANTE CRIPTOGRAFÍA BASADO EN SOFTWARE LIBRE, PARA EL LABORATORIO DE REDES DE LA CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CONTENIDOS **PÁGS.**

RESUMEN

La presente investigación se fundamentó en la implementación de seguridades, mediante criptografía para correo electrónico basado en software libre; para el laboratorio de redes de la Carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi. Se consideró la inseguridad que existe al enviar o recibir mensajes de correo electrónico. Así, resolver este problema con la aplicación de correo electrónico seguro sobre una plataforma Linux. La investigación se desarrolló en base a la información recabada en libros publicados por expertos en seguridad informática. Se utilizó la encuesta como técnica para obtener las necesidades reales de la población, en cuanto al uso de criptografía para correo electrónico. Adicionalmente, para la aplicación se emplearon diversas tecnologías de software libre como: el cliente de correo electrónico Thunderbird, enigmail para cifrar y descifrar mensajes, sistema operativo Centos y las cuentas de usuario de varios proveedores de correo electrónico. Con esta implementación se consiguió garantizar la confidencialidad, integridad y disponibilidad de los mensajes.

ABSTRACT

This research was based in the implementation of security trough cryptography to mail, based on free software for the network laboratory of career Engineering in Computing and Computational Systems of the Technical University of Cotopaxi, It was considered the insecurity that exist to the send and receive clear emails, resolving this problem whit secure email application onto a Linux platform. The research was developed, in base to information collected from books published, for computer security experts; the survey, was used survey as a technique to get the actual requirements over dwellers that use the cryptography by emails. In addition to the application, was used diverse technologies free software, as the email client Thunderbird, enigmail to encrypt and decrypt messages, operating system Centos and user accounts of several providers email. Whit this implementation was got assure the confidentiality, integrity and availability messages.

AVAL DE TRADUCCIÓN

En calidad de Docente del Idioma Inglés del Centro Cultural de Idiomas de la Universidad Técnica de Cotopaxi; en forma legal CERTIFICO que: La traducción del resumen de tesis al Idioma Inglés presentado por el señor Egresado de la Carrera Ingeniería en Informática y Sistemas Computacionales de la Unidad Académica de Ciencias de la Ingeniería y Aplicadas: **ANCHATIPAN NAVAS DANILO FERNANDO**, cuyo título versa **"Implementación de Seguridades Mediante Criptografía para Servidores Basados en Software Libre, para el Laboratorio de Redes de la Carrera de Ingeniería en Informática y Sistemas Computacionales, Durante el Período 2013"**, lo realizó bajo mi supervisión y cumple con una correcta estructura gramatical del Idioma.

Es todo cuanto puedo certificar en honor a la verdad y autorizo al peticionario hacer uso del presente certificado de la manera ética que estimaren conveniente.

Latacunga, mayo del 2015

Atentamente,

Lic. Pablo Cevallos
DOCENTE CENTRO CULTURAL DE IDIOMAS

INTRODUCCIÓN

El acelerado crecimiento que experimenta la Informática en los últimos tiempos, hace posible que en la actualidad se comparta información inmediata sin importar el lugar. De la misma manera sube los índices de los delitos informáticos que día a día expertos realizan un sinnúmero de procedimientos que ayude a contrarrestar éstos ataques informáticos. Posteriormente se publica en libros sus avances en cuanto a seguridad informática; es así que, existe la suficiente información para que esta llegue a su destinatario sin modificaciones en su contenido o peor aún, que no llegue.

Con este antecedente, es preciso mencionar que se escriben muchos libros de seguridad informática y en todos existe el uso de criptografía como una técnica de seguridad. En la actualidad se utiliza con frecuencia para garantizar los canales de comunicación, las transacciones bancarias, el uso de páginas web y sobre todo para enviar o recibir cualquier tipo de información confidencial y segura, considerando que los algoritmos que esta técnica utiliza, está al alcance de cualquier persona. Sin embargo, no pueden ser descifrados ya que la seguridad de la criptografía no radica en la complejidad del algoritmo, sino en la dificultad que existe en descifrar la clave o contraseña, por tal razón la clave se convierte en la única llave capaz de descifrar un mensaje cifrado o viceversa.

La Carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi, fue creada en 1997 como respuesta a la demanda del mercado. Convirtiéndose rápidamente en una carrera deseada por el conglomerado estudiantil, en donde se realiza varias investigaciones, que aportan para el crecimiento tecnológico de la comunidad universitaria. Esta investigación no es la excepción, en virtud de que, es elaborada siguiendo varios aspectos metodológicos necesarios para la consecución de la Tesis como es la investigación científica.

Para lo cual, se recaba valiosa información de expertos que contribuyen a la elaboración del marco teórico. Además, se aplica una encuesta con preguntas dirigidas a los estudiantes de séptimo, octavo, noveno ciclo y a los docentes de la Carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi. Información necesaria para aplicar las seguridades mediante criptografía en el correo electrónico basado en software libre, en el laboratorio de redes de la Carrera, fortaleciendo de esta manera el grado de seguridad que debe existir en el envío o recepción de mensajes de correo electrónico.

La aplicación de criptografía se la realiza, en base a una serie de pruebas de funcionamiento revisando cuidadosamente todo el proceso de instalación de cada uno de los componentes de software libre, los mismos que son registrados en la Tesis, para que sirva de apoyo en futuras investigaciones relacionadas al tema.

Con la investigación se logra demostrar que es posible garantizar la confidencialidad, integridad y disponibilidad de la información utilizando herramientas de software libre, con la criptografía como actor principal en la búsqueda de soluciones para la seguridad de la información.

En el Capítulo I, se establece la fundamentación teórica-conceptual, en base a la información recopilada de libros que sustentan teorías definidas para el uso de criptografía en el servicio de correo electrónico; basado en software libre para el Laboratorio de Redes de la Carrera de Ingeniería en Informática y Sistemas Computacionales.

En el Capítulo II, se detalla el análisis e interpretación de los resultados obtenidos de las encuestas realizadas a los estudiantes de séptimo, octavo, noveno ciclo, y a los docentes de la carrera; para conocer las necesidades reales del uso de herramientas de cifrado en el correo electrónico, basado en software libre para la información segura, ratificando de esta manera la ejecución de la propuesta.

En el Capítulo III, se enfoca en la elaboración y desarrollo de la propuesta para aplicar seguridades en el correo electrónico mediante criptografía asimétrica basado en software libre en el Laboratorio de Redes de la Carrera de Ingeniería en Informática y Sistemas Computacionales.

Finalmente, se encuentra las conclusiones y recomendaciones que la investigación genera.

CAPÍTULO I

FUNDAMENTACIÓN TEÓRICA PARA LA APLICACIÓN DE SEGURIDADES EN EL CORREO ELECTRÓNICO MEDIANTE CRIPTOGRAFÍA BASADO EN SOFTWARE LIBRE, PARA EL LABORATORIO DE REDES DE LA CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI

1.1. Software libre

1.1.1. Concepto de software libre

STALLMAN, Richard, en su publicación *Software libre para una sociedad libre*, expresa que: "Software libre se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software; es decir, el software libre es un asunto de libertad, no de precio" revisado el 29 de abril de 2015, página 59.

Según el investigador, el software libre es la denominación del software que respeta la libertad de los usuarios y una vez desarrollado se puede: usar, copiar, estudiar, modificar y redistribuir libremente de varias formas, sin que esta redistribución sea necesariamente gratuita.

1.1.2. Libertades de los usuarios del software

STALLMAN, Richard, en su publicación *Software libre para una sociedad libre*, expresa: "Las libertades de los usuarios de software se clasifican en cuatro grupos que son:

- La libertad de usar el programa, con cualquier propósito (libertad 0).

- La libertad de estudiar cómo funciona el programa, y adaptarlo a tus necesidades (libertad 1). El acceso al código fuente es una condición previa para esto.

- La libertad de distribuir copias, con lo que puedes ayudar a tu vecino (libertad 2).

- La libertad de mejorar el programa y hacer públicas las mejoras a los demás, de modo que toda la comunidad se beneficie (libertad 3). El acceso al código fuente es un requisito previo para esto" revisado el 29 de abril de 2015, páginas 59-60.

Según el investigador, las libertades de los usuarios de software no deberían ser clasificadas, para ser libre no debe tener ninguna restricción para los usuarios en cuanto a la distribución de copias con modificaciones o no. Sean estas gratuitas o con alguna retribución económica para su distribución; es decir, que no es necesario pedir o pagar permisos para hacer esto.

Las libertades para los usuarios de software libre pueden limitarse o extenderse de acuerdo a la necesidad real de determinado programa; en virtud de que, en la actualidad existe una extensa gama de alternativas para casi el 100% de las actividades que se realizan y no necesariamente significa que no sea comercial.

1.1.3. Ventajas del software libre

- Libre distribución.
- Acceso a su código fuente.
- No tiene restricción en cuanto a quién tiene acceso.
- Bajo costo de adquisición.
- Innovación tecnológica.
- Independencia del proveedor.
- Adaptación del software

1.2. Sistema operativo Centos

WIKIPEDIA, en su publicación *Centos* (en línea), expresa que "El Sistema operativo CENTOS, tomado de las siglas en ingles de Community ENTerprise Operating System, CentOS es un sistema operativo de código abierto con funcionalidades empresariales gratuitas. Es un Clon a nivel binario de la distribución Linux Red Hat Enterprise Linux RHEL, compilado por voluntarios a partir del código fuente liberado por Red Hat" revisado el 03 de mayo de 2015.

SALINAS, Enrique, en su publicación *Sistema operativo Centos* (en línea), expresa que "El sistema operativo Centos es una distribución Linux de clase empresarial derivados de fuentes libremente ofrecidos al público y está basada en la distribución Red Hat Enterprise Linux (RHEL), pero gratuito, aunque no es mantenido por Red Hat" revisado el 03 de mayo de 2015.

Según el investigador, el sistema operativo Centos es un proyecto de libre distribución que nos brinda servicios a nivel empresarial gratuitamente.

1.2.1. Características del sistema operativo Centos

- Robusto.
- Estable.
- Seguro.
- Fácil de instalar.
- Fácil de utilizar.
- Compatible con las arquitecturas de procesamiento de 32 bits y 64 bits.
- Diseñado para servidores.
- Fácil mantenimiento.
- Infraestructura y respaldo de la comunidad.

1.2.2. Ventajas

- Cada una de las versiones recibe soporte y actualizaciones de seguridad frecuentemente hasta el lanzamiento de la siguiente versión, no por eso la versión anterior dejara de recibirla.
- De fácil mantenimiento.
- Es software libre de código abierto.
- Es gratuito.

1.3. Servidores informáticos

WIKIPEDIA, en su publicación *Servidor* (en línea), "Un servidor es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia. Los servidores se pueden ejecutar en cualquier tipo de computadora, incluso en computadoras dedicadas. En la mayoría de los casos una misma computadora puede proveer múltiples servicios y tener varios servidores en funcionamiento. La ventaja de montar un servidor en computadoras dedicadas es la seguridad", revisado el 08 de mayo de 2015.

Según el investigador, los servidores informáticos son equipos de cómputo robustos, con características industriales muy precisos y extremadamente veloces que proveen servicios a los usuarios que forman parte de la red.

1.3.1. Tipos de servidores informáticos

De acuerdo a la función que realice un servidor, se pueden detallar los siguientes tipos:

- Servidor de Aplicaciones (Application Servers).
- Servidor de Audio / Video (Audio/Video Servers).
- Servidor de Chat (Chat Servers).
- Servidor de Fax.
- Servidores FTP (FTP Servers).
- Servidores de Colaboración (Groupware).
- Servidores IRC (IRC Servers).
- Servidores Web (Web Servers).
- Servidores de Noticias (News Servers).
- Servidores Proxy (Proxy Servers).
- Servidor de Archivos.
- Servidor de Base de Datos (Database Servers).
- Servidores de Listas (List Servers).
- Servidor de Impresiones
- Servidor de Correo.
- Servidor de la Telefonía.
- Servidor de Reserva.
- Servidor Dedicado.
- Servidor No dedicado.
- Servidores TeLnet (TeLnet Servers).

1.3.2. Introducción a los servidores GNU/Linux

GÓMEZ, Ramón, en su publicación *10029 Administración de servidores Linux*, expresa que "Linux es un sistema operativo de la familia Unix, gratuito, creado mediante la política de código abierto. Estas características implican un gran ahorro en los costes de instalación de los equipos, pero también una mayor especialización por parte del personal informático" revisado el 08 de mayo de 2015, página 5.

Para el investigador, un servidor GNU/Linux es un equipamiento de software libre, que permite a los usuarios la libertad de modificar o distribuirlo de acuerdo a las necesidades, ahorrando dinero en su implementación, sin importar el número de equipos de cómputo en el que sea instalado y ofrece las siguientes características:

- Desempeña múltiples tareas en forma simultánea de forma segura y confiable.

- Los distintos servicios se pueden detener, iniciar o reiniciar independientemente sin afectar al resto del sistema, permitiéndonos operar las 24 horas del día, así como los 365 días del año.

1.4. Seguridad informática

1.4.1. ¿Qué es la seguridad informática?

COSTAS, Jesús, en su libro *Seguridad informática*, expresa que "La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización", página 19.

Según el investigador, la seguridad informática es el uso de los recursos tecnológicos de manera que, con la aplicación de herramientas de software adecuadas, garantizaremos que la información será revisada y modificada únicamente por quien tiene la autorización para hacerlo.

1.4.2. ¿Qué es la confidencialidad?

COSTAS, Jesús, en su libro *Seguridad informática,* expresa "La confidencialidad es la cualidad que debe poseer un documento o archivo para que sea leído únicamente por quien esté autorizado, persona o sistema", página 23.

MORIANO, Ariel, en su libro *Criptografía: técnicas de desarrollo para profesionales*, expresa que "La confidencialidad o privacidad de la información es el uso o aplicación principalmente de criptografía. Esto implica básicamente tener en secreto una información determinada", página 11.

Según el investigador, la confidencialidad es como su palabra lo expresa confidencial, es decir, nadie ni nada podrá tener acceso al contenido de información reservada o privada si no tiene el consentimiento para hacerlo.

1.4.3. ¿Qué es la integridad?

COSTAS, Jesús, en su libro *Seguridad informática*, expresa que "La integridad es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original", página 25.

MORIANO, Ariel, en su libro *Criptografía: técnicas de desarrollo para profesionales*, expresa que "Al hablar de comprobaciones o verificaciones de integridad nos estamos refiriendo al uso o aplicación de técnicas criptográficas

cada vez más utilizado popularmente, como respuesta a las nuevas formas de ataque de hackers, virus y troyanos", página 12.

Según el investigador, la integridad no es más que originalidad de la información, es decir, que ésta no ha sido modificada en ninguna parte del proceso envío-recepción por personas o medios no autorizados.

1.4.4. ¿Qué es la disponibilidad?

COSTAS, Jesús, en su libro *Seguridad informática*, expresa que "La disponibilidad se trata de la capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios autorizados cuando estos lo requieran", página 26.

Según el investigador, la disponibilidad es la condición que debe cumplir la información para estar presente cuando un usuario o sistema lo requiera. Esta debe también ser recuperable en el momento que se necesite; es decir, la información debe estar en el momento que el usuario requiera de ella.

1.4.5. ¿Qué es la autenticación?

COSTAS, Jesús, en su libro *Seguridad informática,* expresa que "La autenticación es la situación en la cual se puede verificar que un documento ha sido elaborado (o pertenece) a quien el documento dice. Otra manera de definirlo sería, la capacidad de comprobar si una determinada lista de personas ha establecido su reconocimiento sobre el contenido de un mensaje", página 28.

MORIANO, Ariel, en su libro *Criptografía: técnicas de desarrollo para profesionales*, expresa que "La autenticación o identificación implica hablar de la corroboración de la identidad de una entidad", página 12.

Según el investigador, la autenticación es la validación del documento o archivo a través de la verificación de la identidad de la persona o sistema que remite la información, esto puede lograrse si tenemos establecido un listado de personas o entidades.

1.4.6. ¿Qué es el no repudio?

COSTAS, Jesús, en su libro *Seguridad informática*, expresa que "El no repudio o irrenunciabilidad es un servicio de seguridad estrechamente relacionado con la autenticación y que permite probar la participación de las partes en una comunicación", página 28.

MORIANO, Ariel, en su libro *Criptografía: técnicas de desarrollo para profesionales*, expresa que "El no repudio consta de la implementación de un mecanismo o técnica, para prevenir que una entidad niegue un envío previo de información, un mensaje, una acción, etc.", página 13.

Según el investigador, el no repudio es la garantía de que la información no pueda ser negada por quien la envío cuando ésta llegue a su destino.

1.5. Amenazas en un sistema informático

COSTAS, Jesús, en su libro *Seguridad informática*, expresa que "Las amenazas a un sistema informático se pueden clasificar tanto en amenazas provocadas por:

- Personas
- Amenazas lógicas
- Amenazas físicas

1.5.1. Personas

La mayoría de ataques a un sistema va a provenir en última instancia de personas que, intencionada o inintencionadamente, pueden causarnos enormes pérdidas. Estas generalmente se dividen en dos grandes grupos: los atacantes pasivos aquellos que fisgonean por el sistema pero no lo modifican o destruyen y los activos aquellos que dañan el objeto atacado, o lo modifican en su favor (personal, ex empleados, curiosos, hackers, crackers, intrusos remunerados).

1.5.2. Amenazas lógicas

Bajo la etiqueta de 'amenazas lógicas' encontramos todo tipo de programas que de una u otra forma pueden dañar a nuestro sistema. Creados de forma intencionada para ello (software malicioso, también conocido como malware) o simplemente por error (Software incorrecto, herramientas de seguridad, puertas traseras, bombas lógicas, canales cubiertos, virus, gusanos, caballos de Troya, programas conejo o bacterias).

1.5.3. Amenazas físicas

Algunas de las amenazas físicas que pueden afectar a la seguridad y por tanto al funcionamiento de los sistemas son: robos, sabotajes, destrucción del sistema, cortes, subidas y bajadas bruscas de suministro eléctrico, condiciones atmosféricas adversas, las catástrofes naturales", páginas 32-36.

Según el investigador, las amenazas son todo ambiente hostil al cual está expuesta la información ya sea está provocada intencionalmente o involuntariamente por varios factores como son: humanos, tecnológicos o incluso naturales.

1.6. Esteganografía

MORIANO, Ariel, en su libro *Criptografía: técnicas de desarrollo para profesionales*, expresa que "La esteganografía trata como ocultar, dentro de un mensaje público, información secreta. En este caso, el hecho mismo de que existe información 'extra' a la original es un secreto", página 8.

Según el investigador, la esteganografía es la técnica de encubrir o esconder información muy importante dentro de documentos o mensajes visibles por cualquier persona o medio.

1.7. Criptología

El libro de *técnicas criptográficas de protección de datos*, expresa que "La Criptología (del griego criptos=oculto y logos=tratado, ciencia) es el nombre genérico con el que se designan dos disciplinas opuestas a la vez complementarias y son:

- Criptografía
- Criptoanálisis

La criptografía, se ocupa del diseño de procedimientos para cifrar, es decir, para enmascarar una determinada información de carácter confidencial.

El criptoanálisis, por su parte, se ocupa de romper esos procedimientos de cifrado para así recuperar la información original. Ambas disciplinas siempre se han desarrollado de forma paralela; pues, cualquier método de cifrado lleva siempre emparejado su Criptoanálisis correspondiente", página 1.

Según el investigador, la criptología es la ciencia encargada del estudio de dos técnicas opuestas y complementarias a su vez, como son la criptografía y el

criptoanálisis, la primera encargada de codificar la información y el criptoanálisis encargado de decodificar la misma.

1.8. Criptografía

GARCÍA, Alfonso y ALEGRE, María, en su libro *Seguridad informática*, expresan que "La criptografía consiste en ocultar la información de manera que quien la vea no pueda entender su significado. En donde se utiliza sobre todo a la hora de almacenar las claves, al enviar o recibir información, o bien a la hora de almacenar información a la que queremos proteger especialmente su privacidad", página 93.

COSTAS, Jesús, en su libro *Seguridad informática,* expresa que "La criptografía (del griego kripto, "oculto", y graphos, "escribir", literalmente "escritura oculta") es el arte o ciencia de cifrar y descifrar información mediante técnicas especiales y se emplea frecuentemente para permitir un intercambio de mensajes que solo puedan ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos", página 236.

Según el investigador, la criptografía es la técnica de codificar la información utilizando símbolos o signos que unidos o entrelazados entre si no sean entendidos y tampoco tengan ningún significado para quien tenga acceso al archivo. A pesar de intentar decodificar la información no sea posible realizarlo si no dispone de una clave especial o autorización para hacerlo.

1.8.1. Criptografía simétrica o de clave privada.

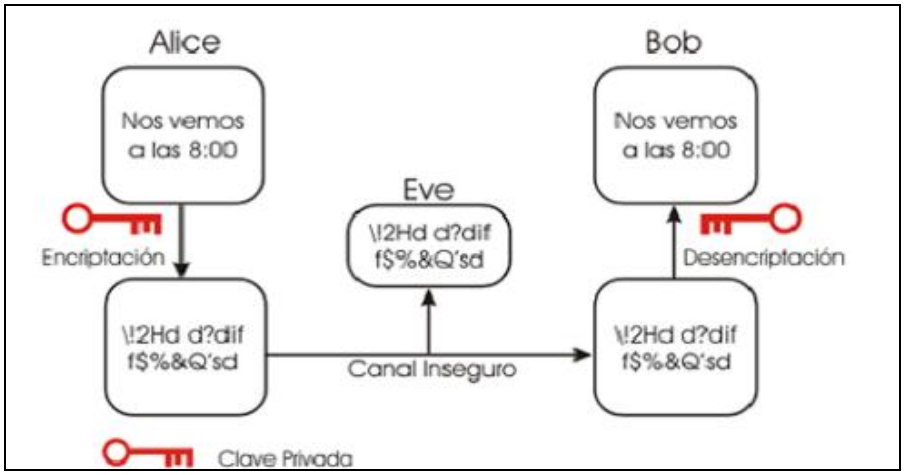
FAUSTER, Amparo y HERNÁNDEZ, Luis, en su libro *Criptografía, protección de datos y aplicaciones*, expresan que "La criptografía simétrica o de clave privada es más eficiente que la criptografía de clave pública al momento de cifrar y descifrar, por el hecho de que usan una sola clave para el proceso", página 176.

COSTAS, Jesús, en su libro *Seguridad informática,* expresa que "La criptografía simétrica o de clave privada es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes, las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez que ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma" página 239.

Según el investigador, la criptografía simétrica o de clave privada es la técnica en la que se utiliza una sola clave para cifrar y descifrar los mensajes. La misma que debe ser compartida con los usuarios del sistema, comprometiendo así, la información transmitida.

En la siguiente figura se ilustra el proceso de cifrado y descifrado con una clave privada, en donde Alice escribe un mensaje (Nos vemos a las 8:00) y lo encripta utilizando una clave privada (\!2Hd d?diff$%Q'sd) una vez que la información está en modo seguro es enviada a Bob, sin embargo durante su envió a través de un canal inseguro la información es atacada por Eve quien a su vez accede a la información encriptada (\!2Hd d?diff$%Q'sd) y sin la clave privada es imposible que descifre el mensaje; mientras que Bob utiliza la clave privada para descifrar el mensaje.

FIGURA 1. CRIPTOGRAFÍA DE CLAVE PRIVADA



Fuente:http://maytics.web44.net/web_documents/criptograf_a_sim_trica_y_asim_trica.pdf

A continuación se citan algunos algoritmos de criptografía simétrica.

- Algoritmo DES (Data Encryption Standar) Estándar para la Encriptación de Datos, usa una clave de 56 bits, es decir 2 elevado a la 56 claves posibles.

- Algoritmo 3DES (Triple DES), usa una clave de 128 bits.

- Algoritmo AES (Advanced Encryption Standar) Estándar para Encriptación Avanzada, usa una clave de 128, 196 o 256 bits.

- Algoritmo IDEA (International Data Encryption Algorithm) Algoritmo Internacional de Encriptación de Datos, usa una clave de 128 bits.

- Algoritmos Blowfish y Twofish, usan claves de hasta 448 bits.

1.8.2. Criptografía asimétrica o de clave pública

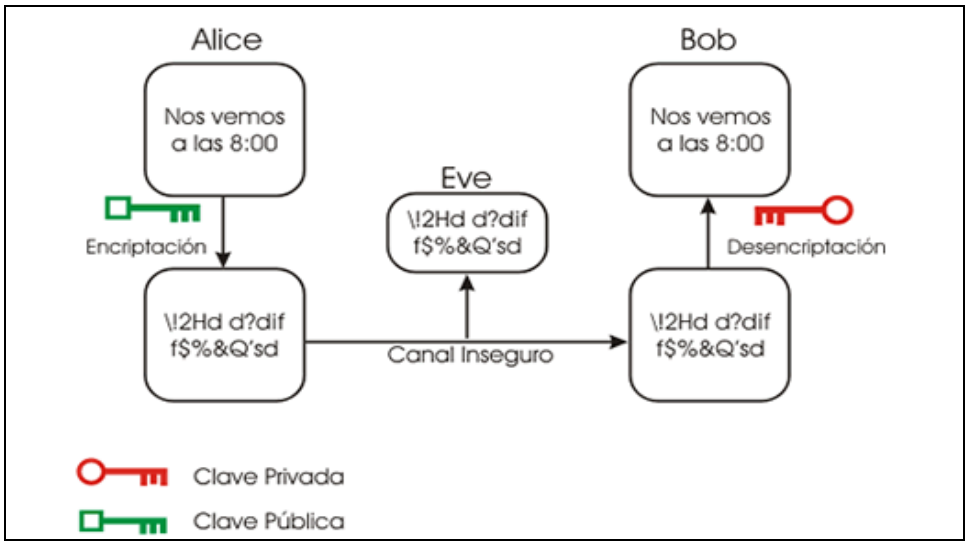
FAUSTER, Amparo y HERNÁNDEZ, Luis, en su libro *Criptografía*, expresan que "La criptografía asimétrica o de clave pública tiene como propiedad característica que cada usuario emplea dos claves en vez de una sola clave, como sucede con la criptografía simétrica. La clave pública es la que cada usuario da a conocer para que sea utilizada para cifrar los mensajes que se le envíen; la otra es la clave privada, que solo conoce dicho usuario y le permite descifrar los mensajes cifrados que recibe", página 174.

COSTAS, Jesús, en su libro *Seguridad informática*, expresa que "En la criptografía asimétrica o de clave pública, cada usuario del sistema criptográfico a de poseer un par de claves (una pública y una privada), esta pareja de claves es complementaría: lo que cifra una sólo lo puede descifrar la otra y viceversa", página 242.

Según el investigador, la criptografía asimétrica o de clave pública es la técnica en la cual se usan dos claves generadas simultáneamente, una pública y una privada, en donde la seguridad radica en la conservación de la clave privada como secreta, ya que si esta se encuentra comprometida toda la información se verá comprometida; lo que no sucede con la clave pública ya que ésta debe ser distribuida para el conocimiento de los usuarios.

En la siguiente figura se ilustra el proceso de cifrado con una clave pública y el proceso de descifrado con una clave privada, en donde Alice escribe un mensaje (Nos vemos a las 8:00) y lo encripta utilizando la clave pública de Bob (\!2Hd d?diff$%Q'sd) una vez que la información está en modo seguro es enviada a Bob; sin embargo, durante su envió a través de un canal inseguro, la información es atacada por Eve y accede a la información encriptada (\!2Hd d?diff$%Q'sd) pero sin la clave privada de Bob es imposible que descifre el mensaje; mientras que Bob utiliza su clave privada para descifrar el mensaje.

FIGURA 2. CRIPTOGRAFÍA DE CLAVE PÚBLICA



Fuente: http://maytics.web44.net/web_documents/criptograf_a_sim_trica_y_asim_trica.pdf

A continuación se citan algunos algoritmos de criptografía asimétrica.

- Algoritmo RSA, obtiene su nombre de las iniciales de los apellidos de sus creadores (Ron Rivest, Adi Shamir y Leonard Adleman), usa claves de 1024 bits pero se recomienda usar una clave de 2048 bits de longitud.

- Algoritmo DSA (Digital Signature Algorithm) Algoritmo de Firma Digital, usa claves de 512, 1024 y 2048 bits.

- Algoritmo Diffie-Hellman.

Según el investigador, la criptografía simétrica, se refiere a que tanto el emisor como el receptor del mensaje utilizan la misma clave, y que, por supuesto, debe ser secreta. En cambio, la criptografía asimétrica es más avanzada y más segura en vista de que su funcionamiento consiste en la existencia de dos claves, una denominada pública y otra privada, de tal manera que una información cifrada por una clave pública solo puede ser descifrada por la otra clave privada. Sin embargo, se debe aclarar que la criptografía asimétrica no reemplaza a la criptografía simétrica, en razón de que, cada técnica ofrece soluciones a problemas diferentes.

1.8.3. Criptografía en el nivel de aplicación

MORIANO, Ariel, en su libro *Criptografía: técnicas de desarrollo para profesionales*, expresa que "Al hablar de criptografía en el nivel de aplicación, también podrían considerarse a los protocolos criptográficos estándares de alto nivel. Estos protocolos de alto nivel, entonces, como han de comunicarse las partes, que algoritmos de cifrado podrán utilizarse, especificaciones de formato de mensajes, etc. Dado el carácter práctico del libro, este capítulo, en realidad, tratara principalmente sobre aplicaciones que implementaron estos protocolos, algunos de los cuales han sido definidos formalmente o estandarizados luego o sobre la

marcha, es decir, después de aparecido en primera instancia el problema que lo implementaba", página 221.

Según el investigador, la criptografía en el nivel de aplicación es el uso en sí de las técnicas criptográficas para solucionar los problemas de inseguridad existentes en la actualidad en el manejo de la información agrupando todos los protocolos y técnicas necesarias para garantizar la seguridad de la información dentro de una red de comunicaciones.

1.8.3.1. Aplicaciones de criptografía de alto nivel

- SSL/TLS, SET y OpenSSL toolkit, el crecimiento explosivo de la World Wide Web para el comercio electrónico y la publicación de información de la más variada índole generó la necesidad de implementar diversos mecanismos de seguridad, varios de ellos basados en técnicas de criptografía moderna.

  Existen en la actualidad, en relación con lo anterior, dos estándares principales: Secure Sockets Layer (SSL) o Capa Segura de Sockets y Secure Electronic Transaction (STET) o transacción Electrónica Segura.

  OpenSSL se trata de un proyecto open-source o de código abierto y libre, que además de implementar un toolkit (kit o caja de herramientas) para los protocolos SSL v2/v3 y TLS v1, implementan una librería criptográfica de uso general sin restricciones.

- PGP, estándar OpenPGP y GnuPG, La historia se remonta al año 1991, cuando Phil Zimmermann autorizó la publicación de sistemas BBSs y foros de USENET, un programa de dominio público llamado Pretty Good Privacy (PGP).

OpenPGP. Fue en julio de 1997 cuando PGP Inc. Propone a la IETF que se desarrolle un estándar, llamado OpenPGP, para la normalización del protocolo y evitar el potencial caos, dada la creciente aparición de diversas implementaciones de PGP. La compañía le cedió a la IETF el permiso para utilizar el nombre OpenPGP para describir esta nueva norma, así como cualquier programa que la soportara. El IETF aceptó la propuesta e inició el Grupo de Trabajo OpenPGP.

GnuPG. Por GNU Privacy Guard, es la implementación completa y libre del estándar OpenPGP por parte del proyecto GNU, tal como se define en la RFC 4880. GnuPG permite cifrar y firmar datos y comunicaciones. Cuenta además con un versátil sistema de gestión de llaves, así como con módulos de acceso para todo tipo de directorios de llave pública.

- SSH y herramientas openSSH, Es una manera segura de conectarse a otro sistema informático. Se trata de un protocolo que implementa una alternativa segura al tradicional servicio "telnet" de los sistemas Unix. Se entiende, por lo general, como parte del paquete "ssh" a un utilitario para la copia segura de archivos ("scp") y un cliente ftp seguro ("sftp").

  Open SSH. Es una versión libre y open-source de las herramientas SSH para diferentes plataformas Unix. openSSH ofrece, además la capacidad de generar túneles de seguridad y varios métodos de autenticación y soporta todas las versiones actuales del protocolo SSH.

  Kerberos. Se trata de un protocolo de autenticación de red y está diseñado para proporcionar autenticación para aplicaciones de tipo cliente/servidor utilizando criptografía simétrica. Una implementación libre, de código abierto, de este protocolo ha sido desarrollada por el Instituto de Tecnología de Massachussets (MIT).

TrueCrypt. Se trata de una utilidad libre, open-sours, para encriptar discos o valúmenes en sistemas Windows Vista/XP, Mac OS X y Linux. Es una de las aplicaciones más populares en la materia.

AxCrypt. De la mano de la empresa Axantum Software AB, desarrolladora del programa para la encriptación de archivos llamado AxCrypt, disponemos de una útil herramienta para la encriptación de archivos integrada con el sistema operativo Windows.

STunnel. El sitio Web de este programa se encuentra en http://www.stunnel.org/. Se trata de *Wrapper* (o enmascarador, nivel de indirección, capa intermedia, etc.), que permitirá encriptar conexiones TCP dentro de, o aplicando el protocolo, SSL. Se encuentra disponible tanto para Unix como para entornos Windows.

- OpenVPN (Virtual Private Network o Red Privada Virtual). Esta metodología posibilita muchas veces establecer un canal seguro para nuestras aplicaciones distribuidas, para hacerlo a través de Internet.

  En lugar de pensar en la incorporación de criptografía en nuestra aplicación para la comunicación segura, puede considerarse la opción de establecer dentro de una red privada, o VPN, en las computadoras que ejecuten nuestra aplicación y así conseguir un medio seguro para la comunicación.

1.8.4. Funciones de una vía y Hash

MORIANO, Ariel, en su libro *Criptografía: técnicas de desarrollo para profesionales*, expresa que "Las funciones de un vía y Hash permiten computar un resultado de manera rápida, pero, en cambio, la obtención de la entrada a partir del resultado será prácticamente inviable. Esto quiere decir que siendo f la función de una vía, se podrá calcular f(x) de manera sencilla, pero obtener x demandará años,

aunque dispongamos de toda la capacidad de procesamiento que podamos adquirir.

El concepto principal de estas funciones es que tomarán como entrada una información o mensaje de longitud variable (una contraseña o los contenidos de un archivo que empaquete el instalador de un programa), que se denominará pre-imagen, para convertirlo en una información de salida de longitud fija (en el algoritmo MD5, por ejemplo, será de 128 bits de longitud; en SHA-1, de 160 bits). A esta salida se la denominará valor de Hash.

Estas instrucciones operan en una dirección (una vía); será posible calcular el valor HASH, a partir de una pre-imagen, pero será inviable generar una pre-imagen cuyo hash corresponda a un resultado en particular", página 31.

Según el investigador, las funciones de una vía y Hash, son técnicas seguras que se utilizan para distribuir información encriptada, Cuando se encripta una determinada información, ésta al multiplicar su volumen y su transmisión tardaría demasiado tiempo; sin embargo, al usar funciones de una vía y Hash se genera una muestra relativamente pequeña de la información, que únicamente podrá ser descifrada por la persona autorizada para hacerlo.

1.8.5. Firma digital

COSTAS, Jesús, en su libro *Seguridad informática*, expresa que "La firma digital permite al receptor verificar la autenticidad del origen de la información así como verificar que dicha información no ha sido modificada desde su generación. De este modo, la firma digital ofrece el soporte para la autenticación e integridad de los datos así como para el no repudio en origen, ya que la persona que origina mensaje firmado digitalmente no puede argumentar que no lo es", página 247.

Según el investigador, una firma digital al igual que una firma manuscrita sirve para validar la legitimidad de un documento y la autenticidad de quien lo firma.

Sin embargo, la firma digital es imposible falsificar siempre y cuando se mantenga la clave secreta segura.

1.8.6. Certificado digital

COSTAS, Jesús, en su libro *Seguridad informática,* expresa que "Un certificado digital es un documento electrónico que asocia una clave pública con la identidad de su propietario. En general un certificado digital es un archivo que puede emplear un software para firmar digitalmente archivos, en los cuales puede verificarse la identidad del firmante", página 250.

FAUSTER, Amparo y HERNÁNDEZ, Luis, en su libro *Criptografía, protección de datos y aplicaciones,* expresa que "Un certificado digital (o electrónico) es la versión digital de un certificado ordinario en el que se garantiza que la clave pública y el resto de la información contenida en el mismo pertenecen al usuario que se especifique en dicho certificado. La validez de dicha información está garantizada por una entidad pública reconocida, a modo de notario electrónico. Estos notarios se conocen como autoridades de certificación", página 249.

Los certificados digitales contienen, entre otras, la siguiente información:

- Identificación del certificado
- Identificador del algoritmo de firma digital que se emplea
- Nombre de la autoridad de certificación que emite el certificado y que garantiza su contenido
- Nombre o identidad del usuario del certificado
- Tipo de criptosistema de clave pública que emplea el usuario
- Clave pública del usuario
- Periodo de validez del certificado
- Firma digital de la autoridad que avala el certificado

Según el investigador, un certificado digital es un archivo electrónico generado por una autoridad certificadora para garantizar la autenticidad del usuario que la posee y sirve también para firmar digitalmente y cifrar información.

1.8.7. Correo electrónico seguro

FAUSTER, Amparo y HERNÁNDEZ, Luis, en su libro *Criptografía, protección de datos y aplicaciones*, expresa que "Un correo electrónico seguro le permite a un usuario recibir correos confidenciales, lo único que debe hacer es lograr que los posibles emisores obtengan su clave pública, que podrán usar para cifrar los mensajes a él dirigidos. Para ello basta que dicho usuario les envié su certificado digital. Quienes reciban este certificado solo tendrán que validarlo para asegurarse de que la clave que contiene es realmente de quien dice ser su propietario. A partir de ese momento, bastará con que emisor y receptor acuerden un software criptográfico capas de utilizar las claves contenidas en los certificados", página 252.

Según el investigador, el correo electrónico seguro no es más que el uso de las herramientas apropiadas para cifrar la información entre el emisor y el receptor.

1.9. Criptoanálisis

FAUSTER, Amparo y HERNÁNDEZ, Luis, en su libro *criptografía, protección de datos y aplicaciones*, expresan que "El criptoanálisis presenta dos tipos de ataques globales, que tienen en cuenta la actitud y objetivos del criptoanalista y que dan lugar a otros ataques más específicos: los cuales son los ataques activos y ataques pasivos.

Se especifica como ataque pasivo si el objetivo del atacante es el de monitorizar el canal de comunicación entre el emisor y el receptor, de modo que este tipo de ataque solo supone una amenaza para la confidencialidad de los datos.

Por otra parte se especifica como ataque activo, si el ataque intenta añadir, borrar o alterar la información transmitida por el canal de comunicación. En este caso el ataque amenaza no solo la confidencialidad de los datos, sino también su integridad y autenticidad.

Por lo que a continuación se enumeran diversos escenarios de ataques criptoanalíticos, desde lo que requieren un mínimo de conocimiento y recursos computacionales por parte del criptoanalista hasta los más irreales a la hora de llevarlos a la práctica.

1. Ataque sobre texto cifrado únicamente: se trata de un ataque pasivo en el que el criptoanalista tiene acceso solo al criptograma. El conocimiento sobre el texto claro es mínimo y se puede reducir al idioma en el que está escrito el mensaje original o alguna información sobre la distribución de textos claros desde un centro de cifrado. Los procedimientos criptográficos que sucumben a este escenario son buenos ejemplos de lo que no debe ser un elemento de cifrado.

2. Ataque sobre texto claro conocido: en este escenario se asume que el criptoanalista conoce una determinada parte del texto claro y su correspondiente texto cifrado. En donde se trata de que, a partir de ambos textos, se puede determinar la clave o al menos se pueda deducir una nueva porción de texto claro. Este tipo de escenario es altamente realista, puesto que el criptoanalista normalmente va a poder deducir alguna porción de texto claro que le permita situarse en estas condiciones; es lo que en Criptografía clásica se denominaba Método de la palabra probable.

3. Ataque sobre texto claro elegido: se trata de un ataque activo en el que el criptoanalista tiene la habilidad de poder cifrar un texto claro de su elección. En la práctica, esta situación puede darse cuando el dispositivo de cifrado, sin conocimiento de la clave, cae en manos del criptoanalista o cuando este puede enviar un texto claro de su elección al centro de cifrado

para que, posteriormente, el correspondiente criptograma sea enviado a un tercero. Este escenario es menos corriente, puesto que necesita una acción específica por parte del atacante.

4. Ataque adaptativo: este escenario es una variante del anterior en el que el criptoanalista puede conseguir un nuevo texto cifrado en función de otros criptogramas obtenidos anteriormente. Todos los textos cifrados corresponden a textos claros de su propia elección. Este ataque requiere una acción todavía más activa por parte del atacante. En la mayoría de los casos tal escenario es claramente irreal, aunque si tiene un alto interés teórico.

La eficacia de un ataque criptoanalítico se mide en términos de la cantidad de pares de texto claro/texto cifrado requeridos, del tiempo necesario para su criptoanálisis y de la probabilidad de éxito del ataque planteado", páginas 36-37.

Según el investigador, el criptoanálisis es la búsqueda del mejor ataque para encontrar debilidades de los sistemas criptográficos. Estos permitan romper su seguridad, sin el conocimiento de la información secreta. Para ello se debe estudiar a profundidad el diseño y las propiedades de los sistemas criptográficos.

CAPÍTULO II

ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS DE LAS ENCUESTAS DIRIGIDAS A ESTUDIANTES Y DOCENTES, PARA APLICAR SEGURIDADES EN CORREO ELECTRÓNICO MEDIANTE CRIPTOGRAFÍA BASADO EN SOFTWARE LIBRE, PARA EL LABORATORIO DE REDES DE LA CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI

2.1. Entorno de la Universidad Técnica de Cotopaxi

La descripción del entorno de la Universidad Técnica de Cotopaxi que se cita en éste capítulo se encuentra disponible en la página web institucional <www.utc.edu.ec>, link del cual se recabó la siguiente información en enero del 2014.

2.1.1. Antecedentes históricos

En Cotopaxi el anhelado sueño de tener una institución de Educación Superior se alcanza el 24 de enero de 1995.

Las fuerzas vivas de la provincia lo hacen posible, después de innumerables gestiones y teniendo como antecedente la Extensión que creó la Universidad Técnica del Norte.

El local de la UNE-C fue la primera morada administrativa; luego las instalaciones del colegio Luis Fernando Ruiz que acogió a los entusiastas universitarios; posteriormente el Instituto Agropecuario Simón Rodríguez, fue el escenario de las actividades académicas: para finalmente instalarse en casa propia, a merced de la adecuación de un edificio a medio construir que estaba destinado a ser Centro de Rehabilitación Social.

En la actualidad son cinco hectáreas las que forman el campus y 82 las del Centro Experimentación, Investigación y Producción Salache. Definiéndose con claridad la postura institucional ante los dilemas internacionales y locales; siendo una entidad que por principio defiende la autodeterminación de los pueblos, respetuosos de la equidad de género.

En los 20 años de vida institucional la madurez ha logrado ese crisol emancipador y de lucha en bien de la colectividad, en especial de la más apartada y urgida en atender sus necesidades. El nuevo reto institucional cuenta con el compromiso constante de sus autoridades hacia la calidad y excelencia educativa.

2.1.2. Filosofía institucional

2.1.2.1. Misión institucional

La Universidad Técnica de Cotopaxi, es pionera en desarrollar una educación para la emancipación; forma profesionales humanistas y de calidad; con elevado nivel académico, científico y tecnológico; sobre la base de principios de solidaridad, justicia, equidad y libertad, genera y difunde el conocimiento, la ciencia, el arte y la cultura a través de la investigación científica; y se vincula con la sociedad para contribuir a la transformación social-económica del país.

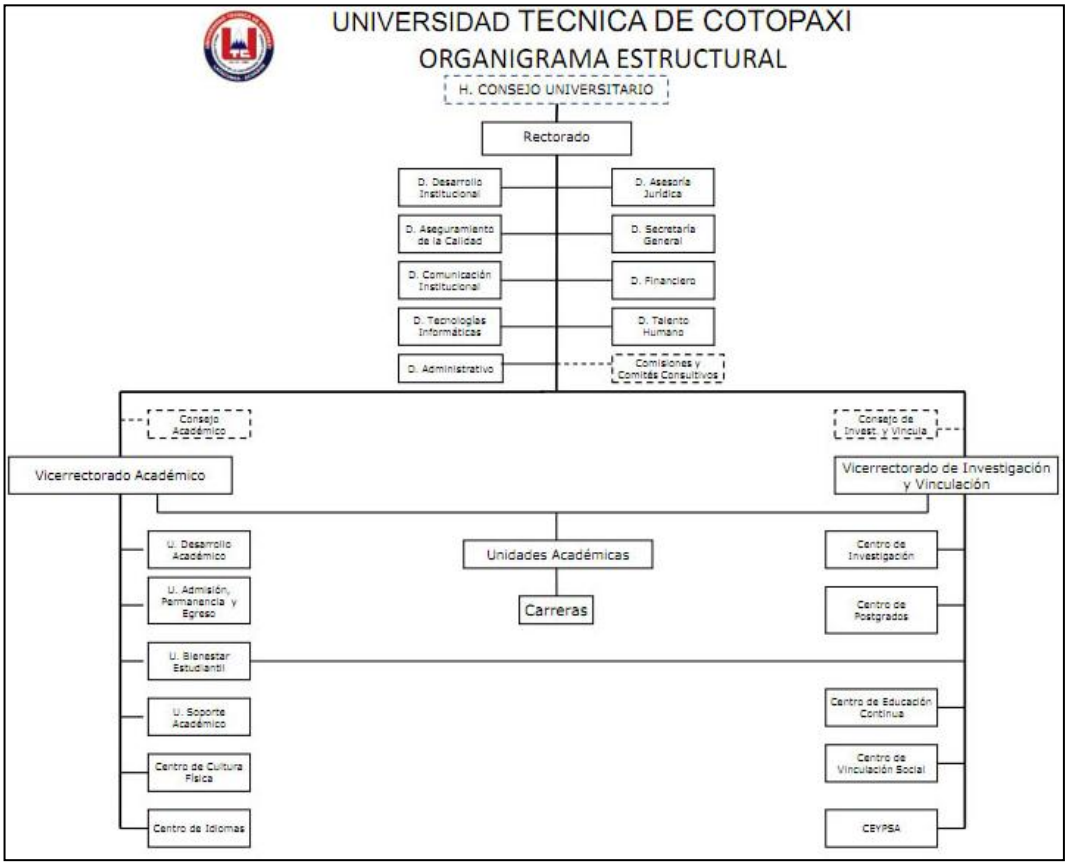
2.1.2.2. Visión institucional

En el año 2015 está previsto ser una universidad acreditada y líder a nivel nacional en la formación integral de profesionales críticos, solidarios y comprometidos en el cambio social; en la ejecución de proyectos de investigación que aporten a la solución de los problemas de la región y del país, en un marco de alianzas estratégicas nacionales e internacionales; dotada de infraestructura física y tecnología moderna, de una planta docente y administrativa de excelencia; que mediante un sistema integral de gestión le permite garantizar la calidad de sus proyectos y alcanzar reconocimiento social.

2.1.3. Organigrama estructural

A continuación se muestra el organigrama estructural.

FIGURA 3. ORGANIGRAMA ESTRUCTURAL U.T.C.



Fuente: http://www.utc.edu.ec/es-es/lautc/organigrama.aspx

2.1.4. Unidad Académica de Ciencias de la Ingeniería y Aplicadas (U.A.CIYA.)

2.1.4.1. Misión

Formar profesionales creativos, críticos y humanistas que utilizan el conocimiento científico y técnico, mediante la promoción y ejecución de actividades de investigación y aplicaciones tecnológicas para contribuir en la solución de los problemas de la sociedad.

2.1.4.2. Visión

Una Unidad Académica con un alto nivel científico, investigativo, técnico y profundamente humanista, generadora de tecnologías, con trabajos inter y multidisciplinario, que se concretan en proyectos investigativos, productivos, comunitarios y de prestación de servicios, a través de convenios con instituciones públicas y privadas, locales, nacionales e internacionales con una administración democrática, horizontal, vinculada con la sociedad.

2.1.5. Ingeniería en Informática y Sistemas Computacionales

La carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi, fue creada en el año de 1997 como respuesta a las demandas del mercado. Su pensum y programas de estudio se han venido actualizando periódicamente para mantenerlo al ritmo de los cambios de la disciplina y de la tecnología que se usa en la profesión.

El principio fundamental en el que se basa el pensum vigente es el concepto de aprendizaje en espiral, es decir en forma sucesiva se realiza pasadas a los contenidos de la profesión con un nivel de profundidad y detalle incremental.

La UTC propone la Carrera de Ingeniería en Informática y Sistemas Computacionales para preparar profesionales capaces de cumplir las demandas de

los usuarios informáticos en las organizaciones, con calidad, técnica, personal, moral y con profundo sentido social, para no solo ocupar puestos de trabajo sino ser capaces de generarlos en miras al desarrollo social del país.

Así mismo complementa la gama de carreras y especialidades que ofrece con ésta de gran impacto social y económico en el momento actual, además de ser capaz de autoabastecerse en la demanda de cursos en el área informática para otras carreras y soluciones informáticas que las dependencias de la institución requieren.

2.1.5.1. Misión

Formar profesionales creativos, críticos y humanistas que utilizan el conocimiento científico y técnico, mediante la promoción y ejecución de actividades de investigación y aplicaciones tecnológicas para contribuir en la solución de los problemas de la sociedad.

2.1.5.2 Visión

Una Unidad Académica con un alto nivel científico, investigativo, técnico y profundamente humanista, generadora de tecnologías, con trabajos inter y multidisciplinario, que se concretan en proyectos investigativos, productivos, comunitarios y de prestación de servicios, a través de convenios con instituciones públicas y privadas, locales, nacionales e internacionales con una administración democrática, horizontal, vinculada con la sociedad.

2.1.5.3. Perfil Profesional

El Ingeniero en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi, es un profesional con un dominio de la teoría y tecnología de punta tanto de hardware como de software, a través de:

- Planificar, analizar, diseñar, seleccionar, construir, operar, mantener, integrar, evaluar, optimizar y auditar sistemas de información, aplicados en las áreas administrativas, técnicas, científicas y sociales.

- Analizar, diseñar e implementar Sistemas Informáticos.

- Proveer tecnologías de mejoramiento de procesos organizacionales.

- Aplicar y construir metodologías y planes de acción para enfrentar problemas informáticos a corto, mediano y largo plazo.

- Diseñar, implementar y administrar redes de computadoras y sistemas digitales.

- Aplicar software utilitario y paquetes informáticos.

- Asesorar procesos de evaluación y control de plataformas de Hardware y Software.

- Incorporar los avances de la tecnología de la informática en la investigación científica.

- Analizar, construir y administrar bases de datos en distintas plataformas.

2.1.5.4. Campo Ocupacional

Los profesionales en Ingeniería Informática y Sistemas Computacionales, estarán capacitados para desarrollar sus actividades en empresas e instituciones a nivel nacional e internacional, donde se manejen tecnologías de la información y comunicación.

2.1.5.5. Infraestructura tecnológica del laboratorio de redes

La Carrera de Ingeniería en Informática y Sistemas Computacionales cuenta con un moderno laboratorio de redes, el mismo que fue implementado con el fin de cubrir las necesidades de la carrera, relacionadas con la falta de infraestructura tecnológica de punta indispensable para realizar prácticas de laboratorio y aplicar los conocimientos teóricos adquiridos por los señores estudiantes en las aulas de clase. De esta manera, el laboratorio de redes contribuirá con la actualización de conocimientos teóricos y con el fortalecimiento de habilidades prácticas que serán de muchísima importancia el momento de aplicar estas cualidades en la vida profesional.

El Laboratorio de Redes de la Carrera de Ingeniería en Informática y Sistemas Computacionales está compuesto por el siguiente equipamiento:

- 5 computadores de escritorio marca HP, modelo Compaq 6300 pro, procesador Intel CORE i7, disco duro de 500 Gb, memoria RAM de 2Gb DDR3 SDRAM, mainboard Intel Q75 Express y procesador gráfico integrado Intel HD.

- 1 switch marca HP, modelo E2620-24, 24puertos 10/100+, 2 puertos 10/100/1000+.

- 2 servidores marca HP, modelo ProLiant DL380 G7, procesador Intel Xeon QuadCore E5640, 18 ranuras DIMM, memoria interna 6Gb/máximo 384 Gb, con una capacidad de almacenamiento de hasta 18 Tb.

- 1 router marca Cisco, modelo 2901, memoria RAM 128 Mb, memoria flash 64Mb, slots atm-wic.

- 1 acces point 3COM 8000, IEEE 802.11b, 11 Mbps, monitor SNMP.

- 1 UPS marca CDP, modelo UPO11-3AX, capacidad 3000 VA, 2400 W, 50/60 Hz, 110/115/120 Vca seleccionable.

2.2. Diseño de la investigación

2.2.1. Investigación bibliográfica

En esta investigación se recabó la información necesaria para documentar los conceptos teóricos en base a libros y publicaciones en internet de expertos en el área de la seguridad informática, enfocándonos principalmente en la criptografía como técnica para garantizar la seguridad de la información. Los datos recopilados ayudaron a estructurar el marco teórico para posteriormente realizar la investigación de campo. En base a los nuevos conocimientos adquiridos con la investigación bibliográfica se aplica las seguridades mediante criptografía para el uso del correo electrónico basado en software libre, en el Laboratorio de Redes de la Carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi.

2.2.2. Investigación de campo

Con esta investigación se consigue valorar la necesidad real que existe para implementar la Tesis; ya que, se elaboró una encuesta de 9 preguntas, dirigida a estudiantes de séptimo, octavo y noveno ciclo, y a docentes de la Carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi. Se efectuó un acercamiento con los estudiantes, lo que ha permitido aclarar la necesidad de la aplicación de criptografía en forma práctica.

2.2.3. Investigación aplicada

Finalmente se utilizó toda la información obtenida para desarrollar la investigación y obtener el conocimiento necesario y aplicar en la Tesis. Para conseguir esto fue preciso realizar varias pruebas de funcionamiento, aplicando

criptografía en la transmisión de mensajes utilizando el correo electrónico seguro sobre una plataforma de software libre.

2.3. Metodología de la investigación

2.3.1. Método Inductivo

Este método de investigación fue aplicado como instrumento de trabajo para establecer los procedimientos de recolección de información a través de la observación y el registro de datos para su posterior análisis, formulando criterios generales del proceso de investigación.

Con este método de investigación observamos que en la actualidad todas las personas universitarias utilizan el correo electrónico como medio de comunicación a través de la internet, y está claro que para realizar cualquier actividad (redes sociales, consultar calificaciones, subscripciones, etc) necesitan una cuenta de correo electrónico y existen muchos proveedores de este servicio, lo que no garantiza la seguridad de los mensajes.

En base a la experiencia que tenemos con el uso del servicio, asumimos que es seguro utilizarlo; sin embargo, se conoce de muchos casos de suplantaciones de identidad para acceder o enviar información, lo que no garantiza que el servicio de correo electrónico sea seguro.

Entonces, vamos a suponer que ningún correo electrónico es seguro, si este fuera el caso, nadie lo utilizaría; ahora, vamos a suponer que todos los correos electrónicos son seguros, en este caso, nadie desarrollaría soluciones para la seguridad informática. Esto quiere decir que, mientras la tecnología informática vaya creciendo, también crecerá la inseguridad.

Con este antecedente, se determinó que se deben mejorar continuamente los procedimientos de acceso a nuestras cuentas de correo electrónico y que se debe utilizar herramientas dedicadas reducir la inseguridad.

2.3.2. Método Deductivo

El método de deductivo fue aplicado como instrumento de conocimiento general, basado en que las personas tenemos la necesidad de sentirnos seguros en cualquier ámbito en el que nos encontremos. Este método nos ayudó a plantear una solución al problema de inseguridad al utilizar el correo electrónico.

Considerando que actualmente el servicio de correo electrónico es el más utilizado a nivel mundial, sabemos también que es el más atacado para obtener información reservada o para enviar información maliciosa. Con esta premisa, diremos que si es el más utilizado por las personas, también es el más atacado por las mismas, entonces debemos utilizar técnicas de seguridad para proteger la información.

2.4. Técnica e instrumento de investigación

De acuerdo a las características del objeto de estudio y a la población en la que se realizó la investigación, se utilizó la encuesta como técnica y el cuestionario como instrumento.

2.4.1. Encuesta

La encuesta es un procedimiento que le permite al investigador recabar la información de una parte de la población o una muestra. La misma que fue diseñada para los estudiantes de séptimo, octavo y noveno ciclo, y para docentes de la Carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi.

2.4.2. Cuestionario

El cuestionario es un instrumento que se emplea para obtener la información requerida. Están constituidos por una serie de preguntas escritas, predefinidas, secuenciadas y separadas por capítulos o temáticas específicas, con el propósito de que muestre la interrelación y las conexiones lógicas entre diferentes áreas.

El cuestionario está estructurado de la siguiente manera:

- Identificación de la entidad que realiza el estudio.
- Información de, a quienes está dirigida.
- Objetivo de la realización de la encuesta.
- Instrucciones para responder las preguntas.
- Y 9 preguntas cerradas fáciles de responder.

Este cuestionario se aplicó a estudiantes de séptimo, octavo, noveno ciclo, y a docentes de la Carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi.

2.5. Población

Para el desarrollo de esta investigación se consultó al señor Ing. Segundo Corrales, Director de la Carrera de Ingeniería en Informática y Sistemas Computacionales sobre el número de docentes de la carrera y el número de los señores estudiantes de séptimo, octavo y noveno ciclo fue consultado en la página web de la Universidad Técnica de Cotopaxi. Obteniendo la siguiente información: forman parte del personal docente 13 y estudiantes 68. Es decir, se han tomado en cuenta a 81 personas, entre estudiantes y docentes, que mantienen una relación directa con el laboratorio de redes de la Carrera.

2.6. Operacionalización de variables

TABLA 1. ANÁLISIS DE VARIABLES

HIPÓTESIS	VARIABLES	INDICADORES
La aplicación de seguridades para el correo electrónico mediante el uso de criptografía basada en software libre garantizará la integridad, disponibilidad, privacidad y no repudio de los mensajes en el Laboratorio de Redes de la Carrera de Ingeniería en Informática y Sistemas Computacionales de la "Universidad Técnica de Cotopaxi.	**V. Dependiente** - Garantizar la integridad, disponibilidad, privacidad y no repudio de la información en el Laboratorio de Redes de la Carrera de Ingeniería en Informática y Sistemas Computacionales de la "Universidad Técnica de Cotopaxi".	• Disponibilidad • Efectividad • No repudio • Resultados • Privacidad • Integridad • Accesibilidad
	V. Independiente La aplicación de técnicas de seguridad para correo electrónico mediante el uso de criptografía basada en software libre.	• Factibilidad • Funcionalidad • Beneficios • Fiabilidad • Privacidad

Fuente: Proyecto de investigación.
Elaborado por: El investigador

2.7. Análisis e interpretación de los resultados de las encuestas aplicadas a estudiantes de séptimo, octavo y noveno ciclo, y docentes de la Carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi.

2.7.1. Objetivo de la encuesta

- Recabar información para determinar la factibilidad del uso de criptografía como técnica de seguridad informática para el envío y recepción de mensajes de correo electrónico basado en software libre.

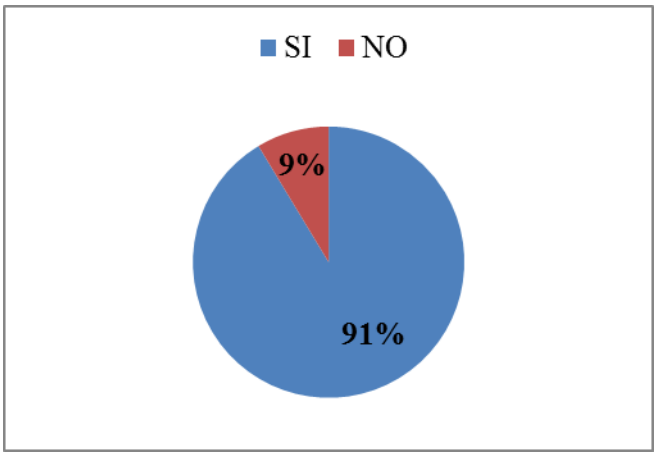
1.- ¿Utiliza actualmente usted software libre?

TABLA 2. UTILIZACIÓN DE SOFTWARE LIBRE

RESPUESTA	POBLACIÓN		TOTAL	PORCENTAJE
	DOCENTES	ESTUDIANTES		
SÍ	13	61	74	91%
NO	0	7	7	9%
TOTAL	13	68	81	100%

Fuente: Encuesta realizada a estudiantes de séptimo, octavo, noveno, y docentes de la Carrera de Sistemas.
Elaborado por: El investigador.

FIGURA 4. UTILIZACIÓN DE SOFTWARE LIBRE



Fuente: Encuesta realizada a estudiantes de séptimo, octavo, noveno, y docentes de la Carrera de Sistemas.
Elaborado por: El investigador.

Análisis e interpretación de resultados

El uso de software libre no es ningún impedimento para aplicar seguridades al servicio de correo electrónico basado en esta tecnología, para el laboratorio de redes de la Carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi, en virtud de que, la mayor parte de la población encuestada utiliza software libre, y la minoría que no lo utiliza debe informarse de las ventajas que ofrece esta tecnología.

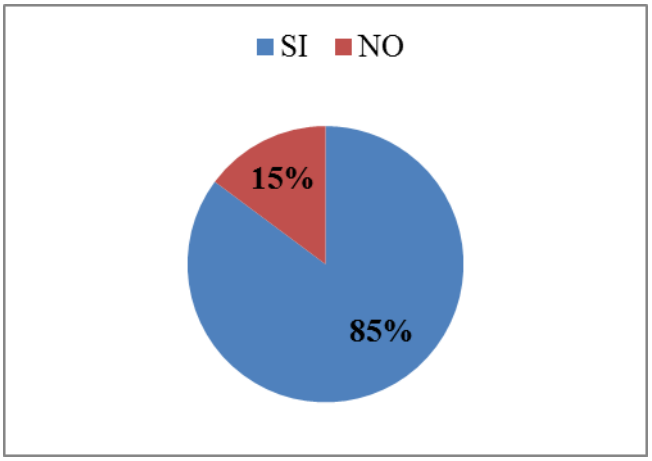
2.- ¿Conoce usted si se puede utilizar el correo electrónico mediante aplicaciones de software libre?

TABLA 3. USO DE CORREO ELECTRÓNICO MEDIANTE APLICACIONES DE SOFTWARE LIBRE

RESPUESTA	POBLACIÓN		TOTAL	PORCENTAJE
	DOCENTES	ESTUDIANTES		
SÍ	12	57	69	85%
NO	1	11	12	15%
TOTAL	13	68	81	100%

Fuente: Encuesta realizada a estudiantes de séptimo, octavo, noveno, y docentes de la Carrera de Sistemas.
Elaborado por: El investigador.

FIGURA 5. USO DE CORREO ELECTRÓNICO MEDIANTE APLICACIONES DE SOFTWARE LIBRE



Fuente: Encuesta realizada a estudiantes de séptimo, octavo, noveno, y docentes de la Carrera de Sistemas.
Elaborado por: El investigador.

Análisis e interpretación de resultados

La mayor parte de la población encuestada conoce que sí se puede utilizar el servicio de correo electrónico mediante aplicaciones de software libre, lo que quiere decir, que la aplicación de este proyecto de investigación está sustentada en forma teórica y su implantación servirá para poner en práctica estos conocimientos.

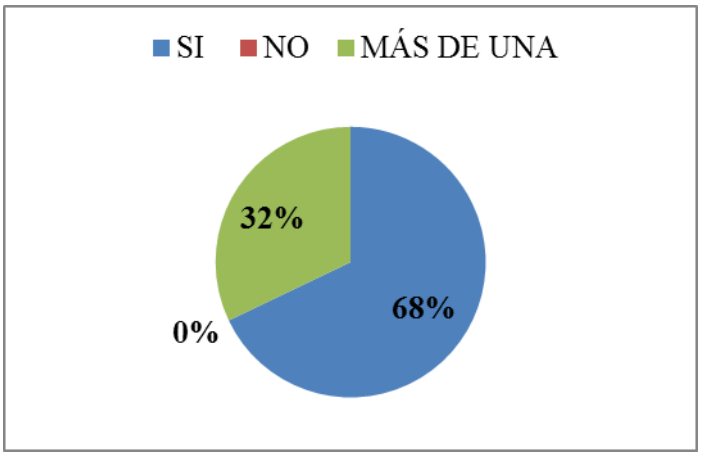
3.- ¿Dispone usted de una cuenta de correo electrónico?

TABLA 4. DISPONIBILIDAD DE UNA CUENTA DE CORREO ELECTRÓNICO

RESPUESTA	POBLACIÓN		TOTAL	PORCENTAJE
	DOCENTES	ESTUDIANTES		
SÍ	9	46	55	68%
NO	0	0	0	0%
MÁS DE UNA	4	22	26	32%
TOTAL	13	68	81	100%

Fuente: Encuesta realizada a estudiantes de séptimo, octavo y noveno, y docentes de la Carrera de Sistemas.
Elaborado por: El investigador.

FIGURA 6. DISPONIBILIDAD DE UNA CUENTA DE CORREO ELECTRÓNICO.



Fuente: Encuesta realizada a estudiantes de séptimo, octavo y noveno, y docentes de la Carrera de Sistemas.
Elaborado por: El investigador.

Análisis e interpretación de resultados.

La totalidad de la población encuestada, dispone de por lo menos una cuenta de correo electrónico, lo que ratifica que este servicio es el más utilizado por las personas para él envió y la recepción de mensajes, y a su vez será el servicio que más ataques reciba por parte de personas no autorizadas para acceder a información reservada.

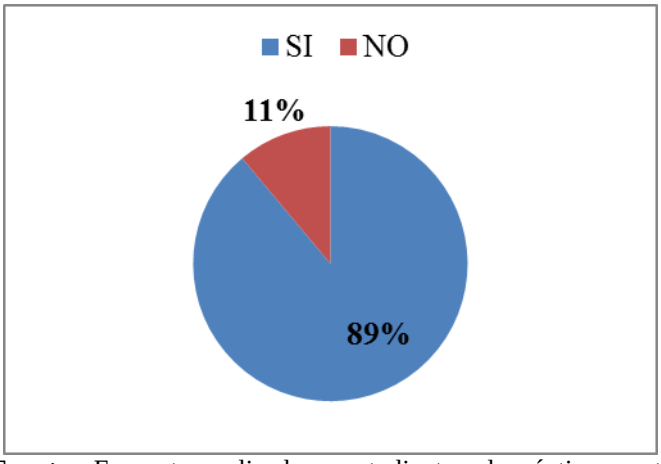
4.- ¿El uso del servicio de correo electrónico es significativo para su vida cotidiana?

TABLA 5. IMPORTANCIA DEL USO DEL SERVICIO DE CORREO ELECTRÓNICO

RESPUESTA	POBLACIÓN		TOTAL	PORCENTAJE
	DOCENTES	ESTUDIANTES		
SÍ	13	59	72	89%
NO	0	9	9	11%
TOTAL	13	68	81	100%

Fuente: Encuesta realizada a estudiantes de séptimo, octavo, noveno, y docentes de la Carrera de Sistemas.
Elaborado por: El investigador.

FIGURA 7. IMPORTANCIA DEL USO DEL SERVICIO DE CORREO ELECTRÓNICO



Fuente: Encuesta realizada a estudiantes de séptimo, octavo y noveno, y docentes de la Carrera de Sistemas.
Elaborado por: El investigador.

Análisis e interpretación de resultados

Para un gran número de la población encuestada es importante el servicio del correo electrónico en su vida diaria, considerando que el uso de este medio de comunicación en la actualidad es requerido casi en todas las actividades sociales, laborales, educativas, etc., que realizamos.

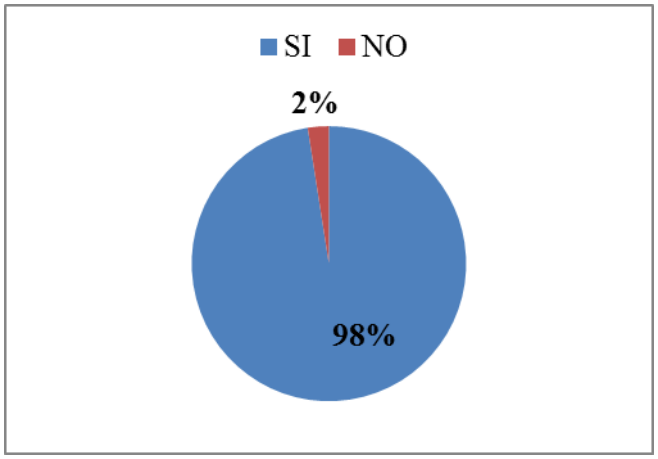
5.- ¿Es importante para usted la seguridad de la información que envía o recibe en un correo electrónico?

TABLA 6. IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN

RESPUESTA	POBLACIÓN		TOTAL	PORCENTAJE
	DOCENTES	ESTUDIANTES		
SÍ	13	66	79	98%
NO	0	2	2	2%
TOTAL	13	68	81	100%

Fuente: Encuesta realizada a estudiantes de séptimo, octavo, noveno, y docentes de la Carrera de Sistemas.
Elaborado por: El investigador.

FIGURA 8. IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN



Fuente: Encuesta realizada a estudiantes de séptimo, octavo, noveno, y docentes de la Carrera de Sistemas.
Elaborado por: El investigador.

Análisis e interpretación de resultados

Es evidente que la seguridad de la información que se envía o se recibe en un correo electrónico tiene un alto grado de importancia, por la misma razón el uso de este servicio ha generado, que la seguridad en el correo electrónico no sea un requerimiento, sino una necesidad.

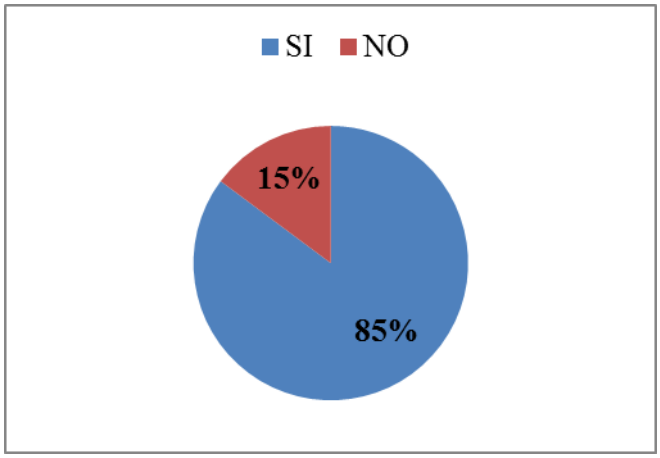
6.- ¿Conoce usted la existencia de factores que pongan en riesgo la seguridad del envió de un correo electrónico?

TABLA 7. EXISTENCIA DE FACTORES DE RIESGO PARA LA SEGURIDAD DE CORREO EELECTRÓNICO

RESPUESTA	POBLACIÓN		TOTAL	PORCENTAJE
	DOCENTES	ESTUDIANTES		
SÍ	12	57	69	85%
NO	1	11	12	15%
TOTAL	13	68	81	100%

Fuente: Encuesta realizada a estudiantes de séptimo, octavo, noveno, y docentes de la Carrera de Sistemas.
Elaborado por: El investigador.

FIGURA 9. EXISTENCIA DE FACTORES DE RIESGO PARA LA SEGURIDAD DE CORREO EELECTRÓNICO



Fuente: Encuesta realizada a estudiantes de séptimo, octavo, noveno, y docentes de la Carrera de Sistemas.
Elaborado por: El investigador.

Análisis e interpretación de resultados

Es bien conocido a nivel general que existen muchos factores que ponen en riesgo la seguridad de la información que viaja sobre una red de comunicaciones y aún más cuando se utiliza el correo electrónico como medio de comunicación. Sabemos que este servicio es el más utilizado en la actualidad, por esta razón, existe la necesidad de implementar un correo electrónico seguro, a fin de evitar ataques cibernéticos.

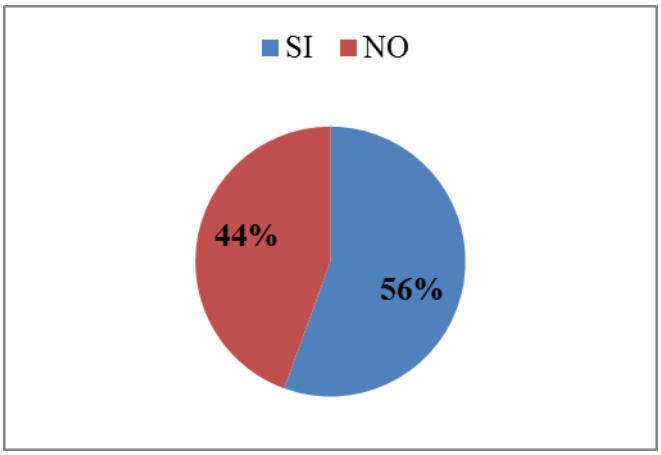
7.- ¿Sabe usted que es criptografía?

TABLA 8. CONOCIMIENTO DE CRIPTOGRAFÍA

RESPUESTA	POBLACIÓN		TOTAL	PORCENTAJE
	DOCENTES	ESTUDIANTES		
SÍ	11	34	45	56%
NO	2	34	36	44%
TOTAL	13	68	81	100%

Fuente: Encuesta realizada a estudiantes de séptimo, octavo, noveno, y docentes de la Carrera de Sistemas.
Elaborado por: El investigador.

FIGURA 10. CONOCIMIENTO DE CRIPTOGRAFÍA



Fuente: Encuesta realizada a estudiantes de séptimo, octavo, noveno, y docentes de la Carrera de Sistemas.
Elaborado por: El investigador.

Análisis e interpretación de resultados

A pesar de que el uso de criptografía se inició hace años atrás. Actualmente esta técnica no es muy conocida por los estudiantes encuestados. Todos están de acuerdo en que no existe seguridad en la red informática, sin embargo, muchos desconocen que la criptografía es la única herramienta utilizada para reducir los riesgos de ataque a la información, incluso que esta técnica bien aplicada elimina los riesgos.

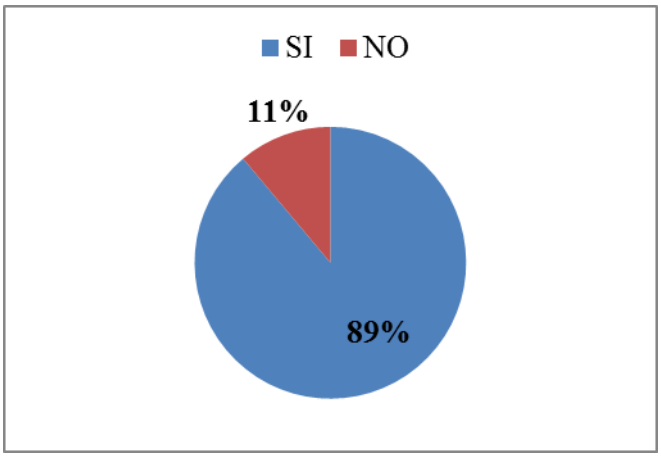
8.- ¿Cree usted necesaria la implementación de alguna técnica de cifrado para el envío o recepción de información a través del servicio de correo electrónico?

TABLA 9. IMPLEMENTACIÓN DE TÉCNICAS DE CIFRADO

RESPUESTA	POBLACIÓN		TOTAL	PORCENTAJE
	DOCENTES	ESTUDIANTES		
SÍ	11	61	72	89%
NO	2	7	9	11%
TOTAL	13	68	81	100%

Fuente: Encuesta realizada a estudiantes de séptimo, octavo, noveno, y docentes de la Carrera de Sistemas.
Elaborado por: El investigador.

FIGURA 11. IMPLEMENTACIÓN DE TÉCNICAS DE CIFRADO



Fuente: Encuesta realizada a estudiantes de séptimo, octavo, noveno, y docentes de la Carrera de Sistemas.
Elaborado por: El investigador.

Análisis e interpretación de resultados

Con los resultados conseguidos en esta pregunta, se hace evidente la necesidad de implementar seguridades mediante criptografía en el correo electrónico basado en software libre, en el laboratorio de redes de la Carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi, a pesar de que cierto número de encuestados no están de acuerdo.

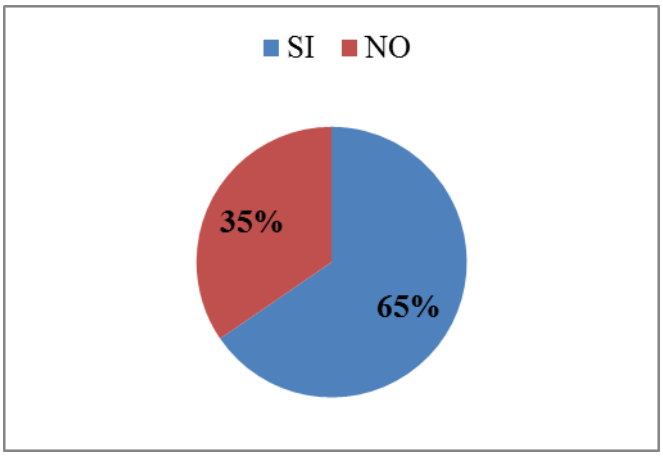
9.- ¿Considera usted que con el uso de criptografía para él envió de un correo electrónico se garantizará la seguridad de la información?

TABLA 10. GARANTÍA EN LA SEGURIDAD DE LA INFORMACIÓN

RESPUESTA	POBLACIÓN		TOTAL	PORCENTAJE
	DOCENTES	ESTUDIANTES		
SÍ	11	42	53	65%
NO	2	26	28	35%
TOTAL	13	68	81	100%

Fuente: Encuesta realizada a estudiantes de séptimo, octavo, noveno, y docentes de la Carrera de Sistemas.
Elaborado por: El investigador.

FIGURA 12. GARANTÍA EN LA SEGURIDAD DE LA INFORMACIÓN



Fuente: Encuesta realizada a estudiantes de séptimo, octavo, noveno, y docentes de la Carrera de Sistemas.
Elaborado por: El investigador.

Análisis e interpretación de resultados

No existe la suficiente certeza por parte de los encuestados que con el uso de criptografía se garantiza la seguridad de la información durante el envío de un correo electrónico; sin embargo, esta duda será aclarada en la realización de las respectivas pruebas de funcionamiento del servicio de correo electrónico seguro.

2.7.2. Análisis general de la encuesta aplicada a estudiantes de séptimo, octavo, noveno ciclo y a docentes de la Carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi.

La encuesta se aplicó a estudiantes de los últimos semestres de la Carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi, que tienen relación directa con el laboratorio de redes, con el fin de aprovechar sus conocimientos para solucionar el problema de inseguridad que existe al utilizar correo electrónico para las diversas actividades que realizamos diariamente.

De igual manera, se aplicó la misma encuesta a docentes de la Carrera, simplemente para corroborar los resultados expedidos por los estudiantes.

Es así que, una vez tabuladas las respuestas proporcionadas a cada una de las preguntas de la encuesta por parte de la población, se puede interpretar que la mayor parte está de acuerdo con casi todas las preguntas planteadas, a excepción de una, en la que se observa que aproximadamente la mitad de la población encuestada desconoce lo que es criptografía.

2.8. Verificación de la hipótesis

La hipótesis planteada expresa: "La aplicación de seguridades para correo electrónico mediante el uso de criptografía basada en software libre garantizará la integridad, disponibilidad, privacidad y no repudio de los mensajes en el Laboratorio de Redes de la Carrera de Ingeniería en Informática y Sistemas Computacionales de la "Universidad Técnica de Cotopaxi".

De los resultados obtenidos a través de la investigación de campo, con la elaboración de encuestas aplicadas al personal docente y señores estudiantes de séptimo, octavo y noveno ciclo de la Carrera de Ingeniería en Informática y

Sistemas Computacionales durante el proceso de esta investigación; se deduce que, con el uso de las herramientas de software libre y técnicas para la aplicación de seguridades mediante criptografía en el correo electrónico, se garantiza: la integridad, disponibilidad, privacidad y no repudio durante el proceso del intercambio de mensajes; cumpliendo así, con el objetivo planteado en la hipótesis de ésta investigación.

Así mismo, se determina que esta investigación demuestra en la práctica los conocimientos teóricos adquiridos durante la investigación bibliográfica, contribuyendo de esta manera al mejoramiento del aprendizaje a través de la práctica y fomentando en el personal docente el crecimiento académico con la búsqueda de nuevas tecnologías de seguridad basadas en software libre, como es la criptografía, tema principal de esta investigación que ha sido aplicada en el Laboratorio de Redes de la Carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi.

CAPÍTULO III

PROPUESTA PARA APLICAR SEGURIDADES EN CORREO ELECTRÓNICO MEDIANTE CRIPTOGRAFÍA BASADO EN SOFTWARE LIBRE, PARA EL LABORATORIO DE REDES DE LA CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI

3.1. Presentación de la propuesta de investigación

En la actualidad, el intercambio de información sobre una red tecnológica se ha desarrollado de tal manera que la comunicación es instantánea, sin importar la distancia en la que se encuentren ubicados los individuos, gracias al fácil acceso que tenemos para navegar en la Internet y a las herramientas informáticas que esta gran Red ofrece para comunicarnos. Esto hace que el proceso de enviar y recibir información sobre una red informática sea posible; sin embargo, el tráfico de información que viaja sobre esta gran red de redes no está segura de llegar a su destino íntegra ni confidencial, provocando que esta forma de comunicación no sea segura cuando utilizamos este recurso, debido al incontable número de usuarios que acceden diariamente a la Internet. Muchos de ellos con el fin de vulnerar la seguridad de la red y acceder a información no autorizada, la misma que debe ser privada para evitar el mal uso de la misma. La causa principal por la que estas intrusiones son posibles se deben a la falta de medidas de seguridad en el manejo de la información considerando que ésta, es el bien más preciado en

todos los ámbitos especialmente en algunos campos en los que se puede considerar más delicado preservar su privacidad, como en el sector financiero, el militar, el tributario, etc.

Para intentar reducir las amenazas que pueden afectar un sistema de información se han establecido un conjunto de procedimientos, dispositivos y herramientas que se van a encargar de asegurar la integridad, disponibilidad, privacidad y no repudio de la información.

En el Laboratorio de Redes de la Carrera de Ingeniería en Informática y Sistemas Computacionales de la "Universidad Técnica de Cotopaxi" se aplicó una medida de seguridad para proteger los mensajes enviados por e-mail, mediante el uso de criptografía utilizando Software Libre, a fin de demostrar didácticamente el uso de esta técnica para mantener a la información ilegible y garantizar que la misma llegue a su destino y sea descifrada mediante una clave por la persona autorizada; garantizando así un proceso de envío y recepción de información a través de un sistema de comunicación seguro (integridad, disponibilidad, privacidad y no repudio), como es el correo electrónico que en la actualidad es el servicio más utilizado en la Internet.

3.2. Justificación

La aplicación de seguridades en el correo electrónico mediante criptografía basado en software libre debe garantizar las características necesarias para que el intercambio de información sea seguro entre el remitente y el receptor. En la actualidad ya no es un requerimiento, es una necesidad, considerando que los servidores de correo electrónico no son de nuestra propiedad; en tal virtud, la ejecución de éste proyecto es factible desde el punto de vista económico, académico y de apoyo institucional, en razón de que, si ponemos en una balanza el valor que tiene la información que manejamos y el coste que tendría protegerla de intrusos sería plenamente justificada; además, se utilizarán técnicas de seguridad basadas en software libre. Académicamente se tendrán disponibles todas las herramientas necesarias para demostrar la funcionalidad de cada uno de

los elementos que hacen posible que la información viaje segura, al utilizar el servicio de correo electrónico y si hablamos de apoyo institucional esta investigación aportará al fortalecimiento del Laboratorio de Redes y será el primer paso que la Carrera de Ingeniería en Informática y Sistemas Computacionales de la "Universidad Técnica de Cotopaxi" realice para cumplir con la misión de preparar profesionales altamente prácticos y con profundos conocimientos teóricos.

La Internet es la red de comunicaciones más utilizada por todas las personas que tenemos acceso, a través de cuentas de usuario de correo electrónico con una clave de ingreso, a pesar de disponer y suponer que nuestra clave es segura podemos ser objeto de ataques informáticos; es decir, no se garantiza la seguridad de la información, esta es la causa por la que se debe implantar este proyecto y un argumento válido para realizar esta investigación es proporcionar al usuario final la certeza de que jamás perderá información valiosa, cuando utilice un medio de comunicación en el que la información viajará encriptada.

La implementación de criptografía para nuestro cliente del correo electrónico utilizando software libre, en el Laboratorio de Redes de la Carrera de Ingeniería en Informática y Sistemas Computacionales de la "Universidad Técnica de Cotopaxi". Es de especial trascendencia y utilidad práctica en el entorno académico, científico y técnico, considerando que la criptografía es una técnica que utiliza fórmulas matemáticas que se encargan de proporcionar seguridad a la información.

3.3. Objetivos

3.3.1. Objetivo General

- Aplicar un sistema de seguridad para el correo electrónico mediante la utilización de la criptografía asimétrica bajo el estándar PGP basado en software libre, en el laboratorio de redes de la carrera de Ingeniería en

Informática y Sistemas Computacionales de la "Universidad Técnica de Cotopaxi", para garantizar la integridad, privacidad y no repudio de la información.

3.3.2. Objetivos Específicos

- Utilizar herramientas de software libre para encriptar la información que será compartida a través del correo electrónico.

- Configurar los aplicativos de software libre para el servicio del correo electrónico Thunderbird en el sistema operativo Centos 6.6 con las características de seguridad que permitirá cifrar y descifrar los mensajes.

- Realizar pruebas de funcionamiento para validar la operatividad del aplicativo de seguridad.

3.4. Análisis de Factibilidad

3.4.1. Factibilidad Técnica

La propuesta para implementar criptografía como técnica de cifrado para los mensajes que luego serán compartidos a través del correo electrónico utilizando software libre, en el laboratorio de redes de la Carrera de Ingeniería en Informática y Sistemas Computacionales. Se considera técnicamente ejecutable, en razón de que, existe suficiente información y conocimiento por parte del investigador, además se analizó que el proyecto posee las características técnicas requeridas para la utilización de herramientas de software libre disponibles para diseñar, implementar, operar y mantener el proyecto.

Es así que, para la aplicación y demostración del uso de criptografía y garantizar la seguridad de la información durante el proceso de transmisión y recepción de

mensajes usando correo electrónico, utilizamos el siguiente equipamiento de hardware y software:

- Computadores de escritorio marca HP, modelo Compaq 6300 pro, procesador Intel CORE i7, disco duro de 500 Gb, memoria RAM de 2Gb DDR3 SDRAM, mainboard Intel Q75 Express y procesador gráfico integrado Intel HD.
- Oracle VM Virtual Box 4.3.8.
- Sistema Operativo CentOS 6.6.
- Cliente de correo electrónico Mozilla Thunderbird.
- Estándar de cifrado OpenPGP (Enigmail).
- Servidor de claves públicas keys.gnupg.net.

3.4.2. Factibilidad Económica.

Se determina que la propuesta es factible económicamente; debido a que, el laboratorio de redes de la Carrera de Ingeniería en Informática y Sistemas Computacionales, cuenta con el equipamiento de hardware requerido y tenemos acceso al software libre que se utilizará para su implementación.

3.4.3. Factibilidad Operacional.

La aplicación es factible operativamente debido a que se cuenta con los elementos necesarios para su manejo.

Considerando que la implementación de criptografía como técnica de seguridad para el envío y recepción de mensajes a través de correo electrónico está realizada con software libre, operativamente contará con el soporte y actualizaciones necesarias para funcionar sin problemas donde éste sea implantado.

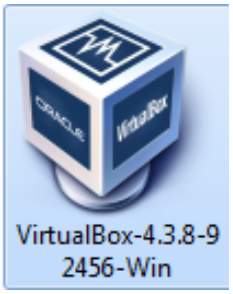
3.5. Desarrollo de la propuesta

3.5.1. Proceso de implementación de Virtual Box

Esta herramienta de virtualización es muy útil para simular la existencia de más de una máquina virtual denominada host, corriendo sobre uno o varios sistemas operativos, permitiéndonos ahorrar recursos de hardware y facilitándonos la instalación de software.

1.- Ejecutamos el programa Virtual Box, haciendo doble clic sobre el siguiente icono.

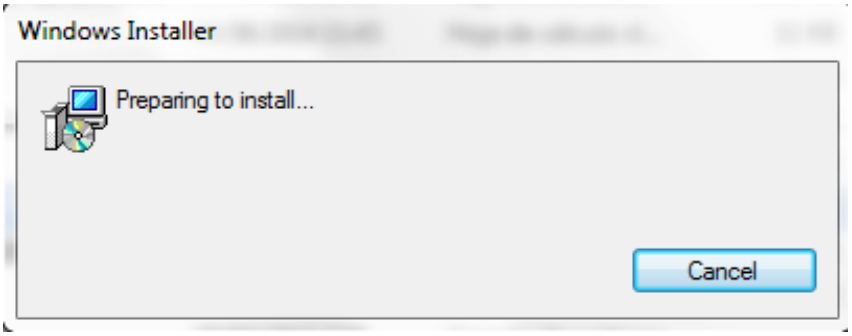
FIGURA 13. ÍCONO DE INSTALACIÓN DE VIRTUAL BOX



Fuente: Proceso de instalación de Virtual Box.
Elaborado por: El investigador.

2.- Windows Installer nos muestra que se está preparando la instalación de Virtual Box, en esta ventana podemos cancelar la instalación si es necesario.

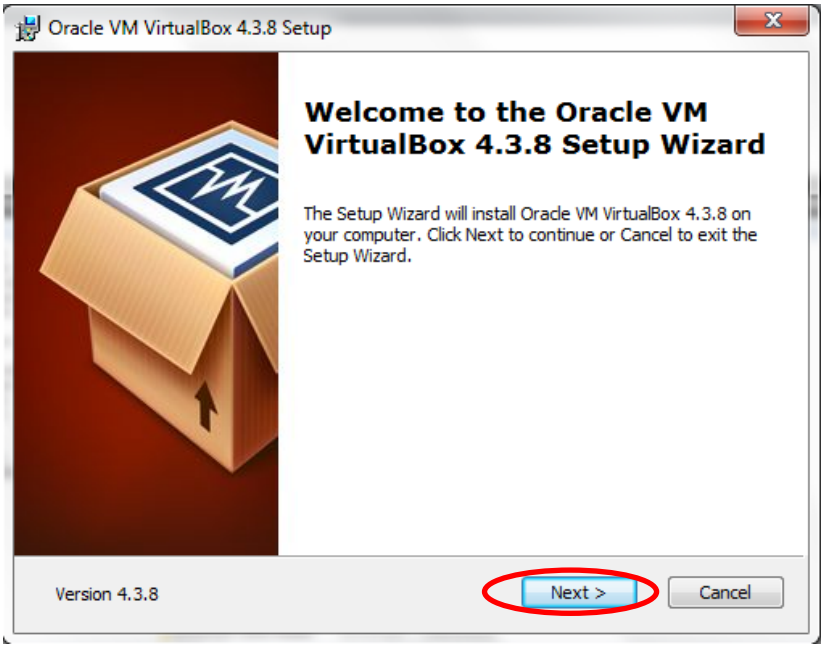
FIGURA 14. PREPARACIÓN PARA INSTALACIÓN



Fuente: Proceso de instalación de Virtual Box.
Elaborado por: El investigador.

3.- Hacemos clic en Next para continuar con la instalación.

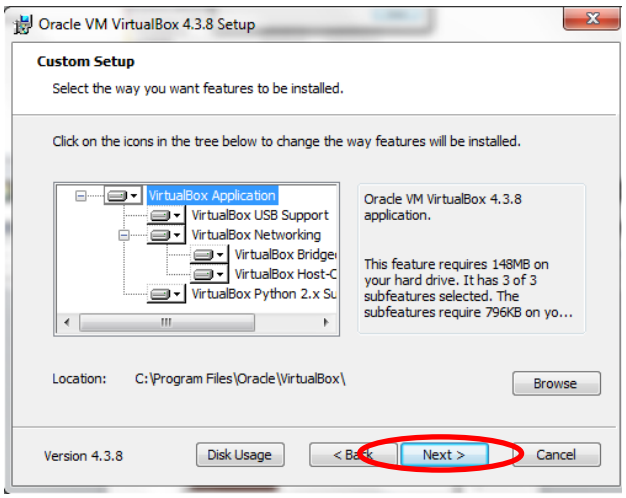
FIGURA 15. VENTANA DE DIÁLOGO DE BIENVENIDA



Fuente: Proceso de instalación de Virtual Box.
Elaborado por: El investigador.

4.- Personalizamos la instalación eligiendo una opción del árbol; también podemos cambiar la ubicación en la que se va a guardar nuestro programa de virtualización; caso contrario hacemos clic en Next.

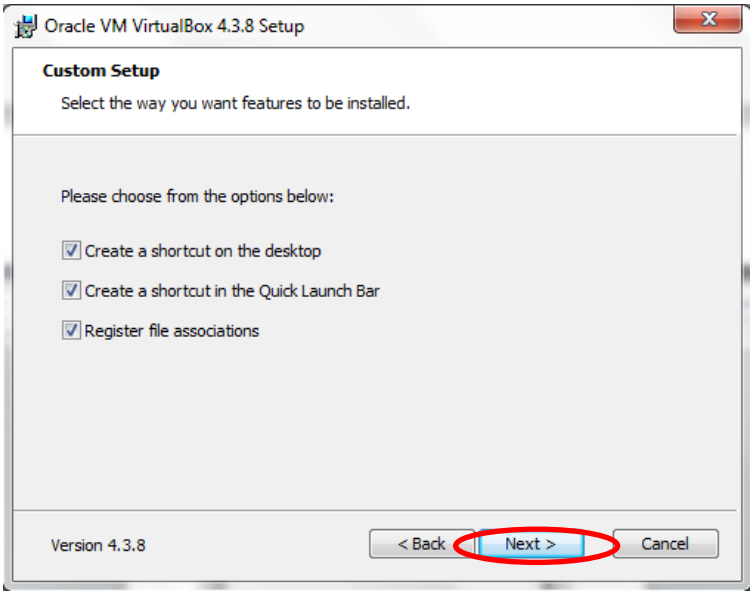
FIGURA 16. PERSONALIZAR LA INSTALACIÓN



Fuente: Proceso de instalación de Virtual Box.
Elaborado por: El investigador.

5.- Hacemos clic en Next, luego de seleccionar las siguientes opciones: crear un acceso directo en el escritorio, crear un acceso directo en la barra de inicio, registrar archivos asociados.

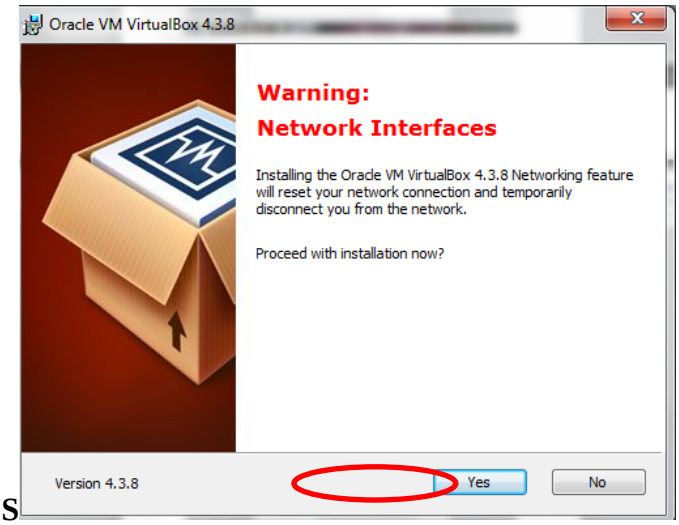
FIGURA 17. CREACIÓN DE ACCESO DIRECTO



Fuente: Proceso de instalación de Virtual Box.
Elaborado por: El investigador.

6.- Aparece una advertencia señalando que la instalación de Oracle Virtual Box reseteara y desconectara temporalmente las conexiones de red. Damos clic en Yes.

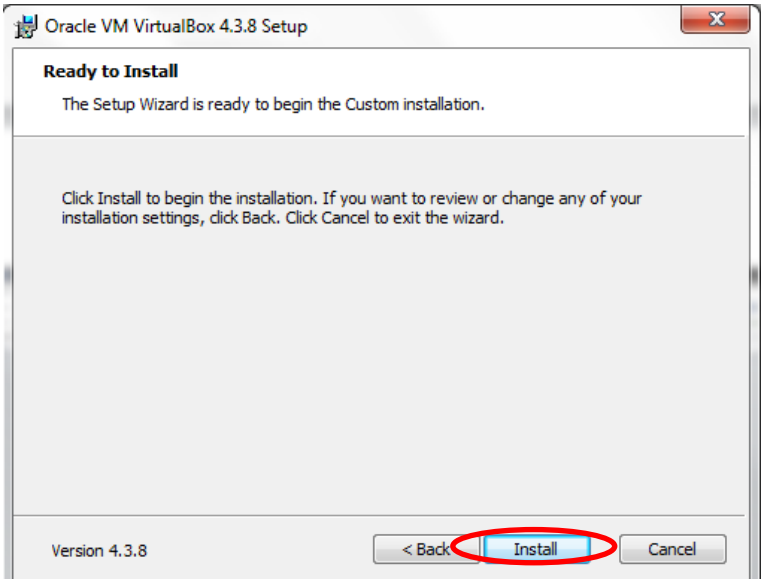
FIGURA 18. VENTANA DE ADVERTENCIA PARA INTERFACES



Fuente: Proceso de instalación de Virtual Box.
Elaborado por: El investigador.

7.- El programa Virtual Box está listo para ser instalado, hacemos clic en Install.

FIGURA 19. INSTALACIÓN DE VIRTUAL BOX



Fuente: Proceso de instalación de Virtual Box.
Elaborado por: El investigador.

8.- Para terminar con el proceso de instalación damos clic en Finish.

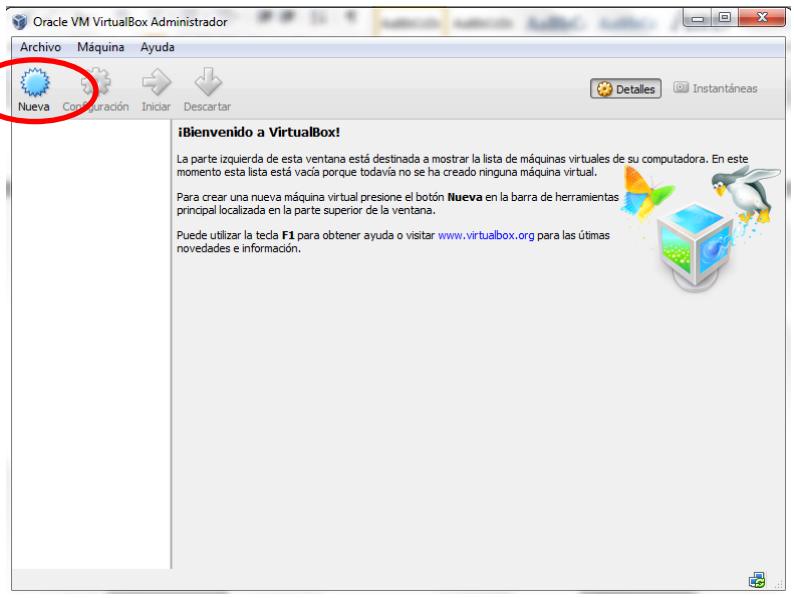
FIGURA 20. FINALIZACIÓN DE LA INSTALACIÓN

Fuente: Proceso de instalación de Virtual Box.
Elaborado por: El investigador.

3.5.2. Proceso de implementación del sistema operativo CentOS

1.- Ejecutamos Virtual Box, para crear una máquina virtual damos clic en Nueva.

FIGURA 21. CREACIÓN DE UNA MÁQUINA VIRTUAL



Fuente: Administrador de Virtual Box
Elaborado por: El investigador.

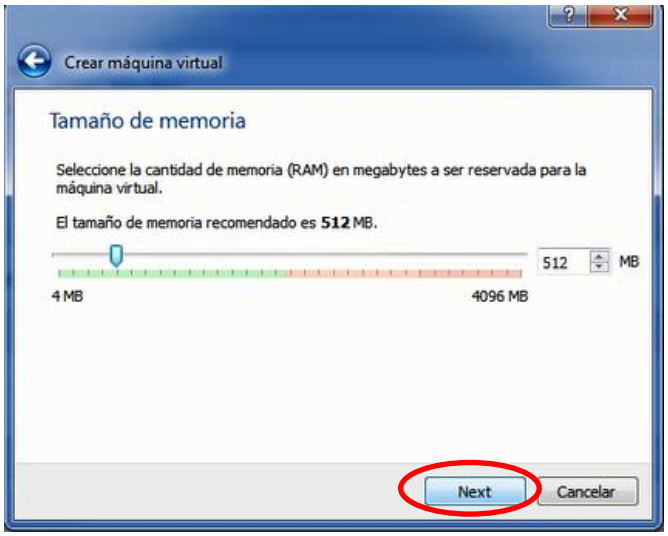
2.- En la siguiente ventana vamos a digitar un nombre para nuestra máquina virtual, elegimos el sistema operativo que instalaremos y la versión (32 o 64 bit).

FIGURA 22. IDENTIFICACIÓN DE LA MÁQUINA VIRTUAL

Fuente: Proceso de creación de una máquina virtual.
Elaborado por: El investigador.

3.- Seleccionamos el tamaño de la memoria RAM para nuestra máquina virtual y damos clic en Next.

FIGURA 23. TAMAÑO DE MEMORIA DE LA MÁQUINA VIRTUAL



Fuente: Proceso de creación de una máquina virtual.
Elaborado por: El investigador.

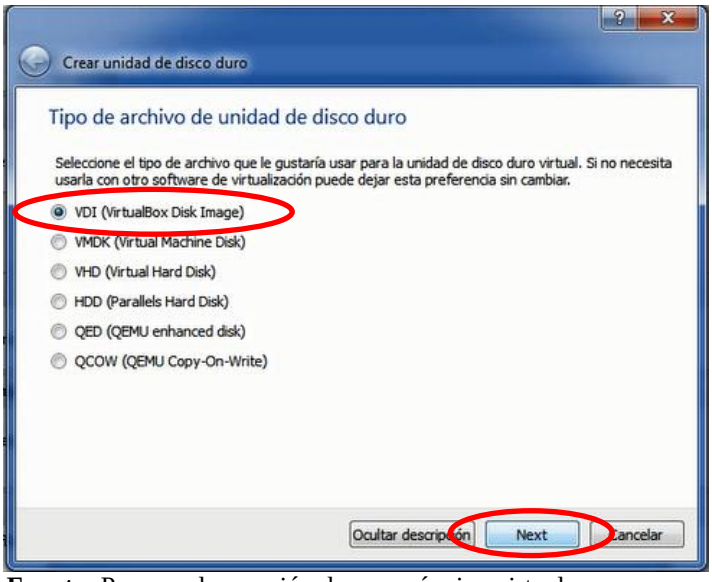
4.- Creamos una unidad de disco duro virtual para la nueva máquina.

FIGURA 24. CREACIÓN DE UN DISCO DURO VIRTUAL

Fuente: Proceso de creación de una máquina virtual.
Elaborado por: El investigador.

5.- Seleccionamos el tipo de archivo que usaremos para la unidad de disco duro virtual y hacemos clic en Next.

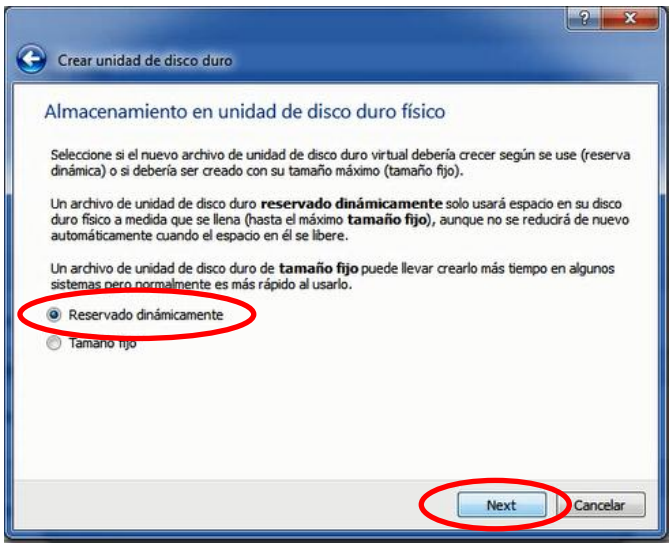
FIGURA 25. TIPO DE ARCHIVO PARA LA UNIDAD DE DISCO DURO



Fuente: Proceso de creación de una máquina virtual.
Elaborado por: El investigador.

6.- Seleccionamos reservado dinámicamente para el almacenamiento en nuestra unidad de disco duro físico, con el fin de usar el espacio únicamente necesario. Hacemos clic en Next.

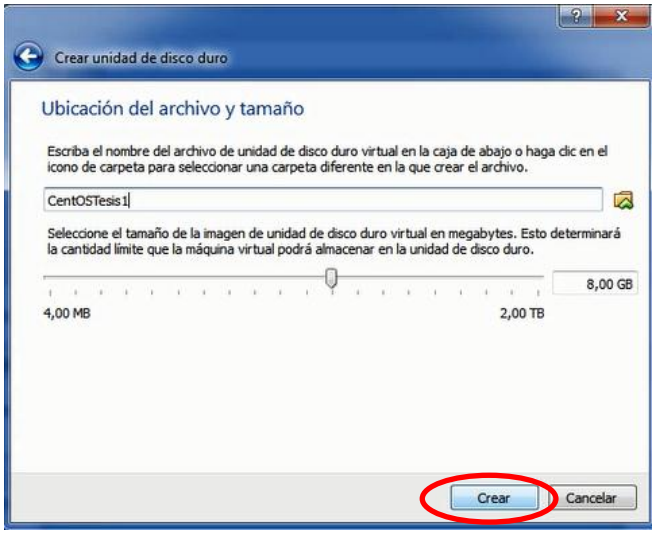
FIGURA 26. ALMACENAMIENTO EN UNIDAD DE DISCO DURO



Fuente: Proceso de creación de una máquina virtual.
Elaborado por: El investigador.

7.- Para crear nuestra unidad de disco duro damos clic en Crear.

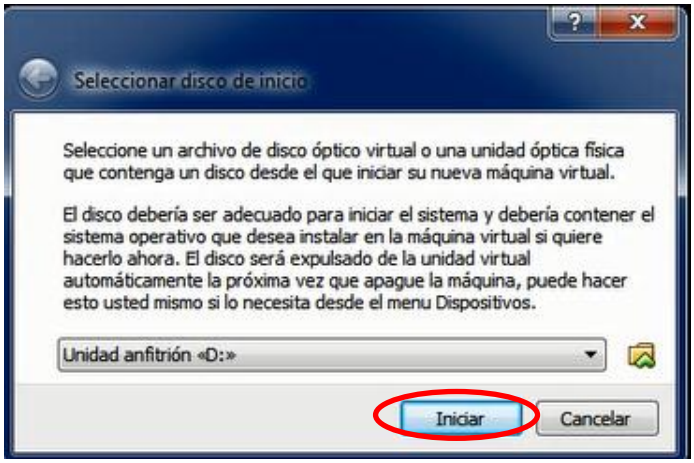
FIGURA 27. CREACIÓN DE LA UNIDAD DE DISCO DURO



Fuente: Proceso de creación de una máquina virtual.
Elaborado por: El investigador.

8.- Para instalar el sistema operativo en la máquina virtual usaremos un CD-R que contiene CentOS. Hacemos clic en Iniciar.

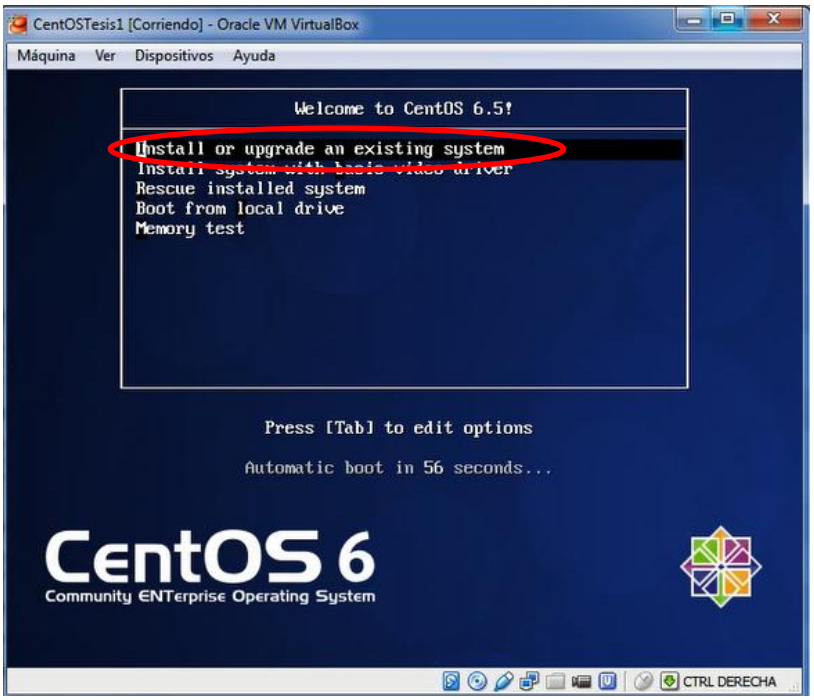
FIGURA 28. INSTALACIÓN DE CENTOS DESDE UNA UNIDAD ÓPTICA



Fuente: Proceso de instalación de CentOS.
Elaborado por: El investigador.

9.- En la ventana de instalación de CentOS seleccionamos instalar o actualizar un sistema existente y presionamos enter.

FIGURA 29. INSTALACIÓN DE CENTOS



Fuente: Proceso de instalación de CentOS.
Elaborado por: El investigador.

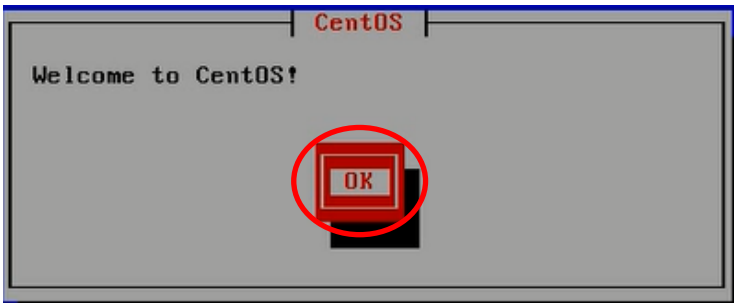
10.- Nos saltamos el siguiente paso presionando enter en Skip.

FIGURA 30. PRUEBA DE INSTALACIÓN

Fuente: Proceso de instalación de CentOS.
Elaborado por: El investigador.

11.- Aparece una ventana que nos da la bienvenida al sistema operativo CentOS, presionamos enter en OK y continuamos.

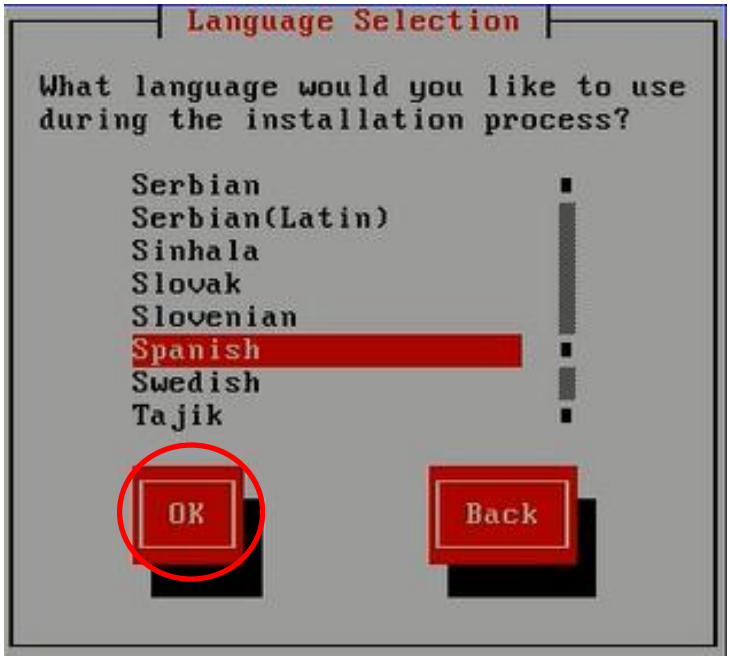
FIGURA 31. BIENVENIDA A CENTOS



Fuente: Proceso de instalación de CentOS.
Elaborado por: El investigador.

12.- Seleccionamos el idioma que deseamos usar durante el proceso de instalación y presionamos enter en OK.

FIGURA 32. SELECCIÓN DEL IDIOMA



Fuente: Proceso de instalación de CentOS.
Elaborado por: El investigador.

13.- Ingresamos una contraseña de súper administrador (root), la misma debe ser fuerte, es decir, deberá tener como mínimo 8 caracteres y se usaran mayúsculas, minúsculas, números, etc. A continuación presionamos enter en OK.

FIGURA 33. INGRESO DE CONTRASEÑA ROOT

Fuente: Proceso de instalación de CentOS.
Elaborado por: El investigador.

14.- Presionamos enter en Aceptar para particionar nuestro disco rígido en una de las siguientes opciones.

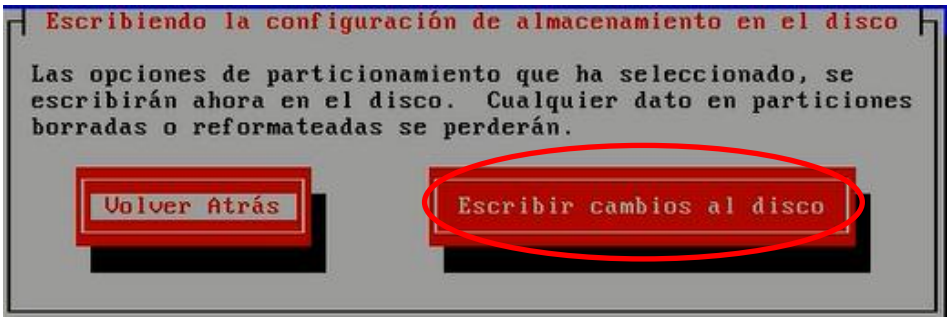
- Usar el disco entero
- Reemplazar el sistema Linux existente
- Usar el espacio libre

FIGURA 34. PARTICIONAMIENTO DE DISCO RÍGIDO

Fuente: Proceso de instalación de CentOS.
Elaborado por: El investigador.

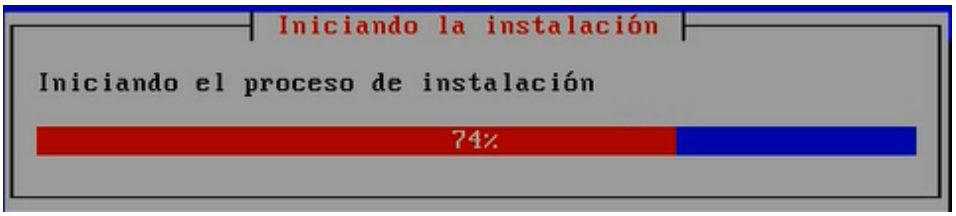
15.- Seleccionamos Escribir cambios al disco y dará inicio el proceso de instalación.

FIGURA 35. CONFIGURACIÓN DE ALMACENAMIENTO



Fuente: Proceso de instalación de CentOS.
Elaborado por: El investigador.

FIGURA 36. PROCESO DE INSTALACIÓN



Fuente: Proceso de instalación de CentOS.
Elaborado por: El investigador.

FIGURA 37. INSTALACIÓN DE PAQUETES NECESARIOS

Fuente: Proceso de instalación de CentOS.
Elaborado por: El investigador.

16.- Una vez que se completa el proceso de instalación de CentOS debemos reiniciar para usar el sistema instalado.

FIGURA 38. REINICIAR EL SISTEMA

Fuente: Proceso de instalación de CentOS.
Elaborado por: El investigador.

17.- Finalmente iniciamos sesión con nuestro usuario y contraseña.

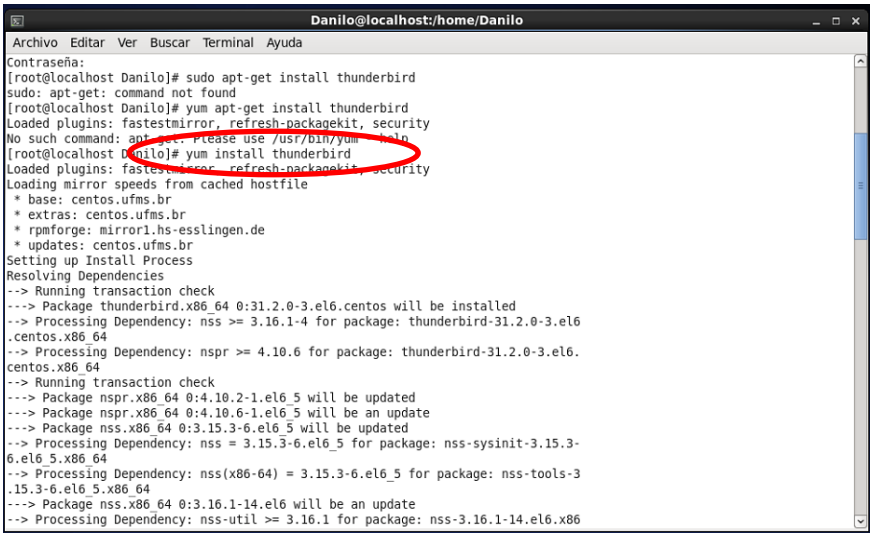
FIGURA 39. INICIO DE SESIÓN

Fuente: Inicio de sesión en CentOS.
Elaborado por: El investigador.

3.5.3. Proceso de implementación del cliente de correo electrónico Thunderbird.

1.- Instalamos el aplicativo gratuito de correo electrónico Thunderbird a través del Terminal de CentOS, ingresando el comando # yum apt-get install thunderbird.

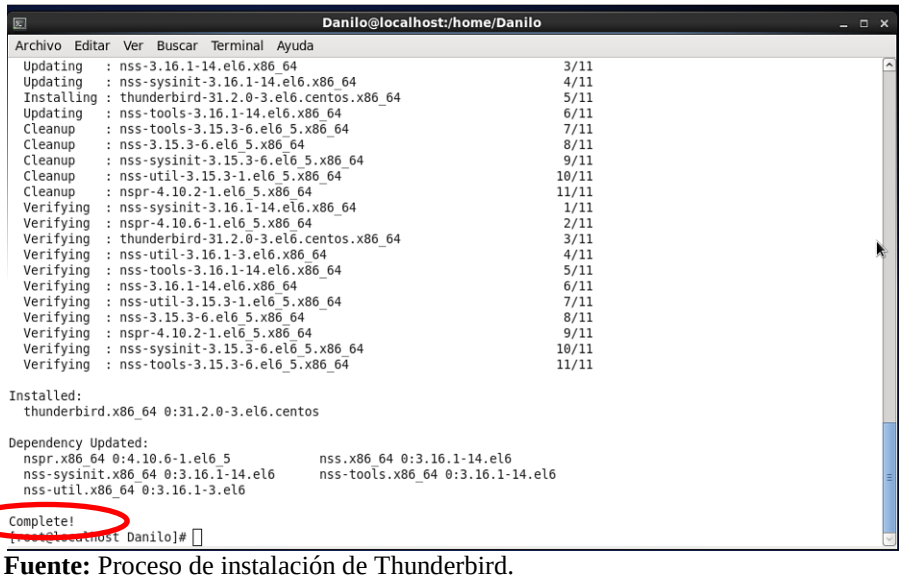
FIGURA 40. INSTALACIÓN DE THUNDERBIRD



Fuente: Proceso de instalación de Thunderbird.
Elaborado por: El investigador

2.- Esperamos varios minutos, mientras se completa el proceso de instalación.

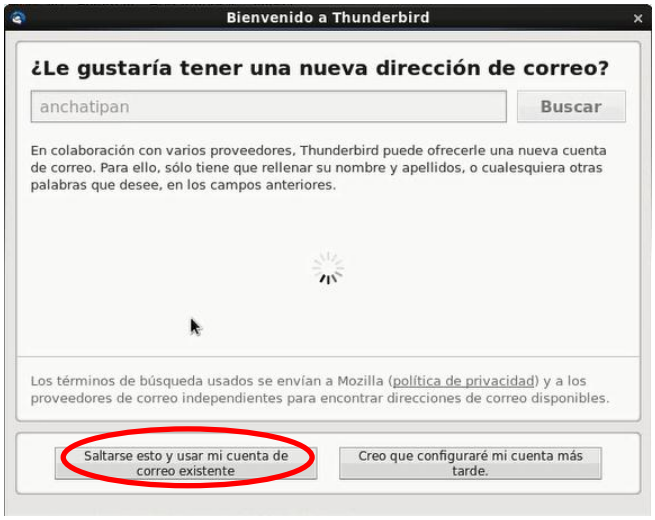
FIGURA 41. INSTALACIÓN COMPLETA



Fuente: Proceso de instalación de Thunderbird.
Elaborado por: El investigador

3.- Una vez instalado Thunderbird, es necesario configurar una cuenta de usuario y va a aparecer la siguiente ventana de bienvenida en la que elegiremos la opción “Saltarse esto y usar mi cuenta de correo existente”.

FIGURA 42. CREACIÓN DE UN USUARIO DE CORREO



Fuente: Proceso de instalación de Thunderbird.
Elaborado por: El investigador

4.- Configuramos la cuenta de correo llenando los campos con el nombre que queremos que se muestre, ingresamos una dirección de correo electrónico existente con su respectiva contraseña. Para mayor seguridad se recomienda desmarcar la opción Recordar contraseña.

FIGURA 43. CONFIGURACIÓN DE CORREO

Fuente: Proceso para la creación de una cuenta.
Elaborado por: El investigador

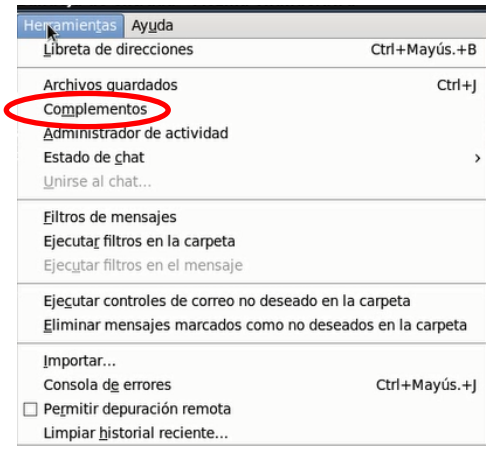
5.- Automáticamente se verifica la configuración del proveedor de correo electrónico, cuando ésta es validada correctamente finalizamos el proceso haciendo clic en Hecho.

FIGURA 44. VERIFICACIÓN DEL PROVEEDOR DE CORREO

Fuente: Proceso para la creación de una cuenta.
Elaborado por: El investigador

6.- Hacemos clic en Herramientas ubicado en la barra de menú de Mozilla Thunderbird y elegimos la opción Complementos, para instalar el complemento enigmail.

FIGURA 45. INSTALACIÓN DEL COMPLEMENTO ENIGMAIL



Fuente: Proceso para la instalación del complemento enigmail.
Elaborado por: El investigador.

7.- Seleccionamos e instalamos Enigmail, cerramos Mozilla Thunderbird y al volver a abrirlo nos aparecerá instalado en la barra de menú.

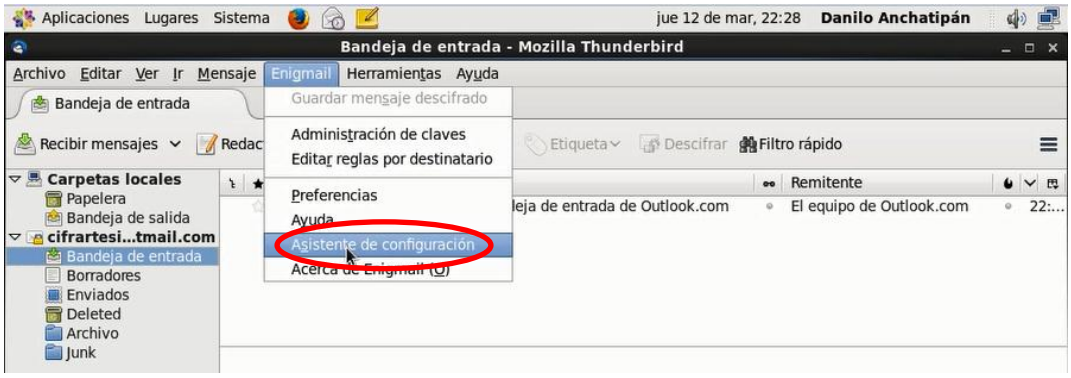
FIGURA 46. INSTALACIÓN DE ENIGMAIL

Fuente: Proceso para la instalación del complemento enigmail**.**
Elaborado por: El investigador.

Antes de comenzar a utilizar nuestra cuenta de correo electrónico para enviar y recibir mensajes cifrados, es preciso configurar Enigmail que es la herramienta que realizara el proceso de cifrado-descifrado.

8.- En la barra de menú elegimos Enigmail, luego hacemos clic en la opción Asistente de Configuración.

FIGURA 47. HABILITACIÓN DE ENIGMAIL

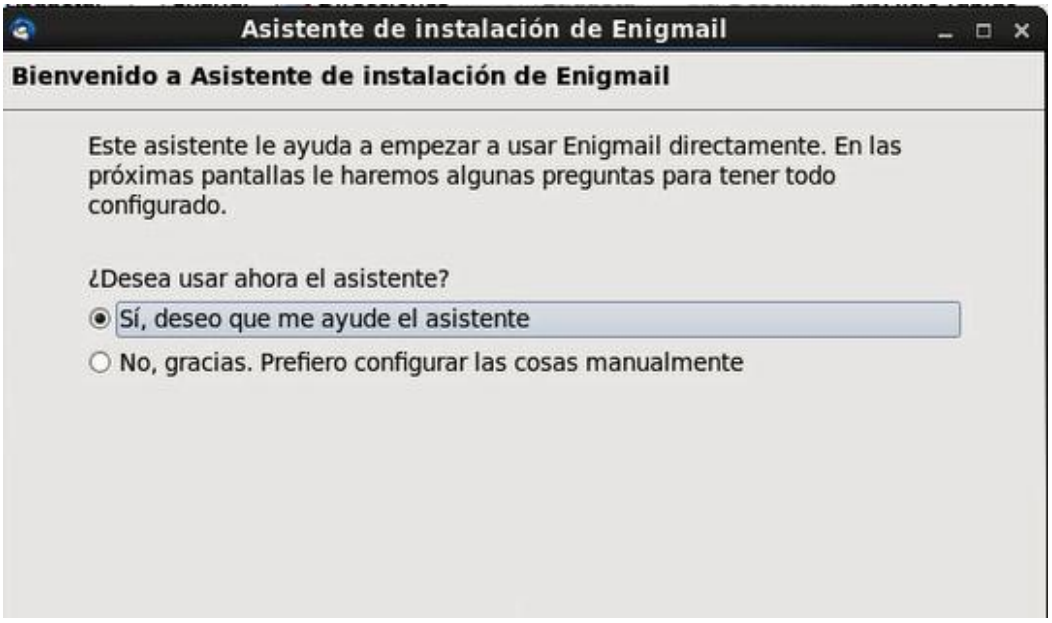


Fuente: Proceso para habilitar Enigmail.
Elaborado por: El investigador

9.- Aparecerá un asistente de instalación de Enigmail, el cual nos preguntara, si queremos que nos ayude o si deseamos configurar las cosas manualmente.

Elegimos sí, deseo que me ayude el asistente, y hacemos clic en Siguiente.

FIGURA 48. ASISTENTE DE INSTALACIÓN



Fuente: Proceso para habilitar Enigmail.
Elaborado por: El investigador.

10.- A continuación debemos elegir cual será el modo que usaremos para enviar correos:

- La primera opción es para descifrar automáticamente el mensaje una vez que ingresamos nuestra clave privada.

- La segunda opción y la más segura es para digitar la clave privada todas las veces que vamos a revisar un correo cifrado.

- La tercera es para que los mensajes no se encripten por defecto, es decir, no es necesario digitar la clave privada para descifrar el mensaje.

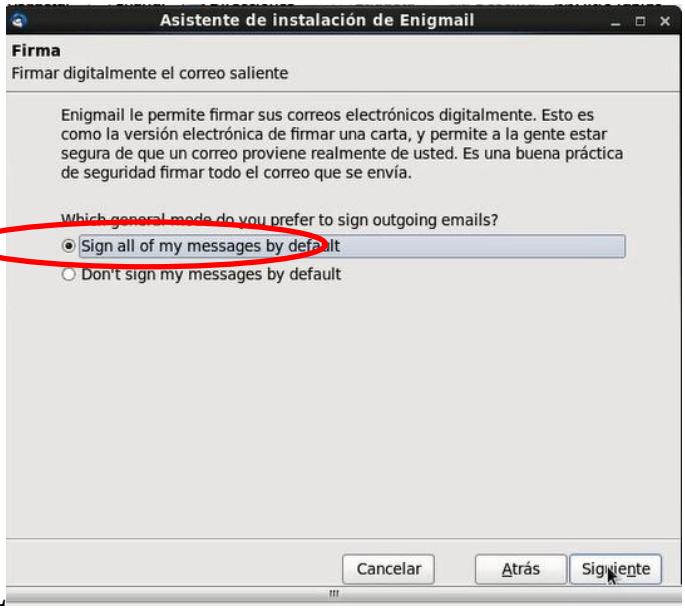
Elegimos la opción más adecuada para nosotros y hacemos clic en Siguiente.

FIGURA 49. NIVEL DE SEGURIDAD

Fuente: Proceso para habilitar Enigmail.
Elaborado por: El investigador.

11.- Seleccionamos firmar digitalmente el correo electrónico para garantizar la autenticidad del remitente del mensaje, esta firma digital nos dará un nivel más de seguridad, lo que no sucedería si elegimos no firmar mis mensajes por defecto.

FIGURA 50. SELECCIÓN DE FIRMA

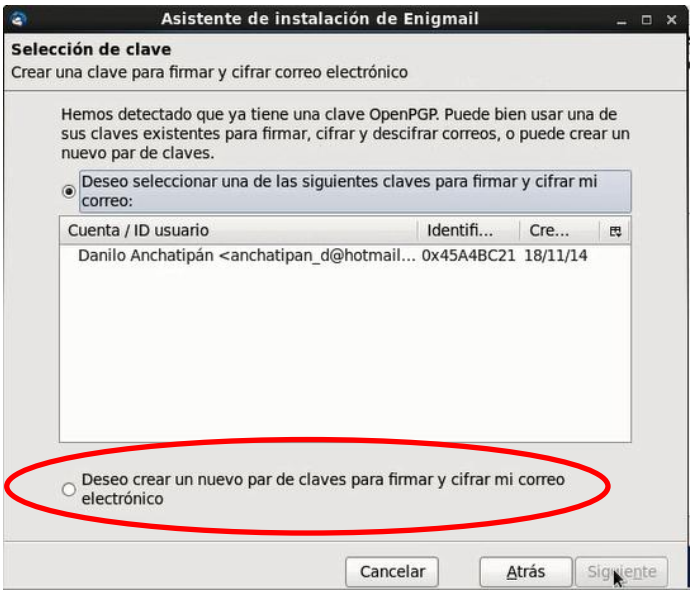


DIGITAL

Fuente: Proceso para habilitar Enigmail.
Elaborado por: El investigador.

12.- Como es la primera vez que realizamos esta tarea, vamos a crear un par de claves para firmar, cifrar y descifrar nuestro correo electrónico.

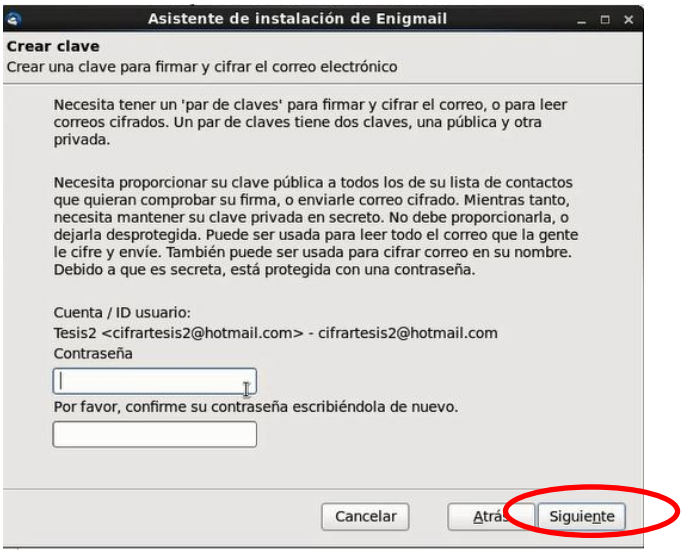
FIGURA 51. CREACIÓN DE UN PAR DE CLAVES



Fuente: Proceso para habilitar Enigmail.
Elaborado por: El investigador

13.- Ingresamos una contraseña, esta será nuestra clave privada y debemos mantenerla en secreto. Una vez realizado esto, el asistente realizara varias tareas, entre ellas está la activación de Enigmail para correo electrónico.

FIGURA 52. CREACIÓN DE UNA CLAVE PRIVADA



Fuente: Proceso para habilitar Enigmail.
Elaborado por: El investigador.

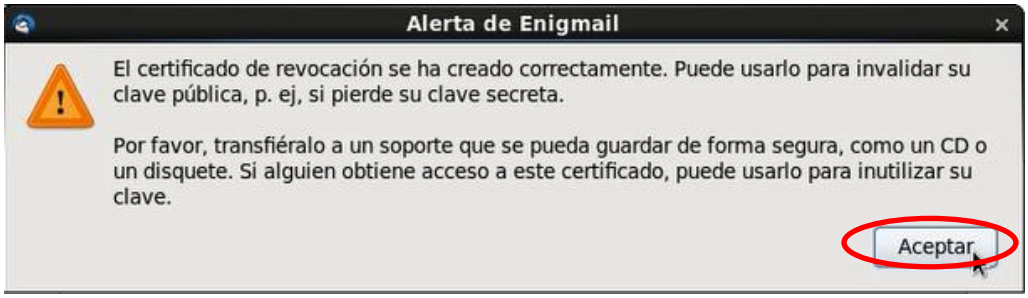
14.- Cuando el proceso finaliza satisfactoriamente, aparece un mensaje con la confirmación de Enigmail. Y nos recomienda crear un certificado de revocación, para invalidar nuestra clave privada cuando esta se ve comprometida.

FIGURA 53. FINALIZACIÓN DEL PROCESO DE GENERACIÓN DE LA CLAVE

Fuente: Proceso para habilitar Enigmail.
Elaborado por: El investigador.

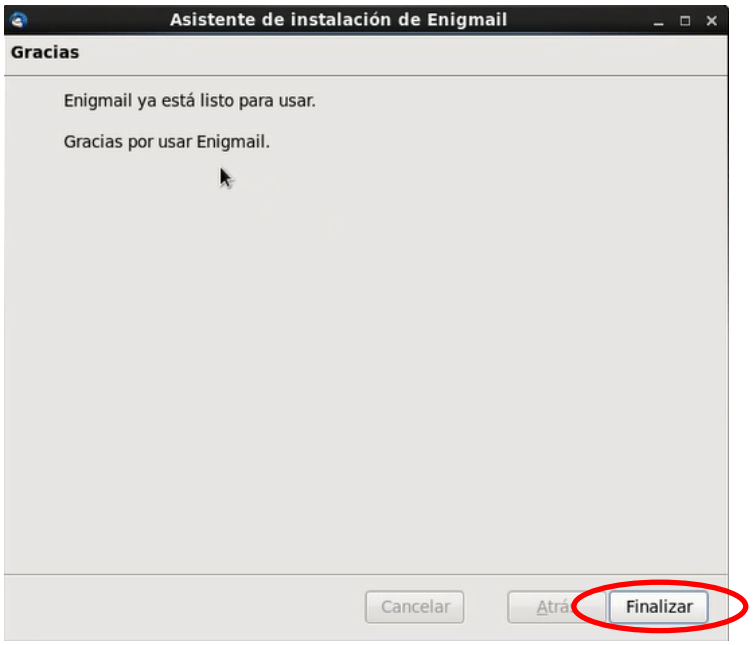
Si el certificado de revocación se genera sin problema nos aparecerá el siguiente mensaje y habremos finalizado con la activación de Enigmail al hacer clic en Aceptar.

FIGURA 54. GENERACIÓN DE CERTIFICADO DE REVOCACIÓN



Fuente: Proceso para habilitar Enigmail.
Elaborado por: El investigador.

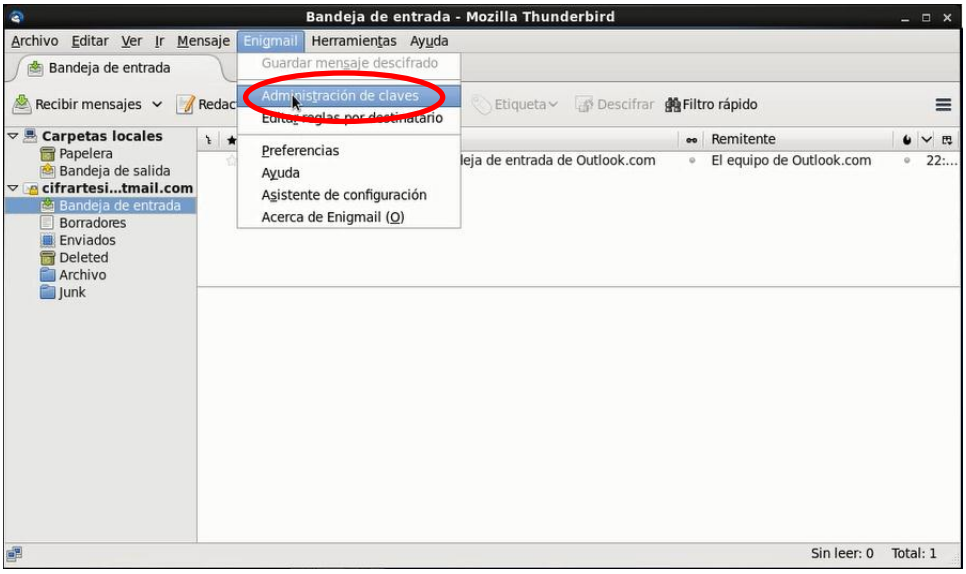
FIGURA 55. FINALIZACIÓN DE LA INSTALACIÓN DE ENIGMAIL



Fuente: Proceso para habilitar Enigmail
Elaborado por: El investigador.

15.- Para revisar la clave que creamos, elegimos en la barra de menú Enigmail y damos clic en la opción Administración de claves.

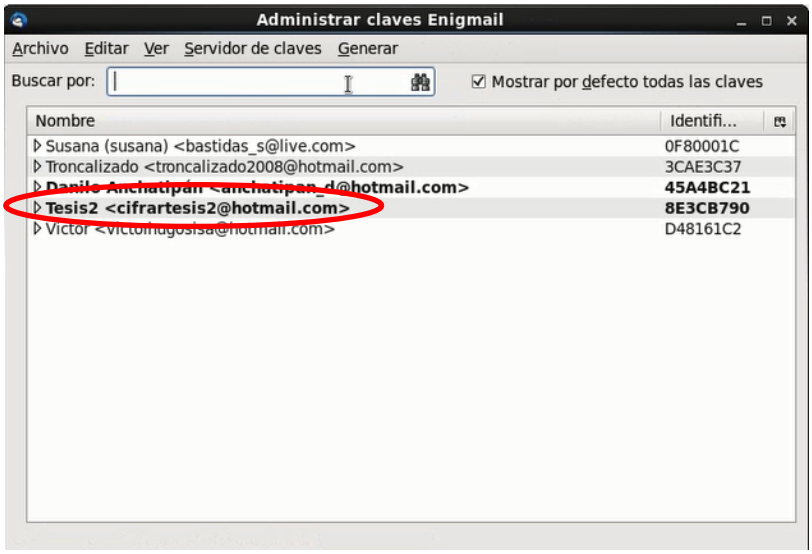
FIGURA 56. ADMINISTRACIÓN DE CLAVES



Fuente: Proceso para compartir la clave pública.
Elaborado por: El investigador.

16.- A continuación nos aparecerá un listado con todas las claves disponibles en el administrador de claves incluida la que acabamos de crear.

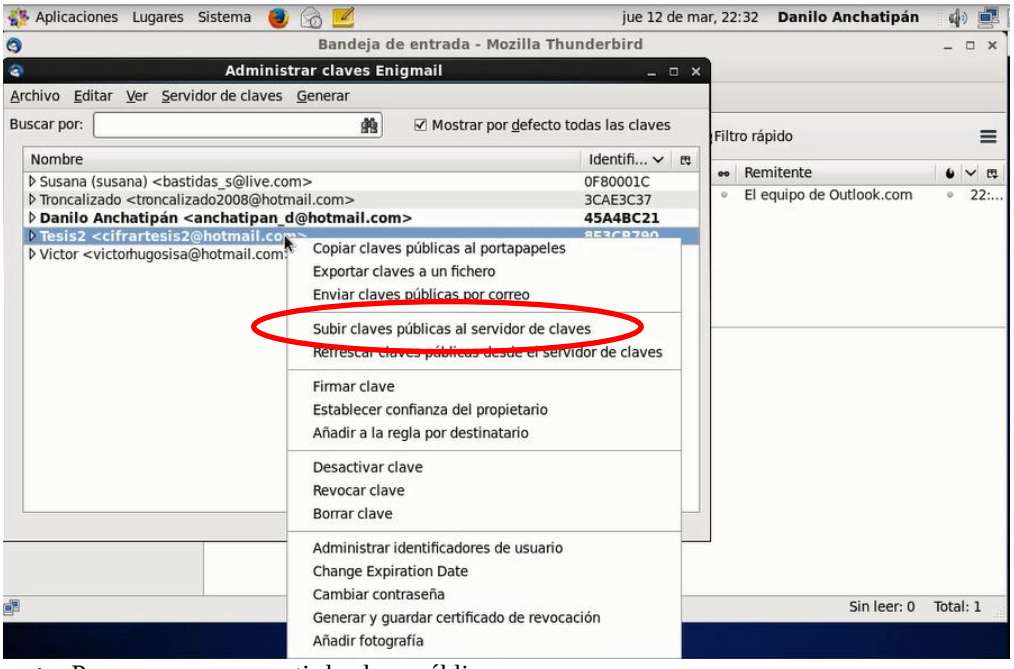
FIGURA 57. ADMINISTRADOR DE CLAVES



Fuente: Administrador de claves Enigmail.
Elaborado por: El investigador.

17.- Para poder cifrar mensajes debemos compartir la clave pública que acabamos de crear, damos clic derecho sobre la clave que vamos a compartir y elegimos "enviar clave pública por correo" o "subir claves públicas al servidor de claves".

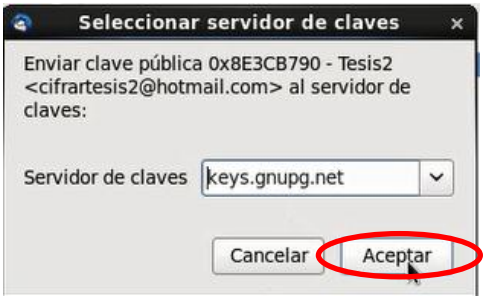
FIGURA 58. COMPARTIR CLAVE PÚBLICA



Fuente: Proceso para compartir la clave pública.
Elaborado por: El investigador.

18. Al elegir subir la clave pública al servidor de claves, debemos seleccionar a que servidor enviaremos nuestra clave.

FIGURA 59. SERVIDOR DE CLAVES



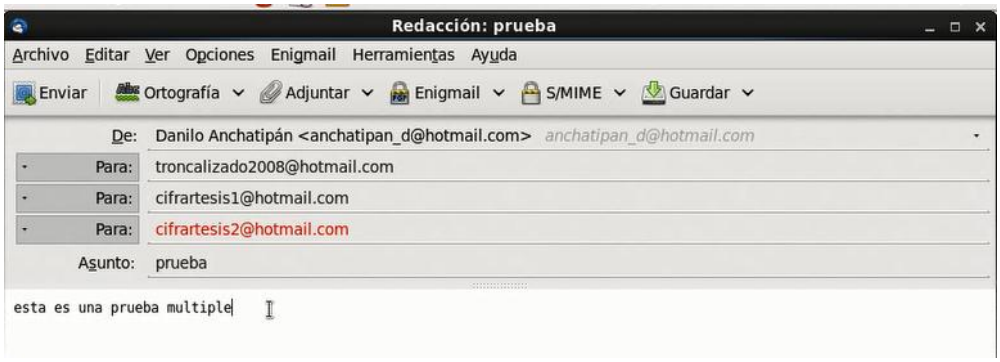
Fuente: Proceso para compartir la clave pública.
Elaborado por: El investigador.

3.5.4. Pruebas de cifrado-descifrado

Para demostrar en forma práctica cómo funciona la seguridad informática, aplicando la criptografía como técnica para proteger la información de intrusos, programas maliciosos, u otras entidades, usaremos el software que instalamos y habilitamos.

1.- Con la cuenta de correo anchatipan_d@hotmail.com vamos a redactar un correo que será enviado de manera confidencial a la cuenta de correo troncalizado2008@hotmail.com.

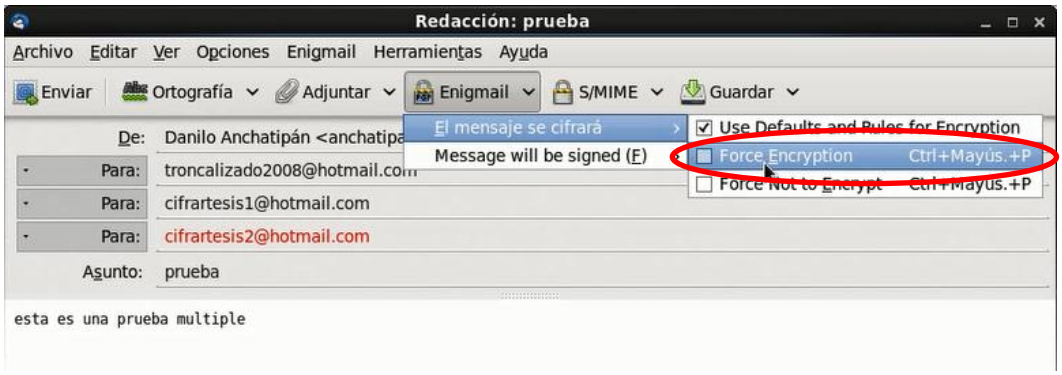
FIGURA 60. REDACCIÓN DE UN MENSAJE



Fuente: Proceso para enviar un mensaje cifrado.
Elaborado por: El investigador.

2.- Para que el mensaje se encripte debemos seleccionar Enigmail, luego marcamos el mensaje se cifrará y damos click en forzar encripción.

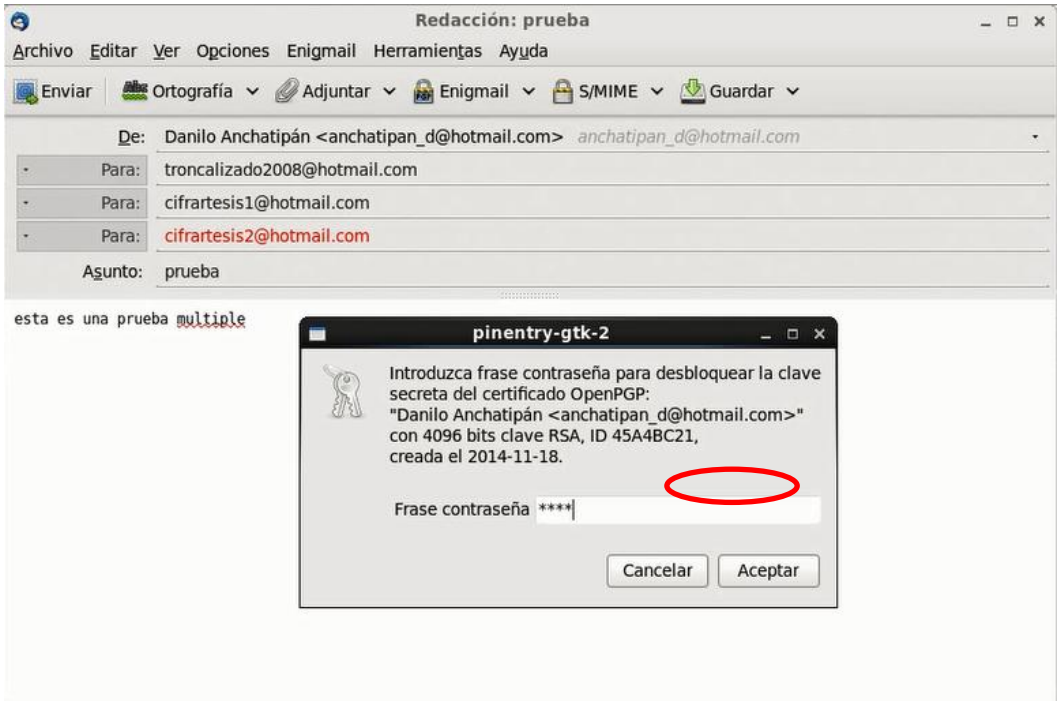
FIGURA 61. ENCRIPTAR MENSAJE



Fuente: Proceso para enviar un mensaje cifrado.
Elaborado por: El investigador.

3.- Al hacer click en enviar, aparecerá una ventana solicitando el ingreso de una clave para cifrar el mensaje.

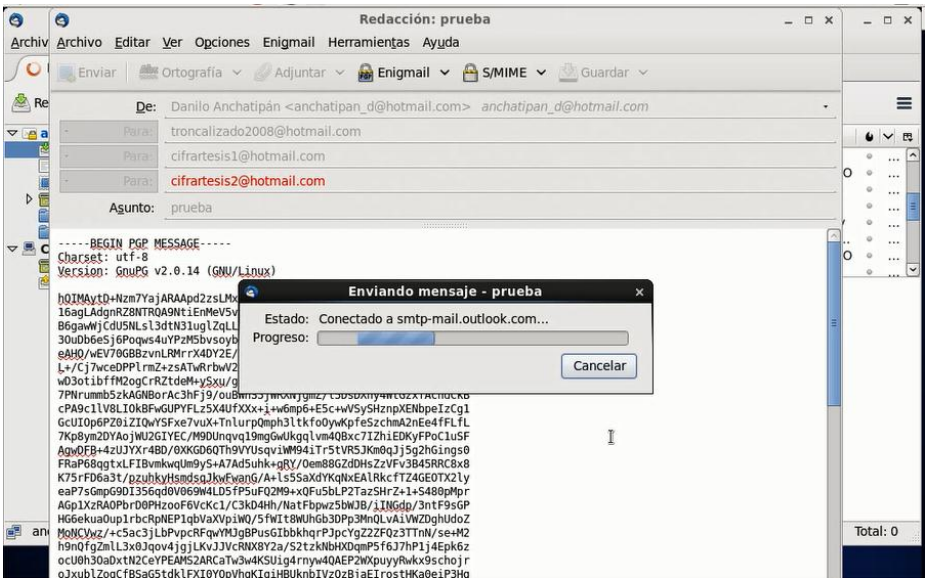
FIGURA 62. INGRESO DE CLAVE DE CIFRADO



Fuente: Proceso para enviar un mensaje cifrado.
Elaborado por: El investigador.

Al hacer click en aceptar el mensaje se enviara cifrado a su o sus destinatarios.

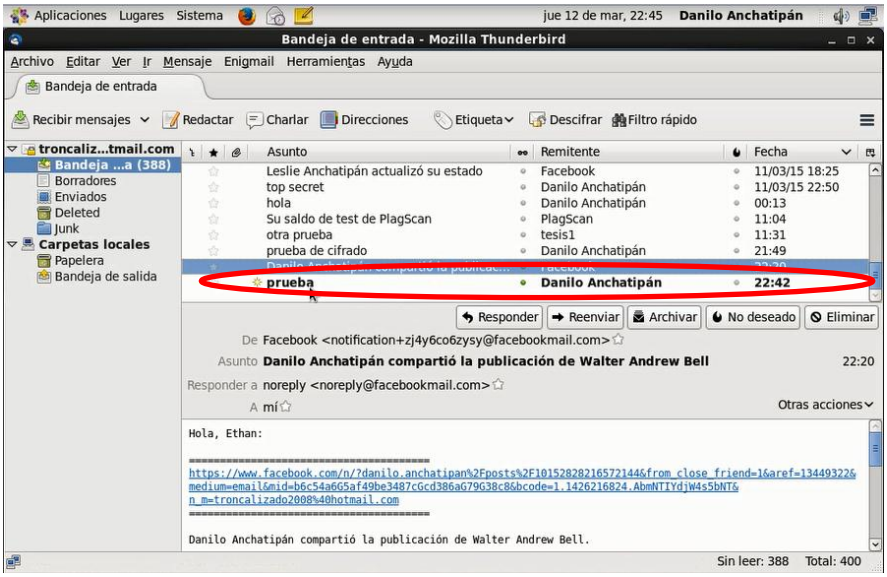
FIGURA 63. MENSAJE CIFRADO



Fuente: Proceso para enviar un mensaje cifrado.
Elaborado por: El investigador.

4.- Verificamos en la cuenta de correo troncalizado2008@hotmail.com que recibimos un mensaje enviado por anchatipan_d@hotmail.com (Danilo Anchatipán).

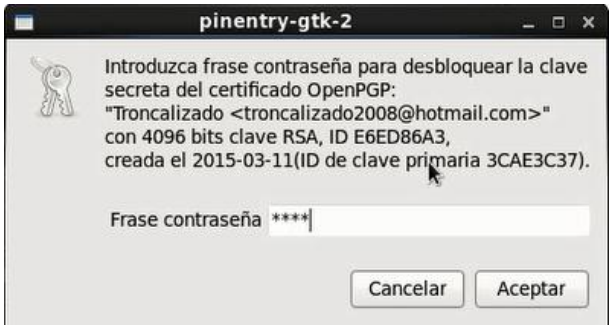
FIGURA 64. LECTURA DE UN MENSAJE CIFRADO



Fuente: Proceso para descifrar un mensaje cifrado.
Elaborado por: El investigador.

5.- Al intentar leer el mensaje “prueba” se solicitará la clave privada de troncalizado2008@hotmail.com.

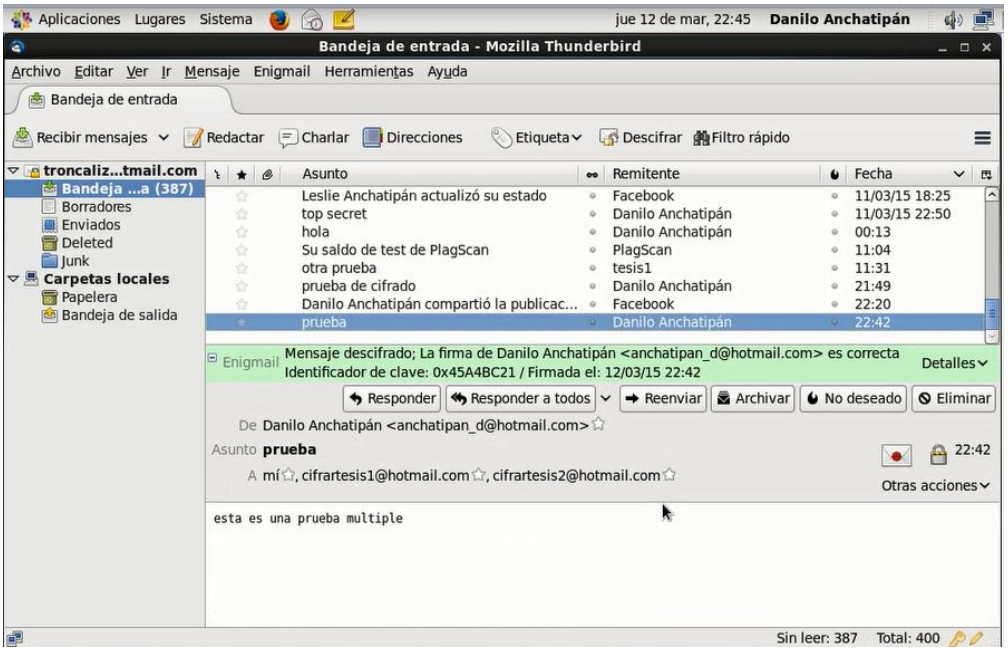
FIGURA 65. INGRESO DE CLAVE PRIVADA PARA DESCIFRAR MENSAJE



Fuente: Proceso para descifrar un mensaje cifrado.
Elaborado por: El investigador.

6.- Si se introduce la clave privada correcta el mensaje se descifrara y se podrá leer el mensaje enviado desde la cuenta de correo anchatipan_d@hotmail.com a la cuenta de correo troncalizado2008@hotmail.com.

FIGURA 66. MENSAJE DESCIFRADO



Fuente: Proceso para descifrar un mensaje cifrado.
Elaborado por: El investigador.

3.6. Informe de validación de la implementación de seguridades mediante criptografía para servidores basados en software libre, para el laboratorio de redes de la Carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi

Presentación

En los capítulos precedentes de la investigación se propuso la implementación de seguridades mediante criptografía basada en software libre, en el laboratorio de redes de la Carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi, para lo cual fue necesario recabar información técnica-científica que me ayudó a entender de forma general la dimensión de los resultados que se pretendía alcanzar, tomando como base el marco teórico del primer capítulo y demostrado en el segundo capítulo con la práctica.

Sin embargo, es necesario demostrar la hipótesis con la aplicación práctica de la investigación.

Trabajos realizados

- Se instaló una máquina virtual en cada uno de los cinco computadores de escritorio que forman parte del laboratorio de redes de la Carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi, siguiendo el procedimiento de implementación de Virtual Box detallado en el capítulo 3 de este proyecto de investigación.

- Se instaló el sistema operativo Centos 6.6 en cada una de las cinco máquinas virtuales de acuerdo al proceso de implementación especificado en el capítulo 3 de este proyecto de investigación.

- Se implementó un cliente de correo electrónico de software libre denominado Thunderbird, y se levantaron todos los servicios necesarios para que esta herramienta nos ayude a cifrar y descifrar los mensajes de correo electrónico en cada una de las cinco máquinas virtuales, con el fin de que, el uso de este aplicativo sea transparente y fácil de manejar para el usuario final.

- Con el fin de realizar pruebas de funcionamiento, se crearon cinco cuentas de usuario de correo electrónico con diferentes proveedores de este servicio, para validar la implementación de seguridades del correo electrónico en nuestro aplicativo Thunderbird.

NOMBRE	CUENTAS DE CORREO ELECTRÓNICO	CONTRASEÑA
Estudiante Uno	estudiante.uno.de.5@gmail.com	Estudiante1
Estudiante Dos	estudiante.dos.de.5@outlook.es	Estudiante2
Estudiante Tres	estudiante.tres.de.5@hotmail.com	Estudiante3
Estudiante Cuatro	estudiante.cuatrode5@yahoo.com	Estudiant4
Estudiante Cinco	estudiante.cinco.de.5@outlook.com	Estudiante5

- Una vez que, las cinco cuentas de usuario de los estudiantes fueron creadas se habilitó el complemento enigmail, y con la ayuda de su asistente generamos un par de claves (una privada y una pública) y un certificado de revocación para eliminar la clave privada cuando se encuentre comprometida su seguridad.

NOMBRE	CUENTAS DE CORREO ELECTRÓNICO	CLAVE PRIVADA
Estudiante Uno	estudiante.uno.de.5@gmail.com	Cifrado1
Estudiante Dos	estudiante.dos.de.5@outlook.es	Cifrado2
Estudiante Tres	estudiante.tres.de.5@hotmail.com	Cifrado3
Estudiante Cuatro	estudiante.cuatrode5@yahoo.com	Cifrado4
Estudiante Cinco	estudiante.cinco.de.5@outlook.com	Cifrado5

- Con todas las configuraciones realizadas en el aplicativo de correo electrónico Thunderbird, iniciamos con las pruebas de funcionamiento; realizando, varias prácticas reales de envío de mensajes encriptados desde cada una de las cuentas de correo. En este punto, es cuando se comprueba la teoría que permitió realizar este proyecto de investigación, en virtud de, que:

  1.- Para cifrar un mensaje es necesario poseer una clave privada, la misma que sirve también para firmar el mensaje, cumpliendo con esto la característica de no repudio.

  2.- Para descifrar el mensaje es necesario poseer también una clave quien recibe el mensaje que fue cifrado con su clave pública, cumpliendo con esto la característica de confidencialidad e integridad de la información.

- Para finalizar se solicitó a tres señores estudiantes de la Carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi, que utilicen la aplicación para encriptar mensajes de correo electrónico y que elaboren un informe de validación con firmas de responsabilidad en el que se debe incluir todas las observaciones pertinentes de la usabilidad de la tesis, documento que se encuentra adjunto.

Conclusión.

- En la práctica es completamente comprobable la hipótesis planteada en esta investigación.

Recomendación.

- Crear la clave privada con una combinación de letras, números y símbolos difíciles de predecir, en razón, de que en esta clave descansa toda la seguridad de nuestro mensaje encriptado.

Elaborado por:

Danilo Fernando Anchatipán Navas
Investigador

UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

Informe de validación

Quienes emitimos el presente informe de validación, certificamos que se realizó pruebas de funcionamiento del siguiente tema de tesis: **"Implementación de seguridades mediante criptografía para servidores basados en software libre, para el laboratorio de redes de la Carrera de Ingeniería en Informática y Sistemas Computacionales, durante el período 2013"**, mismas que se detallan a continuación.

- Se generó claves de cifrado públicas y privadas para cada uno de las cuentas de correo electrónico.

- Se creó un certificado de revocación para eliminar la clave privada si su seguridad se encuentra comprometida

- Una vez efectuado los procesos anteriores, se subió la clave pública a un servidor de claves para que estén disponibles en la red.

- Para iniciar con el envío de mensajes a través del correo electrónico primero cargamos la clave pública de la cuenta de correo con la que vamos a intercambiar información.

- Se enviaron y recibieron varios mensajes de correo electrónico encriptados.

Conclusión

- Una vez realizadas las pruebas de funcionamiento se determina que la aplicación de criptografía en el correo electrónico cumple con las expectativas de los usuarios.

Recomendación

- Que se aplique criptografía para el correo electrónico sobre una plataforma Windows.

Latacunga, 14 de mayo de 2015.

Edison Israel Aispur Calvopiña
…….

Robinson Andrés Briones Correa
……

Erik David Saquinga Hushcasho
…….

Conclusiones

1. Existe poca bibliografía referente a este tema, pero se realiza la revisión de la información de las fuentes bibliográficas electrónicas e impresas existentes, logrando desarrollar las categorías fundamentales del marco teórico que sustentaron el desarrollo de la investigación, en base a criterios de autores que escriben sobre este tema.

2. Dentro del proceso metodológico se determina la factibilidad de la investigación, al encontrar que existen muchas dificultades en el uso de la información confidencial y que viene causando malestar en la comunidad universitaria se llega a determinar a través de la aplicación de encuestas a los estudiantes de séptimo, octavo, noveno ciclo y docentes de la Carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi.

3. Se establece que es necesario generar una propuesta de software libre para encriptar la información de manera segura y confiable, para luego ser compartida a través del correo electrónico.

4. La Aplicación de Seguridades para Correo Electrónico mediante criptografía basado en software libre en el laboratorio de redes de la Universidad Técnica de Cotopaxi permite garantizar la integridad, la privacidad de los mensajes trasmitidos por medio de red, para que se efectivicen de manera segura, confiable, garantizando la confidencialidad del flujo de la información.

5. La utilización de herramientas de software libre (Sistema Operativo Centos) y aplicaciones complementarias comoThunderbird y Enigmail, permite que el envío y recepción de mensajes, garantice la seguridad al permitir cifrar y descifrar los mensajes encriptados, se lo realice de una manera sencilla y sin complicaciones.

6. Para un adecuado funcionamiento de la aplicación es necesario que el sistema operativo este instalado y configurado correctamente.

Recomendaciones

1. En la Universidad Técnica de Cotopaxi, se debe y tiene que implementar lineamientos y políticas que permita mantener segura la información que viaja diariamente por la red a través del e-mail, para lo cual se recomienda que esta aplicación no solamente se quede en el laboratorio de redes sino que se implante en todos los departamentos y sea el usuario quien elija enviar el mensaje encriptado o no dependiendo de la importancia del mensaje.

2. Se recomienda que cuando se refiere a seguridades lo más adecuado es trabajar con Centos, porque es una de las distribuciones Linux desarrollada exclusivamente para trabajar con servidores y seguridades. Thunderbird y Enigmail son complementos que pueden ser instalados y configurados en este sistema operativo por su compatibilidad.

3. Para poder utilizar los mensajes encriptados se recomienda que el usuario tenga conocimientos básicos sobre estas herramientas y su funcionalidad, para lo cual la universidad puede implementar proyectos de capacitación sistemáticas dirigidas a la comunidad universitaria sobre esta temática.

4. Se recomienda que la biblioteca de la Universidad Técnica de Cotopaxi, cuente con más bibliografía impresa referente a seguridades para servidores, criptografía y software libre y a la vez se garantice la actualización del sistema operativo de la encriptación de mensajes vía correo electrónico.

Bibliografía.

CITADA

BARRIOS, Joel, *Configuración de servidores con gnu/linux*, marzo 2015, Alcance Libre, México DF, 2004.

COSTAS, Jesús, *Seguridad informática*, ediciones de la U, Bogotá, 2011, ISBN 978-958-8675-70-1.

DESIREE, Edit, *Seguridad informática y criptografía*, Universidad Nacional del Noreste, Facultad de Ciencias Exactas, Naturales y Agrimensura, Corrientes, Argentina, 2008.

ESTRADA, Edison, *Sistemas de encriptación de datos empleando verificación compartida para redes de área local*, Centro Nacional de Investigación y Desarrollo Tecnológico CENIDET, Cuernavaca, Morelos, 2006.

FUSTER, Amparo, HERNANDEZ, Luis, MARTÍN, Agustín, MONTOYA, Fausto, MUÑOZ, Jaime, *Criptografía, protección de datos y aplicaciones*, primera edición, Alfaomega, México DF, 2012, ISBN 978-607-707-469-4.

GARCÍA, Alfonso y ALEGRE, María, *Seguridad informática*, primera edición, Argentina, 2011.

LÓPEZ, Albert, *Análisis de la vitalización de sistemas operativos*, Facultad de Matemáticas - Universidad de Barcelona – Barcelona, España, 2010.

MORIANO, Ariel, *Criptografía: técnicas de desarrollo para profesionales*.- primera edición, Alfaomega Grupo Editor Argentino, 2009.

PILLA, Julio, *Implementación de seguridad en la red interna de datos para el manejo adecuado de usuarios y acceso remoto en el Instituto Tecnológico Pelileo*, Facultad de Ingeniería en Sistemas Electrónica e Industrial - Universidad Técnica de Ambato, Ambato, 2013.

YÁNEZ, Daniel, *Sistema de detección y prevención de intrusos para el control de la vulnerabilidad en los servidores de la facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato,* Facultad de Ingeniería en Sistemas Electrónica e Industrial - Universidad Técnica de Ambato, Ambato, 2013.

VIRTUAL

GÓMEZ, Ramón. *10029 Administración de servidores Linux, tercera edición.* 3ra. Edición, Sevilla, disponible en https://www.informatica.us.es/~ramon/articulos/AdminLinuxUbuntuFedora.pdf, 2011

MUÑOZ**,** Alfonso, *Libro electrónico de seguridad informática y criptografía*, Versión 4.1, Madrid, disponible en http://www.criptored.upm.es/guiateoria/gt_m001a.htm, 2006.

STALLMAN, Richard, *Software libre para una sociedad libre*, primera edición, Traficante de sueños, Madrid, disponible en http://www.gnu.org/philosophy/fsfs/free_software.es.pdf, 2004, ISBN 84-933555-1-8.

Universidad de Oviedo, *Grupo de Investigación en Algebra, Codificación y Criptografía*, disponible en https://matematicas.uniovi.es/investigacion/algebra.

SALINAS, Edwin, *Sistema operativo Centos*, disponible en http://es.scribd.com/doc/49507015/SISTEMA-OPERATIVO-CENTOS, 2011.