ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN SISTEMAS

ESTUDIO DE LOS PROTOCOLOS DE SEGURIDAD DEL SERVICIO DE CORREO ELECTRÓNICO PARA IMPLEMENTAR UN WEBMAIL EN EL HCPCH.

TESIS DE GRADO

Previo a la obtención del título de

INGENIERO EN SISTEMAS INFORMÁTICOS

Presentado por

JESÚS MANUEL PUETATE ESPINOZA

RIOBAMBA - ECUADOR

2009

AGRADECIMIENTO:

Quiero expresar mis más sinceros agradecimientos al Ing. Danilo Pastor Director de la Tesis de Grado y al Ing. Danny Velasco Miembro de la Tesis de Grado.

Por la ayuda y colaboración en el desarrollo de este proyecto de tesis.

Además a mis padres, hermanos, familiares y amigos que me animan minuto a minuto y que sufren conmigo esta afición, dedicación que no entiende de horas, ni fines de semana; a todos ellos muchas gracias.

La presente tesis de grado dedico a mis padres Rita y Manuel a mi esposa Patricia a mis hermanos que me han dado su apoyo en esta etapa importante de mi vida para hacer realidad mi formación como persona y profesional y de manera especial a mis queridos hijos Sebastián y Anahí

Jesús Manuel Puetate Espinoza.

FIRMAS DE RESPONSABILIDAD

	FIRMA	FECHA
Dr. Romeo Rodríguez DECANO DE LA FACULTAD INFORMÁTICA Y ELECTRÓNICA.	_____	_____
Ing. Iván Menes DIRECTOR DE LA ESCUELA INGENIERÍA EN SISTEMAS	_____	_____
Ing. Danilo Pástor DIRECTOR DE TESIS	_____	_____
Ing. Danny Velasco MIEMBRO TRIBUNAL	_____	_____
Tlgo. Carlos Rodríguez DIRECTOR DPTO. DOCUMENTACIÓN	_____	_____
NOTA DE TESIS		_____

“Yo, Jesús Manuel Puetate Espinoza soy responsable absoluto de las ideas, y resultados expuestos en esta tesis de grado, el patrimonio intelectual de la tesis de grado pertenece a la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO”.

_____

JESÚS MANUEL PUETATE ESPINOZA.

ÍNDICE DE ABREVIATURAS

CA	Autoridad Certificadora
CRL	Lista de Revocación de Certificados
DNS	(Domain Name System), Sistema de Nombres de Dominio
e-mail	(De electronic mail). Correo electrónico.
ESPOCH	Escuela Superior Politécnica de Chimborazo
FIE	Facultad de Informática y Electrónica
HCPCH	Honorable Consejo Provincial de Chimborazo
HTML	HyperText Markup Language
Http	Hyper Text Transfer Protocol (Protocolo de transferencia de Hyper Texto)
https.	SSL.
ISO.	Organización Internacional para la Normalización).
IETF	Grupo de Trabajo de Ingeniería de Internet
MDA	Mail Delivery Agent (Agente de entrega de correo)
MUA	Mail User Agent (gente De Usuario Mail)
MIME	Multipurpose Internet Mail Extensions
MTA	Mail Transfer Agent (Agente de Transporte Mail)
PHP	Hipertext Preprocessor (Pre-procesador de Hipertexto)
PKI	Infraestructura de Clave Pública.
PKCS7	Estándar de Clave Pública
POP3	Postal Office Protocol
PGP	Pretty Good Privacy
PGP/MIME	PGP adaptado al correo electrónico
RFC	Request for Comments (Solicitud de comentarios)
RPM	Red Hat Package Manager

SQL	Structured Query Language
SMTP	Protocolo Simple de Transferencia de Correo
S/MIME	Security MIME
TCP/IP	Protocolo de Control de Transmisión / Protocolo de Internet
VPN	Virtual Private Networks
USI	Unidad de Sistemas Informáticos
URL	Universal Resource Identifier (Identificador Universal de Recursos)
X.509	Formato de certificados digitales

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

La seguridad ha sido un elemento que tomó relevancia en la última década en los mundos de la Computación y las Comunicaciones, esto como un efecto natural en los ambientes que crecen de forma exponencial y que pierden las características de conocimiento y confianza entre quienes interactúan.

La seguridad no fue un aspecto considerado en el diseño inicial de los protocolos de comunicación y sistemas operativos, lo que ha ocasionado oportunidades diversas para acceder de forma no autorizada a redes y sistemas y ha dado lugar a una de las actividades más populares en estos días en el ciberespacio la intrusión de sistemas.

Bajo las siglas PKI se engloba a una tecnología estándar, impulsada por la ISO, ITU, y el IETF, que pretende llevar a la práctica los conceptos teóricos de la Criptografía de Clave Pública. La Criptografía de Clave Pública permite, entre otras cosas, implementar sistemas de firma digital y el cifrado de datos sin necesidad de compartición de secretos.

La firma digital garantiza la Integridad y el cifrado garantiza la Confidencialidad, pero indirectamente la criptografía de clave pública también permite garantizar la Autenticidad del receptor del mensaje cifrado o del emisor del mensaje firmado. Esto se consigue con el uso de certificados digitales, donde se asigna una identidad a una clave pública. La utilización de claves (públicas y privadas) y certificados digitales para firmar y cifrar correos electrónicos, autenticarse ante sitios Web, validar transacciones, solamente tienen éxito cuando existe transparencia entre las aplicaciones y los mecanismos que PKI utiliza para garantizar la seguridad.

CAPÍTULO I

MARCO REFERENCIAL

1.1. ANTECEDENTES

El correo electrónico es una de las aplicaciones de Internet más ampliamente utilizadas para el intercambio de información en el trabajo diario entre personas, empresas u organismos. No solo todos los usuarios tienen una dirección de correo-e sino que cada vez viene siendo más demandado y necesario ofrecer diferentes tipos de acceso al buzón desde la oficina, desde casa o cualquier otro punto a través de conexiones dial-up, VPNs o vía web, soporte a PDAs y teléfonos móviles etc. En definitiva la necesidad de acceder al correo-e es la que justifica el despliegue de nuevas tecnologías de conexión en la institución.

Precisamente por ser tan popular, actualmente el correo electrónico es uno de los servicios más afectados por los problemas de seguridad que proliferan en la Red. El correo-e permite comunicarnos de forma efectiva pero al mismo tiempo aumenta los

riesgos de nuestros sistemas. Un punto de entrada habitual a la red de una organización es por correo electrónico, tanto a través de servidores de correo inseguros o a través de los propios mensajes de correo electrónico.

Las claves de la debilidad de los protocolos del Servicio de correo (SMTP y POP/IMAP) los encontramos en:

• Transporte por la Red del correo en texto claro

• Debilidad del sistema de autenticación para recibir correo

• Ausencia de autenticación para enviar correo

Estos problemas son la causa de los múltiples problemas de seguridad que afectan al servicio, ataques a servidores, virus, gusanos, troyanos, spam, denegación de servicio, malware etc.

Además estos se ven aumentados por la ausencia en las organizaciones de políticas y procedimientos de seguridad así como políticas de uso aceptable de los recursos y la creencia que firewalls y antivirus es todo lo que se necesita.

Los efectos de estos problemas de seguridad en las organizaciones son: pérdida de productividad por ralentización o ausencia de recursos (aplicaciones, red y servidores), pérdida parcial o completa de la información, pérdida de privacidad etc.

La calidad en los Servicios de correo mejorará el servicio en las instituciones, garantizará y potenciará el intercambio de información (mensajes y ficheros).

Es así que la Unidad de Sistemas Informáticos del HCPCH no cuenta con un sistema Web para el servicio de correo electrónica, por lo cual es imprescindible solventar este

problema informático, ya que es una herramienta muy necesaria con la que deben contar las instituciones para mantener una mayor comunicación dentro y fuera de ella.

Esta institución necesita identificarse con su propia imagen por lo cual es necesario la implementación de una interfaz Webmail que le permita a los funcionarios y empleados acceder a su correo a través de la web, y que no tengan que llegar a sus computadoras en sus oficinas para poder revisar su correo institucional.

1.2. JUSTIFICACIÓN

Para sustentar la razón, importancia y visión de la presentación del proyecto de tesis consideramos aspectos técnicos y sociales, encaminados al aporte investigativo así como el aprovechamiento de los recursos tecnológicos con que cuenta la Institución.

La utilización de herramientas de software libre proporciona muchos beneficios una de ellas es de no preocuparse por la adquisición de licencia para su uso, es decir se tiene la libertad y flexibilidad de la utilización.

Una gran parte de la dinámica de las instituciones descansa sobre aplicaciones que dependen del correo electrónico, algunos de estos usos son:

• Comunicación entre directores y empleados

• Canales de distribución de información interna o externa

• Canal de comunicación y soporte de ayuda a clientes y ciudadanos

• Seguimiento de concursos públicos

• Correspondencia con otras entidades de la Administración

• Distribución de ofertas de empleo público

• Distribución rápida y efectiva de información a los ciudadanos

Es por esta razón la importancia de la implementación de este servicio de una manera que sea más confiable utilizando protocolos seguros para mail.

La funcionalidad se basa en la gran mayoría de las ediciones recientes de software de correo electrónico, de esta manera podemos incrementar el nivel de seguridad de la información que contiene los mensajes que viajan a través de la red.

Proporcionan dos servicios de seguridad:

Firmas digitales

Cifrado de mensajes

Estos dos servicios son el núcleo de la seguridad de los mensajes basada en protocolos seguros.

Todos los demás conceptos relacionados con la seguridad de los mensajes sirven de apoyo a estos dos servicios. Si bien todo el ámbito de la seguridad de los mensajes puede parecer complejo, estos dos servicios son la base de dicha seguridad. Una vez que adquiera unos conocimientos básicos de las firmas digitales y del cifrado de mensajes, podrá aprender cómo otros conceptos sirven de apoyo a estos servicios.

Se examinará cada servicio individualmente y después se ofrecerá información acerca de como funcionan conjuntamente los dos servicios.

Descripción de las firmas digitales

Las firmas digitales son el servicio más utilizado en los protocolos seguros. Como su nombre indica, las firmas digitales son la contrapartida digital a la tradicional firma legal en un documento impreso. Al igual que ocurre con una firma legal, las firmas digitales ofrecen las siguientes capacidades de seguridad:

Autenticación Una firma sirve para validar una identidad. Comprueba la respuesta a "quién es usted" al ofrecer una forma de diferenciar esa entidad de todas las demás y demostrar su unicidad. Como no existe autenticación en el correo electrónico SMTP, no hay ninguna forma de saber quién envió realmente un mensaje. La autenticación en una firma digital resuelve este problema al permitir que un destinatario sepa que un mensaje fue enviado por la persona o la organización que dice haber enviado el mensaje.

No rechazo La unicidad de una firma impide que el propietario de la firma no reconozca su firma. Esta capacidad se llama no rechazo. Así, la autenticación proporcionada por una firma aporta el medio de exigir el no rechazo. El concepto de no rechazo resulta más familiar en el contexto de los contratos en papel: un contrato firmado es un documento legalmente vinculante y es imposible no reconocer una firma autenticada. Las firmas digitales ofrecen la misma función y, cada vez en más áreas, se reconocen como legalmente vinculantes, de manera similar a una firma en un papel. Como el correo electrónico SMTP no ofrece ningún medio de autenticación, no puede proporcionar la función de no rechazo. Para el remitente de un mensaje de correo electrónico SMTP es fácil no reconocer la propiedad del mismo.

Integridad de los datos Un servicio de seguridad adicional que ofrecen las firmas digitales es la integridad de los datos. La integridad de los datos es uno de los resultados

de las operaciones que hacen posibles las firmas digitales. Con los servicios de integridad de datos, cuando el destinatario de un mensaje de correo electrónico firmado digitalmente valida la firma digital, tiene la seguridad de que el mensaje recibido es el mismo mensaje que se firmó y se envió, y que no se ha manipulado mientras estaba en tránsito. Cualquier alteración del mensaje mientras estaba en tránsito una vez firmado invalida la firma. De esta forma, las firmas digitales son capaces de ofrecer una garantía que no permiten tener las firmas en papel, ya que es posible alterar un documento en papel una vez que ha sido firmado.

El Honorable Consejo Provincial de Chimborazo con el afán de estar acorde a los avances tecnológicos está desarrollando la implantación de sistemas informáticos para la automatización de procesos, brindando así a los empleados y funcionarios de herramientas que ayuden a realizar de mejor manera las diferentes actividades diarias.

La aplicación Webmail se desarrollara en la Unidad de Sistemas Informáticos del HCPCH y los beneficios que se obtendrán con la implantación de esta aplicación van dirigidas a sumar prestaciones de servicio de internet, pudiendo acceder a su correo a través de la web y se podrá realizar las siguientes tareas, creación de cuentas de usuarios, envío y recepción de mensajes, métodos de revisión de mensajes y bandeja de entrada.

Con este servicio de mensajería propio de la institución permite realizar la imagen del HCPCH

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Estudiar los protocolos de seguridad del servicio de correo electrónico e implementar un Webmail para el Honorable Consejo Provincial de Chimborazo.

1.3.2. OBJETIVOS ESPECÍFICOS

- Estudiar la estructura, protocolos y los conceptos relacionados con el servicio de correo electrónico.
- Analizar los protocolos seguros de correo con sus principales características en seguridad de datos en los mensajes de correo electrónico.
- Configurar una infraestructura para el servicio de correo electrónico en el sistema operativo Linux con las características de seguridad analizadas.
- Diseñar e implementar una interfaz Webmail personalizada para el HCPCH que le permita gestionar la información de los mensajes de correo electrónico.

1.4. HIPÓTESIS

La aplicación de protocolos seguros en el servicio de correo electrónico permitirá implementar un sistema con mejor privacidad en la información.

CAPÍTULO II

MARCO TEÓRICO

2.1. ASPECTOS DEL CORREO ELECTRÓNICO

El correo electrónico, es una de las funciones de Internet más utilizadas en la actualidad, cualquier persona que tenga acceso a internet le permite enviar y recibir mensajes entre emisor y receptor cuando estos han acordado el intercambio. Es uno de los servicios más utilizados debido a que facilita las comunicaciones en cualquier momento y a cualquier parte. Se basa en el protocolo TCP/IP y su esquema de conexión es asíncrono, es decir, no requiere establecer una conexión entre emisor y receptor para transmitir. Por lo tanto al enviar un mensaje se requiere que el receptor revise su correo electrónico para leerlo, de lo contrario este permanece almacenado en un servidor de

correo hasta que el usuario lo busque. Es un error pensar que en el correo electrónico el receptor conocerá el mensaje inmediatamente después de enviado, para esto se requiere una conexión sincrónica o en línea, donde tanto trasmisor como receptor están listos para iniciar la charla.

Aspectos negativos:

- No garantiza que los mensajes lleguen a su destino.
- No asegura que el remitente sea quien dice ser.
- No mantiene el compromiso de avisar de las anomalías en el transcurso del envió del mensaje.
- Problema de seguridad si no se usa con los debidos controles, como virus troyanos, etc.
- El envío de mensajes, permite adjuntar al mensaje, archivos de texto, de video, de audio, imágenes, etc.

Sigue el modelo cliente/servidor: en el equipo servidor están definidas las cuentas de correo de los usuarios y sus buzones, y los clientes gestionan la descarga de correo así como su elaboración.

2.1.1. AGENTES

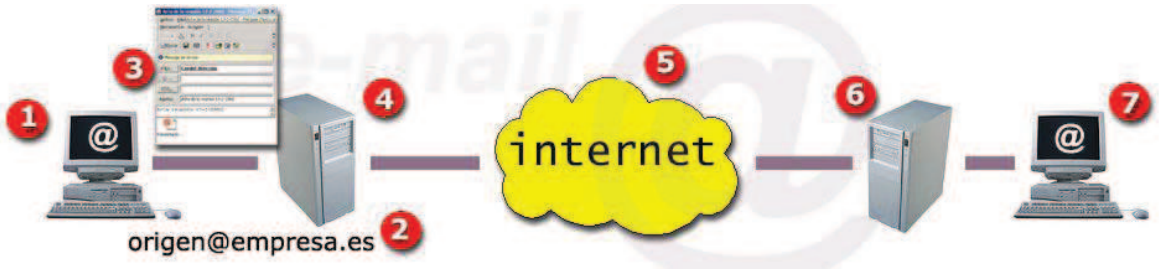


Figura 1: Agentes en una comunicación de correo electrónico

1. El software de correo-e del cliente.

2. La cuenta de origen del emisor. Ésta puede ser enmascarada por varios sistemas.

3. El mensaje puede ser alterado, eliminado o puede contener virus.

4. El servidor de correo del emisor y su software, alojado en proveedor de servicios internet (o en la propia empresa caso de disponer de software de correo servidor).

5. El canal: internet, donde los hackers pueden interceptarlo, otros proveedores de telecomunicaciones, los routers servidores DMZ, etc.

6. El servidor de correo del destino y su software (asociado al dominio de la cuenta y al ISP donde esté alojado este dominio).

7. El software del correo del receptor (MS Outlook, Lotus Notes, Thunderbird, etc.).

Todos estos agentes son potencialmente puntos de riesgo en la seguridad de un envío de correo electrónico.

2.2. FORMATO DE MENSAJES

Los mensajes de correo electrónico tienen una estructura que facilita la identificación del receptor y del remitente, así como detectar errores en la transmisión, etc.

En todo mensaje de distinguen dos partes:

Cabecera: campos con información fundamental para la transferencia del mensaje, puede saber a través de la información de la cabecera, quien le envió el mensaje como fue enviado.

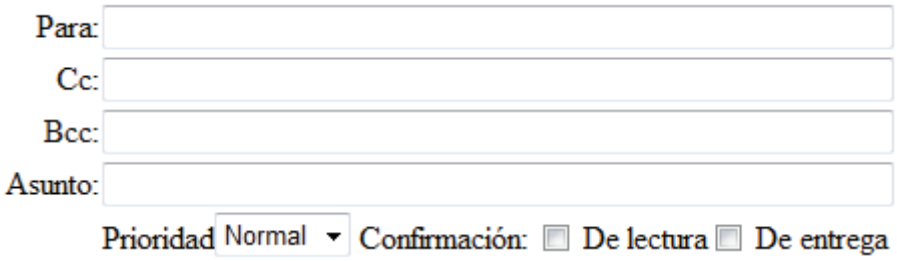


Figura 2: Campos de la Cabecera del mensaje de correo

Cuerpo: contiene la información propiamente dicha. Está compuesto por una serie de líneas con caracteres ASCII, y su tamaño, depende de la cantidad de información que el usuario transmite.

2.3. PROTOCOLOS

Hoy día, el correo electrónico es entregado usando una arquitectura cliente/servidor. Un mensaje de correo electrónico es creado usando un programa de correo cliente. Este programa luego envía el mensaje a un servidor. El servidor luego lo redirige al servidor de correo del recipiente y allí se le suministra al cliente de correo del recipiente.

Para permitir todo este proceso, existe una variedad de protocolos de red estándar que permiten que diferentes máquinas, a menudo ejecutando sistemas operativos diferentes y usando diferentes programas de correo, envíen y reciban correo electrónico o email.

Los protocolos de correo más usados son: SMTP, POP, e IMAP, aunque existen otros como el X.400 que no tienen mucha presencia en el servicio de correo electrónico. Su función es permitir que maquinas que usan diferentes sistemas operativos y utilizan diferentes clientes de correo electrónico se comuniquen y transfieran el correo electrónico.

2.3.1. PROTOCOLOS DE TRANSPORTE DE CORREO (SMTP).

Es un protocolo que se utiliza para dar servicio de Correos Electrónico, desde la PC de un usuario, sobre una conexión TCP/IP, a un servidor remoto, sin ser necesario que exista una conexión interactiva, ya que usa métodos de almacenamiento y reenvío de mensajes.

Este protocolo es un sencillo protocolo cliente/servidor en formato ASCII. Establecida una comunicación TCP entre la computadora transmisora del correo, que opera como cliente, y el puerto 25 de la computadora receptora del correo, que opera como servidor, el cliente permanece a la espera de recibir un mensaje del servidor SMTP esta descrito en la RFC 821 y es el estándar de Internet para el intercambio de correo electrónico. SMTP es un protocolo independiente del subsistema de transmisión usado.

Características.

Es el estándar de Internet para el intercambio de correo electrónico.

Es de tipo cliente/servidor.

Su función es el transporte de correo saliente desde el usuario remitente hasta el servidor que almacena los mensajes de los usuarios destinatarios.

Desde el servidor de correo del remitente se reenvía el mensaje al servidor de correo del destinatario.

Por último, el destinatario se descarga el correo de su buzón en la maquina local con el protocolo POP3, o lo consulta, vía Web, con el protocolo IMAP.

SMTP usa el puerto 25 del servidor, y el protocolo consiste en un conjunto de comandos y respuestas entre el emisor y el receptor.

Para que dos sistemas intercambien correo mediante SMTP, no es necesaria una conexión permanente e interactiva entre ellos.

SMTP no requiere autenticación.

Funcionamiento:

El emisor abre una conexión TCP

El receptor contesta

El emisor se identifica

El receptor acepta

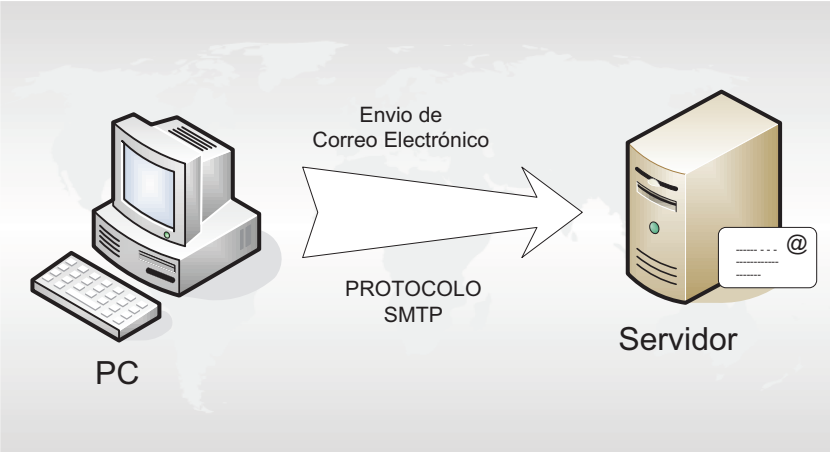


Figura 3: Protocolo SMTP

2.3.2. PROTOCOLO DE OFICINA DE CORREO (POP)

Cuando utilice un servidor POP, los mensajes de correo son descargados a través de las aplicaciones de correo del cliente. Por defecto, la mayoría de los clientes de correo POP son configurados automáticamente para borrar el mensaje en el servidor de correo después que éste ha sido transferido exitosamente, sin embargo esta configuración se puede cambiar.

POP es completamente compatible con estándares importantes de mensajería de Internet, tales como Multipurpose Internet Mail Extensions (MIME), el cual permite los anexos de correo, POP funciona mejor para usuarios que tienen un sistema que le permita leer su correo como son los clientes de correo electrónico. También funciona bien para usuarios que no tienen una conexión permanente a la Internet o a la red que contiene el servidor de correo. Desafortunadamente para aquellos con conexiones lentas, POP requiere que luego de la autenticación los programas cliente descarguen el contenido completo de cada mensaje. Esto puede tomar un buen tiempo si algún mensaje tiene anexos grandes.

Características.

Permite la gestión, acceso y transferencia de mensajes de correo electrónico entre el servidor remoto y la maquina cliente (usuario).

SMTP se usa para el envío de correo, POP para la recepción o descarga de correo.

Va por la tercera versión: POP3

Usa el buzón del usuario, en el servidor de correo, como mecanismo de interconexión.

En el buzón permanecen los mensajes hasta que el usuario los descarga a través de los clientes de correo, que usan el protocolo POP3.

El cliente POP3 se conecta con el servidor a través del puerto TCP 110.

Para que el cliente se conecte, el usuario tiene que tener una cuenta de correo en dicha maquina (lo que le permite tener un buzón).

El usuario se autentica, y el cliente POP3 se conecta con el servidor para saber si tiene mensajes y solicitar la descarga de uno de ellos.

Fases de la comunicación:

Conexión : servidor a la escucha en el puerto 110

Autenticación: El servidor espera un nombre y una clave.

Transacción: El buzón se bloquea y esta disponible para ser consultado.

Actualización: El usuario se desconecta y el servidor actualiza el buzón.

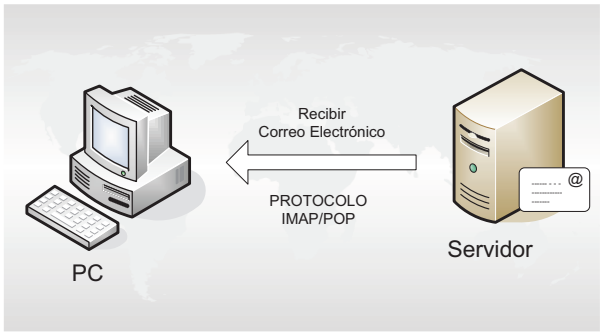


Figura 4: Protocolo POP

2.3.3. PROTOCOLO DE ACCESO A MENSAJES DE INTERNET (IMAP)

Usado por los clientes de correo para acceder a los mensajes almacenados en servidores remotos.

Cuando utilice un servidor de correo IMAP, los mensajes de correo se mantienen en el servidor donde los usuarios los pueden leer y borrarlos. IMAP también permite a las aplicaciones cliente crear, renombrar o borrar directorios en el servidor para organizar y almacenar correo.

IMAP lo utilizan principalmente los usuarios que acceden a su correo desde varias máquinas. El protocolo es conveniente también para usuarios que se estén conectando al servidor de correo a través de una conexión lenta, porque sólo la información de la cabecera del correo es descargada para los mensajes, hasta que son abiertos, ahorrando de esta forma ancho de banda. El usuario también tiene la habilidad de eliminar mensajes sin verlos o descargarlos.

Por conveniencia, las aplicaciones cliente IMAP son capaces de hacer caché de los mensajes localmente, para que el usuario pueda hojear los mensajes previamente leídos cuando no se esté conectado directamente al servidor IMAP.

IMAP, como POP, es completamente compatible con estándares de mensajería de Internet, tales como MIME, que permite los anexos de correo.

Características.

Acceso al correo desde cualquier máquina con acceso a Internet.

Permite manipular remotamente los buzones.

Proporciona movilidad a los usuarios.

El correo permanece en el servidor hasta que sea eliminado por el usuario.

Es compatible con el estándar MIME

Usa el puerto TCP 143

También es posible, haciendo uso de un cliente POP3 descargarlos a una maquina local.

2.4. MIME

MIME es un acrónimo de Extensiones Multipropósito de Correo de Internet, su importancia está dirigida facilitar, a través de correo electrónico, el intercambio de ficheros más complejos que los que sólo contenían caracteres de 7 bits, un grupo de trabajo de la IETF comenzó a trabajar en MIME.

El nuevo estándar ha quedado recogido en dos documentos, *RFC-1521* y *RFC-1522*. Estos escritos, que no son más que la actualización de las *RFC-1341* y *RFC-1342*, fueron puestos al día, a su vez, en marzo de 1994 por la *RFC-1590*.

MIME no establece un nuevo protocolo. Tan sólo constituye una forma normalizada de intercambio de mensajes electrónicos multimedia. Este sistema es compatible con los programas de correo electrónico que surgieron a partir de la *RFC-821*.

Una característica a destacar es que se trata de un sistema multiplataforma, ya que protege el formato binario del fichero, evitando así el tener que convertirlo a ASCII antes de leerlo.

Con respecto a los primeros sistemas, *MIME* dio un paso adelante en "transparencia", ya que las aplicaciones cliente pueden saber automáticamente de qué tipo de formato de fichero se trata, y, por tanto, la codificación y decodificación se realiza de forma transparente para el usuario.

Por otra parte, con *SMTP* sólo se garantizaba la integridad de mensajes cuya longitud de líneas no excediera los 1000 caracteres. *MIME*, por contra, divide el contenido del mensaje en múltiples partes que se recomponen, también de forma transparente, cuando el mensaje llega al receptor.

MIME más que un protocolo es un estándar que especifica como debe un programa (inicialmente un programa de correo o un navegador web) transferir archivos multimedia (video, sonido, por extensión cualquier archivo que no esté codificado en US-ASCII).

Con anterioridad al desarrollo de las extensiones MIME, cualquier archivo que no se limitase a texto ascii debía ser codificado a estos caracteres (uuencode uudecode).

2.4.1. TIPOS MIME

Los tipos MIME son una serie de especificaciones que permiten el intercambio a través de Internet, de todo tipo de archivos de forma transparente para el usuario.

Dan formato a mensajes no-ASCII, para poder ser enviados por Internet. Existen tipos MIME predefinidos (GIF, JPEG, Post-script) pero también podemos definir tipos MIME propios. Actualmente, hay una nueva versión llamada S/MIME que soporta mensajes encriptados. Además de ser usado para las transferencias de correo electrónico, es también usado por los navegadores, para incluir imágenes, videos, sonidos, etc. al contenido de la Web sin estar en formato HTML. En resumen, el tipo MIME, especifica el tipo de dato que contiene la información que se transfiere entre el cliente y el servidor.

Se adjunta información (campo enctype) donde se indica el tipo de contenido. Su objetivo final, es permitir que cualquier tipo de mensaje (texto, imágenes, voz, datos binarios, etc.) pueda ser enviado a través de SMTP de forma sencilla y transparente al usuario.

2.4.2. PRINCIPALES TIPOS MIME SOPORTADOS POR LOS NAVEGADORES:

Tabla II-1: Tipos de MIME

Tipo MIME	Extensión
Imagen	
image/bmp image/x-windows-bmp image/gif image/jpeg image/jpeg image/png	.bmp, .bm .bmp .gif .jpe .jpg .png
Sonido	
audio/basic audio/x-au audio/midi audio/x-midi audio/x-wav audio/mod audio/x-mod audio/mpeg3 audio/x-mpeg-3 audio/x-pn-realaudio audio/x-pn-realaudio	.au, .snd .au .mid, .midi .mid, .midi .wav .mod .mod .mp3 .mp3 .ra, .ram .ra, .ram
Video	
video/avi video/x-motion-jpeg video/quicktime video/mpeg application/x-shockwave-flash	.avi .mjpg .mov .mpg .swf

2.5. ELEMENTOS DEL SERVICIO DE CORREO ELECTRÓNICO

2.5.1. AGENTE DE TRANSFERENCIA DE CORREO (MTA)

Un Agente de Transporte de Correo (MTA) transfiere mensajes de correo electrónico entre hosts usando SMTP. Un mensaje puede involucrar varios MTAs a medida que este se mueve hasta llegar a su destino.

Aunque la entrega de mensajes entre máquinas puede parecer bien simple, el proceso completo de decidir si un MTA particular puede o debería aceptar un mensaje para ser repartido, es más bien complicado. Además, debido a los problemas de spam, el uso de un MTA particular está usualmente restringido por la configuración del MTA o por la configuración de acceso a la red en la que reside el MTA.

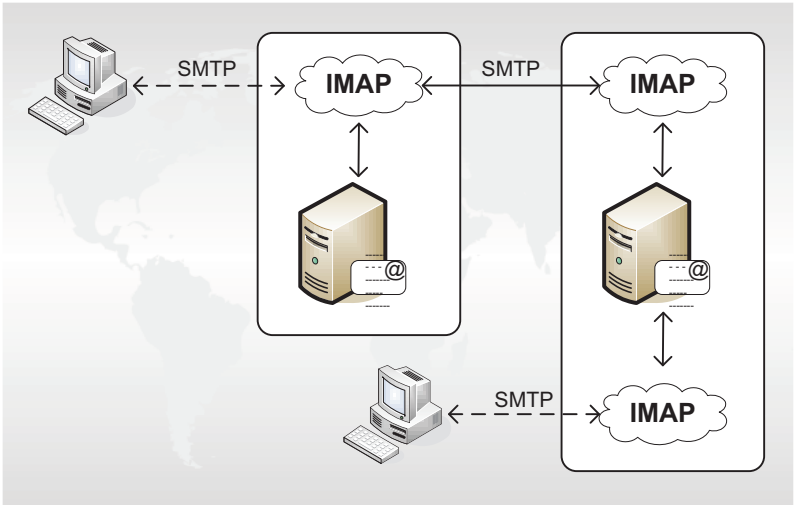


Figura 5: Agente MTA

Funciones.

Responsable del encaminamiento del correo entre dos sistemas.

Es el que se conoce como servidor de correo.

Gestiona la distribución de correo saliente, y está pendiente de la llegada de correo entrante desde Internet.

Ejemplos: Sendmail, Postfix, Qmail, Exim.

2.5.2. AGENTE DE ENTREGA DE CORREO (MDA)

Un MTA invoca a un Agente de entrega de correos (MDA) para archivar el correo entrante en el buzón de correo del usuario. En muchos casos, el MDA es en realidad un Agente de entregas local (LDA), tal como **mail** o Procmail.

Cualquier programa que maneje la entrega de mensajes hasta el punto en que puede ser leído por una aplicación cliente de correos se puede considerar un MDA. Por esta razón, algunos MTAs (tales como Sendmail y Postfix) pueden tener el papel de un MDA cuando ellos anexan nuevos mensajes de correo al archivo spool de correo del usuario. En general, los MDAs no transportan mensajes entre sistemas tampoco proporcionan una interfaz de usuario; los MDAs distribuyen y clasifican mensajes en la máquina local para que lo accese una aplicación cliente de correo.

Características.

Su función es copiar los mensajes del MTA al buzón de correo del usuario.

No transporta mensajes entre sistemas ni es un interfaz de trabajo para el usuario.

Ejemplos: Clientes de correo POP e IMAP.

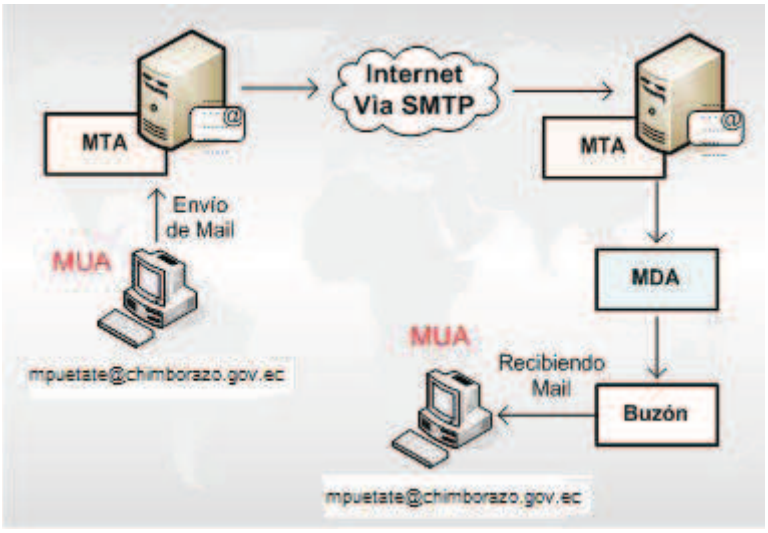


Figura 6: Agente MDA

2.5.3. AGENTE DE USUARIO DE CORREO (MUA)

Un agente de usuario de correo (MUA) es sinónimo con una aplicación cliente de correo. Un MUA es un programa que, al menos le permite a los usuarios leer y redactar mensajes de correo. Muchos MUAs son capaces de recuperar mensajes a través de los protocolos POP o IMAP, configurando los buzones de correo para almacenar mensajes y enviando los mensajes salientes a un MTA.

Características.

Constituye el interfaz de usuario que le permite editar, componer, y enviar correo local.

Son los llamados clientes de correo.

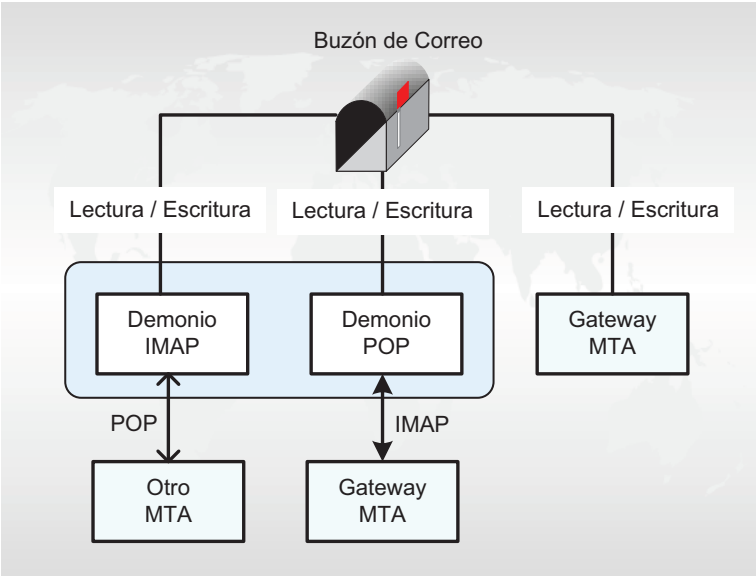


Figura 7: Agenta MUA

2.6. VULNERABILIDADES

El software está desarrollado por humanos, quienes modelan e implantan programas a su criterio, concepto y conocimiento del lenguaje de programación que utilizan, es común, en consecuencia, encontrar imperfecciones en los sistemas. Son estas imperfecciones las que propician oportunidades para accesos no autorizados, las que se conocen como vulnerabilidades de los sistemas.

La propia estructura de la red IP causa que la transmisión de información a través de las redes que los emplean sea insegura. Esto se debe a que los paquetes enviados por el originario de la información tienen que ser leídos por un número indeterminado de Reuters y dispositivos varios, antes de llegar a su destino.

Para estudiar las vulnerabilidades y las soluciones de seguridad en la transmisión y recepción de un mensaje de correo electrónico, debemos tener claro este circuito desde

que el emisor envía un mensaje, hasta que es recibido por el receptor. En todo este camino, intervienen varios agentes, que son todos ellos, a priori, vulnerables.

2.7. PREVENCIÓN DE LOS ATAQUES

Los ataques son los medios por los cuales se explotan las vulnerabilidades, se identifican dos tipos de ataques: extracción pasiva y extracción activa.

En la extracción pasiva el atacante escucha, sin modificar mensajes o afectar la operación de la red. Generalmente no puede detectarse este tipo de ataque, pero sí prevenirse mediante mecanismos como la encriptación de información.

Los objetivos del atacante son la intercepción y el análisis de tráfico en la red. Al estar escuchando el tráfico, el atacante puede identificar:

• El origen y destino de los paquetes de comunicación, así como la información de cabecera.

• Monitorear el tráfico y horarios de actividad.

• Identificar el uso de protocolos y observar la transferencia de datos entre protocolos que no utilicen encriptado, por ejemplo la versión no segura de telnet o ftp que transfieren la clave de usuario en texto simple.

En la extracción activa el atacante modifica los mensajes o irrumpe la operación de la red. El atacante tiene como objetivo modificar datos o bien crear tráfico falso. Este tipo de ataque, generalmente puede detectarse, pero no prevenirse. La gama de actividades identificadas sobre ataques conocidos puede clasificarse en cuatro categorías:

1. Modificación de mensajes: al interceptar mensajes, se altera su contenido o su orden para irrumpir su flujo normal.

2. Degradación y fraude del servicio: tiene como objetivo intervenir el funcionamiento normal de un servicio, impide el uso o la gestión de recursos en la red. Ejemplo de este ataque es el de negación de servicio (DoS, Denial of Service), donde se suprimen los servicios de SMTP, HTTP, FTP, DNS, entre otros.

3. Re actuación: al interceptar mensajes legítimos, se capturan y repiten para producir efectos diversos, como el ingresar dinero repetidas veces en una cuenta de banco.

4. Suplantación de identidad: Este es uno de los ataques más completos y nocivos. El intruso o atacante adopta una identidad con privilegios en una red y explota esos privilegios para sus fines. Un ataque con prioridad de atención para todo administrador de red es el "spoofing" donde el intruso obtiene servicios basados en la autenticación de computadoras por su dirección IP. Es recomendable seguir una estrategia y de preferencia tener una herramienta para combatirlos [Baluja, 2000]. Todos estos ataques tienen un impacto relativo a la política de seguridad de un sistema, aunque en Internet dentro de los más temidos se encuentra el DoS por su relevancia al suprimir el funcionamiento de un sistema, y el Spoofing al obtener privilegios de acceso de forma fraudulenta.

2.7.1. CONTRAMEDIDAS.

Lo más importante es contar con una Política de Seguridad, un documento legal y con apoyo directivo, que define la misión, visión y objetivos de los recursos de red e información en cuestión. En una política se define lo que es permitido y lo que no, las

necesidades de confidencialidad, autenticación y otros servicios de seguridad para los recursos involucrados. Toda red debe contar con una política de seguridad.

Las contramedidas son entonces, las políticas de seguridad apoyadas por todos los medios técnicos o de procedimientos que se aplican y desarrollan para atender vulnerabilidades y frustrar ataques específicos. Como: reglamentos, firewalls, nessus, ssh, tcp-wappers, antivirus, kerberos, radius, entre muchos otros comerciales o de dominio público.

2.7.2. AMENAZAS.

Las amenazas están dadas por condiciones de entorno, dada una oportunidad y adversarios motivados y capaces de montar ataques que explotan vulnerabilidades, podría producirse una violación a la seguridad (confidencialidad, integridad, disponibilidad y/o uso legítimo). Los perfiles de capacidades de los atacantes se identifican como sigue:

• Inserción de mensajes solamente.

• Escuchar e introducir mensajes.

• Escuchar y obstruir.

• Escuchar, obstruir e insertar mensajes.

• Escuchar y remitir un mensaje ("hombre en el medio")

• Capacidades activas y pasivas de forma unidireccional o bidireccional

Cada enlace en una red y cada recurso es susceptible a diferente tipo de amenazas, de ataques, y quizá a diferentes atacantes. El análisis de riesgos y el monitoreo constante de

vulnerabilidades pueden identificar las amenazas que han de ser contrarrestadas, así como especificar los mecanismos de seguridad necesarios para hacerlo.

De acuerdo a la figura, las cuatro categorías generales de amenazas que se utilizan en la actualidad son las siguientes:

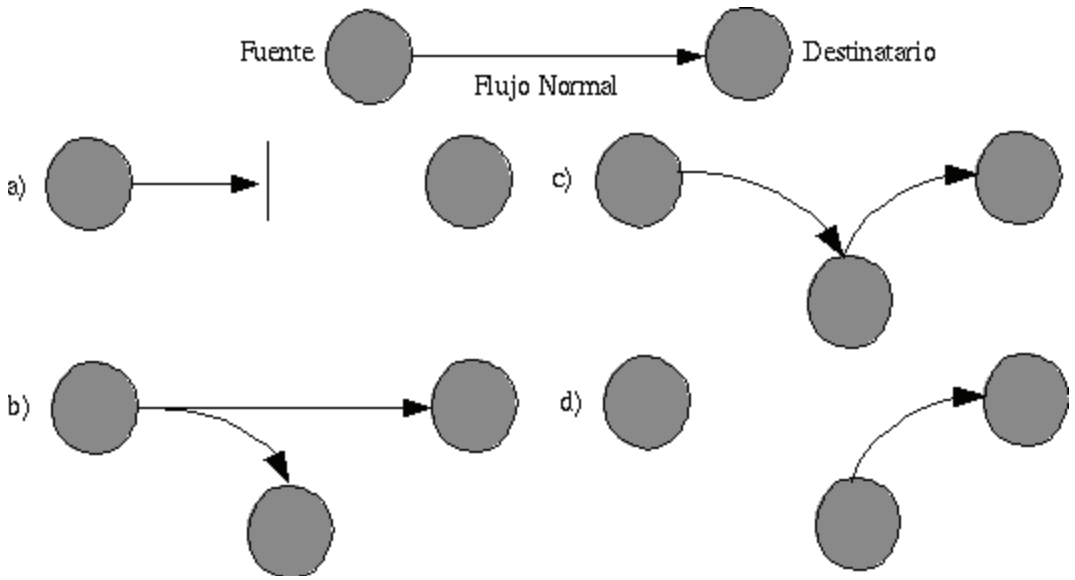


Figura 8: Categorías de amenazas

a) Interrupción, b) Intercepción, c) Modificación, d) Falsificación.

De acuerdo a la figura, las cuatro categorías generales de amenazas que se utilizan en la actualidad son las siguientes:

a). **Interrupción:** es una amenaza contra la disponibilidad, el ataque ocasiona que un recurso del sistema deje de estar disponible, destruir un elemento de hardware o cortar una línea de comunicación.

b). **Intercepción:** es una amenaza contra la confidencialidad, el ataque produce la captura no autorizada de información en el medio de transmisión, mediante el uso de Sniffers, pueden tomar lectura de cabeceras, intercepción de datos.

c). **Modificación:** es una amenaza contra la integridad, el ataque produce no solo el acceso no autorizado a un recurso sino también la capacidad de manipularlo, como modificación del contenido de mensajes interceptados, alterar programas para modificar su funcionamiento.

d). Falsificación: es una amenaza contra la autenticidad, el ataque produce que una entidad no autorizada inserte mensajes falsos en el sistema, como sustitución de usuarios, alterar archivos, inserción de mensajes falsos en la red.

2.8. SISTEMAS SEGUROS DE CORREO ELECTRÓNICO

El correo electrónico es uno de los sistemas telemáticos más vulnerables a los ataques a la seguridad, actualmente el correo electrónico es muy importante a nivel profesional y es la herramienta que se ha desarrollado más rápidamente en internet, pero durante muchos años la parte pendiente ha sido la seguridad con sus cuatro formas: confidencialidad, integridad, autenticación y firmas.

Cuando un usuario envía un mensaje, pierde el control sobre él, es decir, su contenido puede ser leído por cualquiera que lo manipule hasta llegar a su destino.
Se define como correo seguro, aquel que garantiza los siguientes aspectos:

Confidencialidad

Autenticación

Integridad

Algunos conceptos importantes relativos al correo seguro son:

Autoridad de Certificación (CA)

Certificado Digital

Certificado raíz

2.9. ALTERNATIVAS PARA E-MAIL SEGUROS

Los servicios de seguridad pueden ser agregados a cada enlace de comunicación a lo largo de una trayectoria dada, o pueden ser integrados alrededor de los datos que están siendo enviados, siendo esto independiente de los mecanismos de comunicación, este enfoque avanzado es frecuentemente llamado seguridad "nodo-a-nodo". Las dos características de este tipo de seguridad son privacidad (donde el recipiente deseado sólo puede leer el mensaje) y la autentificación (en el otro caso, recipiente puede asegurar la identidad del emisor). La capacidad técnica de estas funciones es bien conocida desde hace tiempo, sin embargo, recientemente ha sido sólo aplicada al correo-e.

Es usual que se cuente con un mecanismo de autentificación de quién origina el mensaje y privacidad para los datos. Además, de proveer un esquema de recepción firmada desde el recipiente. En núcleo de estás capacidades en el uso de la tecnología de llave pública y el uso a gran escala de llaves públicas, lo que requiere un método de certificación que dada una llave pertenece a un usuario dado. Aunque, se ofrecen servicios parecidos al usuario final, los dos protocolos tienen formatos distintos. Adicionalmente, y esto es importante a los usuarios corporativos, en este caso se cuenta con diversos formatos para los certificados. Lo que significa, que no sólo los usuarios no pueden comunicarse con los que usen otro, además, no pueden compartir los certificados de autenticación. La diferencia entre los dos protocolos es

parecida a la diferencia entre los formatos GIF y JPEG, siendo que hacen las mismas cosas, más no su formato entre ellos.

Existen dos propuestas principales para ofrecer los servicios de seguridad que hemos mencionado: S/MIME y PGP. Otros protocolos han sido propuestos en el pasado como son PEM y MOSS, no han tenido mayor presencia. Sin embargo, ahora diversos proveedores de servidores de correo-e, incluyen en sus productos a S/MIME, PGP/MIME y OpenPGP que son versiones del protocolo PGP utilizadas para correo.

2.9.1. CRIPTOGRAFÍA

La criptografía comprende toda una familia de tecnologías que incluyen las siguientes:

Encriptación. Transforma la información en una forma no legible asegurando la privacidad.

Desencriptación. Es el inverso de la encriptación; es decir, transforma la información encriptada a su forma original legible.

Autentificación. Identifica a una entidad como un individuo, una máquina en la red o una organización.

Firmas digitales. La relación de un documento con el dueño de una ``llave" particular siendo el equivalente a la firma de un documento.

Verificación de firmas. Es lo contrario de la firma digital; verifica que una firma en particular sea válida.

Llave simétrica o secreta. Utiliza una misma llave para encriptar y desencriptar la información enviada a través de la red; pero el problema que se presenta es que tanto

quien envía como quien recibe la información deben tener la misma llave asegurándose que nadie más pueda obtenerla porque si intercepta la información pudiera desencriptarla y leerla fácilmente.

Llave asimétrica o pública. Fue inventada en 1976 por Whitfield Diffie and Martin Hellman para resolver el problema presentado por la llave simétrica. Es un método de transmisión de información en donde el que recibe la información puede estar seguro de la identidad de quien la envió. La idea básica de este método es el uso de un par de llaves:

Llave privada. Sólamente su dueño la conoce y se usa para desencriptar la información enviada por otras personas.

Llave pública. Esta se publica y se usa por cualquier persona para encriptar la información antes de enviarla a su destino (dueño).

El par de llaves se genera simultáneamente, usando algoritmos especiales en donde los mensajes que se encriptan con la llave pública de una persona puedan ser desencriptados solamente con la llave privada de esa misma persona y viceversa. Por lo tanto, para establecer una comunicación segura ya no es necesario compartir primeramente una llave privada.

Por ejemplo, si un cliente deseara enviar información segura a un servidor, el servidor daría su llave pública (por correo electrónico) y el cliente haría lo siguiente:

Encripta la información usando la llave pública del servidor y luego se la envía.

El servidor recibiría la información y la desencriptaría usando su llave privada.

Esta transmisión es segura en el sentido de que nadie más que reciba la información podrá leerla porque no sabe el valor de la llave privada.

Existe un problema que reside en el hecho de que la llave pública no puede ser verificada. Cómo se que la llave pública realmente es suya y no una llave pública generada por algún impostor que desee interceptar sus mensajes. Este problema es más serio cuando es usado para verificar automáticamente la comunicación entre dos ``hosts'', tales como un cliente (``browser'') y un servidor (DNS dinámico). Aquí es donde intervienen los certificados.

2.9.2. FIRMAS DIGITALES

El paradigma de firmas electrónicas (también llamadas firmas digitales) es un proceso que hace posible garantizar la autenticidad del remitente (función de autenticación) y verificar la integridad del mensaje recibido.

Las firmas electrónicas también poseen una función de reconocimiento de autoría, es decir, hacen posible garantizar que el remitente ha enviado verdaderamente el mensaje.

2.9.3. FUNCIÓN HASH

Una función hash es una función que hace posible obtener un hash (también llamado resumen de mensaje) de un texto, es decir, obtener una serie moderadamente corta de caracteres que representan el texto al cual se le aplica esta función hash. La función hash debe ser tal que asocie únicamente un hash con un texto plano (esto significa que la mínima modificación del documento causará una modificación en el hash). Además, debe ser una función unidireccional para que el mensaje original no pueda ser

recuperado a partir del hash. Si existiera una forma de encontrar el texto plano desde el hash, se diría que la función hash presenta una "trapdoor".

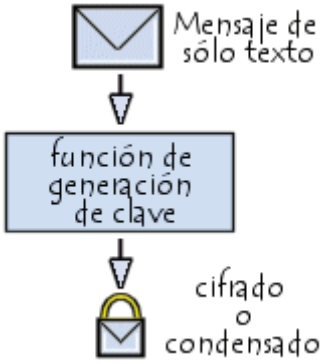


Figura 9: Función Hash

Como tal, puede decirse que la función hash representa la huella digital de un documento.

Los algoritmos hash más utilizados son:

MD5 (*MD* que significa *Message Digest; en castellano, Resumen de mensaje*), el MD5 crea, a partir de un texto cuyo tamaño es elegido al azar, una huella digital de 128 bits procesándola en bloques de 512 bits. Es común observar documentos descargados de Internet que vienen acompañados por archivos MD5: este es el hash del documento que hace posible verificar su integridad.

SHA (*Secure Hash Algorithm; en castellano, Algoritmo Hash Seguro*) crea una huella digital que tiene 160 bits de longitud. SHA-1 es una versión mejorada de SHA que data de 1994. Produce una huella digital de 160 bits a partir de un mensaje que tiene una longitud máxima de 2^{64} bits y los procesa en bloques de 512 bits.

Verificación de la integridad

Al enviar un mensaje junto con su hash, es posible garantizar la integridad de dicho mensaje, es decir, el destinatario puede estar seguro de que el mensaje no ha sido alterado (intencionalmente o por casualidad) durante la comunicación.

Cuando un destinatario recibe un mensaje simplemente debe calcular el hash del mensaje recibido y compararlo con el hash que acompaña el documento. Si se falsificara el mensaje (o el hash) durante la comunicación, las dos huellas digitales no coincidirían.

Sellado de datos

Al utilizar una función hash se puede verificar que la huella digital corresponde al mensaje recibido, pero nada puede probar que el mensaje haya sido enviado por la persona que afirma ser el remitente.

Para garantizar la autenticidad del mensaje, el remitente simplemente debe cifrar (generalmente decimos *firmar*) el hash utilizando su clave privada (el *hash firmado* se denomina sello) y enviar el sello al destinatario.

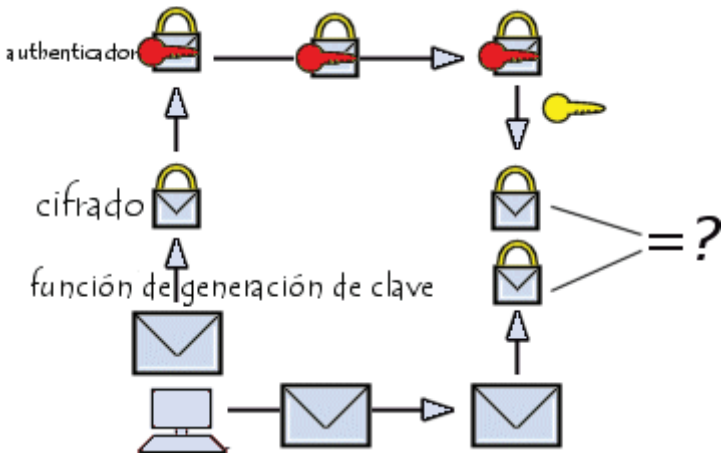


Figura 10: Cifrado de Mensaje

Al recibir el mensaje, el destinatario deberá descifrar el sello con la clave pública del remitente, luego deberá comparar el hash obtenido con la función hash del hash recibido como adjunto. Esta función de creación de sellos se llama sellado.

2.9.4. AUTORIDAD CERTIFICADORA (CA)

Una Autoridad Certificadora es la encargada de confirmar que el dueño de un certificado es realmente la persona que dice ser. Una Autoridad Certificadora puede definir las políticas especificando cuáles campos del *Nombre Distintivo* son opcionales y cuáles requeridos. También puede especificar requerimientos en el contenido de los campos.

Existen varias Autoridades Certificadoras, puede que una autoridad certificadora certifique o verifique la identidad de otra Autoridad Certificadora y así sucesivamente; pero habrá un punto en que una Autoridad no tendrá quién la certifique, en este caso, el certificado es firmado por uno mismo, por lo tanto, la Autoridad Certificadora es verificada o confiada por ella misma.

Las Autoridades Certificadoras (o notarios electrónicos) deben ser entes fiables y ampliamente reconocidos que firman las claves públicas de las personas, certificando con su propia firma la identidad del usuario. Por lo tanto, si se desea establecer una Autoridad Certificadora, éstas deben tomar extremadas precauciones para evitar que sus claves caigan en manos de intrusos, lo cual comprometería todo el sistema. Para ello tendrá que utilizar claves largas y dispositivos especiales para su almacenamiento. Además, cuando emiten un certificado, deben estar seguros de que lo hacen a la persona adecuada. No podemos olvidar que la Autoridad Certificadora es la

responsable, en última instancia, de todo el proceso, con una serie de responsabilidades legales y que basa su negocio en la credibilidad que inspire en sus potenciales clientes. Una Autoridad Certificadora con autentificaciones erróneas no tendrá más remedio que cerrar ya que los usuarios no considerarán sus certificados de la suficiente calidad.

Las Autoridades Certificadoras no solamente ofrecen certificados, sino también los manejan; es decir, determinan cuánto tiempo van a ser válidos y mantienen listas de certificados que ya no son válidos (Listas de Revocación de Certificados o CRLs).

Por ejemplo, si un empleado posee un certificado para una compañía y el empleado sale de la compañía, no solamente con el certificado se indica que ya no existe sino que se tiene que registrar por medio del CRL para que dicho certificado que ya había sido utilizado quede invalidado y no pueda ser utilizado posteriormente.

Varias compañías se han establecido como Autoridades Certificadoras. Entre las cuales destacan:

- VeriSign, Inc. *[http://www.verisign.com]*
- Thawte Certification. *[http://www.thawte.com]*
- Xcert Sentry CA. [http://www.xcert.com]
- Entrust. [http://www.entrust.net]
- Cybertrust. [http://www.baltimore.com]

Estas compañías proveen los servicios de:

- Verificación de solicitud de Certificados.
- Procesamiento de solicitud de Certificados.
- Firma, asignación y manejo de Certificados.

2.9.4.1. **Contenido de un certificado**

Los certificados pueden adoptar múltiples formas. El formato más difundido está definido por la norma del ITU-T X.509 , la cual forma parte del servicio de directorio diseñado por ISO(International Organization for Standardization, Organización Internacional de Estandarización) para el modelo OSI(Open System Interconnection, Interconexión de Sistemas Abiertos).

Un certificado X.509 es típicamente un archivo pequeño que contiene la información mostrada a continuación:

Nombre Distintivo de la entidad. Incluye la información de identificación (el nombre distintivo) y la llave pública.

Nombre Distintivo de la Autoridad Certificadora. Identificación y firma de la Autoridad Certificadora (CA) que firmó el certificado.

Período de Validez. El período de tiempo durante el cual el certificado es válido.

Información adicional. Puede contener información administrativa de la CA como un número de serie o versión.

El *Nombre Distintivo de la entidad* se usa para proveer una identidad en un contexto específico de acuerdo a las necesidades de la aplicación. Los Nombres Distintivos están definidos en el estándar X.509, así como por las necesidades de la aplicación.

2.9.4.2. **Funcionalidad de los certificados**

Los certificados se ofrecen por parte de una Autoridad Certificadora a la solicitud de una persona, entidad u organización que así lo requiera.

Enviar información encriptado usando la verificación de certificados:

Se envía un mensaje pidiendo su certificado.

Usted regresa su certificado.

Se verifica con la Autoridad Certificadora que su certificado sea válido. Especialmente, que dicha Autoridad Certificadora fue quien le dio el certificado y que su llave pública es la misma que la del certificado.

Se recibe la confirmación de la Autoridad Certificadora que el certificado es válido.

La información se encripta usando su llave pública y luego es enviada. Usted recibe la información y la desencripta usando su llave privada.

CAPÍTULO III

ANÁLISIS COMPARATIVO DE PROTOCOLOS SEGUROS

3.1. INTRODUCCIÓN

La determinación del protocolo seguro en el servicio de correo electrónico para la implementación de un sistema Webmail, tiene que ser una de las decisiones más importante que deben tomar los administradores de sistema de mensajería, lo cual debe fundamentarse en minuciosos análisis de acuerdo a métricas o parámetros de comparación y que permita satisfacer los requerimientos de las empresas que necesiten hacer uso de este servicio.

Para la determinación de los criterios de comparación entre los protocolos se basa en características más importantes que se deben tomar en cuenta en la seguridad de datos en los mensajes de correo electrónico.

En este capítulo se presentara los protocolos seguros de correo electrónico opcionales para su implantación del servicio según los parámetros o métricas, estos nos servirán para comparar los protocolos entre ellos tenemos: PGP/MIME, PGP, OPENPGP S/MIME, PEM de entre estos protocolos los más importantes son PGP/MIME y S/MIME.

3.2. DETERMINACIÓN DE LOS PROTOCOLOS A COMPARAR

Existen diferentes protocolos para correo seguro de los cuales escogeremos dos más importantes basados en estudios realizados por usuarios de clientes de correo electrónico por las razones que explicaremos a continuación.

En el portal web de Clientes de correo electrónico seguros con PGP/MIME http://www.bretschneidernet.de/tips/secmua.html.en se realizo un estudio comparativo entre las versiones para correo de PGP como son OpenPGP, PGP/MIME y PGPinline donde demuestra claramente que PGP/MIME tiene varias ventajas sobre las demás versiones antes mencionadas de lo cual se obtuvo los siguientes resultados:

El adjunto del mensaje (ejemplo Texto, hoja de cálculo, documentos PDF etc.) son encriptados y firmados.

No pueden usarse caracteres ASCII.

La firma de PGP es separada del cuerpo del mensaje, está en un adjunto estos son los motivos:

Leer el correo electrónico más fácilmente ya que usted no será impedido por la firma PGPinline.

Responder más fácilmente ya que la firma PGP no necesita ser borrado.

Menos fallas ya que el texto del email no puede ser modificado por la inserción de la firma PGP.

PGP/MIME esta especificado en el RFC 3156, en el sitio web llamado http://www.imc.org/smime-pgpmime.html, especifica claramente en su artículo se seguridades en las comunicaciones que existieron varios protocolos en el pasado como son PEM y MOSS que no tuvieron el suficiente interés en el mercado por lo cual no han podido tener una presencia en la actualidad.

Pero existen dos protocolos propuestos en la actualidad para proporcionar ciertos parámetros de seguridad en el correo electrónico ellos son S/MIME y PGP en sus versiones (PGP/MIME y OpenPGP).

En el documento de aplicaciones seguras en internet publicado en la página web http://www.scribd.com/doc/4605572/Aplicaciones-Seguras se determina que el protocolo PEM fue uno de los primeros sistemas de correo seguro que se desarrollaron: la primera versión se publicó en la especificación RFC 989. Estaba basado directamente en el estándar RFC 822, y solamente contemplaba el envío de mensajes de texto ASCII. Actualmente está en desuso, pero algunas de las técnicas que usaba se continúan utilizando actualmente en los sistemas más modernos.

Es por esto que para la realización de este estudio comparativo se han seleccionado a los protocolos seguros S/MIME y PGP/MIME por las siguientes razones.

Los dos protocolos tienen mayor presencia en los diferentes clientes de correo electrónico actuales como son Outlook, kmail, thunderbird de mozilla y en squirrelmail existen plug-in que le permiten leer correos enviados con s/mime.

Los diferentes desarrolladores de software de correo electrónico utilizan estos dos estándares para agregar seguridades a sus sistemas.

Proporcionan seguridad a las aplicaciones en internet mediante firmas digitales y cifrado del mensaje

3.3. PROTOCOLO PGP/MIME

PGP/MIME es una norma para algunos de los complementos PGP que integran las funciones PGP directamente a las aplicaciones de correo electrónico populares. Si se está usando una aplicación de correo electrónico que es soportada por uno de los complementos que ofrecen PGP/MIME, se podrá cifrar y firmar, así como descifrar y autenticar automáticamente los mensajes de correo electrónico y archivos adjuntos cuando envíe o reciba un correo electrónico.

3.3.1. CARACTERÍSTICAS.

PGP/MIME es un sistema de criptografía híbrido que usa una combinación de funciones tomadas de la criptografía de clave pública y de la criptografía simétrica.

Cuando un usuario cifra un texto con PGP, los datos primero se comprimen. Esta compresión de datos permite reducir el tiempo de transmisión a través del canal de comunicación, ahorra espacio en disco y, lo más importante, aumenta la seguridad criptográfica.

La mayoría de los criptoanálistas sacan provecho de los modelos encontrados en formato de sólo texto para descubrir el cifrado. La compresión reduce estos modelos de sólo texto y mejora considerablemente su resistencia a los criptoanálistas.

El cifrado se realiza, principalmente, en dos fases:

PGP crea una clave secreta IDEA en forma aleatoria y cifra los datos con esta clave.

PGP cifra la clave secreta IDEA y la envía usando la clave pública RSA del receptor.

El descifrado también se produce en dos fases:

PGP descifra la clave secreta IDEA usando la clave privada RSA.

PGP descifra los datos con la clave secreta IDEA obtenida previamente.

El método de cifrado combina la fácil utilización del cifrado de la clave pública con la velocidad del cifrado convencional. El cifrado convencional es aproximadamente 1000 veces más rápido que los algoritmos de cifrado de clave pública. El cifrado de clave pública resuelve el problema de la distribución de la clave. Combinados, estos dos métodos mejoran el rendimiento y administración de las claves sin poner el peligro la seguridad.

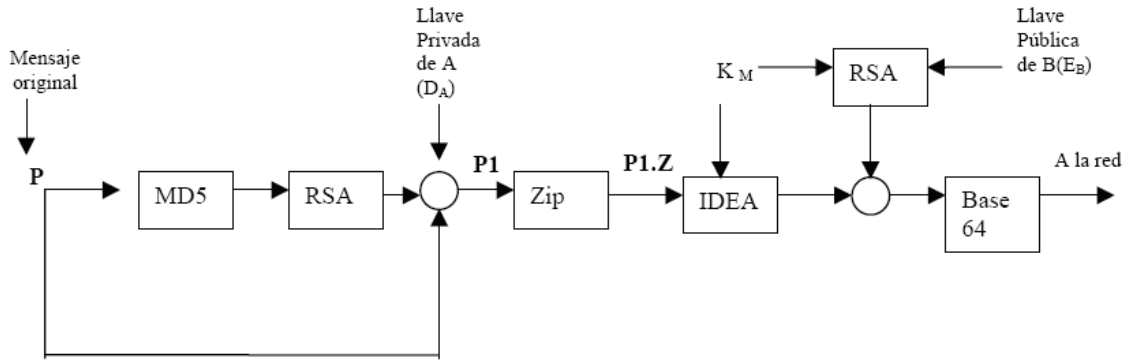


Figura 11: Operación de pgp/mime para enviar mensajes

3.3.2. FUNCIONES.

La PGP ofrece las siguientes funciones:

Firmas digitales y verificación de la integridad de los mensajes: función que se basa en el uso simultáneo de la función hash (MD5) y del sistema RSA. La función MD5 condensa el mensaje y produce un resultado de 128 bits que después se cifra, gracias al algoritmo RSA, por la clave privada del emisor.

Cifrado de archivos locales: función que utiliza el algoritmo IDEA.

Generación de claves públicas o privadas: cada usuario cifra su mensaje mediante las claves privadas IDEA. La transferencia de las claves electrónicas IDEA utiliza el sistema RSA. Por lo tanto, PGP ofrece dispositivos para la generación de claves adaptados al sistema. El tamaño de las claves RSA se propone de acuerdo con varios niveles de seguridad: 512, 768, 1024 ó 1280 bits.

Administración de claves: función responsable de la distribución de la clave pública del usuario a los remitentes que desean enviarle mensajes cifrados.

Certificación de claves: esta función permite agregar un sello digital que garantice la autenticidad de las claves públicas. Es una característica original de PGP, que basa su confianza en una noción de proximidad social en vez de en una entidad de certificación central.

Revocación, desactivación y registro de claves: función que permite producir certificados de revocación.

3.3.3. FORMATO DE LOS MENSAJES PGP

Los datos que procesa PGP se codifican con unas estructuras de datos llamadas paquetes PGP. Un mensaje PGP está formado por uno o más paquetes PGP.

Un paquete PGP es una secuencia de bytes, con una cabecera que indica de qué tipo de paquete se trata y su longitud y, a continuación, unos campos de datos que depenen del tipo de paquete.

A continuación veremos los principales tipos de paquetes PGP.

Paquete de datos literales

Sirve para representar datos en claro, sin cifrar (sería el análogo del contenido Data en PKCS #7).

En un paquete de este tipo existe un campo que da el valor de los datos, y otro que indica si este valor se debe procesar como texto o como datos binarios. En el primer caso, las secuencias <CR><LF> que haya en el texto corresponden a finales de línea y se pueden convertir a la representación local cuando se tengan que visualizar o guardar en fichero, mientras que en el segundo caso no se tienen que modificar.

Paquete de datos comprimidos

En este tipo de paquete hay un campo que indica el algoritmo de compresión, y otro que contiene una secuencia de bytes comprimida. Cuando se descomprimen estos bytes, el resultado debe ser uno o más paquetes PGP.

Normalmente lo que se comprime es un paquete de datos literales, opcionalmente precedido por un paquete de firma.

Paquete de datos cifrados con clave simétrica

El contenido de este paquete es directamente una secuencia de bytes cifrados con un algoritmo simétrico. El resultado de descifrarlos tiene que ser un o más paquetes PGP.

Típicamente lo que se cifra simétricamente son paquetes de datos en claro o paquetes de datos comprimidos.

Los paquetes de este tipo se usan para enviar un mensaje de correo cifrado con sobre digital, o bien cuando el usuario quiere simplemente cifrar un fichero. En el primer caso, es preciso adjuntar al mensaje la clave simétrica cifrada de tal forma que sólo la pueda descifrar el destinatario o destinatarios.

Esto se realiza con paquetes cifrados con clave pública, en el segundo caso, la clave no se guarda en ningún sitio sino que el usuario la tiene que recordar cuando quiera descifrar el fichero. En realidad, el usuario no da directamente la clave de cifrado si no una *passphrase*, a partir de la cual se obtiene la clave simétrica aplicándole una función de *hash*.

Paquete de datos cifrados con clave pública

En este tipo de paquete hay un campo que sirve para identificar la clave pública utilizada, otro que indica el algoritmo de cifrado, y otro con los datos cifrados.

Habitualmente este paquete se utilizaba para cifrar una clave de sesión, con la cual se habrá generado un paquete de datos cifrados simétricamente, para enviar un mensaje con sobre digital. La clave pública utilizada en este caso es la de cada uno de los destinatarios del mensaje.

Paquete de firma

Un paquete de este tipo contiene campos con la siguiente información:

• Clase de firma, que puede ser:

– Firma de datos binarios.

– Firma de texto canónico.

– Certificado, es decir, asociación de clave pública con nombre de usuario.

– Revocación de clave pública.

– Revocación de certificado.

– Fechado (*timestamp*).

• Fecha y hora en que se creó la firma.

• Identificador de la clave con la que se ha creado.

• Algoritmos utilizados para el *hash* y el cifrado asimétrico.

• La firma, que se obtiene aplicando los algoritmos especificados en los datos que hay que firmar, concatenados con los campos autenticados.

El modo de saber a qué datos corresponde una firma depende del contexto.

Si es la firma de un mensaje de correo, en el mismo mensaje tiene que haber el paquete con los datos (normalmente datos literales) despues del de firma. Si es un certificado o una revocación, la firma tiene que ir después de los paquetes de clave pública y de nombre de usuario correspondientes.

Paquete de clave pública

Este tipo de paquete contiene la siguiente información relativa a una clave pública:

• La fecha de creación de la clave.

• El algoritmo al que corresponde la clave.

• Los valores de los componentes de la clave. Si el algoritmo es RSA, estos valores son el módulo *n* y el exponente público *e*.

La clave pública de un usuario se utiliza para enviarle datos cifrados o para verificar las firmas que genere. Pero los paquetes correspondientes (datos cifrados con clave pública o firma, respectivamente) no contienen el valor de la clave pública utilizada, sino solamente su identificador de clave.

El identificador de una clave pública es un número de ocho bytes que se puede utilizar para buscar el valor de la clave en una base de datos.

Paquete de nombre de usuario

El contenido de un paquete de este tipo es simplemente una cadena de caracteres, que se utiliza para identificar el propietario de una clave pública.

Por tanto, tiene la misma función que el DN del sujeto en los certificados X.509, pero sin ninguna estructura predefinida.

Aunque su formato es libre, se suele seguir el convenio de identificar a los usuarios con direcciones de correo electrónico RFC 822

Paquete de clave privada

Este tipo de paquete sirve para guardar los componentes de la clave privada de un usuario. Nunca existe ningún motivo para enviarlo a otro usuario y, por lo tanto, el formato exacto del paquete puede depender de la implementación.

Para asegurar la confidencialidad, en el fichero donde se guarde este paquete los componentes secretos de la clave deberían estar cifrados, normalmente con una clave simétrica derivada de una *passphrase*. De este modo, cada vez que el usuario quiera descifrar o firmar un mensaje con su clave privada, deberá indicar esta *passphrase* para poder obtener los valores necesarios.

Un usuario puede tener varias claves, asociadas al mismo o a distintos nombres.

En el fichero en el que hayan los paquetes de clave privada, a continuación de cada uno habrá el paquete o paquetes de nombre de usuario correspondientes.

Paquete de nivel de confianza en una clave

Este tipo de paquete tampoco se envía nunca sino que solamente se guarda en el almacén de claves propio de cada usuario, ya que únicamente tiene significado para quien lo ha generado. Sirve para indicar el grado de fiabilidad de una clave certificadora, es decir, se utiliza para asociar otras claves con nombres de usuarios.

3.3.4. FORMATO DEL CERTIFICADO PGP

Un certificado PGP incluye la siguiente información, entre otras:

El número de versión de PGP: identifica la versión PGP utilizada para crear la clave asociada con el certificado.

La clave pública del dueño del certificado: la parte pública de su par de claves combinada con el algoritmo de la clave, sea RSA, DH (Diffie-Hellman) o DSA (Digital Signature Algorithm).

Información del dueño del certificado: incluye información relacionada con la identidad del usuario, como su nombre, identificación de usuario, fotografía, etc.

La firma digital del dueño del certificado: también llamada firma automática, ésta es la firma que se realiza con la clave privada correspondiente a la clave pública asociada con el certificado.

El período de validez del certificado: las fechas de inicio y de vencimiento del certificado. Indica la fecha de vencimiento del certificado.

El algoritmo de cifrado simétrico preferido para la clave: indica el algoritmo de cifrado que el dueño del certificado prefiere para aplicar al cifrado de la información. Los algoritmos posibles son CAST, IDEA y triple DES.

El hecho de que un certificado pueda contener varias firmas es uno de los aspectos exclusivos del formato de los certificados PGP. Varias personas pueden firmar el par clave/identificación para certificar de forma segura que la clave pública pertenece al dueño especificado. Algunos certificados PGP se componen de una clave pública con varios nombres, cada uno de los cuales brinda una manera diferente de identificar al dueño de la clave.

En un certificado, una persona debe afirmar que una clave pública y el nombre del dueño de la clave están asociados. Cualquiera puede validar los certificados PGP. Los certificados X.509 siempre tienen que ser validados por una entidad de certificación o

una persona designada por la CA. Los certificados PGP también usan una estructura jerárquica con la ayuda de la CA para validar los certificados.

Hay algunas diferencias entre un certificado X.509 y un certificado PGP, las más importantes se detallan a continuación:

Para crear su propio certificado PGP, debe solicitar un certificado X.509 emitido por una entidad de certificación y obtenerlo; Los certificados X.509 usan sólo un nombre para el dueño de la clave y sólo una firma digital para certificar la validez de la clave.

3.3.5. MODELOS DE CONFIANZA DE PGP

En general, la CA debe tener plena confianza para establecer la validez de los certificados y llevar a cabo el proceso manual de validación. Sin embargo, es difícil establecer una relación de confianza con personas que la CA no considera explícitamente fiables.

En un entorno PGP, cualquier usuario puede actuar como entidad de certificación, por lo tanto, puede validar otro certificado de clave pública de un usuario de PGP. Sin embargo, dicho certificado no se puede considerar válido por otro usuario a menos que un tercero reconozca a la persona que valida el certificado como un remitente fiable. Es decir, se respetará mi opinión que establece que las claves de otras personas son correctas, sólo si se me considera un remitente de confianza, de lo contrario, mi opinión acerca de la validez de las claves de los demás se pondrá en tela de juicio.

Supongamos, por ejemplo, que su conjunto de claves contiene la clave de Alicia. Usted la ha validado y, para mostrar su aprobación, la firma. Además, sabe que Alicia es bastante exigente cuando se trata de validar las claves de otros usuarios. En

consecuencia, otorga a suma confianza a la clave de Alicia. Alicia, por lo tanto, se transforma en una entidad de certificación. Si ella firma la clave de otro usuario, esta clave aparece como válida en su conjunto de claves.

3.3.5.1. **Distribución de claves PGP**

La certificación de claves en PGP no sigue un modelo jerárquico, como el de las autoridades de certificación X.509, sino un modelo descentralizado de confianza mutua, a veces llamado malla de confianza.

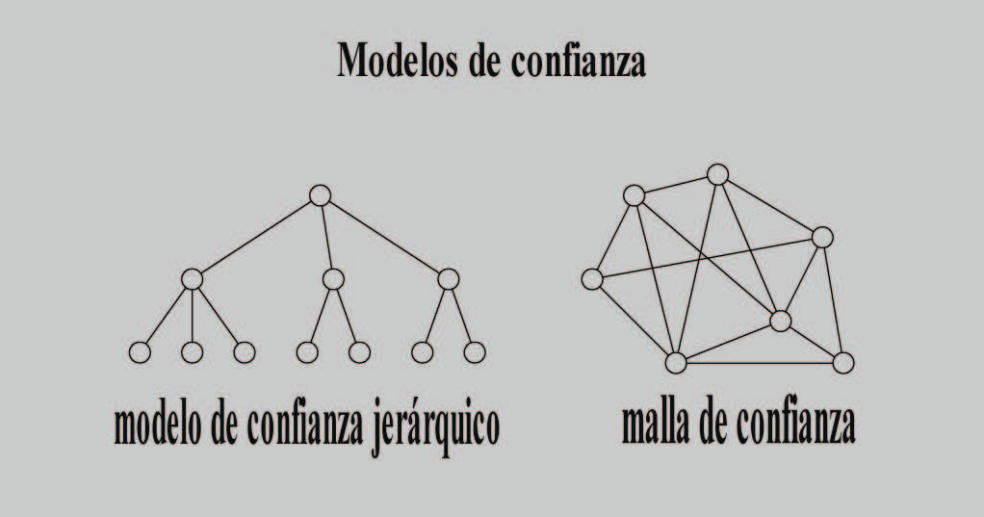


Figura 12: Modelo de Confianza

Cuando un usuario genera su par de claves PGP (pública y privada), a la clave pública le tiene que asociar un nombre de usuario y, a continuación, tiene que autocertificar esta asociación, es decir, firmar con su clave privada la concatenación de la clave pública y el nombre. El paquete de la clave pública, el del nombre de usuario y el de la firma forman un bloque de clave.

3.3.5.2. **El proceso de certificación PGP**

Para facilitar el intercambio y la certificación de claves, PGP asigna a cada clave pública una huella, que es simplemente un hash del valor de la clave.

Esta huella se utiliza para que un usuario pueda comprobar que la clave que ha recibido de otro, o de un servidor de claves, sea efectivamente la que quería recibir y no una falsificación. El identificador de clave no es suficiente para este fin, ya que es posible para un impostor construir una clave pública de la cual conozca la clave privada y que tenga el mismo identificador que otra clave pública. En cambio, construir una clave con la misma huella que otra es prácticamente imposible.

3.3.5.3. **Revocación del certificado PGP**

Sólo el dueño del certificado (el dueño de la clave privada correspondiente) u otro usuario, asignado como entidad de revocación por el dueño del certificado, podrá revocar el certificado PGP. Nombrar una entidad de revocación es útil, ya que normalmente los usuarios PGP revocan los certificados porque se pierde la contraseña compleja de la clave privada correspondiente. Este procedimiento se puede llevar a cabo sólo si se puede acceder a la clave privada. Un certificado X.509 puede ser revocado sólo por su emisor.

Cuando se revoca un certificado, no hace falta notificar a sus potenciales usuarios. Para anunciar una revocación de los certificados PGP, el método usual consiste en colocar esta información en un servidor de certificados. De esta manera, se advierte a los usuarios que desean comunicarse con usted que no debe utilizar la clave pública.

3.3.6. ESTRUCTURA DEL MENSAJE PGP

Si es un mensaje cifrado con sobre digital, primero hay tantos paquetes como destinatarios, cada uno con la clave de sesión cifrada con la clave pública del destinatario correspondiente. A continuación aparece el cuerpo del mensaje, posiblemente comprimido, en un paquete cifrado simétricamente con la cleve de sesion.

Si es un mensaje firmado, primero encontramos el paquete de firma, y después el cuerpo del mensaje en un paquete de datos literales. Opcionalmente, estos dos paquetes se pueden incluir dentro de un paquete comprimido.

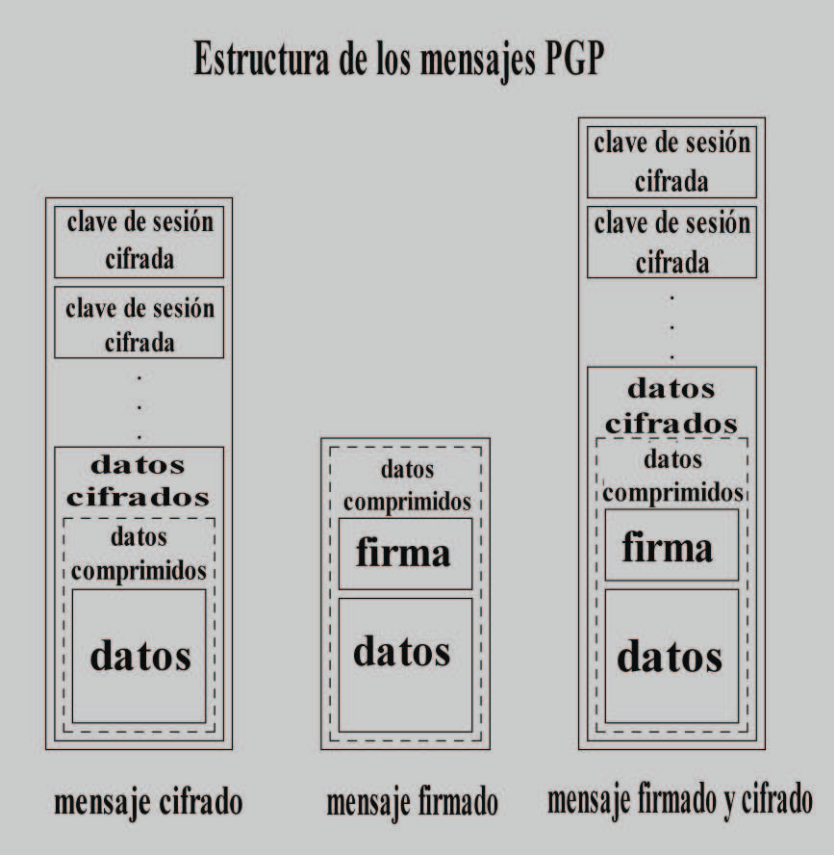


Figura 13: Estructura del Mensaje PGP

Si es un mensaje firmado y cifrado, la estructura es como la de los mensajes cifrados, con la excepción de que cuando se descifra el paquete de datos cifrados el resultado es un mensaje firmado, es decir, un paquete de firma seguido de un paquete de datos literales, o bien un paquete comprimido que cuando se descomprime da los dos paquetes anteriores.

3.3.6.1. **Mensaje cifrado y/o firmado**

```
-----BEGIN PGP MESSAGE-----
Version: 2.6.3y

iQBDAwUBObNQzFDy7z4CpbtnAQF9aQFrBtyRK8bdaPFlht7KeFzO/N0lJTcnYhbS
TvlZsTwr6+iQJqHP5nKnYr0W/Q9mo60AI3QAAAAAAEV4ZW1wbGUgZGUgbWlzc2F0
Z2Ugc2lnbmF0Lg0K
=8gbQ
-----END PGP MESSAGE-----
```

Figura 14: Mensaje cifrado y/o Firmado

Como delimitador inicial de encapsulación se utiliza la cadena “BEGIN PGP MESSAGE” entre dos secuencias de cinco guiones, y el delimitador final es igual pero cambiando “BEGIN” por “END”.

• . Después del delimitador inicial puede haber distintas cabeceras, con campos como Version para indicar qué versión de PGP ha generado el mensaje, Comment para introducir comentarios del usuario, o Charset, para especificar el juego de caracteres utilizado en el texto del mensaje.

• Después de las cabeceras aparece una línea en blanco, y el paquete o paquetes PGP que forman el mensaje codificado en base 64.

• Inmediatamente después de los paquetes PGP y antes del delimitador de final, aparece una línea de cinco caracteres: el primero es el signo ‘‘=” y los otros cuatro son la

codificación en base 64 de un CRC de 24 bits de todos los bytes de los paquetes. Este CRC sirve para comprobar que no se hayan producido modificaciones en el mensaje que hayan podido afectar a la descodificación.

En la terminología PGP, la secuencia de líneas desde el delimitador de encapsulación de inicio hasta el del final se llama armadura ASCII del mensaje.

3.3.6.2. **Mensajes PGP firmados en claro**

Igual que S/MIME, PGP también define un formato para enviar mensajes firmados en claro, que permite leer el contenido a los usuarios que no disponen de PGP. Éste es un ejemplo:

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: MD5

Ejemplo de mensaje firmado.

-----BEGIN PGP SIGNATURE-----
Version: 2.6.3y

iQBDAwUBObNQzFDy7z4CpbtnAQF7aQFrBtyRK8bdaPFlht7KeFzO/N0lJTcnYhbS
TvlZsTwr6+iQJqHP5nKnYr0W/Q9mow==
=5TnX
-----END PGP SIGNATURE-----
```

Figura 15: Mensajes PGP firmados en claro

En este caso aparecen dos submensajes encapsulados, con la siguiente estructura:

• El delimitador de inicio de la primera parte es la cadena “BEGIN PGP SIGNED MESSAGE”, con una secuencia de cinco guiones delante y detrás.

• En el primer submensaje aparecen cero o más cabeceras Hash, que indican el algoritmo (o algoritmos) de *hash* utilizados para calcular la firma (o firmas), seguidos de una línea en blanco y del cuerpo del mensaje.

La especificación del algoritmo al inicio permite procesar el mensaje en un solo paso. En ausencia de este campo, se entiende por defecto que la función de *hash* utilizada es MD5.

Después del primer submensaje aparece la armadura ASCII de uno o más paquetes de firma, con un delimitador de inicio formado por la cadena "BEGIN PGP SIGNATURE", también con cinco guiones delante y detrás, y con un delimitador de final igual, aunque cambiando "BEGIN" por "END".

Las firmas se calculan a partir del cuerpo del mensaje en forma canónica, es decir, representando los finales de línea con <CR><LF>. Además, PGP siempre elimina los espacios en blanco y los tabuladores que haya antes de un final de línea en el momento de obtener las firmas.

3.3.6.3. **Mensajes de bloques de claves públicas**

Hay otro formato de armadura PGP que sirve para enviar bloques de claves públicas y certificados. El delimitador de inicio consta de la cadena "BEGIN PGP PUBLIC KEY BLOCK" rodeada de dos secuencias de cinco guiones, y el de final es igual, aunque cambiando "BEGIN" por "END". Éste es un ejemplo:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3y

mQA9AzmvN9AAAAEBbAw1Es5ojfSWtFCPLLOdONBOz+8u96IVp1GIYqVU2ewWQbH8
TAd0UPLvPgKlu2cAEQEAAbQhVXN1YXJpIDEgPHVzdWFyaS0xQGNhbXB1cy51b2Mu
ZXM+1QBCAwUQOa830FDy7z4CpbtnAQFdoQFox7LHdl8wdIA69f4REn14bVYxBaxw
4Y35PJwRWqI2c+8T75vqUdBh1ydsZ2Fo
=N1nr
-----END PGP PUBLIC KEY BLOCK-----
```

Figura 16: Mensajes de bloques de claves públicas

Cualquiera de los tipos de armadura que hemos visto se puede utilizar para intercambiar información PGP con otros medios de transferencia además del correo electrónico: FTP, HTTP, etc.

3.4. PROTOCOLO S/MIME

El S/MIME es un proceso de seguridad utilizado para el intercambio de correo electrónico que hace posible garantizar la confidencialidad y el reconocimiento de autoría de los mensajes electrónicos.

El S/MIME está basado en el estándar MIME, cuyo objetivo es permitir a los usuarios adjuntar a sus mensajes electrónicos archivos diferentes a los archivos de texto ASCII Por lo tanto, el estándar MIME hace posible que podamos adjuntar todo tipo de archivos a nuestros correos electrónicos.

3.4.1. CARACTERÍSTICAS.

Antes de que existiera S/MIME, los administradores utilizaban un protocolo de correo electrónico ampliamente aceptado, el Protocolo simple de transferencia de correo (SMTP), que no era seguro de manera inherente, o utilizaban soluciones más seguras pero patentadas. Los administradores elegían una solución que hiciera hincapié en la seguridad o en la conectividad. Con S/MIME, los administradores disponen ahora de una opción de correo electrónico que es más segura y está ampliamente aceptada. S/MIME es un estándar tan importante como SMTP, ya que lleva SMTP un nivel más allá: permite distribuir la conectividad de correo electrónico sin poner en peligro la seguridad.

La versión 3 soporta nuevos servicios, conocidos como ESS, que incluyen:

• Recibos firmados.

• Etiquetas de seguridad, que dan información sobre el nivel de sensibilidad del contenido de un mensaje (según una clasificación definida por una determinada política de seguridad).

• Listas de correo seguras.

• Certificados de firma, que permiten asociar directamente una firma con el certificado necesario para validarla.

3.4.2. EL FORMATO PKCS #7

PKCS #7 es un formato para representar mensajes protegidos criptográficamente.

Cuando la protección está basada en criptografía de clave pública, en PKCS #7 se utilizan certificados X.509 para garantizar la autenticidad de las claves.

La norma PKCS #7 define unas estructuras de datos para representar cada uno de los campos que forman parte de un mensaje. A la hora de intercambiar estos datos se deben codificar según las reglas especificadas por la notación ASN.1 (la misma que se utiliza para representar los certificados X.509 y las CRL).

Ésta es la estructura general de un mensaje PKCS #7, descrita con la misma notación que utilizamos para los certificados (“opc.” significa opcional y “rep.”Significa repetible):

Campo	Tipo
contentType	identificador único
content (opc.)	Data, SignedData, EnvelopedData, SignedAndEnvelopedData, DigestedData, o EncryptedData

Figura 17: Formato PKCS #7

El campo contentType es un identificador que indica cuál de las seis estructuras posibles hay en el campo content. Estas estructuras son:

1) Data: sirve para representar datos literales, sin aplicarles ninguna protección criptográfica.

2) SignedData: representa datos firmados digitalmente.

3) EnvelopedData: representa un mensaje con sobre digital (es decir, un mensaje cifrado simétricamente al que se añade la clave simétrica cifrada con la clave pública de cada destinatario).

4) SignedAndEnvelopedData: representa datos firmados y "cerrados" en un sobre digital.

5) DigestedData: representa datos a los cuales se les añade un resumen o hash.

6) EncryptedData: representa datos cifrados con clave secreta.

El campo content es opcional, porque en ciertos casos existe la posibilidad de que los datos de un mensaje no estén dentro del propio mensaje, sino en algún otro lugar.

De estos seis posibles tipos de contenido, los tres últimos no se utilizan en S/MIME: para datos firmados y con sobre se utiliza una combinación de SignedData y EnvelopedData, y los mensajes que sólo contienen datos con hash o datos cifrados simétricamente no se envían nunca con correo electrónicoseguro.

Por lo tanto, los tipos de contenido PKCS #7 que puede haber en un mensaje S/MIME son Data, SignedData o EnvelopedData.

3.4.3. FORMATO DE LOS MENSAJES S/MIME

Un mensaje S/MIME es un mensaje MIME con las siguientes características:

• Su tipo de contenido (campo Content-Type de la cabecera MIME) es "application/pkcs7-mime".

• En su cuerpo hay una estructura PKCS #7 codificada según la notación ASN.1.

Para los mensajes S/MIME que sólo estén firmados existe una representación alternativa, llamada **firma en claro**, que veremos más adelante.

Compatibilidad con versiones anteriores de S/MIME

Para los tipos de contenido, como "pkcs7-mime" y otros que veremos a continuación, las primeras versiones de S/MIME utilizaban nombres que empezaban por "x-".

En las versiones experimentales de algunos protocolos es habitual utilizar un prefijo como éste para representar valores que aún no están estandarizados. Por compatibilidad con estas versiones, las aplicaciones de correo S/MIME deberían tomar en consideración los nombres antiguos equivalentes a los nombres sin prefijo.

Nombre antiguo	Nombre actual
x-pkcs7-mime	pkcs7-mime
x-pkcs7-signature	pkcs7-signature
x-pkcs10	pkcs10

La cabecera MIME Content-Type, además del valor “application/pkcs7-mime”, debe tener al menos uno de estos dos parámetros:

• smime-type: indica el tipo de contenido PKCS #7 que hay en el cuerpo del mensaje.

• name: indica un nombre del fichero asociado al contenido del mensaje.

3.4.4. FICHERO ASOCIADO A UN MENSAJE S/MIME

El parámetro name sirve para mantener la compatibilidad con las primeras versiones de S/MIME, en las cuales no estaba definido el parámetro smime-type. En estas versiones, la especificación del tipo de contenido PKCS #7 se realizaba con la extensión de un nombre de fichero. La parte del nombre que haya antes de la extensión es indiferente, pero por convencionalmente suele ser “smime”.

Para especificar este nombre de fichero se puede utilizar el parámetro name de la cabecera Content-Type, y también el parámetro filename de la cabecera MIME Content-Disposition (definida en la especificación RFC 2183), con el valor de esta cabecera igual a “attachment”.

Además, dado que el cuerpo del mensaje son datos binarios (la representación ASN.1 de una estructura PKCS #7), normalmente habrá una cabecera Content-Transfer-Encoding con valor “base64” para indicar que estos datos están codificados en base 64.

Existen tres formatos básicos de mensajes S/MIME: los mensajes con sobre digital, los mensajes firmados, y los mensajes firmados en claro.

3.4.4.1. **Mensajes S/MIME con sobre digital**

Un mensaje S/MIME con sobre digital tiene las siguientes características:

• En el cuerpo del mensaje hay una estructura PKCS #7 con tipo de contenido EnvelopedData.

• El valor del parámetro smime-type es “enveloped-data”.

• Si se especifica un nombre de fichero asociado, su extensión es .p7m.

Éste es un mensaje S/MIME con sobre digital:

```
From: usuario-1@uoc.edu
Subject: Ejemplo 1
To: usuario-2@uoc.edu
MIME-Version: 1.0
Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
        name="smime.p7m"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7m"

MIAGCSqGSIb3DQEHA6CAMIACAQAxgDBzAgEAMC8wKjELMAkGA1UEBhMCRVMxDDAKBgNVBAoT
A1VPQzENMAsGA1UEAxMEQ0EtMQIBBjANBgkqhkiG9w0BAQEFAAQuCYHs970aZmmqKTr3gemZ
LzHVtB266O/TrIv4shSvos8Ko8mUSQGov0JSIugmeDBzAgEAMC8wKjELMAkGA1UEBhMCRVMx
DDAKBgNVBAoTA1VPQzENMAsGA1UEAxMEQ0EtMQIBBzANBgkqhkiG9w0BAQEFAAQuC14oIhps
+mh8Wxp79A81uv2ltG3vt6J9UdJQcrDL92wD/jpw1IKpoR224LT4PQAAMIAGCSqGSIb3DQEH
ATARBgUrDgMCBwQIZbTj6XqCRkGggARAF8K8apgPtK7JPS1OaxfHMDXYTdEG92QXfAdTPetA
FGuPfxpJrQwX2omWuodVxP7PnWT2N5KwE1oc6faJY/zG0AAAAAAAAAAAAAAA=
```

Figura 18: Mensajes S/MIME con sobre digital

3.4.4.2. **Mensajes s/mime firmados**

Un mensaje S/MIME firmado tiene un formato análogo al de los mensajes con sobre digital. Sus características son:

• En el cuerpo del mensaje hay una estructura PKCS #7 con tipo de contenido SignedData.

• El valor del parámetro `smime-type` es "`signed-data`".

• Si se especifica un nombre de fichero asociado, su extensión es la misma que en los mensajes con sobre digital, es decir `.p7m`.

Este es un ejemplo de mensaje S/MIME firmado:

```
From: usuario-1@uoc.edu
Subject: Ejemplo 2
To: usuario-2@uoc.edu
MIME-Version: 1.0
Content-Type: application/pkcs7-mime; smime-type=signed-data;
        name="smime.p7m"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7m"

MIAGCSqGSIb3DQEHAqCAMIACAQExDjAMBggqhkiG9w0CBQUAMIAGCSqGSIb3DQEHAaCAJIAE
OUNvbnRlbnQtVHlwZTogdGV4dC9wbGFpbg0KDQpFeGVtcGxlIGRlIG1pc3NhdGdlIHNpZ25h
dC4NCgAAAAAAAKCAMIIBSDCCAQWgAwIBAgIBBjANBgkqhkiG9w0BAQQFADAqMQswCQYDVQQG
EwJFUzEMMAoGA1UEChMDVU9DMQ0wCwYDVQQDEwRDQS0xMB4XDTAwMDkwMTAwMDAwMFoXDTEw
MDkwMTAwMDAwMFowVTELMAkGA1UEBhMCRVMxDDAKBgNVBAoTA1VPQzElMCMGCSqGSIb3DQEJ
ARYWdXN1YXJpLTFAY2FtcHVzLnVvYy5lczERMA8GA1UEAxMIdXN1YXJpLTEwSTANBgkqhkiG
9w0BAQEFAAM4ADA1A14MNRLOaI30lrRQjyyznTjQTs/vLve1FadR1GKlVNnsFkGx/EwHdFDy
7z4CpbtnAgMBAAEwDQYJKoZIhvcNAQEEBQADLgACRZrDsL/MJv9VZdbxNMpbjKcwwFPPVG9L
TqOZ8sTdAF09UnFsSj5jE0ABAPEAADGAMIGBAgEBMC8wKjELMAkGA1UEBhMCRVMxDDAKBgNV
BAoTA1VPQzENMAsGA1UEAxMEQ0EtMQIBBjAMBggqhkiG9w0CBQUAMA0GCSqGSIb3DQEBAQUA
BC4DMwI+4fvRqBPhFj/wB7gI+Or7nSYfkqP1fxbjdTqwu9B5jsnxDIs+PUYsboQIAAAAAAAA
AAA=
```

Figura 19: Mensajes s/mime firmados

3.4.4.3. **Mensajes S/MIME firmados en claro**

Cuando se envía un mensaje firmado, los receptores que utilicen un lector de correo apropiado podrán leer el mensaje y verificar la firma. Muchas veces interesa que el mensaje pueda ser leído por todos, aunque no se disponga de un lector con soporte para correo seguro.

Este es un mensaje firmado en claro:

```
From: usuario-1@uoc.edu
Subject: Ejemplo 3
To: usuario-2@uoc.edu
MIME-Version: 1.0
Content-Type: multipart/signed; boundary="20040301104740";
        protocol="application/pkcs7-signature"; micalg=md5

--20040301104740
Content-Type: text/plain

Ejemplo de mensaje firmado.

--20040301104740
Content-Type: application/pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"

MIAGCSqGSIb3DQEHAqCAMIACAQExDjAMBggqhk1G9w0CBQUAMIAGCSqGSIb3DQEHAQAAoIAw
ggFIMIIBBaADAgECAgEGMA0GCSqGSIb3DQEBBAUAMCoxCzAJBgNVBAYTAkVTMQwwCgYDVQQK
EwNVT0MxDTALBgNVBAMTBENBLTEwHhcNMDAwOTAxMDAwMDAwWhcNMTAwOTAxMDAwMDAwWjBV
MQswCQYDVQQGEwJFUzEMMAoGA1UEChMDVU9DMSUwIwYJKoZIhvcNAQkBFhZ1c3VhcmktMUBj
YW1wdXMudW9jLmVzMREwDwYDVQQDEwh1c3VhcmktMTBJMA0GCSqGSIb3DQEBAQUAAzgAMDUC
Lgw1Es5ojfSWtFCPLLOdONBOz+8u96IVp1GIYqVU2ewWQbH8TAd0UPLvPgKlu2cCAwEAATAN
BgkqhkiG9w0BAQQFAAMuAAJFmsOwv8wm/1Vl1vE0yluMpzDAU89Ub0tOo5nyxN0AXT1ScWxK
PmMTQAEA8QAAMYAwgYECAQEwLzAqMQswCQYDVQQGEwJFUzEMMAoGA1UEChMDVU9DMQ0wCwYD
VQQDEwRDQS0xAgEGMAwGCCqGSIb3DQIFBQAwDQYJKoZIhvcNAQEBBQAELgMzAj7h+9GoE+EW
P/AHuAj46vudJh+So/V/FuN1OrC70HmOyfEM1z49RixuhAgAAAAAAAAAAA==
--20040301104740--
```

Figura 20: Mensajes S/MIME firmados en claro

3.4.4.4. **Distribución de claves con S/MIME**

Como hemos visto hasta este punto, el método que se utiliza en PKCS #7 y por lo tanto, en S/MIME, para identificar los usuarios y sus claves públicas es por medio de sus certificados X.509.

Esto quiere decir que un usuario no necesita verificar las identidades de los demás porque de esto ya se encargan las autoridades de certificación. Lo único que debe hacer el usuario es comprobar si el certificado (o cadena de certificados) de su corresponsal está firmado por una CA reconocida y es un certificado válido, es decir, no está caducado ni revocado.

S/MIME define un tipo especial de mensaje que sirve para transportar certificados o listas de revocación. Se trata de un mensaje S/MIME con las siguientes características:

• En el cuerpo del mensaje hay una estructura PKCS #7 con tipo de contenido SignedData, pero sin datos firmados (campo content del elemento contentInfo) ni firmas (campo signerInfos con 0 elementos). Por lo tanto, los campos con información útil son certificates y crls.

• El valor del parámetro smime-type es “certs-only”.

• Si se especifica un nombre de fichero asociado, su extensión es .p7c (por ejemplo, “smime.p7c”).

Éste es un mensaje S/MIME con sólo certificados:

```
From: usuario-1@uoc.edu
Subject: Mi certificado y el de la CA
To: usuario-2@uoc.edu
MIME-Version: 1.0
Content-Type: application/pkcs7-mime; smime-type=certs-only;
        name="smime.p7c"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7c"

MIAGCSqGSIb3DQEHAqCAMIACAQExADALBgkqhkiG9w0BBwGggDCCAUgwggEFoAMCAQICAQYw
DQYJKoZIhvcNAQEEBQAwKjELMAkGA1UEBhMCRVMxDDAKBgNVBAoTA1VPQzENMAsGA1UEAxME
Q0EtMTAeFw0wMDA5MDEwMDAwMDBaFw0xMDA5MDEwMDAwMDBaMFUxCzAJBgNVBAYTAkVTMQww
```

Figura 21: Mensajes S/MIME con certificado

Finalmente, existe otro tipo de mensaje S/MIME para enviar peticiones de certificación a una CA. Una petición de certificación es un mensaje que contiene los datos necesarios para que la CA genere un certificado, básicamente el nombre del titular y su clave pública.

3.4.5. DESCRIPCIÓN DE LOS SERVICIOS S/MIME

S/MIME proporciona dos servicios de seguridad:

Firmas digitales

Cifrado de mensajes

Estos dos servicios son el núcleo de la seguridad de los mensajes basada en S/MIME**.** Todos los demás conceptos relacionados con la seguridad de los mensajes sirven de apoyo a estos dos servicios. Si bien todo el ámbito de la seguridad de los mensajes puede parecer complejo, estos dos servicios son la base de dicha seguridad. Una vez que adquiera unos conocimientos básicos de las firmas digitales y del cifrado de mensajes, podrá aprender cómo otros conceptos sirven de apoyo a estos servicios.

Descripción de las firmas digitales s/mime

Las firmas digitales son el servicio más utilizado de S/MIME. Como su nombre indica, las firmas digitales son la contrapartida digital a la tradicional firma legal en un documento impreso. Al igual que ocurre con una firma legal, las firmas digitales ofrecen las siguientes capacidades de seguridad:

Autenticación Una firma sirve para validar una identidad. Comprueba la respuesta a "quién es usted" al ofrecer una forma de diferenciar esa entidad de todas las demás y demostrar su unicidad. Como no existe autenticación en el correo electrónico SMTP, no hay ninguna forma de saber quién envió realmente un mensaje. La autenticación en una firma digital resuelve este problema al permitir que un destinatario sepa que un mensaje fue enviado por la persona o la organización que dice haber enviado el mensaje.

No rechazo La unicidad de una firma impide que el propietario de la firma no reconozca su firma. Esta capacidad se llama no rechazo. Así, la autenticación proporcionada por una firma aporta el medio de exigir el no rechazo. El concepto de no rechazo resulta más familiar en el contexto de los contratos en papel: un contrato firmado es un documento legalmente vinculante y es imposible no reconocer una firma autenticada. Las firmas digitales ofrecen la misma función y, cada vez en más áreas, se reconocen como legalmente vinculantes, de manera similar a una firma en un papel. Como el correo electrónico SMTP no ofrece ningún medio de autenticación, no puede proporcionar la función de no rechazo. Para el remitente de un mensaje de correo electrónico SMTP es fácil no reconocer la propiedad del mismo.

Integridad de los datos Un servicio de seguridad adicional que ofrecen las firmas digitales es la integridad de los datos. La integridad de los datos es uno de los resultados de las operaciones que hacen posibles las firmas digitales. Con los servicios de integridad de datos, cuando el destinatario de un mensaje de correo electrónico firmado digitalmente valida la firma digital, tiene la seguridad de que el mensaje recibido es el mismo mensaje que se firmó y se envió, y que no se ha manipulado mientras estaba en tránsito. Cualquier alteración del mensaje mientras estaba en tránsito una vez firmado invalida la firma. De esta forma, las firmas digitales son capaces de ofrecer una garantía que no permiten tener las firmas en papel, ya que es posible alterar un documento en papel una vez que ha sido firmado.

La autenticación, el no rechazo y la integridad de los datos son las funciones básicas de las firmas digitales. Juntas, aseguran a los destinatarios que el mensaje provino del remitente y que el mensaje recibido es el mismo que se envió.

Por simplificar, una firma digital realiza una operación de firma sobre el texto del mensaje de correo electrónico cuando éste se envía y una operación de comprobación cuando se lee el mensaje, tal y como se muestra en la figura siguiente.

Operaciones de firma digital y operaciones de comprobación sobre un mensaje de correo electrónico.

La operación de firma que se realiza cuando se envía el mensaje requiere información que sólo el remitente puede proporcionar. Esta información se utiliza en una operación de firma capturando el mensaje de correo electrónico y realizando una operación de firma sobre el mensaje. Esta operación produce la firma digital real.

Figura 22: Operación de Firma de mensaje

Esta firma se anexa entonces al mensaje y se incluye con él cuando se envía.

Firma digital de un mensaje de correo electrónico

Se captura el mensaje.

Se recupera información que identifica de manera única al remitente.

Se realiza la operación de firma sobre el mensaje utilizando la información única del remitente para producir una firma digital.

Se anexa la firma digital al mensaje.

Se envía el mensaje.

Figura 23: Firma Digital en mensaje de correo electrónico

Como esta operación requiere información única del remitente, las firmas digitales ofrecen autenticación y no rechazo. Esta información única puede demostrar que el mensaje sólo puede proceder del remitente.

Ningún mecanismo de seguridad es perfecto. Es posible que usuarios no autorizados obtengan la información única que se utiliza para las firmas digitales e intenten suplantar a un remitente. Sin embargo, el estándar S/MIME puede resolver estas situaciones de forma que las firmas no autorizadas aparezcan como no válidas.

Cuando el destinatario abre un mensaje de correo electrónico firmado digitalmente, se realiza un procedimiento de comprobación en la firma digital. Se recupera del mensaje la firma digital incluida con el mensaje. También se recupera el mensaje original y se realiza una operación de firma, que produce otra firma digital. La firma digital incluida con el mensaje se compara con la firma digital producida por el destinatario. Si ambas firmas coinciden, se sabe que el mensaje procede del remitente que dice haberlo enviado. Si las firmas no coinciden, el mensaje se marca como no válido. La figura siguiente muestra la secuencia de comprobación de un mensaje.

Comprobación de una firma digital de un mensaje de correo electrónico

Se recibe el mensaje.

Se recupera la firma digital del mensaje.

Se recupera el mensaje.

Se recupera información que identifica al remitente.

Se realiza la operación de firma sobre el mensaje.

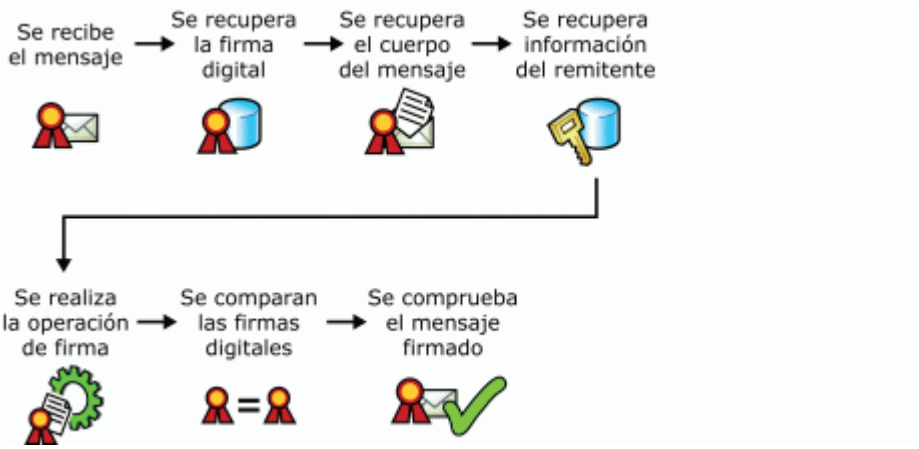


Figura 24: Comprobación de Firma

La firma digital incluida con el mensaje se compara con la firma digital producida al recibirlo.

Si las firmas digitales coinciden, el mensaje es válido.

En conjunto, el proceso de firma digital y comprobación de la firma digital autentica al remitente de un mensaje de correo electrónico y determina la integridad de los datos dentro del mensaje firmado. La autenticación de remitentes proporciona la capacidad adicional de no rechazo, que impide que los remitentes autenticados digan que ellos no enviaron el mensaje. Las firmas digitales son una solución a la suplantación y manipulación de los datos, que son posibles con el correo electrónico en Internet basado en el estándar SMTP.

Descripción del cifrado de mensajes

El cifrado de mensajes ofrece una solución para la revelación de información. El correo electrónico en Internet basado en SMTP no protege los mensajes. Un mensaje de correo electrónico SMTP en Internet puede ser leído por cualquiera que lo vea mientras viaja o que lo vea donde está almacenado. S/MIME resuelve estos problemas mediante el uso del cifrado.

El cifrado es una forma de modificar información de manera que no se pueda leer o entender hasta que vuelva a cambiarse a un formato legible y entendible.

Si bien el uso del cifrado de mensajes no está tan extendido como el de las firmas digitales, resuelve lo que muchas personas perciben como la mayor debilidad del correo electrónico en Internet. El cifrado de mensajes ofrece dos servicios de seguridad específicos:

Confidencialidad El cifrado de mensajes protege el contenido de un mensaje de correo electrónico. Sólo el destinatario al que va dirigido el mensaje puede ver el contenido, y el contenido sigue siendo confidencial y no puede conocerlo nadie más que quien pueda recibir o ver el mensaje. El cifrado ofrece confidencialidad mientras el mensaje está en tránsito y mientras está almacenado.

Integridad de los datos Como ocurre con las firmas digitales, el cifrado de mensajes ofrece servicios de integridad de los datos como resultado de las operaciones específicas que hacen posible el cifrado.

La confidencialidad y la integridad de los datos proporcionan las funciones básicas del cifrado de mensajes. Garantizan que sólo el destinatario al que va dirigido puede ver un mensaje y que el mensaje recibido es el mensaje que se envió.

El cifrado de mensajes hace que el texto de un mensaje sea ilegible al realizar una operación de cifrado sobre el mismo cuando se envía. Cuando se recibe el mensaje, se vuelve a hacer legible el texto realizando una operación de descifrado cuando se lee el mensaje, como se muestra en la figura siguiente.

Operaciones de cifrado y descifrado sobre un mensaje de correo electrónico

Figura 25: Operación de Cifrado y descifrado

La operación de cifrado que se realiza cuando se envía el mensaje captura el mensaje de correo electrónico y lo cifra utilizando información específica del destinatario al que va dirigido. El mensaje cifrado reemplaza al original y se envía el mensaje al destinatario. La figura siguiente muestra la secuencia de cifrado de un mensaje de correo electrónico.

Cifrado de un mensaje de correo electrónico

Se captura el mensaje.

Se recupera información que identifica de manera única al destinatario.

Se realiza la operación de cifrado sobre el mensaje utilizando la información del destinatario para producir un mensaje cifrado.

El mensaje cifrado reemplaza al texto del mensaje.

Se envía el mensaje.

Figura 26: Cifrado de mensaje

Como esta operación requiere información única acerca del destinatario, el cifrado de mensajes ofrece confidencialidad. Sólo el destinatario al que va dirigido el mensaje posee la información para realizar la operación de descifrado. Esto asegura que sólo el destinatario al que va dirigido puede ver el mensaje, ya que hay que proporcionar la información única del destinatario antes de poder ver el mensaje sin cifrar.

Cuando el destinatario abre un mensaje cifrado, se realiza una operación de descifrado sobre el mensaje cifrado. Se recuperan tanto el mensaje cifrado como la información única del destinatario. La información única del destinatario se utiliza entonces en una operación de descifrado que se realiza sobre el mensaje cifrado. Esta operación devuelve el mensaje no cifrado, que se muestra entonces al destinatario. Si el mensaje se ha alterado durante el tránsito, la operación de descifrado dará un error. La figura siguiente muestra la secuencia de descifrado de un mensaje de correo electrónico.

Descifrado de un mensaje de correo electrónico

Se recibe el mensaje.

Se recupera el mensaje cifrado.

Se recupera información que identifica de manera única al destinatario.

Se realiza la operación de descifrado sobre el mensaje cifrado utilizando la información única del destinatario para producir un mensaje no cifrado.

Se devuelve el mensaje sin cifrar al destinatario.

Figura 27: Descifrado de mensaje

El proceso de cifrado y descifrado de mensajes proporciona confidencialidad de los mensajes de correo electrónico. Este proceso resuelve una gran debilidad del correo electrónico de Internet: el hecho de que cualquiera puede leer cualquier mensaje.

Funcionando en conjunto las firmas digitales y el cifrado de mensajes

Las firmas digitales y el cifrado de mensajes no son servicios mutuamente exclusivos. Cada servicio resuelve determinados problemas de seguridad. Las firmas digitales resuelven los problemas de autenticación y no rechazo, mientras que el cifrado de mensajes resuelve los problemas de confidencialidad. Como cada uno de estos servicios resuelve problemas diferentes, una estrategia de seguridad de los mensajes suele requerir ambos servicios al mismo tiempo. Estos dos servicios están diseñados para utilizarse conjuntamente, ya que cada uno resuelve por separado un extremo de la relación remitente-destinatario. Las firmas digitales resuelven los problemas de seguridad relacionados con los remitentes y el cifrado resuelve problemas de seguridad relacionados principalmente con los destinatarios.

Cuando las firmas digitales y el cifrado de mensajes se utilizan conjuntamente, los usuarios se benefician de ambos servicios. El uso de ambos servicios en los mensajes no cambia el tratamiento o el procesamiento de ninguno de los servicios: cada uno

funciona como se ha explicado en secciones anteriores de este documento. Para mostrar cómo funcionan conjuntamente las firmas digitales y el cifrado de mensajes, la figura siguiente ilustra la secuencia de firma y cifrado de un mensaje de correo electrónico.

Firma digital y descifrado de un mensaje de correo electrónico

Figura 28: Firma digital y descifrado

Se captura el mensaje.

Se recupera información que identifica de manera única al remitente.

Se recupera información que identifica de manera única al destinatario.

Se realiza la operación de firma sobre el mensaje utilizando la información única del remitente para producir una firma digital.

Se anexa la firma digital al mensaje.

Se realiza la operación de cifrado sobre el mensaje utilizando la información del destinatario para producir un mensaje cifrado.

Se reemplaza el mensaje original con el mensaje cifrado.

Se envía el mensaje.

La figura siguiente muestra la secuencia de descifrado y comprobación de la firma digital.

Descifrado de un mensaje de correo electrónico y comprobación de una firma digital

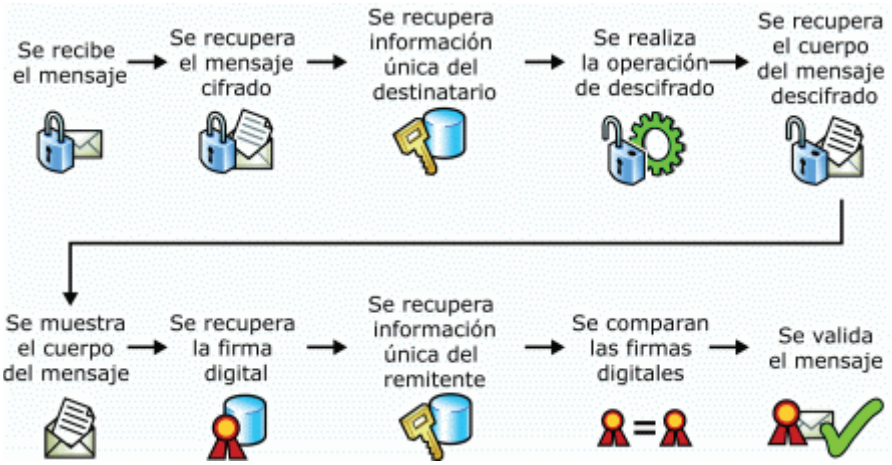


Figura 29: Descifrado de un mensaje de correo electrónico y comprobación de una firma

Se recibe el mensaje.

Se recupera el mensaje cifrado.

Se recupera información que identifica de manera única al destinatario.

Se realiza la operación de descifrado sobre el mensaje cifrado utilizando la información única del destinatario para producir un mensaje no cifrado.

Se devuelve el mensaje no cifrado.

Se devuelve el mensaje sin cifrar al destinatario.

Se recupera la firma digital del mensaje no cifrado.

Se recupera información que identifica al remitente.

Se realiza la operación de firma sobre el mensaje no cifrado utilizando la información del remitente para producir una firma digital.

La firma digital incluida con el mensaje se compara con la firma digital producida al recibirlo.

Si las firmas digitales coinciden, el mensaje es válido.

3.4.6. MENSAJES CON TRIPLE ENVOLTORIO

Una de las mejoras de S/MIME versión 3 que merece la pena destacar es el "triple envoltorio". Un mensaje S/MIME con triple envoltorio es aquel que se firma, se cifra y se firma de nuevo. Este nivel adicional de cifrado proporciona un nivel adicional de seguridad. Cuando los usuarios firman y cifran mensajes con Outlook Web Access con el control S/MIME, el mensaje tiene triple envoltorio automáticamente. Outlook y Outlook Express no aplican triple envoltorio a los mensajes, pero pueden leer este tipo de mensajes.

Las firmas digitales y el cifrado de mensajes se complementan entre sí, y ofrecen una solución global a los problemas de seguridad que afectan al correo electrónico de Internet basado en SMTP.

Los certificados digitales y el cifrado de mensajes son la funcionalidad básica de S/MIME. El concepto auxiliar más importante para la seguridad de los mensajes es la

criptografía mediante claves públicas. La criptografía mediante claves públicas hace que sean viables las firmas digitales y el cifrado de mensajes dentro de S/MIME

3.5. DETERMINACIÓN DE LOS PARÁMETROS DE COMPARACIÓN

Para poder escoger el protocolo seguro de correo electrónico, utilizaremos una metodología en la que se establecerá escalas cuantitativas y cualitativas, que permitirá dar valoración a cada uno de los parámetros, siendo unos más importantes que otros, luego se establecerán conclusiones, justificación y finalmente se escogerá el protocolo que se ajuste a nuestras necesidades tecnológicas. Ya que se ha citado los fundamentos teóricos y se ha determinado los parámetros para escoger el protocolo, procederemos a analizar esta información a través de cuadros comparativos, donde se citará los parámetros por medio de los cuales se determinar las diferencias entre ellos.

3.5.1. SERVICIOS DE SEGURIDAD

La autenticación puede contribuir al desarrollo de confianza entre las partes involucradas en todos los tipos de transacciones tras abordar sólo un conjunto de medidas de seguridad, aseguran que cada interlocutor es quién dice ser.

Define mecanismos para garantizar la procedencia de la información, ya sea a nivel de usuario o de computadora.

Permite a un usuario firmar un documento antes de enviarlo, lo cual permite:

Tener certeza de que el documento no ha sido modificado puesto que ha sido firmado, si se alterara el mensaje la firma no sería válida.

Verificar que el documento ha sido firmado por una determinada persona.

3.5.2. SOPORTE CRIPTOGRÁFICO

Para asegurar la confidencialidad de la información es posible codificar la información intercambiada mediante el uso de la criptografía de mensajes. Los mensajes son cifrados por el remitente y descifrados por el destinatario, utilizando claves que solamente ellos conocen.

De esta manera, los datos de los correos electrónicos que transitan por las redes y servidores de Internet están codificados, y son totalmente ininteligibles para terceras personas que pudieran hacer un uso fraudulento de tales datos.

3.5.3. MANEJO DE CERTIFICADOS DIGITALES

Un certificado digital es un contenedor de datos que alberga identidades (por ejemplo de una persona, sus nombre, dirección e mail) con un par de claves encriptadas públicas y/o privadas. Los certificados se usan en una gran variedad de contextos de seguridad en red para establecer la autenticación y privacidad entre usuarios de red y usuarios de aplicaciones.

3.5.4. ESTRUCTURA DE LOS MENSAJES

La estructura de los mensajes determina la manera en que va a estar compuesto por que en ella se encuentran varios paquetes que indica de qué tipo de se trata y demas parametros que contiene un mensaje de correo electronico.

Determina ademas como protege los datos o el flujo de información frente a accesos, modificaciones, pérdidas, etc.

3.5.5. ACCESIBILIDAD

Determinar si puede ser implementado un servicio de correo electrónico seguro en diferentes ámbitos en que van hacer utilizados por un número de usuarios, la accesibilidad a una licencia, documentación para su utilización y un manejo adecuado del servicio.

3.6. ANÁLISIS COMPARATIVO

En esta sección se muestra el estudio de los protocolos de seguridad del servicio de correo electrónico a manera de cuadros comparativos seguidos de una interpretación y calificación por parte del autor, dichos cuadros comparativos se encuentran clasificados de acuerdo a los parámetros de comparación definidos anteriormente.

Para obtener los resultados cuantitativos y cualitativos que permitan una selección mas sustentada de un protocolo, la calificación de cada parametro de comparación está basada en la siguiente escala:

Tabla 2: Escala de valores

Regular	Bueno	Muy Bueno	Excelente
< 30%	>= 30% y < 60%	>= 60% y < 90	>= 90%

Cada parámetro de comparación lo podemos asociar según la clasificación descrita en la siguiente tabla cualitativa en magnitud en que porcentaje se cumpla.

Tabla 3: Escala de valoraciones cualitativas

<=0%	>25% y <=50%	>50% y <=90%	>90% y <=100%
En desacuerdo	Parcialmente de acuerdo	Mayoritariamente de acuerdo	Totalmente de acuerdo
Ninguno	Parcialmente	En su mayor parte	Totalmente
No se cumple	Se cumple insatisfactoriamente	Se cumple aceptablemente	Se cumple plenamente
No satisfactorio	Poco satisfactorio	Satisfactorio	Muy satisfactorio
Malo	Regular	Bueno	Muy bueno
Inadecuado	Mas o menos	Adecuado	Muy adecuado
Insatisfecho	Regularmente satisfecho	Satisfecho	Muy satisfecho
Insuficiente	Parcial	Suficiente	Excelente
Deficiente	Poco eficiente	Eficiente	Muy eficiente
Ningún avance	Cierto avance	Avance significativo	Objetivo logrado
Nunca	Pocas veces	Muchas veces	Siempre
ninguno	poco	Mucho	Todo

Cada uno de los ítems de la interpretación incluye la siguiente nomenclatura **(x,y)/z,** en donde:

x: representa el puntaje que obtiene el protocolo PGP/MIME.

y: representa el puntaje que obtiene el protocolo S/MIME.

z: representa la base sobre la cual se está calificando el ítem.

La calificación definitiva de la herramienta en base a cada criterio se obtiene sumando los puntajes de todos los ítems de interpretación, basándose en las siguientes fórmulas:

Pp = $\sum(x)$, puntaje acumulado del protocolo PGP/MIME en el parámetro.

Ps = $\sum(y)$, puntaje acumulado del protocolo S/MIME en el parámetro.

Pc = $\sum(z)$, puntaje sobre el que se califica el parámetro.

Cp = (Pp / Pc) *100%, porcentaje de calificación total que obtuvo PGP/MIME en el parámetro.

Cs = (Ps / Pc) *100%, porcentaje de calificación total que obtuvo S/MIME en el parámetro.

3.6.1. SERVICIOS DE SEGURIDAD

3.6.1.1. **Determinación de Variables**

Autenticación.

Integridad.

Confidencialidad.

No repudio.

3.6.1.2. **Valoraciones**

Autenticación.

Mediante mecanismos de Autenticación podemos permitir el ingreso de usuarios a un sistema de correo seguro haciendo uso de sus datos privados para autenticarse, valoracion (3 puntos).

Integridad.

Asegurar que los mensajes transmitidos que han sido firmados digitalmente no sufran ninguna modificación en el camino entre el emisor y receptor, sin que esta sea percibida. Los métodos son utilizados para verificar que el mensaje no ha sido modificado mientras transitaba. Por lo general, esto se realiza a través de clasificación de códigos de mensajes firmados digitales, valoracion (3 puntos).

Confidencialidad.

El cifrado de mensajes protege el contenido de un mensaje de correo electrónico. Sólo el destinatario al que va dirigido el mensaje puede ver el contenido, y el contenido sigue siendo confidencial y no puede conocerlo nadie más que quien pueda recibir o ver el mensaje. El cifrado ofrece confidencialidad mientras el mensaje está en tránsito y mientras está almacenado, valoracion (3 puntos).

No repudio.

Para evitar que un extremo niegue haber enviado un dato o haberlo recibido, en el caso de que haya ocurrido. Es la garantía de transmisión y recepción de información, busca proteger al emisor de que el receptor niegue haber recibido el mensaje, y proteger al receptor de que el transmisor niegue haber enviado el mensaje.

Deberá asegurar que el emisor del correo electrónico firmado digitalmente no pueda negar posteriormente el envío del mismo, valoracio (1 punto).

Tabla 4: Servicio de seguridad

VARIABLES	PROTOCOLOS	
	PGP/MIME	S/MIME
Autenticación	Muy Bueno	Muy Bueno
Integridad	Muy Bueno	Muy Bueno
Confidencialidad	Muy Bueno	Muy Bueno
No Rechazo	Muy Bueno	Muy Bueno

3.6.1.3. **Interpretación.**

La autentificación del mensaje también es proporcionada. La llave secreta del dueño puede ser usada para encriptar un mensaje, con esto "fírmalo". Esto crea una firma

digital al mensaje, el cual el receptor puede checar usando la llave pública del transmisor para desencriptarlo. Esto muestra que el transmisor fue el verdadero creador del mensaje, y que consecuentemente no ha sido alterado por nadie más, porque él únicamente posee la llave secreta para crear esa firma. La falsificación de un mensaje firmado es imposible, y el transmisor no podrá denegar esa firma, (3,3)/3.

PGP/MIME proporciona el servicio de integridad a travez de funciones criptograficas hash al igual que S/MIME, La integridad de datos nos permite estar seguros de que los datos no han sido cambiados que nadie haya cambiado el contenido de un correo electrónico (3,3)/3.

Mediante la confidencialidad se permite la protección de la información contra lectura por parte de terceros no autorizados, unicamente puede acceder al contenido de la informacion quien tenga la llave para desemcriptar la informacion, PGP/MIME Y S/MIME lo proporcionan mediante algoritmos de encriptacion(3,3,)/3.

El No repudio o la denegacion de un correo electronico PGP/MIME utiliza mensajes criptograficos firmados S/MIME utiliza las firmas digitales(1,1)/1 .

3.6.1.4. **Calificación.**

Pc = $\sum(z)$ = 3 + 3 + 3 + 1 = **10**

Pp = $\sum(x)$ = 3 + 3 + 3 + 1= **10**

Ps = $\sum(y)$ = 3 + 3 + 3 + 1= **10**

Cp = Pp / Pc = (10 / 10)*100 = **100%**

Cs = Ps / Pc = (10 / 10)*100 = **100%**

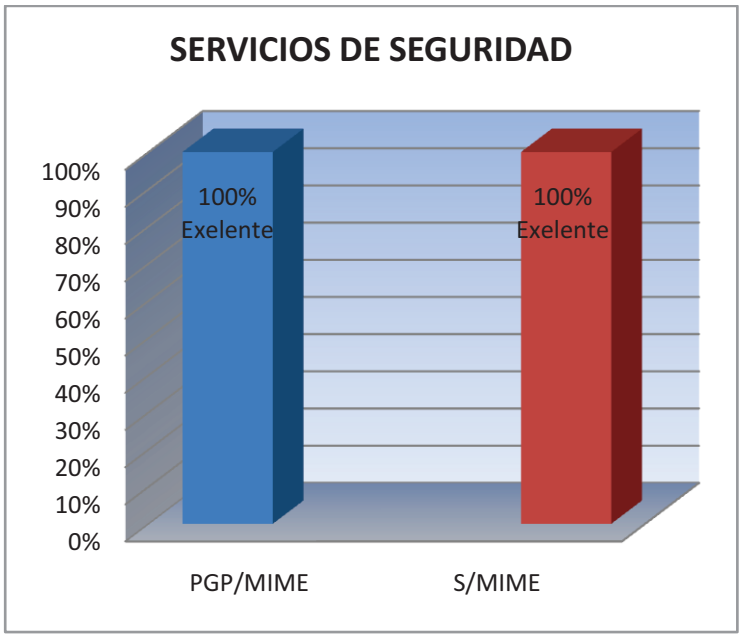


Figura 30: Servicio de Seguridad

3.6.2. SOPORTE CRIPTOGRÁFICO

3.6.2.1. **Determinación de Variables**

Cifrado

Firma Digital

Funcion Hash.

3.6.2.2. **Valoraciones**

Cifrado

Los sistemas de clave simétrica utilizan una misma clave para cifrar y descifrar, de forma que tanto el emisor como el receptor del mensaje deben ponerse de acuerdo previamente en la clave a utilizar, (4 puntos).

Firma Digital

La firma digital es un aspecto muy importante en seguridades de correo electronico es la forma de autenticar a los usuarios, (4 Puntos)

Funciones Hash.

Las funciones resumen hacen corresponder un mensaje de longitud arbitraria a otro de longitud fija (el hash, normalmente más pequeña). Esta función debe cumplir dos condiciones: ha de ser difícil encontrar dos mensajes diferentes cuyo hash sea el mismo y dado el hash ha de ser imposible conocer el mensaje original, (2 puntos).

Tabla 5: Soporte Criptográfico

VARIABLES	PROTOCOLOS	
	PGP/MIME	S/MIME
Algoritmo simétrico de encriptación.	Muy Bueno	Muy Bueno
Algoritmo de firma	Bueno	Muy Bueno
Funciones Hash	Muy Bueno	Muy Bueno

3.6.2.3. **Interpretación.**

Con la encriptación clave-pública, el objeto es encriptado usando un algoritmo simétrico de encriptación. Cada clave simétrica se utiliza solamente una vez. Puesto que se utiliza solamente una vez, la clave sesión está limitado al mensaje y es transmitida con él. Para proteger la clave, esta es encriptada como clave- pública, PGP/MIME y S/MIME utilizan similares algoritmos para encriptar, (4 , 4)/4.

Firmas Digitales: PGP/MIME utiliza el siguiente mecanismo las frases clave se pasan a través delas funsiones de hash para producir una huella digital que un cifrado simétrico usa para descifrar la clave privada.

S/MIME por su parte utiliza los mismos algoritmos para firmar las llaves de los usuarios, (2 , 4)/4.

Función Hash: Garantiza la integridad del mensaje obteniendo un resumen del texto PGP/MIME al igual que S/ MIME utilizan las mismas funciones hash SHA-1, (2 , 2)/2.

3.6.2.4. **Calificación.**

Pc = $\sum(z)$ = 4 + 4 + 2= **10**

Pp = $\sum(x)$ = 4 + 2 +2= 8

Ps = $\sum(y)$ = 4 + 4 + 2= **10**

Cp = Pp / Pc = (8 / 10)*100 = 8**0%**

Cs = Ps / Pc = (10 / 10)*100 = **100%**

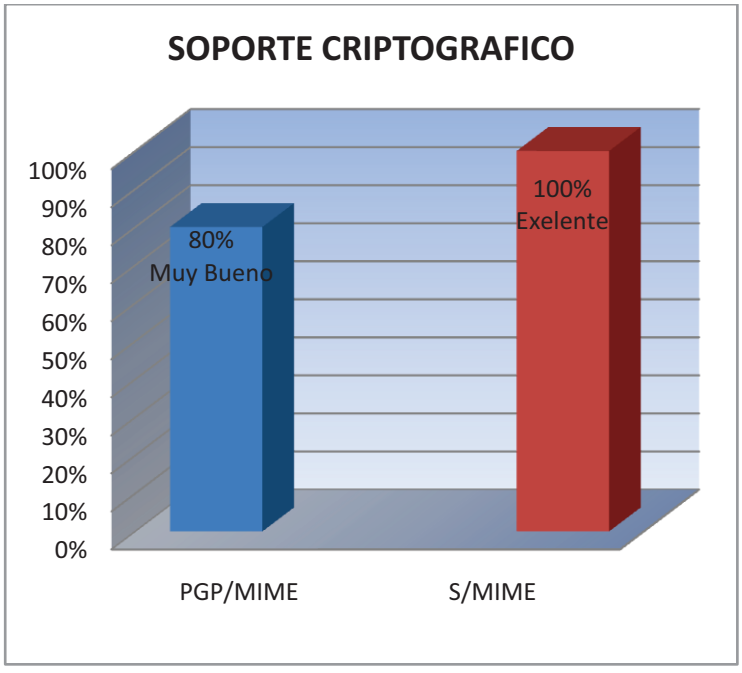


Figura 31: Soporte criptográfico

3.6.3. MANEJO DE CERTIFICADOS DIGITALES

Es la forma en que cada uno de los protocolos maneja los certificados digitales, en la manera en que son emitidos por una CA o por los mismos usuarios de correo electronico, el tiempo de vigencia y revocacion de los mismos.

3.6.3.1. **Determinación de Variables**

Autoridades de Certificación.

Redes de Confianza.

Infraestructura de llave publica (PKI).

Certificados X.509v3.

Mensajes en Formato Binario.

Tiempo de validez de certificado.

3.6.3.2. **Valoraciones**

Autoridades de Certificación.

Una Autoridad de certificadora (CA por sus siglas en inglés Certification Authority) es una entidad de confianza, responsable de emitir y revocar los certificados digitales o certificados, utilizados en la firma electrónica, para lo cual se emplea la criptografía de clave pública, (4 puntos).

Redes de Confianza.

Se genera una red de confianza donde existe usuarios que entyre ellos pueden certificar a otro usuario de su red y de esta manera sucesiva mente se va generando una red, es

unas red no muy funcional por el hecho de cuando existan muchos usuarios la red crecera y existira un poco confianza entre ellos, funcional para pocos usuarios o de uso domestico, (2 puntos).

Infraestructura de llave pública (PKI).

Una PKI habilita a usuarios de redes públicas inseguras, como internet, básicamente a intercambiar datos privados de manera segura mediante el uso de un par de claves criptográficas, pública y privada, que se obtiene y comparte a través de una autoridad de confianza. La infraestructura de clave pública proporciona un certificado que identifica un individuo u organización y servicios de directorio que puede almacenar y, si fuera necesario, revocar los certificados, (4 puntos).

Certificados X.509v3.

x.509 es un estándar para una Infraestructura de Llave Publica (PKI), el cual especifica el formato para certificados de claves públicas, y un algoritmo de validación de la ruta del certificado, (2 puntos).

Mensaje en Formato Binario.

Los mensajos son manejados de forma binaria por que se necesitan enviar o recibir mensajes en texto plano y luego pueden ser encriptados los datos, (2 puntos).

Tiempo de validez del certificado.

Un certificado emitido para un usuario determinado debe o puede estar controlado por una lista donde indica su valides y su estado actual del certifiacdo para su uso, (2 puntos).

Tabla 6: Manejo de certificados digitales

VARIABLES	PROTOCOLOS	
	PGP/MIME	S/MIME
Autoridades de Certificación	Malo	Muy Bueno
Redes de confianza	Muy Bueno	Malo
Infraestructura de llave pública (PKI)	Poco eficiente	Muy eficiente
Certificados X.509v3	Malo	Muy Bueno
Mensajes en Formato binario	Muy Bueno	Bueno
Tiempo de Validez del certificado	Poco eficiente	Muy eficiente

3.6.3.3. **Interpretación.**

Cada clave es certificada por una sola entidad CA, las CAs son certificadas por otras en orden jerárquico donde los certificados raíces son usualmente distribuidos con los programas como navegadores y clientes de correo, (0 , 4)/4.

Cada usuario puede firmar (certificar) las claves de otros usuarios entre ellos forman lo que es una red de confianza pero en realidad no se puede comprobar a una persona o entidad quien dice ser por que se encuentra registrada con una CA, este esquema lo utiliza PGP/MIME, (1 , 0)/2

Infraestructura de clave pública, el protocolo S/MIME utiliza la infraestructura de clave pública centralizada con lo que puede tener el control de varios aspectos de manejo o distribución de las claves, PGP/MIME no utiliza este protocolo, PGP/MIME utiliza la infraestructura distribuida, (2,4)/4

S/MIME basa su formato en certificados X.509v3 donde describe varios parámetros como son nombre y clave del usuario, tiempo de validez del certificado, la CA que emitió el certificado y la firma de la CA lo cual garantiza con esto Autenticación de la persona que envía el mensaje , (0,2)/2.

Todas las salidas de PGP son secuencias binarias (mensajes codificados, binarios codificados). Sin embargo, en determinados casos como el correo electrónico puede ser útil enviar la información en modo texto, esto permite una fácil distribución de la clave privada o incluso que un mensaje pudiera copiarse a mano y después cifrar por medios informáticos (2,1)/2.

Los certificados pueden ser revocados y antes de utilizar una firma pueden ser chequeados sin aun siguen validos, (1 , 2)/2.

3.6.3.4. **Calificación.**

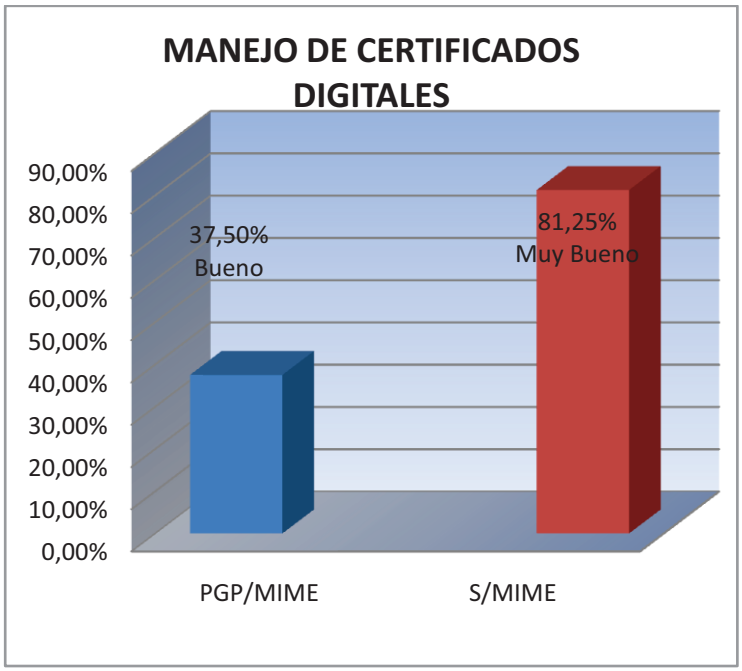


Figura 32: Manejo de certificados Digitales

Pc = $\sum(z) = 4 + 2 + 4 + 2 + 2 + 2 = \mathbf{16}$

Pp = $\sum(x) = 0 + 1 + 2 + 0 + 2 + 1 = 6$

Ps = $\sum(y)$ = 4 + 0 + 4 + 2 + 1 + 2= **13**

Cp = Pp / Pc = (6 / 16)*100 = **37.5%**

Cs = Ps / Pc = (13 / 16)*100 = **81.25%**

3.6.4. ESTRUCTURA DE LOS MENSAJES

El estructura de los mensajes determina la manera en que va a estar compuesto por que en ella se encuentran varios paquetes indica de qué tipo de paquete se trata y su longitud y, a continuación, unos campos de datos que depenen del tipo de paquete.

Determina ademas como protege los datos o el flujo de información frente a accesos, modificaciones, pérdidas, etc.

3.6.4.1. **Determinación de variables.**

Mensajes firmados en claro

Datos comprimidos.

Encapsulamiento del mime de datos firmados

Encapsulamiento del mime de datos encriptados

3.6.4.2. **Valoraciones.**

Mensajes firmados en claro

Lo que se hace en estos casos es formar un mensaje con dos partes, la primera se representa como un mensaje normal, que puede ser leído por cualquier cliente de correo,

y la segunda es la firma de la primera. Un mensaje de este tipo se llama mensaje firmado en claro.

De esta forma, quien disponga de un lector de correo seguro podrá leer el mensaje y verificar la firma, y quien utilice un lector tradicional podrá igualmente leer el mensaje, aunque no podrá comprobar si la firma es auténtica, (2 puntos).

Datos comprimidos

Sirve para disminuir el tamaño de los paquetes de datos que van hacer trasferidos por la red , (2 puntos).

Encapsulamiento del mime de datos firmados

Determina la forma en que van a estar constituidos los datos firmados en el MIME, los diferentes formatos adoptados por cada uno de los protocolos, (4 puntos).

Encapsulamiento del mime de datos encriptados

Los datos luego de ser firmados son encriptados para mayor seguridad, para representar estos datos se utiliza diferentes formatos, (4 puntos).

Tabla 7: Estructura de los mensajes

VARIABLES	PROTOCOLOS	
	PGP/MIME	S/MIME
Mensajes firmados en claro	Muy Adecuado	Muy Adecuado
Datos comprimidos	Eficiente	No aplica
Encapsulamiento del MIME de datos firmados	Eficiente	Muy eficiente
Encapsulamiento del MIME de datos cifrados	Eficiente	Muy eficiente

3.6.4.3. **Interpretación.**

Mensajes firmados en claro

Igual que S/MIME, PGP/MIME también define un formato para enviar mensajes firmados en claro, que permite leer el contenido a los usuarios que no disponen de clientes configurados para leer mensajes firmados, (2,2)/2.

Datos comprimidos

El algoritmo utilizado por PGP/MIME para encriptar los paquetes de datos es el Zip, S/MIME no comprime sus datos, (2,0)/2.

Encapsulación del mime de los datos firmados

PGP/MIME encapsula el mime de los datos firmados con armadura ASCII, el termino multipart se refiere que son varios paquetes firmados.

El protocolos S/MIME tiene dos formas para poder encapsular el MIME de los datos firmados, multipart/firmado y con el estandart del contenido de mensaje CMS, (2,4)/4.

Encapsulación del mime de los datos encriptados

S/MIME utiliza el formato pkcs7-mime para mostrar los datos MIME encriptados lo cual seran desencriptados con clientes de correo que se hayan configurados sus cuentas con certificados digitales.

PGP/MIME encripta el mime con algoritmos de encriptacion utilizados por PGP, (3,4)/4.

3.6.4.4. **Calificación.**

Pc = $\sum(z) = 2 + 2 + 4 + 4 =$ **12**

Pp = $\sum(x) = 2 + 2 + 2 + 3 =$ **9**

Ps = $\sum(y) = 2 + 0 + 4 + 4 =$ **10**

Cp = Pp / Pc = (9 / 12)*100 = **75%**

Cs = Ps / Pc = (10 / 12)*100 = **83%**

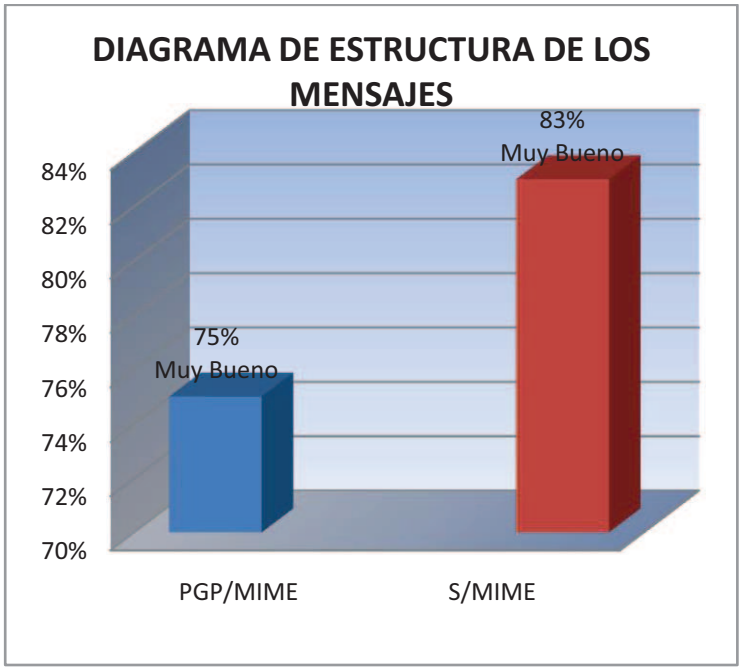


Figura 33: Estructura de los Mensajes

3.6.5. ACCESIBILIDAD

3.6.5.1. **Determinación de variables.**

Plataforma.

Licencia.

Documentacion.

Ambito.

3.6.5.2. **Valoraciones.**

Plataforma.

Es de mucha importancia determinar bajo que plataforma funciona correctamente un sistema ya que de esto depende el costo final de un sistema informatico, 4 puntos).

Licencia.

Con este parámetro podemos determminar bajo que circunstancias bamos a utilizar un determinado sistema, por lo cual es impresindible tener una licencia de un sistema o utilizar software libre, (2 puntos).

Documentación.

Para poder realizar una investigacion necesitamos de documentacion actualizada y legible, sin esto es una tarea muy dificil poder instalar configurar y poner en marcha un sistema, (3 puntos).

Ámbito

Tenemos que determinar en que ambitos un sistema va hacer funcional por que muchos de ellos tienen sus restricciones y al no cumplir con sus reglas un sistema puede caer o tener fallas, se debe determinar tambien en los entornos en quie va a funsionar,(4 puntos).

Tabla 8: Accesibilidad

VARIABLES	PROTOCOLOS	
	PGP/MIME	S/MIME
Plataforma	EXCELENTE	EXCELENTE
Licencia	BUENO	BUENO
Documentación	POCO	MUCHO
Ámbito	POCO	MUCHO

3.6.5.3. **Interpretación.**

Al referirse a la plataforma S/MIME y PGP/MIME encontramos disponibles en el sistema operativo Linux y Windows en varios clientes de correo que vienen instalados con paquetes de herramientas, (4,4)/4

El uso S/MIME y PGP/MIME lo podemos encontrar con licencia libre o en ciertos casos es necesario pagar por la utilizacion de estos sistemas, (1,1)/2.

La documentacion que existe para poder realizar el estudio de PGP/MIME es bien limitada por su poco uso no existe una amplia descripcion hacerca del protocolo, (1,3)/3.

PGP/MIME tiene en bajo alcanze para manejar seguridades de correo electronico por el hecho de que un usuario puede certificar a otro usuario y se forma una red de confianza y esta al crecer se hace inmanejable, designado mas para un uso domestico con usuarios locales, por su parte S/MIME por hecho de manejarse mediante autoridades de

certificacion tiene un mayor alcanze de usuarios fue creado con fines empresariales y profesionales, (2,6)/6.

3.6.5.4. **Calificación.**

Pc = $\sum(z) = 4 + 2 + 3 + 6 =$ **15**

Pp = $\sum(x) = 4 + 1 + 1 + 2 =$ **8**

Ps = $\sum(y) = 4 + 1 + 3 + 6 =$ **14**

Cp = Pp / Pc = (8 / 15)*100 = **53%**

Cs = Ps / Pc = (14 / 15)*100 = **93%**

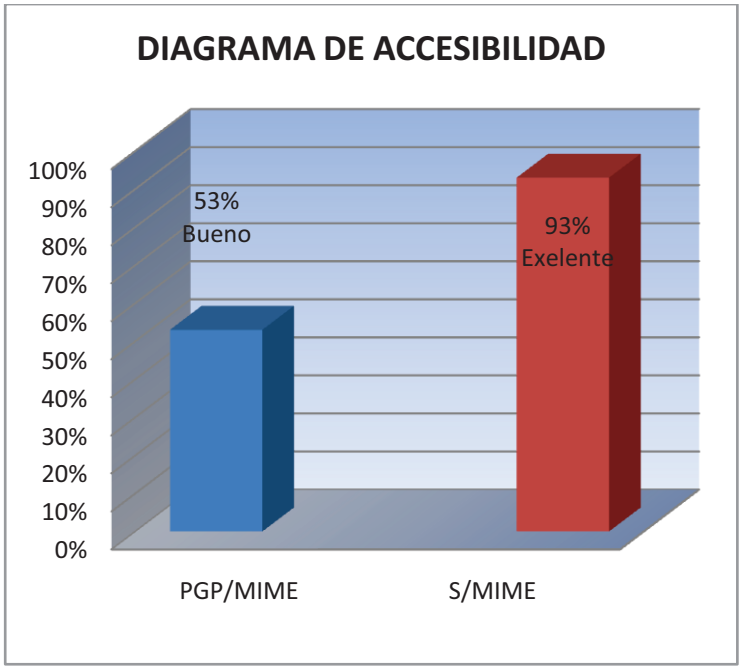


Figura 34: Accesibilidad

3.7. PUNTAJES ALCANZADOS

El puntaje final y el porcentaje sobre el Total de cada protocolo se los obtiene de la siguiente manera:

Puntaje Total de la Evaluación: (PT) = $\sum(Pc)$

Puntaje Final del protocolo PGP/MIME: (PFp) = $\sum(Pp)$

Puntaje Final del protocolo S/MIME: (PFs) = $\sum(Ps)$

Tabla 9: Resultado Final

Parámetros	Variables	PGP/MIME	S/MIME
1	1.1	3	3
	1.2	3	3
	1.3	3	3
	1.4	1	1
2	2.1	4	4
	2.2	2	4
	2.3	2	2
3	3.1	0	4
	3.2	1	0
	3.3	2	4
	3.4	0	2
	3.5	2	1
	3.6	1	2
4	4.1	2	2
	4.2	2	0
	4.3	2	4
	4.4	3	4
5	5.1	4	4
	5.2	1	1
	5.3	1	3
	5.4	2	6
Totales		**40**	**57**

PT = 10 + 10 + 16 + 12 + 15 = **63**

PFp = 10 + 8 + 6 + 9 + 8 = **41**

PFs = 10 + 10 + 13 + 10 + 14 = **57**

Porcentaje Total del protocolo PGP/MIME: (%P) = (PFp/PT)*100%

Porcentaje Total del protocolo S/MIME: (%S) = (PFs/PT)*100%

Un resumen de los resultados obtenidos mediante este estudio se muestra a través de la siguiente figura:

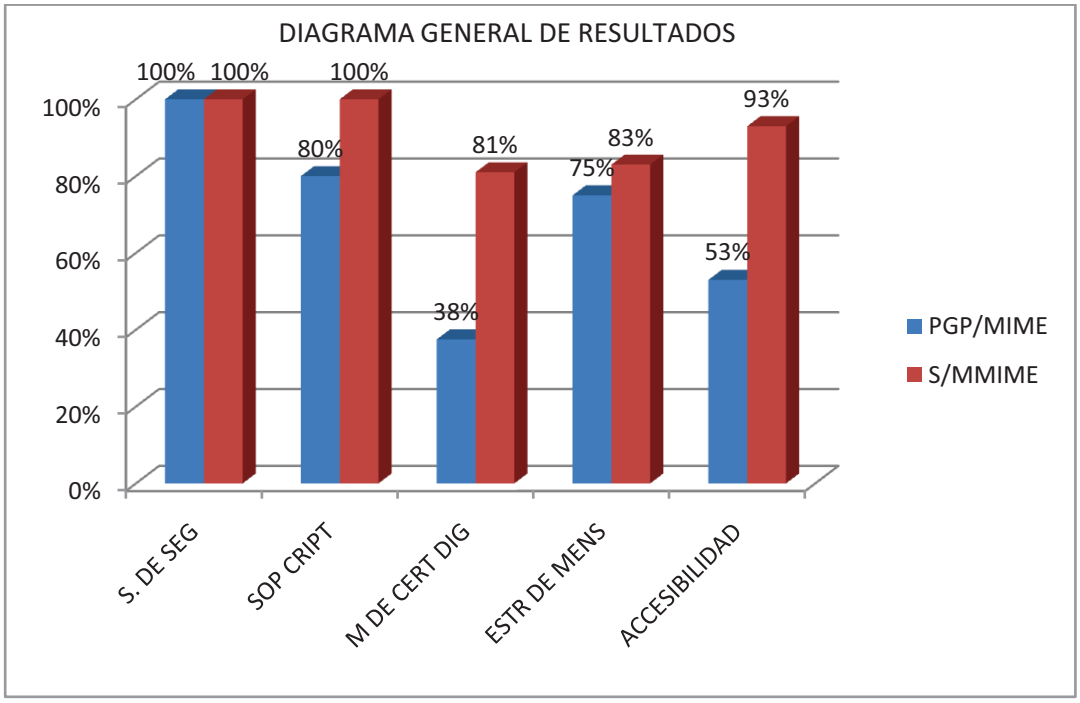


Figura 35: Diagrama general de resultados

%P = (41/63)*100% = **65%**

%S = (57/63)*100% = **90%**

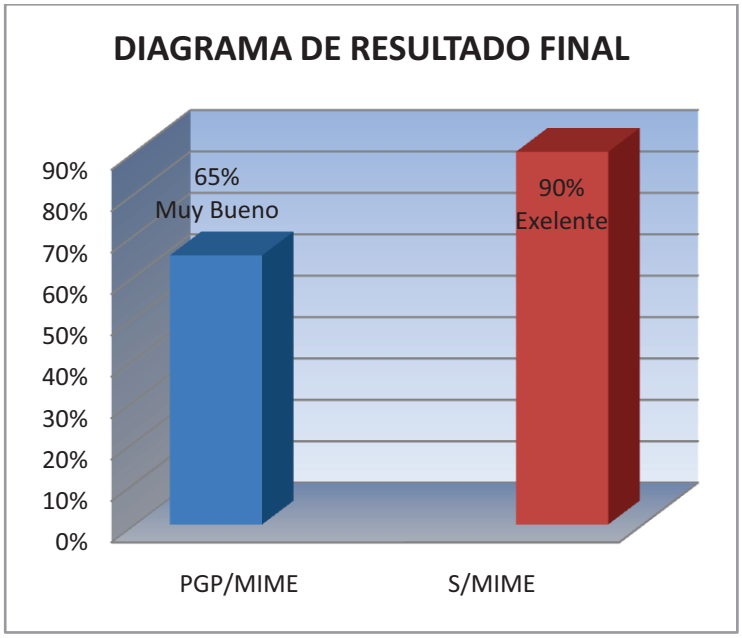


Figura 36: Resultado final

Interpretación.

En base a los resultados que hemos obtenido de este análisis comparativo de los parametros planteadas, podemos observar que PGP/MIME es un protocolo que tiene caracteristicas un poco similares a las de S/MIME se diferencian en un 25%.

3.8. RESULTADOS DEL ANÁLISIS

- Del análisis comparativo que se realizo se tomo en cuenta parámetros necesarios en cuanto a seguridad se refiere como lo es servicio de seguridad, soporte criptográfico, certificados digitales, estructura de los mensajes y accesibilidad.
- En lo relacionado a la seguridad los dos protocolos presentan similitudes en cuanto al proceso de proteger la información mediante encriptación de los datos utilizando algoritmos que no pueden ser violados su seguridad.

- El proceso de certificación de los usuarios existe mucha diferencia por lo que S/MIME utiliza las Autoridades de Certificación para certificar a los usuarios es una manera mas segura de confiar en un usuario, por lo contrario PGP/MIME utiliza lo que son las mallas o redes de confianza donde un usuario puede certificar a otro usuario.

- S/MIME maneja las listas de revocación de los certificados es otro aspecto importante que debe ser tomado en cuenta, el protocolo PGP/MIME no utiliza esta forma de mantener el control de los usuarios certificados.

- La accesibilidad para poder implementar un servicio de correo electrónico seguro con PGP/MIME es un poco limitado para el número de usuarios por que fue creado con fines de pequeñas redes o usuarios locales o domesticos por su parte S/MIME fue creado para fines empresariales y profesionales por lo que abarca un mayor número de usuarios que pueden acceder al servicio.

- Se puede sustentar y concluir que el protocolo seguro en el servicio de correo electrónico S/MIME es el mas óptimo para ser utilizado dado que puede ser utilizado con un mayor número de usuarios certificados.

- Esta conclusión sustentamos con los datos obtenidos en las tablas de los cuadros de comparación, con esta desion tomada podremos demostrar nuestra hipotesis al incrementar la seguridad de la información en los datos de mensajes de correo electrónico.

CAPÍTULO IV

CONFIGURACIÓN DE SEGURIDADES EN LA INFRAESTRUCTURA DE CORREO ELECTRÓNICO

4.1. INTRODUCCIÓN

En este capítulo detallaremos los pasos necesarios para la instalación y configuración de la infraestructura del sistema de correo electrónico tomando en cuenta el resultado obtenido del estudio de los protocolos seguros para el servicio de correo electrónico realizado en el capitulo anterior para agregar seguridad al correo electrónico.

Determinaremos el software necesario en sus versiones respectivas para el correcto funcionamiento del sistema y la configuración adecuada de cada uno de los archivos.

Como sistema operativo Linux, utilizaremos la distribución **Centos 5.2** con un kernel 2.6.18-9.el5 y usando exclusivamente software libre.

Se ha elegido **Postfix** en su versión 2.5.3 como MTA. A Postfix se le han agregado los siguientes mecanismos de seguridad: TLS (Transport Layer Security) para cifrar las conexiones y SASL (Simple Authentication and Security Layer) como sistema de autentificación.

Todo el correo que pase a través del servidor SMTP será revisado en busca de virus y SPAM. Para llevar a cabo esta tarea se utilizará AMaViSd-new (en su versión 20030616p10-5) como interfaz entre el servidor de correo SMTP y las aplicaciones ClamAV (v. 0.84-2.sarge.10) y Spamassassin (v. 3.0.3-2sarge1), las cuales analizarán el correo en busca de virus y SPAM respectivamente.

Para la consulta de mensajes por parte de los usuarios se dispondrá de un servidor POP3 e IMAP, con sus respectivas versiones seguras con protocolo SSL, para lo cual se hará uso de Courier (courier-pop y courier-pop-ssl versión 0.47-4sarge5, courier-imap y courier-imap-ssl versión 3.0.8-4sarge5).

Los usuarios del correo no serán usuarios físicos de la máquina sino que serán usuarios virtuales almacenados en una Base de Datos **MySQL** (v 5.0.45-7.el-5).

Ha sido seleccionada esta tecnología para evitar que el archivo /etc/passwd se haga enorme.

Para crear una autoridad certificadora y generar certificados propios se ha dispuesto de **OpenSSL** 0.9.8e-7.el5.

4.2. GUÍA PARA LA IMPLEMENTACIÓN.

- Instalación de los módulos de Php.
- Instalación del servidor web apache.
- Instalación y configuración del servidor de base de datos MySQL.
- Instalación y configuración Cyrus Sasl.
- Instalación de Postfix.
- Instalación de librerías CPAN.
- Instalación y configuración Clamav
- Instalación y configuración spamassassin
- Instalación y configuración Amavis-New
- Instalación y configuración Courier-Imap

4.3. INSTALACIÓN DE LOS MÓDULOS DE PHP

Para el normal funcionamiento del lenguaje PHP se instala en el servidor el modulo principal de php y varios módulos para poder acceder a bases de datos y realizar métodos de autenticación de usuarios.

php-5.1.6-23.2.el5-3.i386.rpm

php-odbc-5.1.6-23.2.el5-3.i386.rpm

php-mysql-5.1.6-23.2.el5-3.i386.rpm

php-mbstring-5.1.6-23.2.el5-3.i386.rpm

php-common-5.1.6-23.2.el5-3.i386.rpm

php-cli-5.1.6-23.2.el5-3.i386.rpm

4.4. INSTALACIÓN DEL SERVIDOR WEB APACHE

El servidor web apache es otra de las herramientas que necesitamos que este instalado en nuestro sistema de correo electrónico, ya que los mensajes de correo viajan por internet atreves del servidor web.

4.5. INSTALACIÓN Y CONFIGURACIÓN DEL SERVIDOR DE BASE DE DATOS MYSQL

Instalamos los paquetes necesarios para el servidor MySQL mediante los siguientes comandos.

```
$ rpm -ivh mysql-5.0.45-7.el5.i386.rpm
$ rpm -ivh mysql-server-5.0.45-7.el5.i386.rpm
$ rpm -ivh mysql-devel-5.0.45-7.el5.i386.rpm
$ rpm -ivh mysql-shared-5.0.45-7.el5.i386.rpm
```

Podemos arrancar o parar el servicio con los comandos:

```
$ /etc/init.d/mysql start
$ /etc/init.d/mysql stop
```

4.5.1. DISEÑO DE LA BASE DE DATOS

Creamos la base de datos llamada dbpostfix para almacenar la información de los usuarios del sistema de correo electrónico, previo a esto debe estar creado un usuario para la base de datos llamado postfix, a quien le damos todos los permisos sobre la base de datos Postfix, el archivo sql para la creación de las tablas (ver Anexo)

```
$ mysql
mysql> CREATE DATABASE dbpostfix;
```

4.6. INSTALACIÓN Y CONFIGURACIÓN DE CYRUS SASL.

Para la instalación de este paquete primero descomprimimos en el directorio /usr luego procedemos a la instalación utilizando los siguientes comandos

```
$ tar –zvxf cyrus-sasl-xxx.tar.gz
$ export CPPFLAGS="-I/usr/include/mysql"
$ export LDFLAGS="-L/usr/lib/mysql -lmysqlclient -lz -lm"
$ ./configure \
        --enable-anon \
        --enable-plain \
        --enable-login \
        --enable-sql \
        --disable-krb4 \
        --disable-otp \
        --disable-cram \
        --disable-digest \
        --with-mysql=/usr/lib/mysql \
        --without-pam \
        --without-saslauthd \
        --without-pwcheck \
        --with-plugindir=/usr/local/lib/sasl2
$ make
$ make install
```

Configuramos el archivo smtpd.conf

```
$ vi /usr/local/lib/sasl2/smtpd.conf
pwcheck_method: auxprop
auxprop_plugin: sql
sql_engine: mysql
mech_list: sql plain login
sql_hostnames: localhost
sql_user: postfix
sql_passwd: your-password
sql_database: postfix
sql_statement: SELECT clear FROM postfix_smtp WHERE email = '%u@%r'
sql_verbose: yes
```

4.7. SERVIDORES DE CORREO ELECTRÓNICO.

4.7.1. INSTALACIÓN Y CONFIGURACIÓN DE POSTFIX

Instalaremos los paquetes de Postfix con soporte para MySQL, los archivos más importantes de configuración de Postfix son los siguientes:

main.cf (/etc/postfix/main.cf): archivo de configuración principal de Postfix donde se encuentran los parámetros que controlan el comportamiento del MTA.

master.cf (/etc/postfix/master.cf): archivo de configuración del demonio master. Determina qué procesos serán arrancados y con qué opciones.

aliases (/etc/aliases): archivo de alias. Equivalencia entre una dirección ficticia y una dirección local real.

Creamos un usuario postfix y un grupo postdrop, editamos los archivos /etc/passwd y /etc/group para que el usuario postfix tenga el mismo número de identificación que el grupo postdrop.

```
$ vi /etc/passwd

postfix:x:501:501:/var/spool/postfix:/bin/true

$ vi /etc/group

postfix:x:501:
postdrop:x:502:

$ tar -zxvf postfix-2.0.16.tar.gz
$ make makefiles \
        'CCARGS=-DHAS_MYSQL -I/usr/include/mysql -DUSE_SASL_AUTH -
I/usr/local/include/sasl' \
        'AUXLIBS=-L/usr/lib/mysql -lmysqlclient -lz -lm -L/usr/local/lib -lsasl2'
$ make install
```

4.7.1.1. **MAIN.CF**

En la ruta /etc/postfix, por defecto, tenemos el archivo principal de configuración de Postfix denominado main.cf.

Entre sus parámetros más importantes que se encuentran para configurar el servidor de correo tenemos:

myhostname: indica a Postfix el nombre del servidor, si no lo ponemos lo cogerá de la información que esté almacenada en /etc/hostname.

mydomain: con este parámetro postfix puede servir a varios dominios.

myorigin: será, para el correo local, el origen del correo cuando en el mail sólo se indica el usuario.

mydestination: aquí se declaran todos los dominios que deben considerarse locales al sistema a efectos de encaminamiento del correo electrónico.

home_mailbox: la siguiente opción nos permite elegir en qué tipo de "formato" se van a guardar los mensajes en el buzón de cada usuario: mbox (fichero) o maildir (directorio).

mynetworks: el rango de direcciones IP que van a poder enviar a través de este MTA, es decir, redes a las que permito hacer relay puesto que son locales a Postfix. Las redes deberán ser especificadas en formato Classless Internet

mynetworks = 172.30.0.0/16, 127.0.0.0/8

queue_directory: especifica el lugar de la cola de Postfix. Es también el directorio raíz de los demonios de Postfix (que corren enjaulados).

command_directory y **daemon_directory**: contienen la ruta donde están los comandos y los demonios de Postfix, respectivamente.

mail_owner: indica el usuario que es propietario de la cola de Postfix. Se debe usar un usuario dedicado y como la instalacion de Postfix crea el usuario y el grupo postfix, usaremos éste.

virtual_mailbox_base: este parámetro es lo que se le agrega al valor que tenemos en la Base de Datos MySQL para conseguir llegar hasta el buzón del usuario. Vamos a dejarlo con "/"

virtual_mailbox_base=/

virtual_uid_maps y **virtual_gid_maps**: señalamos a Postfix que los UserIDs y GroupIDs de los usuarios de correo los obtendrá por medio del archivo indicado, que accederá a MySQL.

virtual_uid_maps=mysql:/etc/postfix/ids.cf

virtual_gid_maps=mysql:/etc/postfix/gids.cf

virtual_mailbox_maps: con este parámetro indicamos que mediante el archivo mysql_virt.cf vamos a acceder a MySQL para ver dónde están los buzones de los usuarios:

virtual_mailbox_maps=mysql:/etc/postfix/mysql_virt.cf

local_transport: le indicamos que deberá entregar el correo a usuarios virtuales y no a locales.

local_transport = virtual

disable_vrfy_command: para no permitir la verificación que hacen los spamers buscando usuarios válidos, deberemos deshabilitar el verify (que se usa para saber si un usuario existe o no en nuestro sistema).

disable_vrfy_command = yes

message_size_limit: para evitar que nuestros propios usuarios provoquen un DoS tratando de enviar un mensaje excesivamente grande, limitaremos el tamaño máximo a 10 Mb (incluidas cabeceras). Si no, podría suceder que Postfix se bloquease al intentar procesar este tipo de mensajes.

message_size_limit = 10485760

```
$ vi /etc/postfix/main.cf

home_mailbox = Maildir/
recipient_delimiter = +
mydestination = $myhostname, $transport_maps
alias_maps = mysql:/etc/postfix/mysql-aliases.cf
relocated_maps = mysql:/etc/postfix/mysql-relocated.cf
transport_maps = mysql:/etc/postfix/mysql-transport.cf
virtual_maps = mysql:/etc/postfix/mysql-virtual.cf
local_recipient_maps = $alias_maps $virtual_mailbox_maps unix:passwd.byname

virtual_mailbox_base = /home/vmail       y
virtual_mailbox_maps = mysql:/etc/postfix/mysql-virtual-maps.cf  y
virtual_uid_maps = mysql:/etc/postfix/mysql-virtual-uid.cf              y
virtual_gid_maps = mysql:/etc/postfix/mysql-virtual-gid.cf              y

queue_directory = /var/spool/postfix     y
command_directory = /usr/sbin            y
daemon_directory = /usr/libexec/postfix  y
mail_owner = postfix                                y

myhostname = smtp.chimborazo.gov.ec     y
mydomain = Chimborazo.gov.ec            y
myorigin = $mydomain                    y

unknown_local_recipient_reject_code = 550
debug_peer_level = 2
debugger_command = \
        PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin \
```

```
        xxgdb $daemon_directory/$process_name $process_id & sleep 5 \
sendmail_path = /usr/sbin/sendmail
newaliases_path = /usr/bin/newaliases
mailq_path = /usr/bin/mailq
setgid_group = postdrop
html_directory = no
manpage_directory = /usr/local/man
sample_directory = /etc/postfix
readme_directory = no

broken_sasl_auth_clients = yes
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_recipient_restrictions = permit_sasl_authenticated,reject_unauth_destination
smtpd_sasl_local_domain = $myhostname
```

4.7.1.2. **MASTER.CF**

El programa master es el encargado de organizar a los diferentes procesos de Postfix, arrancando en cada momento el necesario. Para ello sigue las indicaciones de su fichero de configuración: master.cf que normalmente se encuentra en el directorio */etc/postfix*, en él se especifican los procesos y sus parámetros.

Service, type, prívate, unprivileged, chroot, wakeup, maxprocess, command.

Service: nombre del servicio que se está configurando.

Type: tipo de comunicación de transporte utilizado por el servicio para comunicarse con otros módulos.

Private: indica cuándo el canal de comunicación de un proceso debe estar accesible a procesos ajenos a Postfix.

Unprivileged: especifica con qué privilegio de usuario se ejecuta el servicio.

Chroot: indica si el servicio se ejecuta en un entorno *chroot*, lo que proporciona niveles adicionales de seguridad.

Wakeup: indica los segundos que deben transcurrir para que el proceso master envíe una señal para despertar el servicio correspondiente.

Maxprocess: número máximo de procesos que puede tener en ejecución el servicio. Por defecto, se admiten 50.

Command: nombre del programa a ejecutar y parámetros a pasar.

4.7.2. INSTALACIÓN Y CONFIGURACIÓN DE COURIER IMAP

Courier utiliza un servicio de autentificación común para todos sus servicios (POP3, POP3S, IMAP, IMAPS). Este servicio se puede configurar de manera que haga la autentificación desde varias fuentes(MySql, Ldap), Para instalarlo ejecutamos sus rpms.

El servicio de autentificación está formado por un demonio llamado authdaemon, cuyo fichero de configuración es /etc/courier/authdaemonrc. Por defecto viene configurado para la autentificación vía PAM así que debemos editar el archivo authdaemonrc para sustituir la línea authmodulelist="authpam" por authmodulelist="authmysql" para que a partir de ahora se use MySQL.

También hay que indicar a courier dónde debe mirar los usernames y passwords; para

ello tenemos que modificar el archivo authmysqlrc y tener especial cuidado con los espacios que se dejan entre el nombre de la variable y el valor de la misma, puesto que esos espacios se tomarán como parte del valor a la hora de intentar conectarse a la base de datos (por ejemplo, si dejamos un espacio delante de la contraseña, tomará

el valor de la contraseña con el espacio y no podrá acceder a la base de datos).

```
$ vi /usr/local/courier/etc/authdaemonrc

authmodulelist="authmysql"


$ vi /usr/local/courier/etc/authmysqlrc

MYSQL_SERVER smtp
MYSQL_USERNAME postfix
MYSQL_PASSWORD postfix
MYSQL_PORT 0
MYSQL_DATABASE dbpostfix
MYSQL_USER_TABLE postfix_users
MYSQL_CLEAR_PWFIELD clear
MYSQL_UID_FIELD uid
MYSQL_GID_FIELD gid
MYSQL_LOGIN_FIELD email
MYSQL_HOME_FIELD homedir
MYSQL_MAILDIR_FIELD maildir
MYSQL_QUOTA_FIELD quota
```

4.8. INSTALACION Y CONFIGURACIÓN DE AMAVIST-NEW

Amavisd-new es una aplicación basada en un script de Perl flexible y de alto rendimiento que se ejecuta como un servicio, con un proceso maestro y otro hijo.

Sirve de interfaz de filtrado entre un MTA y otras aplicaciones (un antivirus o un antispam) actuando como un servidor SMTP, recibiendo el mensaje de correo del servidor Postfix, procesándolo y enviándolo o devolviéndolo al servidor SMTP.

Acompañaremos a AMaVIS de dos aplicaciones auxiliares: ClamAV para el filtro de correo con virus y Spamassassin para el filtrado de correo no deseado.

El funcionamiento de filtrado es el siguiente: un correo ha de llegar a nuestro puerto 25

(Postfix). Este será enviado al puerto 10024 (por ejemplo) de AMaVIS, y AMaVIS una vez analizado, nos lo enviaría de nuevo a otro puerto (el 10025 por ejemplo) de Postfix sin restricción alguna entre ellos. El porqué de que se envíe a otro puerto es que si AMaVIS devuelve el correo analizado a Postfix por el 25, Postfix volverá a entregárselo y entraría en un bucle infinito. Si hacemos que Postfix reciba correo de AMaVIS en otro puerto, el problema se soluciona.

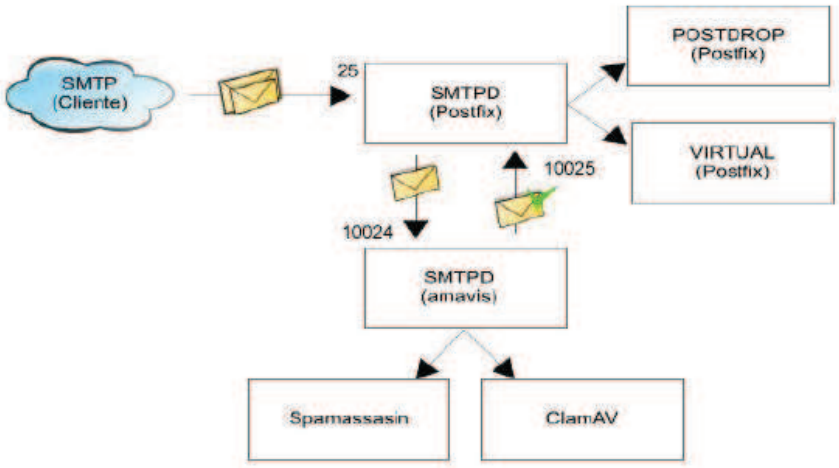


Figura 37: Amavis

4.8.1. INSTALACIÓN DE CLAMAV.

ClamAV es otra herramienta utilizada en la inspección de mensajes electrónicos que permite identificar si el contenido del correo es un virus. AMaVIS le pasará los mensajes para que los inspeccione y luego ClamAV los devolverá. luego de instalarlo editamos el archivo principal de configuracion /etc/amavisd.conf

#wget -c http://kent.dl.sourceforge.net/sourceforge/clamav/clamav-0.83.tar.gz

```
#groupadd clamav
#useradd -g clamav -s /bin/false -c "Clam Antivirus" clamav
#tar -zxf clamav-0.83.tar.gz
#cd clamav-0.83
#./configure --sysconfdir=/etc
#make
#make install
#mkdir /var/lib/clamav
#chown clamav:clamav /var/lib/clamav

$mydomain = 'chimborazo.gov.ec';
$virus_admin      = "genco\@$mydomain";
$mailfrom_notify_admin     = "genco\@$mydomain";
$mailfrom_notify_recip     = "genco\@$mydomain";
$mailfrom_notify_spamadmin = "NOSPAMMER\@$mydomain";
```

Actualizamos la base de datos del antivirus.

```
#touch              /var/log/clam-update.log
#chmod    600    /var/log/clam-update.log
#chown clamav /var/log/clam-update.log
```

Luego de haber configurado iniciamos el servicio con el siguiente comando.

```
#/usr/local/sbin/clamd
```

4.9. INSTALACIÓN DE SPAMASSASSIN

El spamassassin es un filtro anti-SPAM que funciona en la parte del servidor y realiza un análisis de cada mensaje que le pasa AMaVIS, aplicando una serie de reglas que van puntuando el nivel de SPAM. Consiste en un mecanismo heurístico basado en reglas y ponderaciones predefinidas incorporados en un algoritmo bayesiano. Además los usuarios pueden entrenarle para que aprenda.

Para proceder a instalarlo:

yum install spamassassin

Para enseñar los correos positivos y negativos

sa-learn –spam –dir path/chimborazo.gov.ec/buzon/cur

4.10. CONFIGURACIÓN DE S/MIME EN EL CLIENTE DE CORREO ELECTRÓNICO

Para configurar S/MIME en nuestro sistema de correo electronico necesitamos que todos los sistemas que forman parte de la infraestructura de correo esten funcionando de manera correcta y se pueda enviar y reciber correos firmados y encriptados.

S/MIME se encuentra disponible en gran parte en los clientes de correo electrónico.

4.11. CLIENTE DE CORREO ELECTRÓNICO

Para el desarrollo de este trabajo de tesis se a elejido el cliente de correo electronico Thunderbird, por tener soporte para S/MIME y por el hecho de mayor seguridad, código abierto, gratuito, multiplataforma, extensible.

4.12. INSTALACIÓN DE THUNDERBIRD

Para la instalación del cliente de correo electronico thunderbird ejecutamos el siguiente comando y de manera automatica se instala y esta listo para ser configurado con sus caracteristicas de seguridad que posee.

Yum install thunderbird*

Luego instalamos componentes para S/MIME en thunderbird

Perl MCPAN –e Shell

Instalado todo los modulos para las librerias glib y gtk2 de la siguiente manera:

Yum install glib*,gtk*

Esto permite que se creen los certificados

Install MIME::body

4.12.1. GESTIÓN DE CERTIFICADOS DIGITALES

Hoy por hoy el uso de certificados digitales se ha hecho tan frecuente e importante, sobre todo al momento de garantizar la privacidad y seguridad tanto en el intercambio de documentos como en establecer comunicaciones seguras en los distintos servicios que hacen uso del Internet.

Dentro la gestión de certificados digitales, se deben considerar los siguientes pasos:

✔ Crear la estructura de certificación y archivo de configuración

✔ Iniciar la CA

✔ Creacion de Certidficados.

✔ Cambio de formato de certificados

✔ Dando de alta nuestro certificado en Thunderbird

✔ Revocar los certificados

✔ Obtener información de certificados

✔ Conversión de formatos de los certificados.

4.12.2. CREACIÓN DE LA ESTRUCTURA DE CERTIFICADOS

Para la creación de la estructura creamos un directorio en el que vamos a guardar todos los archivos que contengan los certificados de los usuarios y además el archivo de creación de la CA con su certificado, lo podemos crear en el directorio que se desee.

En nuestro caso creamos con el siguiente comando:

mkdir /root/mpuetate

Y con esto ya tenemos nuestro directorio.

4.12.3. INICIAR LA CA

Antes de actuar en una entidad certificadora (CA), primero debemos:

✔ Crear la llave con la que firmaremos los certificados

✔ Crear un certificado autorfirmado

Creación de la clave de seguridad para la creación de certificados:

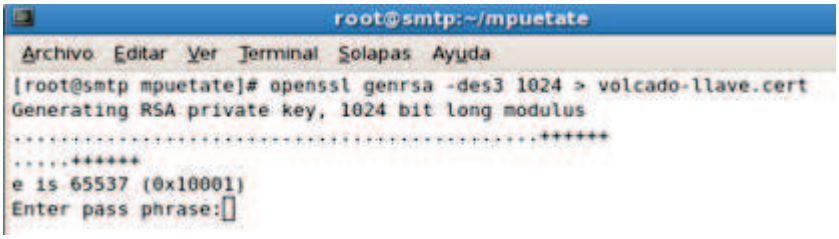


Figura 38: Creación de una CA

Este fichero solo contiene una contraseña de seguridad encriptada por un algoritmo. Vamos a verificar que el fichero se ha creado. para ello tecleamos ls y nos muestra los ficheros de la carpeta CA:

volcado-llave.cert

4.12.4. CREACIÓN DE CERTIFICADOS

Creamos un certificado x509 que identifica a una empresa certificadora a la cual llamamos llave certificadora personal con identificador con duración de 3650 días.

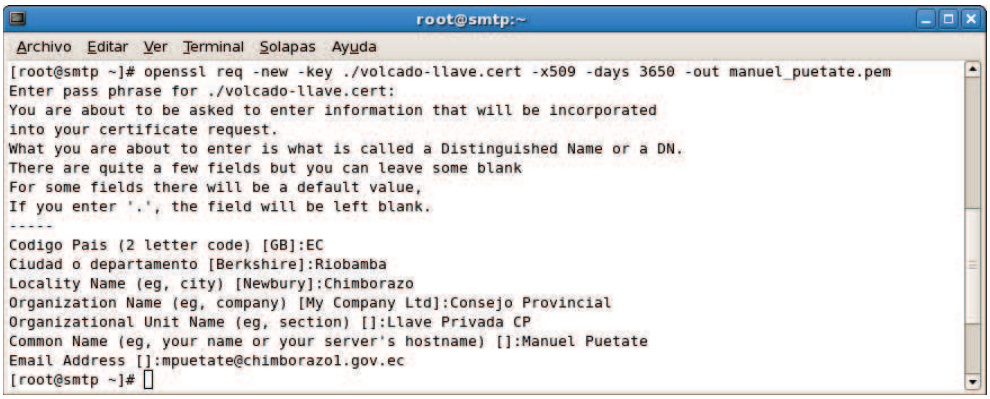


Figura 39: Creación de un Certificado X509

Nuevamente ls y veremos el fichero generado.

volcado-llave.cert

certificado_emilio.pem

Se creará el certificado de la AC y su clave privada. Cada vez que queramos firmar un certificado tendremos que utilizar la clave que se nos pidió al crear la AC.

4.12.5. CAMBIO DE FORMATO DE CERTIFICADO

Por ultimo vamos a crear un certificado en formato Pkcs12 conteniendo el certificado y la llave publica:

Figura 40: Creación de un certificado Pkcs12

4.12.6. DANDO DE ALTA NUESTRO CERTIFICADO EN THUNDERBIRD.

Para ello en Thunderbird nos dirigimos a Editar > Preferencias > Avanzadas y de este ventana llamada **Preferencias** seleccionamos la pestaña > Certificados y después pulsamos el botón ver certificados, nos mostrará una nueva ventana llamada **Administrador de certificados** de la cual seleccionamos la pestaña **[Autoridades]**. Esta pestaña es en la que previamente nos damos de alta como entidad certificadora si no cuando importemos el certificado PKCS12 no será validado como un certificado de confianza.

En este punto pulsar importar dentro de la pestaña Autoridades seleccionamos el certificado con la extension .pem aceptamos y nos mostrara una ventana de descarga de certificado en la cual debemos validar la casilla Confiar en esta CA para identificar usuarios de correo.

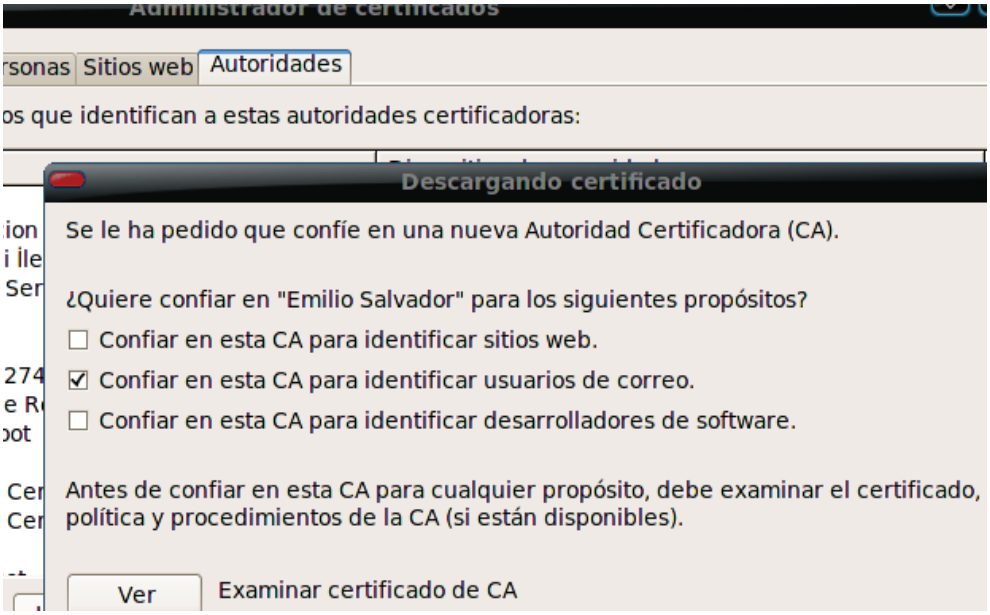


Figura 41: Administración de certificados

El certificado de la CA ha sido importado si cerramos Thunderbird y lo volvemos a abrir lo encontraremos en la lista de certificados como entidad llave certificadora personal.

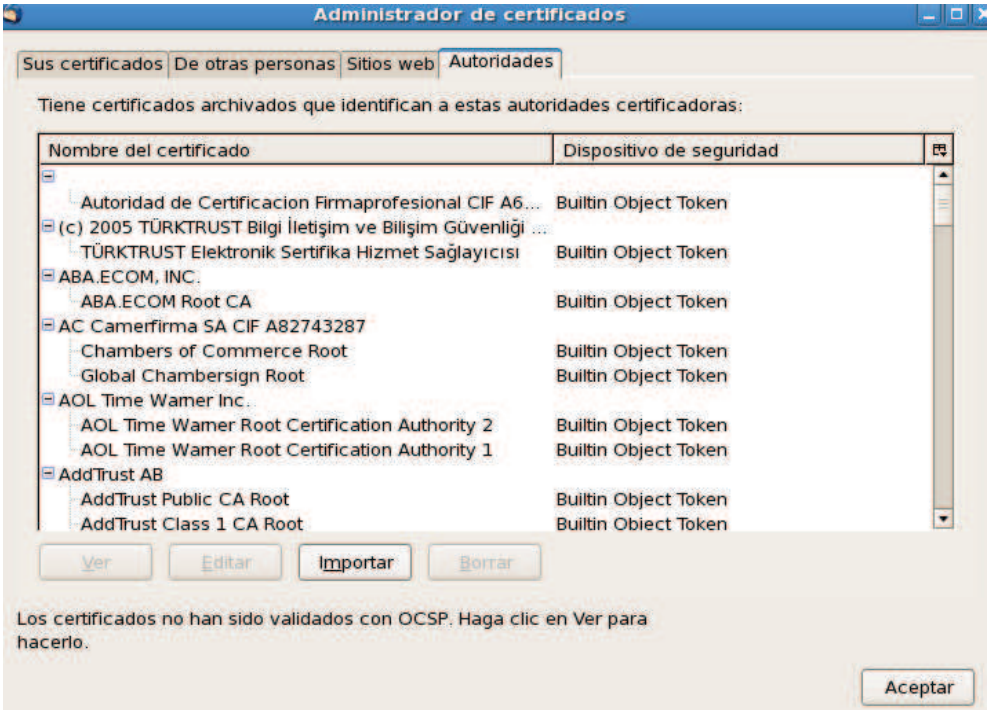


Figura 42: Lista de CA

Incorporar nuestro certificado personal que contiene nuestra contraseña al thunderbird esto se realiza en la misma ventada de administrador de certificados pero esta vez enla pestaña **[Sus certificados]** para poder acceder al almacén de certificados personales tecleamos la contraseña la misma del certificado o la de nuestro perfil de usuario en Linux. Luego una contraseña mas la de nuestro certificado.

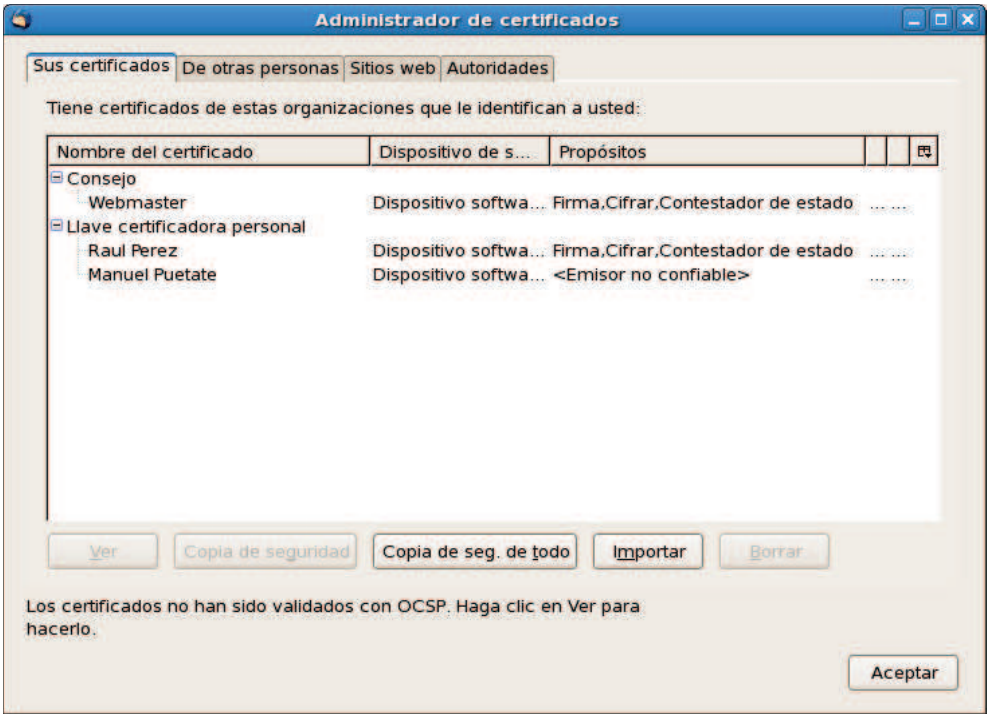


Figura 43: Certificados Importados

4.12.7. ENVÍO Y RECEPCIÓN DE MENSAJES FIRMADOS Y CIFRADOS

Luego de instalar e importar correctamente los componentes y los certificados estan listos para ser usados para el correo electronico seguro con S/MIME.

En el cliente de correo configuramos las cuentas de usuarios con su respectivo certificado digitales.

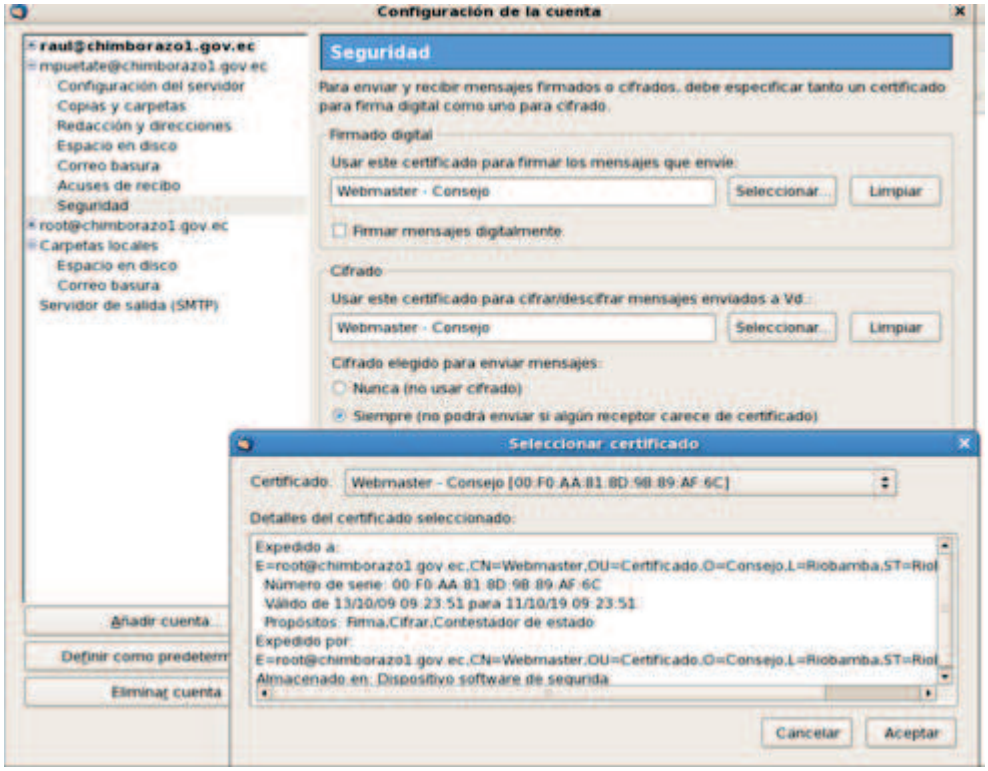


Figura 44: Seguridades en cuentas de usuarios

Cuando los certificados aun no han sido incluidos en el cliente de correo para un usuario determinado no se va a poder leer el mensaje o no se puede enviar mensajes con firma digital y cifrados.

4.13. DEMOSTRACIÓN DE LA HIPÓTESIS.

Hasta el momento se ha desarrollado un marco teórico sobre lo que implica la utilización de protocolos seguros en las cominicaciones en el servicio de correo electrónico como medio de mejoramiento de la privacidad de la información en los mensajes.

En este apartado se realizó la comprobación de la hipótesis: "*La aplicación de protocolos seguros en el servicio de correo electrónico permitirá implementar un sistema con mejor privacidad en la información*", para lo cual se realizo prubas con un sistema de correo tradicional y con un sistema de correo que haga uso de protocolos seguros, basado en esto se llego a determinar el nivel de aseveración alcanzado al plantear la hipótesis en este trabajo de investigación.

4.13.1. SISTEMA DE CORREO TRADICIONAL VS CORREO SEGURO

Tanto en el correo tradicional como en el correo seguro se llevan a cabo pruebas como son: confidencialidad, integridad, autenticación en la gestión de la información en los mensajes a continuación se detallan los datos obtenidos en ambos sistemas en las pruebas mencionadas.

4.13.2. PRUEBA DE CONFIDENCIALIDAD

Para realizar esta prueba capturamos datos con la herramienta wireshark

a. Correo tradicional.

El correo electrónico en Internet basado en SMTP no protege los mensajes. Un mensaje de correo electrónico SMTP en Internet puede ser leído por cualquiera que lo vea mientras viaja o que lo vea donde está almacenado.

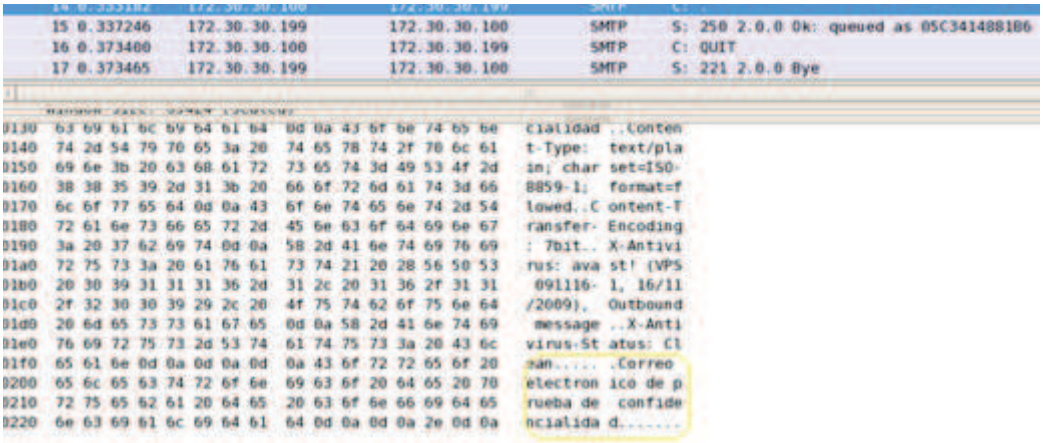


Figura 45: Prueba confidencialidad sistema tradicional

b. Correo seguro.

El cifrado de mensajes protege el contenido de un mensaje de correo electrónico. Sólo el destinatario al que va dirigido el mensaje puede ver el contenido, y el contenido sigue siendo confidencial y no puede conocerlo nadie más que quien pueda recibir o ver el mensaje.

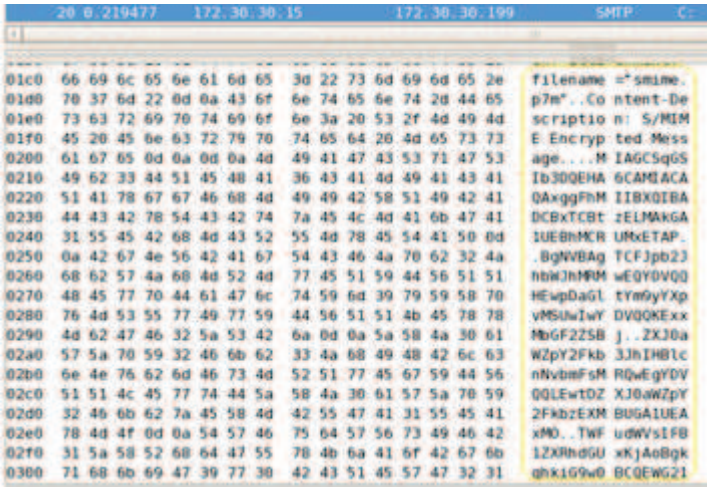


Figura 46: Prueba confidencialidad correo seguro

4.13.3. PRUEBA DE INTEGRIDAD

Para realizar esta prueba capturamos datos con la herramienta wireshark

a. Correo tradicional.

Utilizando un correo tradicional no podemos encriptar y firmar digitalmente un mensaje lo cual reduce notablemente el nivel de integridad, por que los datos pueden ser leídos o capturados mientras transita por la red.

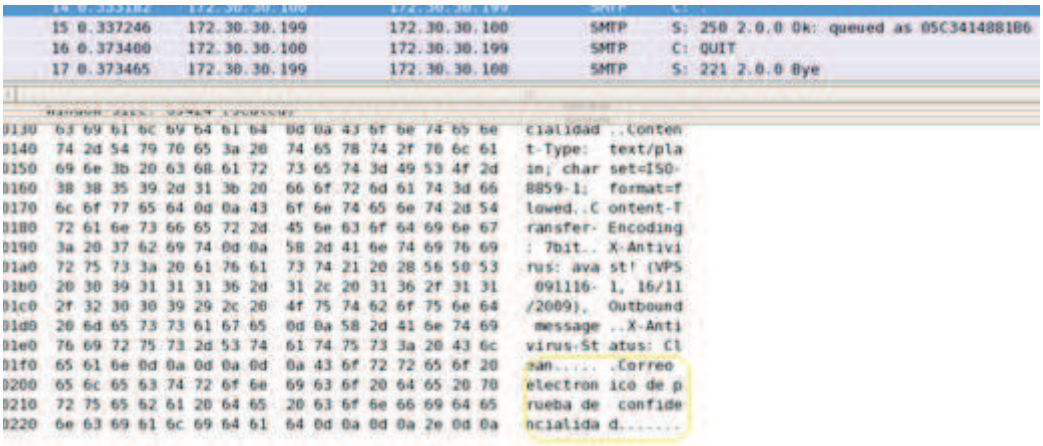


Figura 47: Prueba integridad sistema tradicional

b. Correo seguro.

La integridad de los datos es uno de los resultados de las operaciones que hacen posibles las firmas digitales, un mensaje no puede ser leído si no se valida una firma.

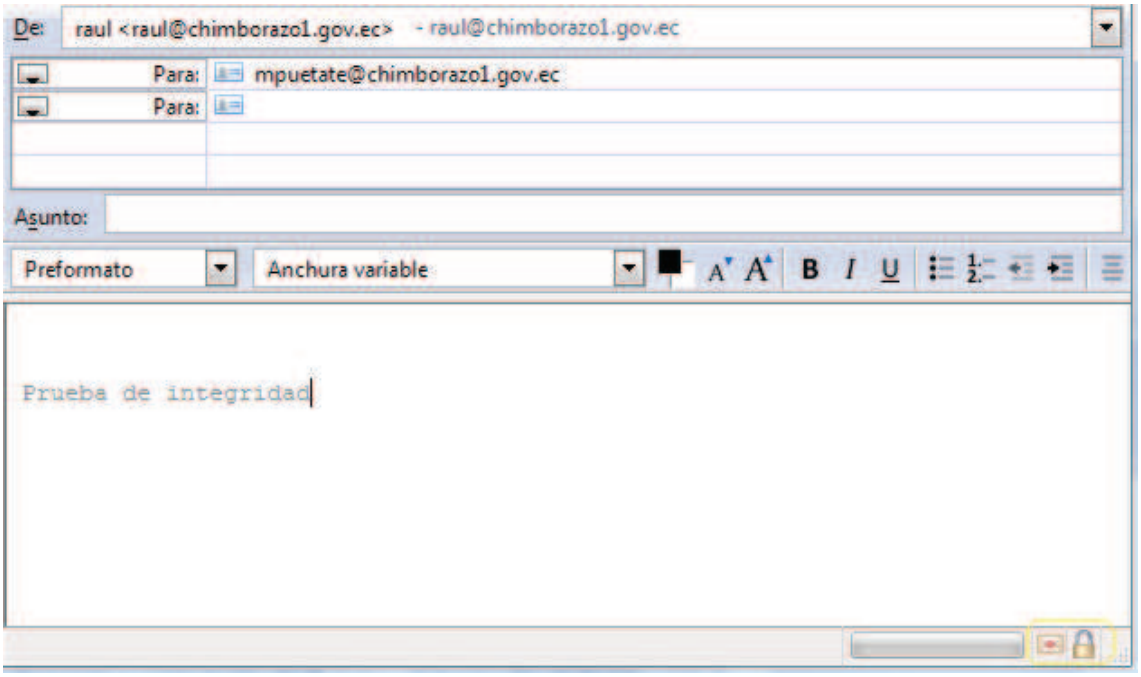


Figura 48: Prueba integridad correo seguro

4.13.4. PRUEBA DE AUTENTICACIÓN

Para la comprobación de la Autenticación redactamos un mensaje y verificamos si el mensaje que le llega al destinatario es realmente del remitente quien dice ser.

a. Correo tradicional.

Enviamos este mensaje de correo electrónico.

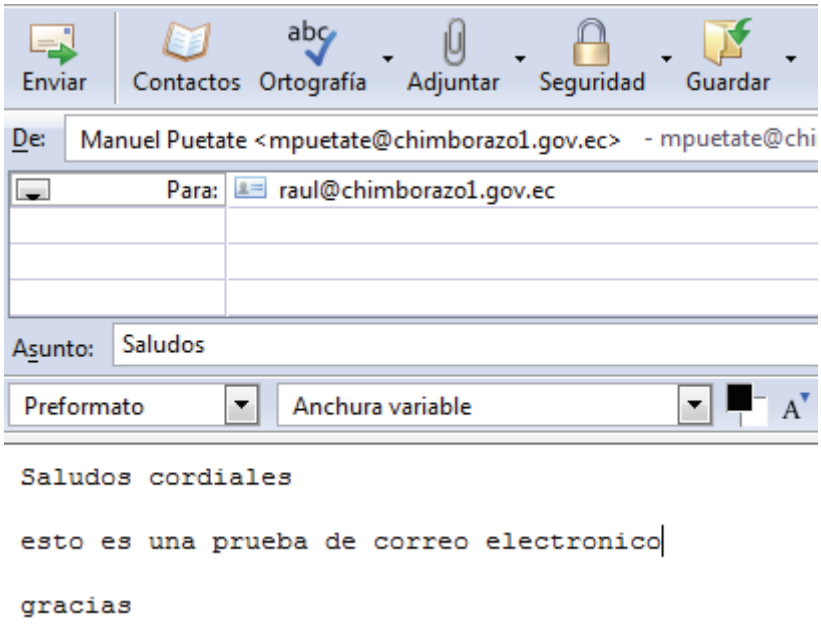


Figura 49: Prueba autenticación sistema tradicional

El mensaje llega pero no podemos comprobar si la entidad del remitente es realmente quien dice ser, como no existe autenticación en el correo electrónico SMTP, no hay ninguna forma de saber quién envió realmente un mensaje.

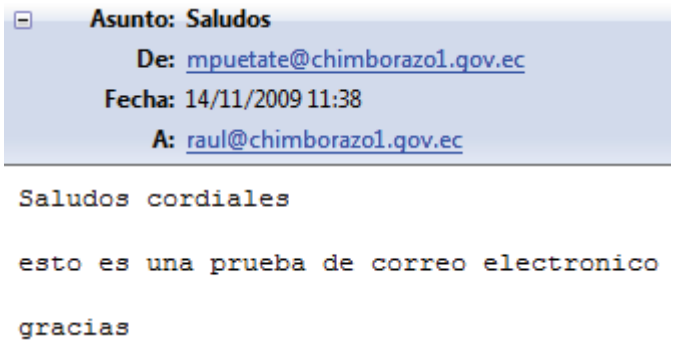


Figura 50: Prueba 2 integridad sistema tradicional

b. Correo seguro.

Configuramos la cuenta de correo seleccionando el certificado digital individual para firmar digitalmente un mensaje.

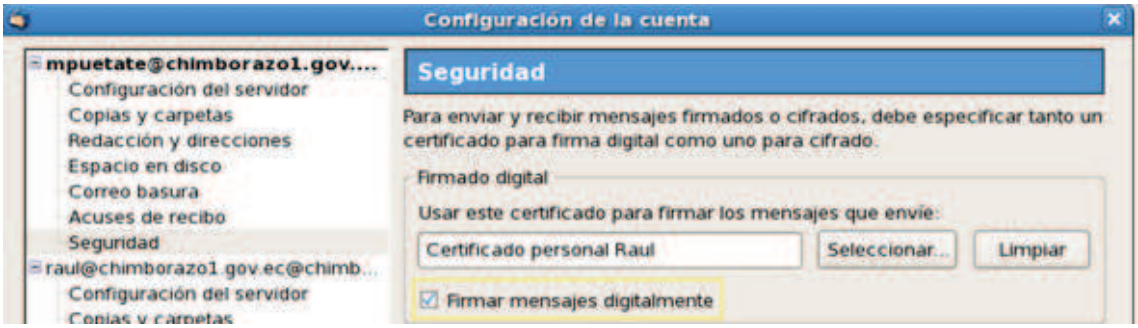


Figura 51: Demostración autenticación correo seguro

La autenticación en una firma digital resuelve este problema al permitir que un destinatario sepa que un mensaje fue enviado por la persona o la organización que dice haber enviado el mensaje.

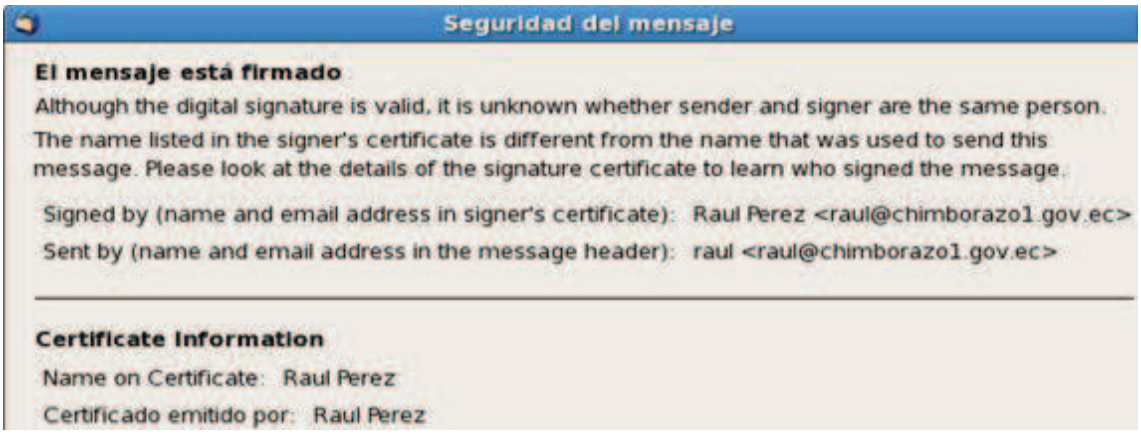


Figura 52: Demostración 2 de autenticación

4.13.5. RESULTADO DE PRUEBAS

- El correo electrónico tradicional no puede garantizar mucho su confidencialidad por el hecho de no tener mecanismos para hacerlo, un sistema de correo con S/MIME resuelve este problema utilizando encriptación de los datos
- La integridad de los datos es otro aspecto que debe ser tomado en cuenta, un sistema de correo tradicional no encripta y firma los mensajes, S/MIME resuelve

este problema utilizando certificados digitales para firmar y cifrar la información.

- El sistema de correo tradicional no posee mecanismos de autenticación para saber que el remitente es realmente quien dice ser, con S/MIME se trata de resolver este problema utilizando certificados digitales para firmar los mensajes y de esta manera comprobar su identidad.
- Al culminar estas pruebas que nos permite verificar el nivel de seguridad de cada sistema se concluye que con un sistema de correo seguro mejora significativamente la *privacidad de la información*, se puede decir que aumentaríamos en un porcentaje considerable y de esta manera queda demostrada la hipótesis planteada en este proyecto de investigación.

CAPÍTULO V

IMPLEMENTACIÓN DE LA INTERFAZ WEBMAIL PERSONALIZADA PARA H.C.P.CH

5.1. INTRODUCCIÓN

En este capítulo detallaremos los pasos necesarios para la instalación y personalización de un Webmail para el acceso de los usuarios de correo electrónico a sus cuentas personales permitiéndoles de esta manera el envió y recepción de mensajes vía web.

Usando exclusivamente software libre para este caso utilizamos squirrelmail por lo que es una de los webmails más utilizados y fácil de instalación y configuración, realizamos las respectivas configuraciones para conectarlo a nuestro servidor de correo electrónico explicado en el capitulo anterior.

Para la administracion de cuentas de usuarios implemantamos una aplicación web que me va a permitir la creacion de cuentas de usuarios utilizando el internet.

Tambien configuramos el cliente de correo Thunderbird para accesar al correo de manera local.

5.2. CLIENTES DE CORREO ELECTRÓNICO

Los clientes de correo electrónico son los agentes de usuario de correo (MUA). Son los elementos que relacionan los usuarios con sus buzones, y les permite llevar a cabo la descarga de mensajes de correo usando los protocolos POP3 e IMAP, así como escribir nuevos mensajes, organizarlos en carpetas, mantener una libreta de direcciones, etc.

5.3. TIPOS DE CLIENTES DE CORREO

Podemos distinguir tres tipos de clientes de correo según la forma de acceder a ellos:

5.3.1. INSTALADOS EN UN PC

Se ejecutan directamente desde un computador personal lo mas comun es que vengan instalados con un sistema operativo, acceden a su correo electronico de manera local mediante el protocolo pop y utilizan smtp para enviar mensajes.

Tenemos clientes por ejemplo para windows (Outlook) en linux(evolution, kmail, thunderbird, etc);

5.3.2. SERVICIO DE CORREO ELECTRÓNICO VÍA WEB (WEBMAIL)

Una segunda opción para el correo electrónico es el uso de cuentas de correo basadas en Web. Esto te permitirá utilizar el explorador web para chequear tu correo. Desde que el correo de estas cuentas normalmente es almacenado en el servidor de correo web –no en tu computadora – es más conveniente utilizar estos servicios desde varias computadoras. Es posible que tu proveedor de servicios de internet (ISP) te permita acceder a tu correo electrónico a través de POP o vía Web.

Sin embargo, deberás recordar que las páginas web son almacenadas de manera temporal o local en computadoras locales. Si chequeas tu correo a través de un sistema basado en web en una máquina que no sea la tuya, existe la posibilidad de que tus correos puedan ser consultados por otros que utilicen la misma computadora.

Las cuentas de correo basadas en web puedes obtenerlas de manera fácil y gratuita. Esto significa que te brindan la oportunidad de tener varias identidades en línea. Tú puedes, por ejemplo, tener una dirección de correo electrónico exclusivamente para tus amigos, y otra para tus familiares. Esto es considerado como aceptable, mientras no pretendas defraudar a alguien.

Características:

Posee un sistema de ayuda

Interfaz sencilla

Permite adjuntar archivos

Permite organizar los mensajes en carpetas

El usuario puede establecer sus preferencias

Cada usuario tiene su propia libreta de direcciones

Tiene una limitación de espacio para los mensajes y una de tamaño para los datos adjuntos.

No usa ninguna aplicación intermedia.

Permite el reenvío automático de mensajes.

Las carpetas se almacenan en el propio servidor.

Ejemplos: Squirremail, Neomail, Hotmail, Yahoo, Gmail, Horde, etc.

5.3.3. RESIDENTES EN EL SERVIDOR

Hace falta conectarse al servidor mediante terminal remota usando, bien conexión encriptada (ssh, que es la opción preferida) Una vez abierta la terminal remota del servidor, se ejecuta alguno de los clientes de correo instalados en él, normalmente pine.

5.4. GUÍA PARA LA IMPLEMENTACIÓN DEL WEBMAIL.

Implementacion del modulo de administracion del correo

Instalacion de squirrelmail

Instalacion de plug-in

Personalizacion del webmail

Configuración de un cliente de correo (thunderbird)

5.4.1. IMPLEMENTACIÓN DEL MODULO DE ADMINISTRACIÓN DEL CORREO

En este modulo creamos una aplicación web que permite al administrador del sistema la creacion de cuentas de correo electronico como tambien cambiar las contraseñas en caso que algun usuario lo requiera y no pueda acceder.

5.4.1.1. **Pantalla de ingreso.**

Como todo sistema de gestion de usuarios el ingreso debe estar controlado mediante un login y su password por lo que esta tarea solo se le asigna a una persona con permisos.

Figura 53: Pantalla de Ingreso

5.4.1.2. **Pantalla del menú principal.**

En la pantalla pricipal del administrador se encuentra el menu que le permite crear las cuentas de correo, cambiar claves y cerrar la sesion del administrador.

Figura 54: Menú Principal

5.4.1.3. **Pantalla crear cuentas de usuarios.**

Desde esta interfaz podemos crear cuentas de usuario que van a poder hacer uso de nuestro sistema de correo electronico, para lo cual se pide el ingreso de datos personales del usuario y se le asigna un nombre de usuario y clave que luego puede ser cambiado por el usuario.

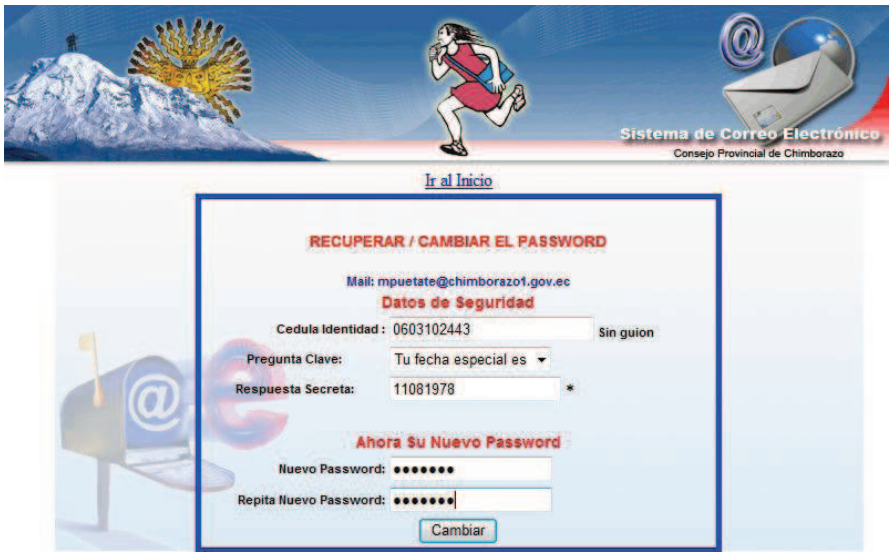


Figura 55: Crear Cuentas de usuarios

5.4.1.4. **Pantalla de cambio de password.**

En esta pantalla podemos cambiar el password de un usuario que por alguna circunstancia olvido o simplemente no puede acceder a su correo.

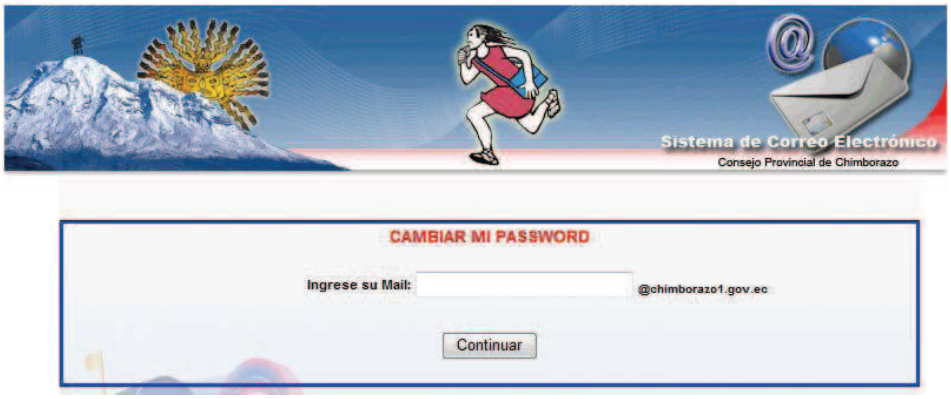


Figura 56: Pantalla de cambio de password

Si la clave a podido ser cambiada no emite un mensaje de que el password a sido cambiado satisfactoriamente.

Figura 57: Confirmación de cambio password

5.4.2. INSTALACIÓN Y CONFIGURACIÓN DE SQUIRRELMAIL

SquirrelMail es un interesante, extensible, funcional y robusto software para correo y que permite acceder al usuario a su correo electrónico desde el navegador de su predilección.

SquirrelMail está escrito en PHP4 y cumple con los estándares como correo a través de interfaz HTTP. Incluye su propio soporte para los protocolos IMAP y SMTP. Además todos las página se muestran con HTML 4.0 sin la necesidad de JavaScript para una máxima compatibilidad con cualquier navegador.

SquirrelMail incluye toda la funcionalidad deseada para un cliente de correo como un robusto soporte MIME, libreta de direcciones y administración de carpetas.

5.4.2.1. **Instalación del software requerido.**

```
yum -y install squirrelmail httpd
```

5.4.2.2. **Configuración de SquirrelMail.**

Cambie al directorio /usr/share/squirrelmail/config/ y ejecute el guión de configuración que se encuentra en el interior:

```
cd /usr/share/squirrelmail/config/

./conf.pl
```

Lo anterior le devolverá una interfaz de texto muy simple de utilizar, como la mostrada a continuación:

```
--------------------------------------------------------
SquirrelMail Configuration : Read: config.php (1.4.3)
--------------------------------------------------------
Main Menu --
1.  Organization Preferences
2.  Server Settings
3.  Folder Defaults
4.  General Options
5.  Themes
6.  Address Books (LDAP)
7.  Message of the Day (MOTD)
8.  Plugins
9.  Database


D.  Set pre-defined settings for specific IMAP servers

C.  Turn color on
S   Save data
Q   Quit

Command >>
--------------------------------------------------------
```

Figura 58: Configuración de Squirrelmail

Ingrese hacia las preferencias de la organización y defina el nombre de la empresa, el logotipo y sus dimensiones, El mensaje en la barra de título de la ventana del navegador, el idioma a utilizar, URL y el título de la página principal del servidor de red.

```
--------------------------------------------------------
SquirrelMail Configuration : Read: config.php (1.4.3)
--------------------------------------------------------
Organization Preferences
1.  Organization Name      : Consejo Provincial de
Chimborazo
2.  Organization Logo      : ../images/sm_logo.png
3.  Org. Logo Width/Height : (900/134)
4.  Organization Title     : Consejo Provincial de
Chimborazo
5.  Signout Page           :
6.  Default Language       : es_ES
7.  Top Frame              : _top
8.  Provider link          : http://www.chimborazo.gov.ec/
9.  Provider name          : Consejo Provincial de
Chimborazo

R   Return to Main Menu
C.  Turn color on
S   Save data
Q   Quit
Command >>
--------------------------------------------------------
```

Figura 59: Datos Principales de configuración squirrelmail

En las opciones de servidores defina solamente el dominio a utilizar. Si el servidor de correo va a coexistir en el mismo sistema con el servidor HTTP, no hará falta modificar más en esta sección. Si lo desea, puede especificar otro servidor SMTP e IMAP localizados en otro equipo.

```
--------------------------------------------------------
SquirrelMail Configuration : Read: config.php (1.4.3)
--------------------------------------------------------
Server Settings

General
-------
1.  Domain                 : Chimborazo.gov.ec
2.  Invert Time            : false
3.  Sendmail or SMTP       : SMTP

A.  Update IMAP Settings   : localhost:143 (courier)
B.  Change Sendmail Config : smtp:25

R   Return to Main Menu
C.  Turn color on
S   Save data
Q   Quit

Command >>
--------------------------------------------------------
```

Figura 60: Configuraciones del servidor

En las opciones de las carpetas cambie Trash por Papelera, Sent por Enviados y Drafts por Borradores.

```
--------------------------------------------------------
SquirrelMail Configuration : Read: config.php (1.4.3)
--------------------------------------------------------
Folder Defaults
1.  Default Folder Prefix         :
2.  Show Folder Prefix Option     : INBOX.false
3.  Trash Folder                  : INBOX.Papelera
4.  Sent Folder                   : INBOX.Enviados
5.  Drafts Folder                 : INBOX.Borrador
6.  By default, move to trash     : true
7.  By default, move to sent      : true
8.  By default, save as draft     : true
9.  List Special Folders First    : true
10. Show Special Folders Color    : true
11. Auto Expunge                  : true
12. Default Sub. of INBOX         : true
13. Show 'Contain Sub.' Option    : false
14. Default Unseen Notify         : 2
15. Default Unseen Type           : 1
16. Auto Create Special Folders   : true
17. Folder Delete Bypasses Trash  : false
18. Enable /NoSelect folder fix   : false

R   Return to Main Menu
C.  Turn color on
S   Save data
Q   Quit
Command >>
--------------------------------------------------------
```

Figura 61: Configuraciones de Carpetas

Finalmente escoja y habilite las extensiones (plug-ins) que considere apropiados para sus necesidades:

```
--------------------------------------------------------
SquirrelMail Configuration : Read: config.php (1.4.3)
--------------------------------------------------------
Plugins
  Installed Plugins
    1. delete_move_next
    2. squirrelspell
    3. newmail
    4. calendar
    5. filters
    6. mail_fetch
    7. translate
    8. abook_take
    9. message_details
    10. sent_subfolders
    11. s/mime

  Available Plugins:
    12. bug_report
    13. info
    14. listcommands
    15. spamcop
    16. fortune
    17. administrator

R   Return to Main Menu
C.  Turn color on
S   Save data
Q   Quit

Command >>
--------------------------------------------------------
```

Figura 62: Configuración de Plugins

Guarde los cambios pulsando la tecla «S» y luego la tecla «Enter».

5.4.3. PERSONALIZACIÓN DEL WEBMAIL

5.4.3.1. **Diseño de interfaz principal.**

Esta interfaz esta diseñada para que los usuarios que fueron creados por el administrador puedan ingresar mediante su clave y su password acceder a los buzones de correo electronico.

Esta diseñada de acuerdo a la personalizacion sugerida por el administrador del sistema del correo.

Figura 63: Pantalla de ingreso

5.4.3.2. **Pantalla de Buzón de correo**

En esta pantalla el usuario luego de logearse puede acceder a sus correos para leer su informacion, puede seleccionar de el munu principal, los correos que se encuentran en su bandeja de entrada , borrador, enviados y papeleria.

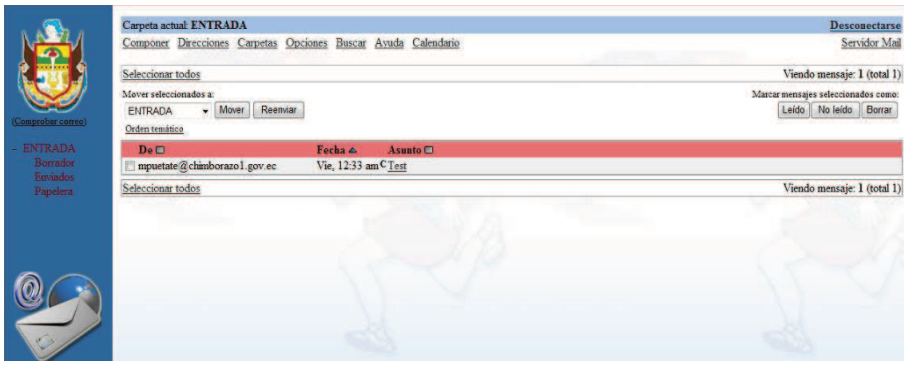


Figura 64: Buzón de correo

5.4.3.3. **Pantalla de Redactar un mensaje.**

En esta interfaz podemos compoder un nuevo mensaje de correo electronico.

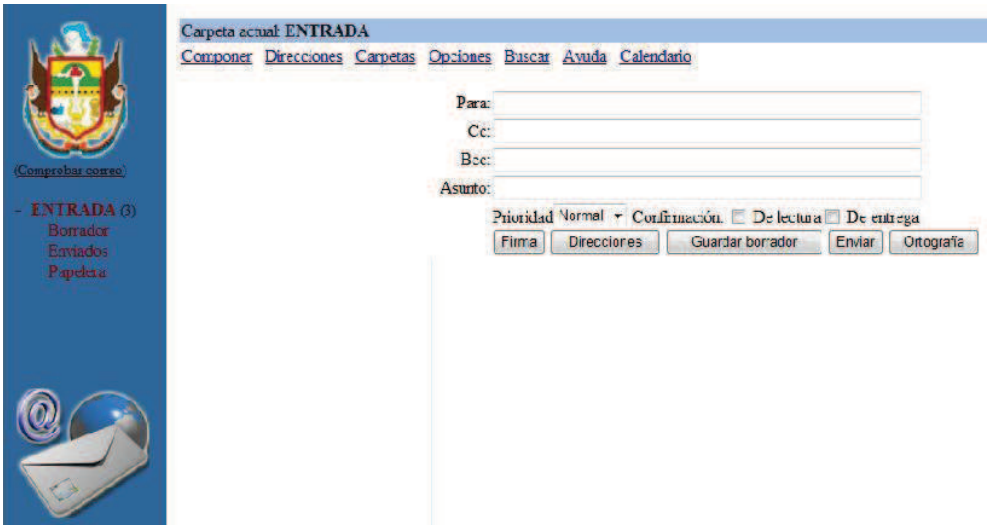


Figura 65: Redactar un mensaje

5.4.3.4. **Pantalla créditos.**

En esta interfaz hacemos referencia aspectos tecnicos, como son quien desarrollo la personalizacion del sistema y el apoyo de los técnicos para poder cumpliri con este objetivo.

Figura 66: Pantalla de créditos

5.4.3.5. **Desconectarse del sistema.**

Luego de haber realizado todas las tareas en nuestro sistema de correo electronico cerramos la sesion con el sistema.

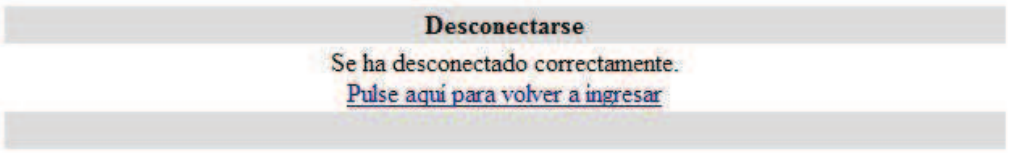


Figura 67: Desconectarse del sistema

CONCLUSIONES

- Conforme la presencia de Internet y sus servicios se vuelve más preponderante en nuestras vidas, hemos visto como se incrementa su mal uso, sobre todo del correo-e. Por lo que resulta importante contar con mecanismos para asegurar que la información que se transmita sobre Internet y otras redes sea altamente confiable.
- En el estudio comparativo entre los protocolos de correo seguro PGP/MIME y S/MIME se obtuvo resultados de un 65%(Muy Bueno) y 90%(Excelente) respectivamente lo cual se determina como la opción para utilizar en un sistema de correo a S/MIME.
- Al configurar la infraestructura de correo seguro se comprobó que la privacidad de la información aumenta considerablemente debido a que se utiliza mecanismos en los que podemos verificar su confidencialidad, integridad, autenticación mediante firma digital y cifrado de los datos, de esta manera evitando que los mensajes puedan ser manipulados por terceras personas.
- S/MIME es un protocolo que puede ser utilizado en ámbitos empresariales a diferencia de PGP/MIME es un protocolo que se desempeña en ámbitos para usuarios locales o pocos usuarios.
- Con la personalización del sistema Webmail es otra alternativa para que los usuarios de correo electrónico del HCPCH puedan acceder a sus cuentas de vía web.

RECOMENDACIONES

- Analizar la infraestructura y sistemas informáticos existentes antes de decidir la utilización de un determinado protocolo para seguridades, ya que a pesar de ser uno mejor que otro simplemente no se pueden utilizar en un entorno dado.
- Realizar un estudio adecuado donde desee implementar un servicio de correo electrónico seguro, por el hecho que tener a los usuarios certificados mediante una CA comercial tiene considerables costos económicos lo que no puede ser asumidos por pequeñas instituciones de bajos recursos económicos.
- Utilizar software libre para la implementación de sistemas informáticos, haciendo uso de herramientas libres podemos crear nuestra CA para los certificados digitales de los usuarios.
- Designar un servidor únicamente para el servicio de correo electrónico para la Institución por lo que son varios sistemas los que tienen que interactuar entre sí para que no colapse y caiga el sistema.
- Incentivar a los usuarios del correo electrónico para que utilicen un sistema seguro, aun que requiere un poco mas de trabajo en su configuración pero es un esfuerzo valedero porque su información puede ser interceptada y manipulada lo que afectaría gravemente a la Institución.
- Para la administración del sistema de correo electrónico es importante que la persona designada para su gestión esté empapada de conocimientos sobre el servicio, ya que los cambios en sus configuraciones pueden afectar todo el sistema.

RESUMEN

El objetivo de esta Tesis fue seleccionar, mediante un estudio entre PGP/MIME y S/MIME, el protocolo más adecuado para la configuración de un Sistema de servicio de correo electrónico seguro para la Unidad de Sistemas Informáticos del Honorable Consejo Provincial de Chimborazo.

La investigación se basó en el Método Científico; y, en el proceso se utilizó Apache (Servidor Web), Mysql (Servidor Base de Datos), PHP (Lenguaje de Programación), Cyrus-sasl (Recolección de correo interno), Postfix(Agente de Transporte de correo), Courier-Imap (Autentificación POP/IMAP), Thunderbird (Cliente de correo) , Squirrelmail (Webmail) y Linux (Sistema Operativo).

Como resultado del estudio comparativo se obtuvo un porcentaje final del **90%**(Excelente) para el protocolo S/MIME, **65%**(Muy Bueno) para el protocolo PGP/MIME, esto determinó como protocolo más apropiado a S/MIME; con la configuración de la infraestructura utilizando protocolo seguro se logro incrementar la privacidad de los mensajes mediante el uso de firmas digitales y cifrado de los datos, la gestión de correo es simple y más segura

Se concluye que es posible implementar una infraestructura del servicio de correo electrónico seguro bajo plataforma LINUX desarrollado con Software libre, minimizando el costo de implementación y mantenimiento para cualquier organización.

SUMMARY

To select more adequate and safe service between PGP/MIME and S/MIME to configure an email system for the Informatic System Unit at the Honorable Consejo Provincial of Chimborazo, was the objective if this research thesis.

The investigation was based on the Scientific Method; Apache was used during the process (Web Server), Mysql (Data Base Server), PHP (Program Language) Cyrus-sasl (Collecting of inter-office mail), Postfix (Agent of mail transport) Courier-Imap (Authentication POP/IMAP), Thunderbird (Mail Customer), Squirrelmail (Webmail), and Linux (Operative System)

As a result of the comparative study, the final percentage was 90% (excellent) for S/MIME protocol, 65% (Very Good) for PGP/MIME, determining to S/MIME as the more adequate protocol; with the configuration of the infrastructure by using a safe protocol, privacy of messages by means of digital signatures and data encoding were increased, therefore the management of mailing is simple and safe.

It is concluded that to implement an email service infrastructure under LINUX platform developed with free Software is possible, decreasing cost of implementation and maintenance for any organization.

ANEXOS

MANUAL DE USUARIO

1. INTRODUCCIÓN

Bienvenidos al Manual Usuario del sistema Webmail del Honorable Consejo Provincial de Chimborazo se describirán el funcionamiento de la aplicación, el cual proporcionara a los usuarios facilidad para acceder a sus cuentas de correo personales en cualquier lugar que exista acceso a internet.

Entre las opciones constará lo siguiente:

- ✓ Creación de cuentas de usuario por el administrador del sistema.
- ✓ Gestión del correo por los usuarios.

La presente aplicación de correo Webmail está destinado a los empleados y funcionarios del **HCPCH**, para que tengan mayor accesibilidad y poder comunicarse de una manera más rápida y efectiva. El administrador del servidor de correo electrónico podrá crear cuentas personales, para lo cual utilizara la información básica personal.

2. GENERALIDADES DEL SISTEMA

2.1. DEFINICIONES

HCPCH: Honorable Consejo Provincial de Chimborazo

USI: Unidad de Sistemas Informáticos

Webmail: Interfaz de correo Web

2.2. Requisitos

2.2.1. Requisito Hardware

- ✓ Memoria: 64 MB o superior, 128 MB
- ✓ Un puerto RJ-45
- ✓ Monitor
- ✓ Teclado
- ✓ Mouse

2.2.1. Requisito software

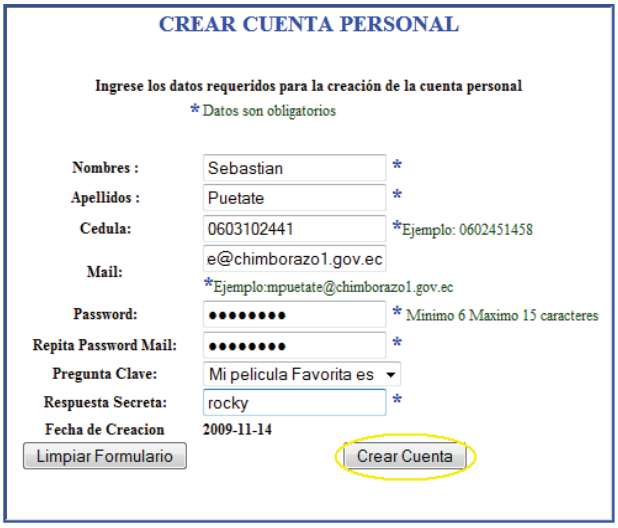
- ✓ Windows 98 SE, Me, 2000 y XP, Vista, Linux.
- ✓ Navegador web.

3. CREACIÓN DE CUENTAS DE USUARIO

Para realizar esta actividad debe ser el administrador del servidor de correo para lo cual cuenta con un nombre de usuario respectivamente que son encriptados para no ser interpretados sus datos.

Luego presionamos el botón Ingresar y nos muestra la siguiente pantalla de administración de las cuentas de los usuarios.

Del menú de la parte izquierda seleccionamos la tarea a realizar, presionaos el botón Cuentas Personales.



Ingresamos los datos correspondientes de un usuario determinado asignándole su Mail y su password, presionamos Crear Cuenta.

Y la cuenta de correo electrónico solicitada al administrador se a creado correctamente.

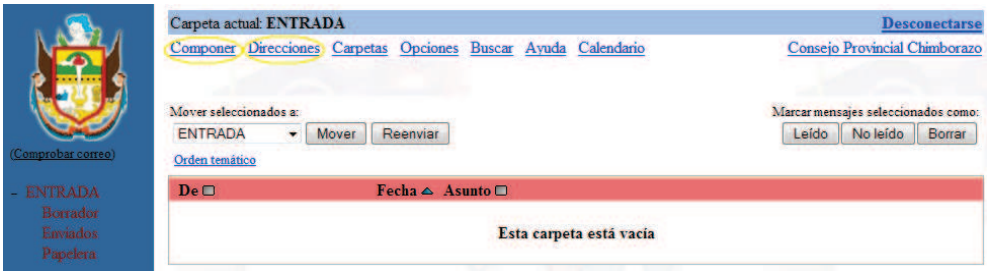
Si elegimos la opción Cambiar Clave nos desplego la siguiente pantalla.

Ingresamos los datos del usuario que desee cambiar su password por diversas razones que puede existir.

4. GESTIÓN DE CUENTAS DE USUARIO

Para ingresar a nuestra cuenta de correo personal digitamos en el browser la dirección de nuestro servidor de correo.

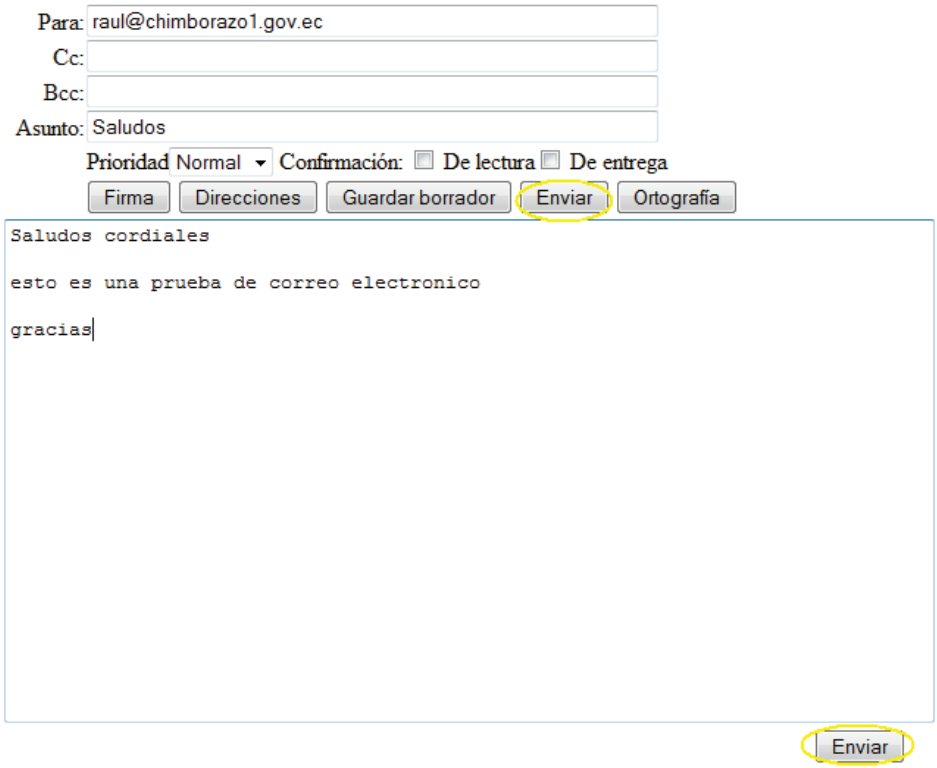
Pulsamos el botón Ingresar y estamos dentro de nuestras cuentas de correo.



Donde podemos escoger la opción de deseo ejecutar del menú parte superior, podemos añadir direcciones de un contacto a quien deseo enviar un correo.

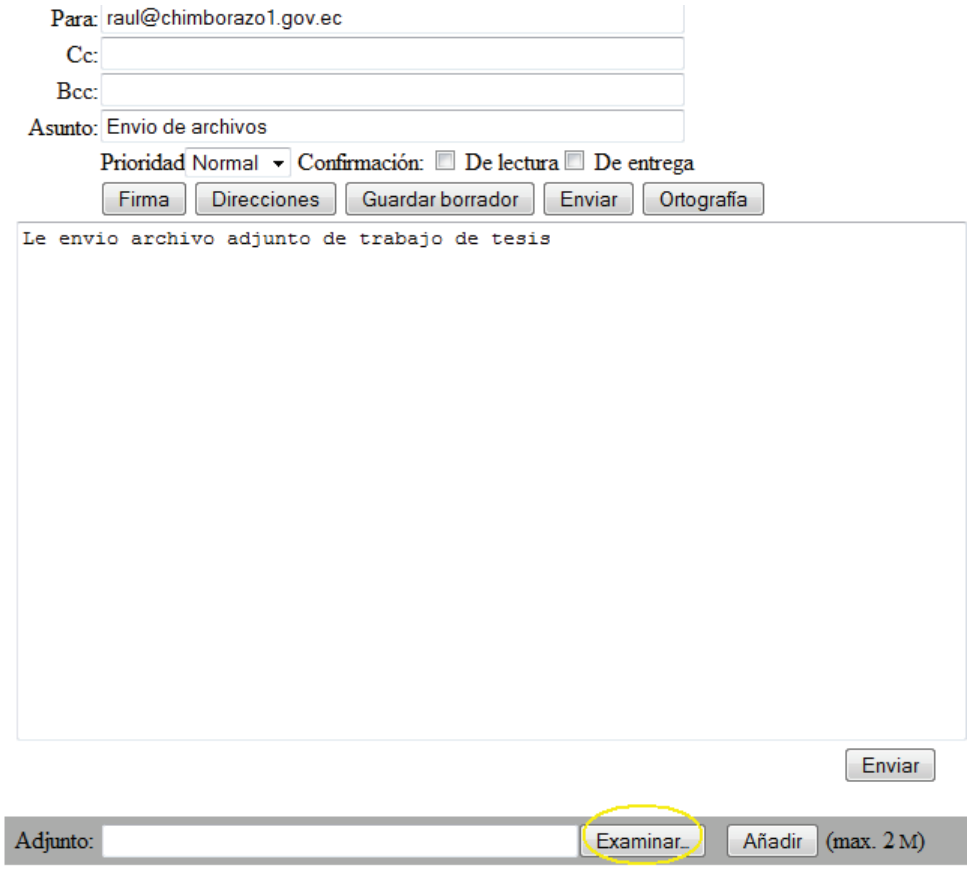
Presionamos el botón añadir dirección y esta adjuntado el contacto a nuestra lista.

Para redactar un correo seleccionamos la opción Componer y podemos enviar un correo.

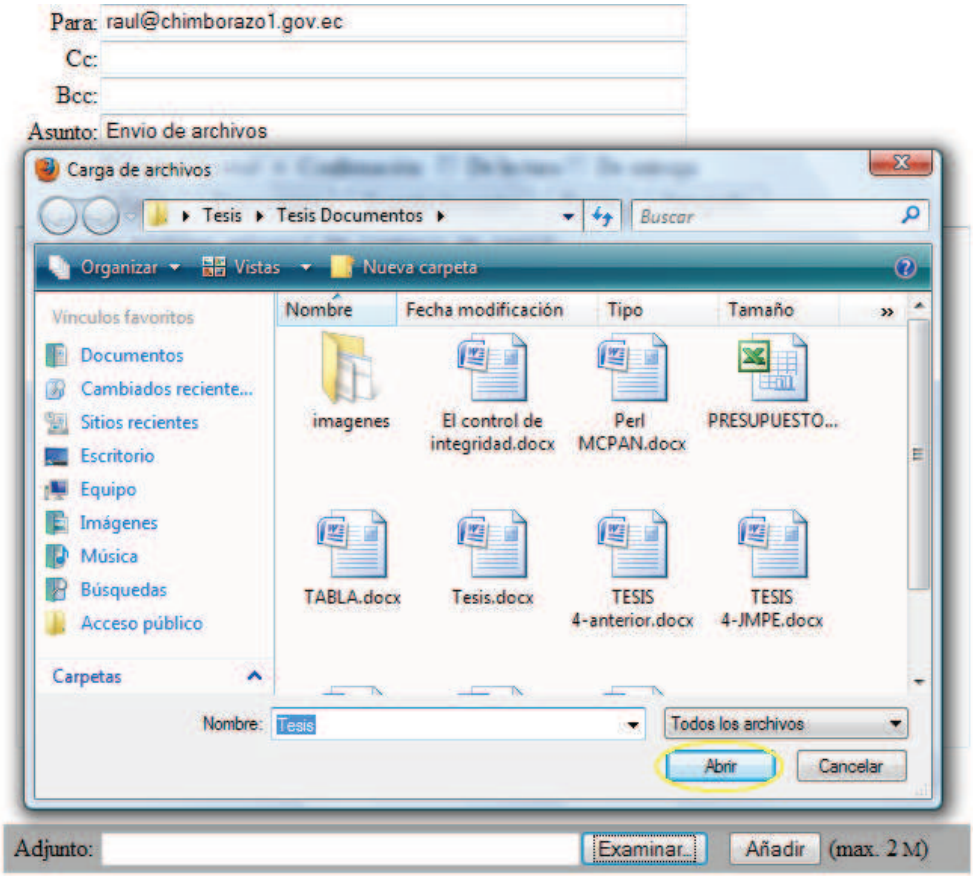


Al presionar el botón Enviar tanto de la parte superior como de la parte inferíos podemos enviar nuestro mensaje de correo.

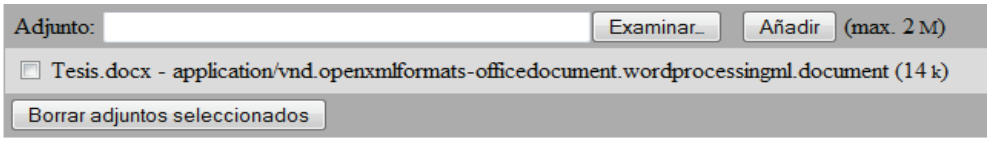
Además dentro de la opción componer un mensaje podemos adjuntar uno o varios archivos siempre y cuando no exceda el tamaño máximo permitido para poder enviar los datos.



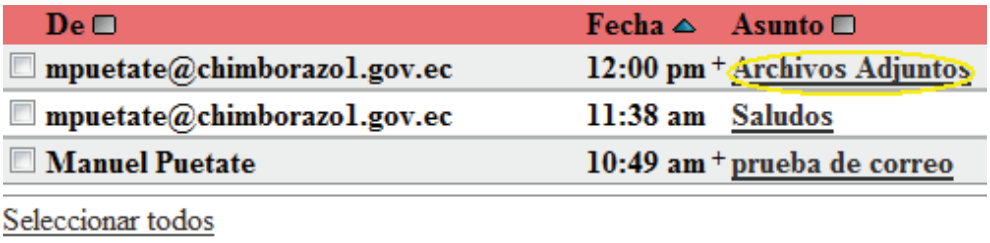
Presionamos el botón examinar para seleccionar los archivos que vamos adjuntar en el mensaje.

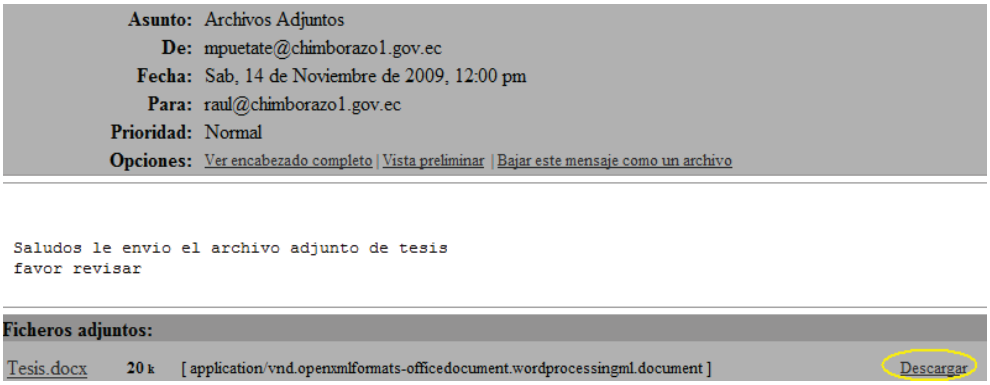


Presionamos el botón abrir para seleccionar el archivo, luego de esto nuestro archivo esta adjuntado y lo podemos enviar.

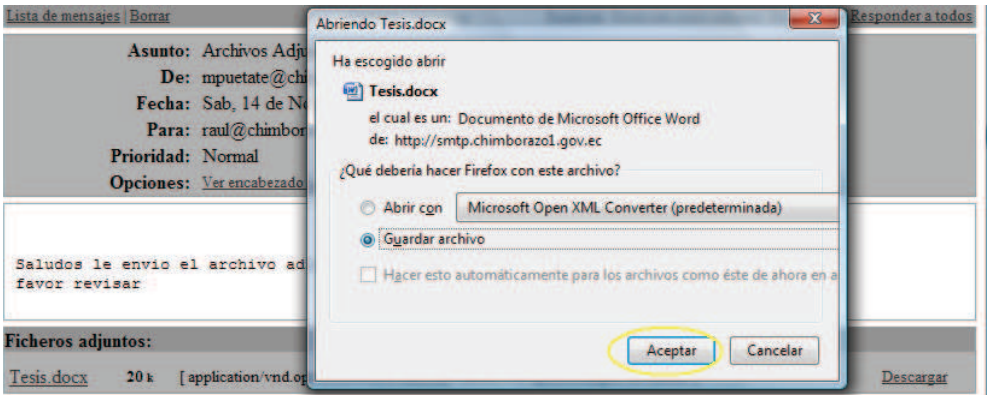


Al revisar nuestra cuenta encontramos al mensaje y procedemos a leer.





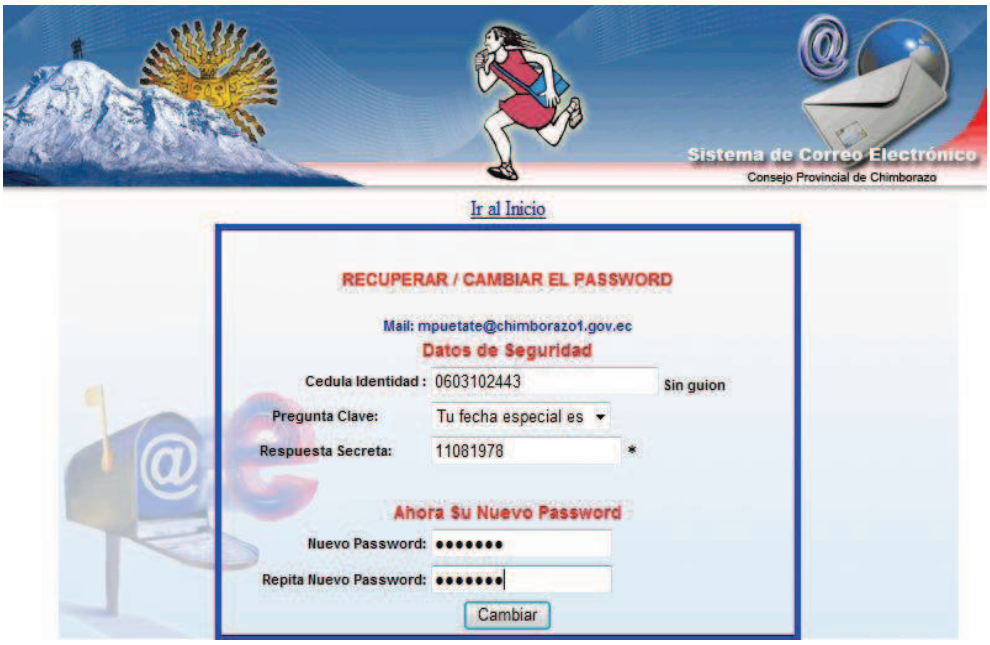
Presionamos el botón Descargar para bajar el archivo adjunto en el mensaje



Seleccionamos la opción que se desee realizar, abrir el archivo o guardarlo en una rata determinada.

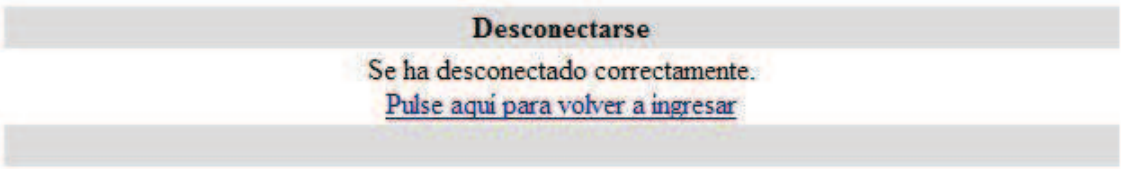
Existe también la posibilidad de que un usuario de correo pueda cambiar su clave luego de haber sido creada por el administrador de esta manera su clave será única, para ejecutar esta acción debe acordarse de algunos datos importantes ingresados al momento de crear la cuenta.

Ingresa los datos requeridos y presiona el botón cambiar y nos muestra la pantalla que el password ha sido cambiado.



Podemos también ejecutar la acción créditos donde encontramos información para pedir ayuda o soporte técnico del sistema Webmail

Terminado la gestión de correo nos desconectamos de nuestra cuenta para que la sesión se cancele.



7. RECOMENDACIONES

- El administrador debe solicitar datos verdaderos a los usuarios para la creación de cuentas por que esos datos son importantes para luego modificar los datos de los usuarios.
- Los usuarios de correo electrónico deben tener conocimientos de navegación web para que sea más fácil su gestión de cuestas personales

8. SOPORTE

Si necesita información adicional sobre el sistema comunique con:

Jesús Manuel Puetate Espinoza. Email: mpuetate_1104@hotmail.com

manuelpuetate@yahoo.con

jpuetate@espoch.edu.ec

BIBLIOGRAFÍA

BIBLIOGRAFÍA DE INTERNET

CERTIFICADOS DIGITALES

http://www.openssl.org/docs/apps/CA.pl.html

http://helektron.com/2007/06/06/tutorial-como-crear-una-autoridad-certificadora-ca-con-openssl/

12/08/2009

http://www.thawte.com/es/

https://www.thawte.com/secureemail/personal-email-certificates/index.html

http://www.gwolf.org/files/pki/node1.html

26/08/2009

http://www.scribd.com/doc/4605572/Aplicaciones-Seguras

30/09/200

CORREO ELECTRÓNICO.

http://www.postfix.org

http://courier-mta.org

http://mysql.com

30/09/2009

http://amavis.org

http://clamav.net

http://spamassassin.apache.org/

http://www.openssl.org

02-02-2009

http://documentacion.irontec.com/sistema_correo.pdf

http://www.e-ghost.deusto.es/docs/articulo.postfixmysql.html

23-02-2009

http://www.linuxparatodos.net/portal/staticpages/index.php?page=como-squirrelmail

http://www.filetransit.com/freeware.php?name=Webmail

http://dev.mysql.com/doc/refman/5.0/es/replication.html

16-03-2009

PROTOCOLOS SEGUROS

http://es.kioskea.net/contents/crypto/s-mime.php3

17-11-2008

http://ftp.nluug.nl/crypto/pgp/5.5/docs/spanish/pgp553i-macintosh-spanish.pdf

17-11-2008

http://www.scribd.com/doc/4680062/Seguridad-Informatica-y-Criptografia-Aplicaciones-de-Correo-Seguro

24-11-2008

http://asignaturas.diatel.upm.es/seguridad/email_pem.htm

http://spi1.nisu.org/recop/al01/impulsor/pgp.pdf

www.marknoble.com/tutorial/smime/smime.aspx

http://www.geocities.com/jagtez/EstructDatos/PGP5.html

2-12-2008

http://servidor.acis.org.co/pipermail/segurinfo/2008-August/003566.html

http://blog.s21sec.com/2009/06/firmado-y-cifrado-de-e-mail-con-smime-y.html

16-12-2008