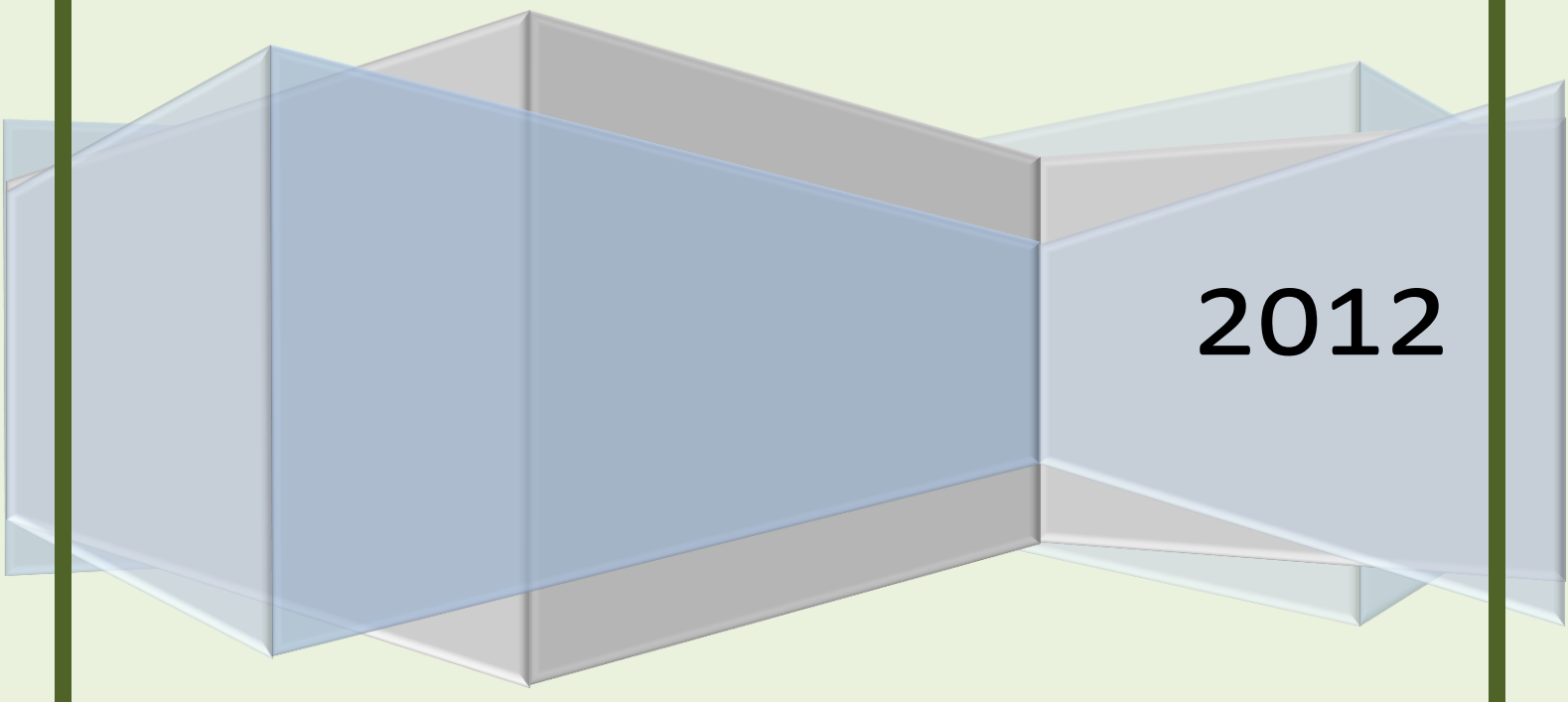
SERVICIOS DE RED E INTERNET

2º ASIR

UD6-CORREO

Vicen



2012

INDICE UD6.- **“Instalación y administración de servicios de correo electrónico”**

•Características del servicio de correo electrónico.

•Elementos del servicio de correo electrónico:

- Agentes de correo electrónico.
- Servidores de correo electrónico. Open Relay y Smart host.
- Clientes de correo electrónico : entornos-DOS, gráficos y navegadores.
- Mensajes de correo.
- Direcciones , cuentas de correo y servidores DNS.
- Protocolos y servicios de descarga de correo: SMTP/ESMTP, POP, IMAP.

•Funcionamiento del servicio de correo electrónico.

•Cuentas de correo, alías y buzones de correo.

•Estructura de los mensajes de correo electrónico.

- Cabecera, Cuerpo, MIME.

•Monitorización y registros del servicio de correo electrónico.

•Servicio de correo electrónico vía web.

•Correo seguro:

- Firma digital y cifrado de mensajes.

•Veracidad del correo:

- Correo basura (“Spam”)fraude, engaño, cadenas y virus informáticos.

UD 6: Instalación y administración de servicios de correo electrónico

•Características del servicio de correo electrónico.

El correo electrónico, también llamado e-mail, es un mensaje, carta o información que se manda de una computadora a otra. Es uno de los servicios que ofrece Internet.

Sus principales características son:

- Es rápido y económico. El envío a cualquier parte del mundo tarda unos segundos en ser recibido, además cuesta lo mismo enviar un mensaje de tres líneas que uno de mil y, el precio es el mismo sin importar el destino.
- Permite trabajar directamente con la información recibida utilizando, por ejemplo, un procesador de textos, una hoja de cálculo o el programa que sea necesario, cosa que no ocurre con el correo tradicional o el fax. Es decir, cualquier mensaje se puede modificar, reutilizar, imprimir, etc.
- Puede enviar o recibir mucha información, ya que se pueden mandar archivos que contengan libros, revistas, datos.
- Es multimedia ya que se pueden incorporar imágenes y sonido a los mensajes.
- Permite enviar mensajes a grupos de personas utilizando las listas de correo.
- No utiliza papel.
- Puede consultarse en cualquier lugar del mundo.
- Es muy fácil de usar.

•Elementos del servicio de correo electrónico:

Desde el punto de vista del usuario, para tener el servicio de correo electrónico basta con tener

1. Una **dirección electrónica** (*e-mail address*) y

2. Un programa **cliente de correo** (como *Pine*, *Eudora*, *Outlook* de Microsoft, *Messenger* de Netscape, etc.) que se puede ejecutar desde algún computador personal que tenga conexión a la red.

Para quien presta el servicio de correo electrónico, el asunto es más complicado, pues debe tener un computador, más potente que un PC y conectado en todo momento a la red, donde se tenga instalado:

1. Un **servidor de correo** (*Sendmail*, *Netscape-Mail*, *Microsoft-Exhange*, etc.) debidamente configurado y

2. Un **servidor para acceder los mensajes de correo** (*POP* ó *IMAP*).

- Agentes de correo electrónico.

MUA El MUA o cliente de correo, es el programa que le va a permitir a un usuario (como mínimo) leer y escribir mensajes de correo electrónico. Típicamente, esto se hace a través de una interfaz que puede ser gráfica (Ximina Evolution, Outlook, Wemail, etc) o en texto (Pine, Mutt, etc). Debe tener funcionalidades de agente de acceso a correo para permitir la recuperación de correo a través de POP ó IMAP y debe tener funcionalidad MIME (Multipurpose Intenet Mail Extensions, Extensiones de Correo de Internet Multipropósito). La funcionalidad MIME es la habilidad para leer o incluir texto no ASCII (texto plano) en el cuerpo de un mensaje. MIME especifica formas de incluir otra clase de documentos incluyendo imágenes y otros archivos binarios. Esta habilidad depende tanto del MUA como de la existencia de otras aplicaciones capaces de entender el formato del archivo y que puedan ser llamadas o cargadas por el MUA para su visualización.

MTA El MTA se encarga de la transferencia de los mensajes de correo electrónico entre las máquinas que usan el protocolo SMTP. Un mensaje puede pasar por varios MTA hasta llegar al destino final. Los MTA escuchan en los puertos 25 y 587. Típicamente se contactan el uno al otro usando el puerto 25. Los agentes de registro usan el puerto 587. A la transferencia de correo electrónico para un cliente se denomina reenvío (o envío). Sendmail es un MTA.

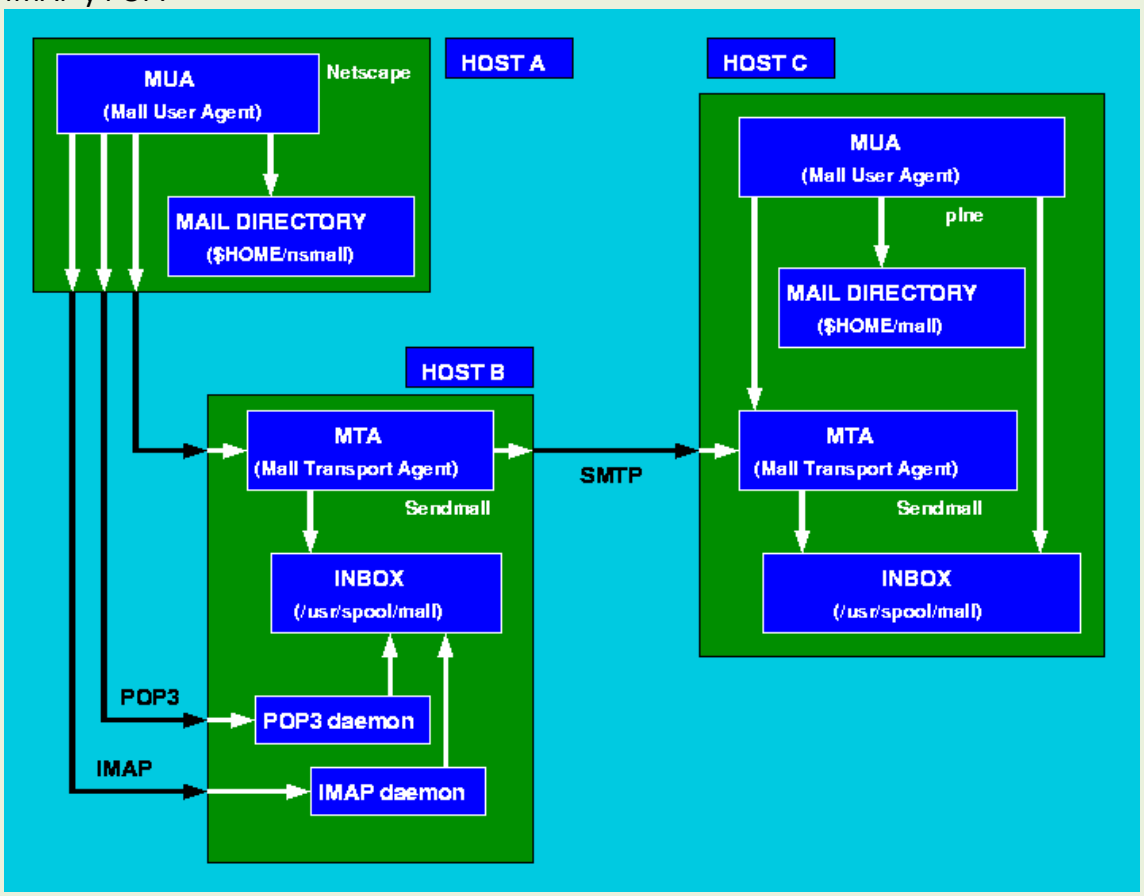
MDA

Los agentes MTA utilizan programas MDA (Mail Delivery Agent, Agente de Entrega de Correo) para entregar el correo electrónico al buzón de un usuario concreto. En muchos casos, el agente MDA es realmente un LDA (Local Delivery Agent, Agente de Entrega Local), como bin/mail o Procmail. Cualquier programa que gestione realmente un mensaje para entregarlo al punto donde lo leerá un agente MUA se puede considerar un agente MDA. Los agentes MDA no transportan mensajes entre sistemas ni actúan como interfaz para el usuario final.

Muchos usuarios no utilizan directamente agentes MDA, porque sólo se necesitan agentes MTA y MUA para enviar y recibir correo. Sin embargo, algunos agentes MDA se pueden utilizar para ordenar los mensajes antes de que los lea el usuario, lo cual es de gran ayuda si recibe una gran cantidad de correo.

MSA El MSA o Agente de Registro de Correo es un agente nuevo que divide la carga de trabajo del MTA en servicios con muchos usuarios y mejora el desempeño. La idea es que el agente de servicio se preocupe de las tareas relativas al direccionamiento, tomando cierta parte de la carga de trabajo del MTA primario. Éste simplemente puede confiar la validez de las direcciones cuando recibe un correo de agentes de registro conocidos. El MSA corrige direcciones, y arregla y reescribe encabezados. Procesa el correo de su propia cola y lo envía a un agente de transferencia local.

MAA El MAA ó Agente de Acceso al Correo es usado para recuperar el buzón de mensajes de un servidor de correo electrónico. Ejemplos de MAAs son el protocolo IMAP y POP.



- Servidores de correo electrónico. Open Relay y Smart host.

Se denomina ataque por Open Relay al mecanismo de usar el MTA (*Mail Transport Agent*, Agente de Transporte de Correo) como puente para correos (usualmente spam, aunque pueden ser muchas otras cosas, como los Hoax) que de otra manera no podrían llegar a destino, gracias a que los servidores bloquearon la dirección IP de origen.

De esta manera, la gente que manda spam de forma indiscriminada se ve obligada a usar otros servidores para esta tarea. Estos servidores que permiten que se envíe correos a través de ellos, se los denomina **Open Relay**.

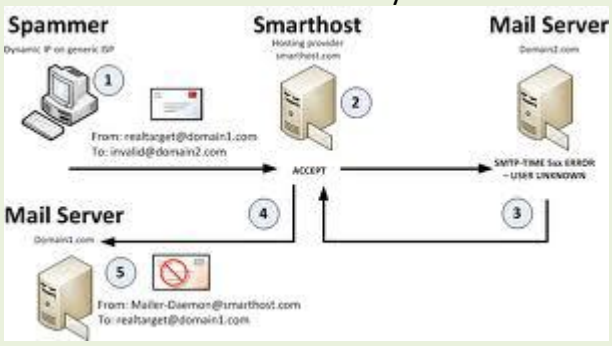
Para solucionar esto (o castigar a la gente que tiene el MTA aceptando este *"puenteo de correos"* para cualquier lugar) se crearon listas negras en tiempo real que bloquean dichos hosts en los cuales se detectó un MTA que hacía **Open Relay**. Y para que se saque una IP de estas listas negras, se deben pasar ciertas pruebas y esperar cierto tiempo.

Hay muchos tipos de servicios que bloquean estas direcciones. Pero los más importantes realizan el bloqueo por IP y algunos otros bloquean por rangos de IP. Los que bloquean por rangos de IP investigan primero cual es el rango de IP que tiene la compañía (basándose en la IP que encontraron haciendo **Open Relay**), y bloquean dicho rango.

Cabe destacar también, que no se considera que está en falta a quien realiza estos ataques, sino a quien tiene un servidor que los permite (por acción u omisión).

Existe cierta divergencia en la definición del acrónimo RBL. Una sería *Relay Black List* (Lista Negra de Relays), y la otra sería *Realtime Black List* (Lista Negra en Tiempo Real).

Un **Smart host** es un tipo de servidor de retransmisión de correo que permite a un SMTP del servidor a la ruta de correo electrónico a un servidor de correo intermedio y no directamente al servidor del destinatario. A menudo, este smart host requiere autenticación del remitente para verificar que el remitente tiene los privilegios que el correo enviado a través del host inteligente. Esta es una distinción importante a partir de un relay abierto que reenviará el correo del remitente sin necesidad de autenticación. Las técnicas más comunes incluyen la autenticación SMTP-AUTH y POP antes de SMTP .



- Clientes de correo electrónico: entornos-DOS, gráficos y navegadores.

DOS -> Pine o Post
WINDOWS -> MS-OutLook Express, NetScape Messenger, WinBox, MailDrop
Macintosh -> MS-OutLook Express, NetScape Messenger, MailDrop, Eudora
UNIX -> pine, mutt, mailx, mail

Un **cliente de correo electrónico**, o también llamado en inglés **mailer** o **Mail User Agent (MUA)** es un programa de ordenador usado para leer y enviar mensajes de correo electrónico.

Originalmente, los clientes de correo electrónico fueron pensados para ser programas simples para leer los mensajes del correo de usuario, enviados por elagente de reparto de correo (MDA) conjuntamente con el agente de transferencia de correo (MTA) a un buzón local.

Los formatos de buzón de correo más importantes son mbox y Maildir. Estos simplísimos protocolos para el almacenamiento local de los mensajes de correo electrónico realizan de una forma muy sencilla la importación, exportación y copia de seguridad de las carpetas de correo.

- **Mozilla Thunderbird.** Para una amplia mayoría de usuarios es el mejor, por su velocidad y simplicidad de uso. También es cierto que es el preferido por muchos usuarios que han migrado a Linux desde sistemas Windows porque ya lo utilizaban en este sistema operativo.

http://www.mozillamessaging.com/es-ES/thunderbird/

- **Evolution**. Es una auténtica suite de correo, ya que además de disponer de la gestión de email, incluye un calendario, libreta de direcciones, lista de tareas y funciones diversas de gestión. Ha sido una parte oficial de GNOME y su desarrollo está patrocinado principalmente por Novell. Su interfaz de usuario y su funcionalidad le hacen ser muy similar al Outlook de sistemas Windows.

http://projects.gnome.org/evolution/

- **Kmail**. Cliente de correo electrónico del entorno de escritorio KDE.

http://userbase.kde.org/Kmail

- **Zimbra.** Cliente web / servidor de correo electrónico y calendario / agenda de código libre, desarrollado en Java y complementado con AJAX. Proporciona sincronización nativa para una gran variedad de dispositivos móviles como BlackBerry e iPhone.

http://www.zimbra.com/

- **Spicebird**. Proyecto derivado de Thunderbird, que integra correo electrónico, agenda de contactos, calendario y mensajería instantánea. Desarrollado por una compañía india de nombre Synovel. De código abierto y multiplataforma.

http://www.spicebird.com/

- **Balsa**. Cliente ligero para GNOME.

http://balsa.gnome.org/

- **Claws Mail**. Conocido tambien como Sylpheed-Claws, es un cliente de correo y noticias basado en GTK+. Muy recomendado para los usuarios de netbooks por su ligereza

http://www.claws-mail.org/

- **Gnus**. Lector de mensajes bajo Emacs o Xemacs.

http://www.gnus.org/

- **Sylpheed**. Cliente de correo basado en GTK+ de aspecto similar al Outlook de Microsoft.

http://sylpheed.sraoss.jp/en/

- **Mulberry**. Cliente de correo electrónico simple, potente y versátil. De código libre y multiplataforma.

Más información:
http://www.mulberrymail.com/index.shtml

- **Scribe**. Cliente de correo electrónico pequeño y rápido que incluye agenda de contactos y calendario.

http://www.memecode.com/scribe.php

En modo texto

- **Mutt**. Cliente de correo para consola para sistemas tipo Unix. Fue escrito originalmente por Michael Elkins en 1995 y publicado bajo Licencia Pública General GNU.

http://www.mutt.org/

- **Alpine**. Es un cliente basado en Pine Message System, fácil de usar y rápido. Alpine presume que es apropiado tanto como para nuevos usuarios como para los más avanzados. Es desarrollado en la Universidad de Washington. Posee una interfaz de usuario en formato texto.

http://www.washington.edu/alpine/

En WINDOWS

1. Mozilla Thunderbird

Es el cliente de correo electrónico gratuito de Mozilla y es uno de los mejores clientes para Windows 7, y otros sistemas operativos también. Su configuración es muy simple, incluye un **formato de dos columnas** qué hace más cómoda la lectura de los correos y una interfaz clara y efectiva.

Los correos electrónicos pueden ser vistos en un pequeño panel en la parte inferior del cliente o haciendo doble clic para abrirlos en una nueva pestaña. Incluye características interesantes cómo etiquetas, filtros, búsqueda rápida y carpetas inteligentes.

2. Postbox Express

Es fácil de configurar e instalar. Insertando nombre de usuario y contraseña todo lo demás es detectado. Pero lo más interesante y relevante es qué Postbox Express es **capaz de tomar todas tus carpetas creadas en Gmail** y reproducirlas con exactitud.

Su interfaz es clara e incluye una fila de iconos con todas las funciones básicas en la parte superior del programa, tiene un diseño en base a dos columnas y permite el uso de pestañas. PostBox Express es una gran opción dada sus características y sencillez.

3. Opera Mail

Es un interesante cliente de correo electrónico qué a diferencia de los anteriores requiere una acreditación diferente ya qué para ser utilizado deberás usar el navegador Opera (se accede a través del mismo)

La configuración es simple, la interfaz clara y tiene la capacidad de **desempeñarse eficazmente al recibir correos en HTML**. Opera utiliza un interfaz con pestañas que es la misma que la del navegador web y permite leer los nuevos correos a través de las mismas en lugar de abrirlos en una nueva ventana.

- Mensajes de correo.

Un mensaje de Correo Electrónico consta de dos partes. La primera se denomina *encabezado*, la que contiene el mensaje en sí, recibe el nombre de *cuerpo* del mensaje.

El mensaje comienza con el encabezado y está separado del cuerpo exactamente por una línea que normalmente se añade automáticamente. El encabezado posee información sobre el remitente, los destinatarios, la fecha de envío, el tema del mensaje, etc.

Las líneas mas importantes del encabezado son:

- **From:** Es la dirección del remitente. Sólo puede haber una línea de este tipo en el encabezado.
- **To:** El o los destinatarios de este mensaje. Esta línea puede especificar más de una dirección de destino.
- **Cc:** Copia a destinatarios. Ésta línea equivale a la copia en papel carbón en el caso del correo normal. Se manda a los destinatarios indicados una copia (meramente informativa) de la carta.
- **Bcc:** Esta sería una copia oculta. Se mandará una copia a la dirección aquí indicada sin que los otros destinatarios tengan conocimiento de ello.
- **Subject:** Tema del mensaje. El texto es libre, pero debes escoger uno que sea breve y que describa el contenido del mensaje. Ten cuidado con los signos de puntuación, usa los apropiados pues, por ejemplo:

  Llamadas telefonicas gratuitas?
  no es lo mismo que:
  Llamadas telefonicas gratuitas!

Date: Indica la fecha y hora en que el mensaje fue enviado.
Message-Id: Es un identificador de cada mensaje, es único y lo inserta el ordenador que lo envía. Por ejemplo:

<93116.130423TAMARIRA@EVALUN11.BITNET>

Received: Es la información que se utiliza para comprobar los problemas que hayan aparecido en el reparto de un mensaje. En ella se muestra las direcciones de las máquinas por las que pasó el mensaje en dirección a su destino, junto con la fecha y hora en que lo hizo.

Resent-From: Dirección de la persona o programa desde el cual llega el mensaje. El hecho de decir "reenviado" te notifica de que el mensaje le ha llegado a la persona que se indica en este campo y ella, a su vez, te manda una copia.

Reply-To: Obviamente, la dirección a la que debes contestar. No tiene que ser la misma desde donde se ha enviado la carta.

Un ejemplo, de los tres formatos posibles en los que puede aparecer la dirección electrónica de alguien que te envía un mensaje, sería:

From: Raul Tamarit <tamarira@vm.ci.uv.es>
From: tamarira@vm.ci.uv.es
From: tamarira@vm.ci.uv.es (Raul Tamarit)

Aunque la cadena de caracteres "Raul Tamarit" especifica el nombre del remitente, ésta no forma parte de la dirección utilizada por el sistema que se encarga de distribuir los mensajes. El sistema tratará por igual estos tres hipotéticos mensajes, ya que sólo mira la cadena "tamarira@vm.ci.uv.es". Ésta es la llamada *direccion de correo*, y corresponde a un buzón (electrónico) en el que se deposita el correo destinado a esa dirección.

Echemos un vistazo al caracter @ que hay en la Dirección de Correo:
tamarira @ vm.ci.uv.es

La parte de la izquierda del caracter @ se llama *buzón local*; mientras que la parte que figura a la derecha, es el *dominio*. Si no se especifica ni el caracter @ ni el dominio, por ejemplo:

To: tamarira

ello indica que el mensaje se envía a una dirección *local*, es decir a una dirección en tu mismo dominio. En este caso, éste debería ser "vm.ci.uv.es" para que el mensaje llegue. Observa que el formato aquí descrito **corresponde al formato de direcciones de correo electrónico para la Internet**. La Internet se ha convertido en tan popular y tiene tantos usuarios que su formato de dirección a pasado a ser (casi) el estándar. **En otras redes, las direcciones de correo se escribirán de distinta manera**, por ejemplo:

+ Formato BITNET: tamarira at evalun11

+ Formato UUCP: mcvax!ukc!gatekeeper!hotspot!federico

+ Formato X400: S=tamarira; OU=vm; OU=ci; O=uv;
P=iris; A=mensatex; C=es

- Direcciones, cuentas de correo y servidores DNS.
- Protocolos y servicios de descarga de correo: SMTP/ESMTP, POP, IMAP.

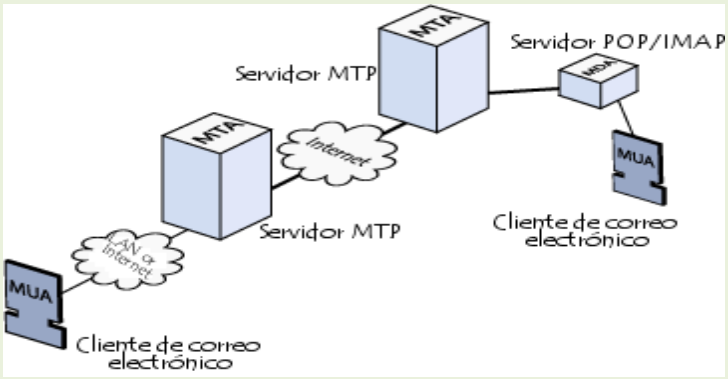
•Funcionamiento del servicio de correo electrónico.

El correo electrónico gira alrededor del uso de las casillas de correo electrónico. Cuando se envía un correo electrónico, el mensaje se enruta de servidor a servidor hasta llegar al servidor de correo electrónico del receptor. Más precisamente, el mensaje se envía al servidor del correo electrónico (llamado **MTA**, del inglés *Mail Transport Agent [Agente de Transporte de Correo]*) que tiene la tarea de transportarlos hacia el MTA del destinatario. En Internet, los MTA se comunican entre sí usando el protocolo SMTP, y por lo tanto se los llama **servidores SMTP** (o a veces *servidores de correo saliente*).

Luego el MTA del destinatario entrega el correo electrónico al servidor del correo entrante (llamado **MDA**, del inglés *Mail Delivery Agent [Agente de Entrega de Correo]*), el cual almacena el correo electrónico mientras espera que el usuario lo acepte. Existen dos protocolos principales utilizados para recuperar un correo electrónico de un MDA:

- POP3 (*Post Office Protocol [Protocolo de Oficina de Correo]*), el más antiguo de los dos, que se usa para recuperar el correo electrónico y, en algunos casos, dejar una copia en el servidor.
- IMAP (*Internet Message Access Protocol [Protocolo de Acceso a Mensajes de Internet]*), el cual se usa para coordinar el estado de los correos electrónicos (leído, eliminado, movido) a través de múltiples clientes de correo electrónico. Con IMAP, se guarda una copia de cada mensaje en el servidor, de manera que esta tarea de sincronización se pueda completar.

Por esta razón, los servidores de correo entrante se llaman **servidores POP** o **servidores IMAP**, según el protocolo usado.



Usando una analogía del mundo real, los MTA actúan como la oficina de correo (el área de clasificación y de transmisión, que se encarga del transporte del mensaje), mientras que los MDA actúan como casillas de correo, que almacenan mensajes (tanto como les permita su volumen), hasta que los destinatarios controlan su casilla. Esto significa que no es necesario que los destinatarios estén conectados para poder enviarles un correo electrónico.

Para evitar que cualquiera lea los correos electrónicos de otros usuarios, el MDA está protegido por un nombre de usuario llamado **registro** y una **contraseña**.

La recuperación del correo se logra a través de un programa de software llamado **MUA** (*Mail User Agent [Agente Usuario de Correo]*).

Cuando el MUA es un programa instalado en el sistema del usuario, se llama **cliente de correo electrónico** (tales como Mozilla Thunderbird, Microsoft Outlook, Eudora Mail, Incredimail o Lotus Notes).

Cuando se usa una interfaz de web para interactuar con el servidor de correo entrante, se llama **correo electrónico**.

•Cuentas de correo, alías y buzones de correo.

Correo electrónico (**correo-e**, conocido también como *e-mail*), es un servicio de red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente (también denominados mensajes **electrónicos** o cartas **electrónicas**) mediante sistemas de comunicación electrónicos. Principalmente se usa este nombre para denominar al sistema que provee este servicio en Internet, mediante el protocolo SMTP, aunque por extensión también puede verse aplicado a sistemas análogos que usen otras tecnologías. Por medio de mensajes de correo electrónico se puede enviar, no solamente texto, sino todo tipo de documentos digitales. Su eficiencia, conveniencia y bajo coste están logrando que el correo electrónico desplace al correo ordinario para muchos usos habituales.

Un alias es la primera parte que forma un correo que esta antes de la @, por ejemplo el en david@dominio.com el alias es david.

El alias de correo es un servicio que le permite asignar a un mismo email varios alias, cuando alguien mande un email a cualquiera de los alias previamente configurados por el cliente este será recibido por el alias principal.

Esto quiere decir lo siguiente, usted puede crear el correo david@dominio.com que es su email principal(alias david), en ocasiones es necesario tener activa varias cuentas que son controladas por usted como pueden ser comercial@dominio.com (alias comercial), info@dominio.com (alias info), para tener el control de las mismas usted puede o bien créalas de manera independiente y configurarlas a su vez independientemente en su Outlook, lo cual es ineficiente, redireccionarlas todas al email principal lo cual es costoso, o la manera más sencilla asignarle a la cuenta principal los alias info y comercial. De esta manera cuando alguien mande un email a comercial@dominio.com será recibido en su cuenta de david@dominio.com

Este servicio es ilimitado y puede configurarlo online a traves del panel de control plesk.

•Estructura de los mensajes de correo electrónico.

Un correo electrónico tiene las siguientes partes básicas:
1) El encabezado, un conjunto de líneas que contienen información sobre la transmisión del mensaje, tales como la dirección del remitente, la dirección del destinatario, o fechas y horas que muestran cuándo los servidores intermediarios enviaron el mensaje a los agentes de transporte (MTA), que actúan como una oficina de clasificación de correo. El encabezado comienza con una línea De y cambia cada vez que atraviesa un servidor intermediario. Usando los encabezados, se puede ver el camino exacto que recorrió el correo electrónico, y cuánto tiempo le llevó a cada servidor procesarlo.

2) El mensaje propiamente dicho, está compuesto de los dos elementos que se muestran a continuación:

a) **los campos del encabezado**, un conjunto de líneas que describen las configuraciones del mensaje, tales como el remitente, el receptor, la fecha, etc. Cada uno tiene el siguiente formato:

Nombre: Valor Un correo electrónico incluye por lo menos los siguientes tres encabezados:
De: la dirección de correo electrónico del remitente

A: la dirección de correo electrónico del destinatario

Fecha: la fecha cuando se envió el mail

Puede contener los siguientes campos opcionales:
Recibido: información diversa sobre los servidores intermediarios y la fecha cuando se procesó el mensaje.
Responder a: una dirección para responder.
Tema: el tema del mensaje
ID del mensaje: una identificación única para el mensaje.

b) **El cuerpo del mensaje,** que contiene el mensaje, separado del encabezado por un salto de línea.

El correo electrónico está compuesto por líneas de caracteres de 7 bits US-ASCII visualizables. Cada línea tiene como máximo 76 caracteres, por razones de compatibilidad, y termina con caracteres CRLF (\r\n). Servicios de Red e Internet Tema

- Cabecera, Cuerpo, MIME.

Cuando un usuario de correo electrónico se las ve por primera vez con la cabecera de un mensaje, su interpretación no es tan evidente como pudiera parecer a simple vista. Sin embargo, su correcto entendimiento puede ser fundamental.

Para ver cómo funcionan la cabecera de un mensaje de correo, vamos a utilizar un ejemplo real, que analizaremos punto por punto. A continuación se muestra la cabecera de un mensaje de correo, que en Pegasus se puede ver pulsando la tecla Backspace, la combinación CTRL+H, o eligiendo la opción *Show all headers* del menú *Reader*.

```
Resent-from: "CARLOS MENENDEZ GARCIA"
<@list.cren.net:carlosmenendez@GEOCITIES.COM>
Resent-to: Carlos
Resent-date :Sun, 15 Dec 1996 22:39:02 +0000
Received: from bitnic.cren.net (bitnic.cren.net [207.86.28.132]) by list.cren.net
(8.7.6/8.6.12)
   with SMTP id QAA07781 for ;   Sun,15 Dec 1996 16:14:20 -0500 (EST)
Message-Id: <199612152114.QAA07781@list.cren.net>
Received: from BITNIC.CREN.NET by bitnic.cren.net (IBM VM SMTP V2R2)
   with BSMTP id 5214; Sun, 15 Dec 96 16:12:33 EST
Received: from BITNIC.CREN.NET (NJE origin LISTSERV@BITNIC) by
BITNIC.CREN.NET (LMail
   V1.2a/1.8a) with BSMTP id 5212; Sun, 15 Dec 1996 16:12:30 -0500
Date: Sun, 15 Dec 1996 16:12:28 -0500
From: BITNET list server at BITNIC (1.8a)
Subject: File: "BITNET SERVERS"
To: carlosmenendez@GEOCITIES.COM
Content-Type: multipart/mixed; boundary="--------geoboundary"
X-PMFLAGS: 570425472 0
```

Veamos, uno por uno, los campos de la cabecera:

Resent-from:	Mensaje reenviado por el usuario especificado. En este caso se reenvió en una red local, por eso la dirección no tiene el formato de Internet (*geo*). Como CARLOS MENENDEZ GARCIA se encuentra entre comillas, es un distintivo, y no tiene significado funcional.
Resent-to:	Mensaje reenviado al usuario especificado En el caso contemplado se reenvió dentro de una red local, al usuario *carlos*
Resent-	Fecha y hora de reenvío del mensaje. En las cabeceras de los mensajes de

date:	correo, el campo de la fecha debe estar en un formato determinado por unas normas muy rígidas (piénsese que tiene que poderse interpretar correctamente por una gran cantidad de sistemas distintos). En el ejemplo, se reenvió el Domingo 15 de diciembre de 1996 (los programas utilizan siempre el inglés), a las 22:39:02. A la derecha aparece la expresión +0000, que alude a la constante que hay que añadir a la hora GMT para ver la hora real de reenvío del mensaje. En este caso, no hay que añadir ninguna hora, pero podría haber sido, por ejemplo, +0200, -0300, o cualquier otro valor.
Received:	Cada vez que el mensaje pasa por un servidor, aparece este campo de datos, especificándose el nombre del servidor, su dirección IP (número que se asigna a cada servidor), el programa de correo utilizado, y la fecha y la hora en que se recibió en el servidor
Message-Id:	Número de identificación del mensaje. Se trata de un número único, que lo distingue de cualquier otro mensaje enviado por la red En el ejemplo que nos ocupa, la identificación del mensaje es *199612152114.QAA07781@list.cren.net*
Date:	Fecha y hora de envío del mensaje En el ejemplo, el mensaje se envió el Domingo 15 de Diciembre de 1996, a las 16:22:25, hora correspondiente a GMT-5, es decir a las 21:22:25 GMT.
From:	Remitente original del mensaje En el ejemplo, el origen del mensaje es *LISTSERV@BITNIC.CREN.NET*, cuyo alias es *BITNET list server at BITNIC (1.8a)*.
Subject:	Asunto del mensaje El asunto del mensaje del ejemplo es *File: "BITNET SERVERS"*
To:	Destinatario del mensaje El destinatario del mensaje es *carlosmenendez@GEOCITIES.COM*
Content-Type:	Tipo de contenido del mensaje; en realidad, es el formato con el que se envió el mensaje
X-PMFLAGS:	Este campo aparece sólo si el mensaje se envió con Pegasus, y alude a ciertos parámetros del programa

El cuerpo del correo electrónico es la parte en donde escribiremos el mensaje propiamente dicho. Los programas modernos de correo electrónico permiten un "formateo" del texto muy parecido al de los programas de tratamiento de texto convencionales, incluso pueden permitir poner dibujos de fondo.

Los ficheros adjuntos ("Attachments" en inglés) en realidad no forman parte del correo, sino que el programa de correo permite elegir cualquier archivo que tengamos en el disco duro y, por así decirlo, pegarlo al correo, una vez hecho esto el programa de correo se encarga de enviarlo junto con el correo en el momento en que decidamos enviar este.

MIME (*Extensiones Multipropósito de Correo Internet*) es un estándar propuesto en 1991 por Bell Communications para expandir las capacidades limitadas del correo electrónico y en particular para permitir la inserción de documentos (como imágenes, sonido y texto) en un mensaje. Fue definido originalmente en junio de 1992 por las RFC 1341 y 1342.

MIME describe el tipo de contenido del mensaje y el tipo de código usado con encabezados.

MIME incorpora las siguientes características al servicio de correo electrónico:

- Capacidad de enviar múltiples adjuntos en un solo mensaje
- Longitud ilimitada del mensaje
- Uso de conjuntos de caracteres no pertenecientes al código ASCII
- Uso de texto enriquecido (diseños, fuentes, colores, etc.)
- Adjuntos binarios (ejecutables, imágenes, archivos de audio o video, etc.), que se pueden dividir de ser necesario

MIME usa directivas especiales en los encabezados para describir el formato utilizado en el cuerpo de un mensaje, de modo que el cliente de correo electrónico pueda interpretarlo correctamente:

- Versión de MIME: esta es la versión de MIME estándar usada en el mensaje. Actualmente sólo existe la versión 1.0.
- Tipo de contenido: describe el tipo y el subtipo de datos. Puede incluir un parámetro de "juego de caracteres", separado por un punto y coma, que define qué juego de caracteres utilizar.
- Codificación de transferencia de contenido: define la codificación usada en el cuerpo del mensaje.
- Identificación de contenido: representa una identificación única para cada segmento del mensaje.
- Descripción de contenido: proporciona información adicional sobre el contenido del mensaje.
- Disposición de contenido: define la configuración de los adjuntos, particularmente el nombre vinculado al archivo, usando el atributo *nombre del archivo*.

Tipos de MIME primarios

Los tipos de MIME, usados en el encabezado *Tipo de contenido*, se usan para clasificar los documentos adjuntos de un correo electrónico. Un tipo de MIME está compuesto de la siguiente manera:

Tipo de contenido: tipo_mime_principal/subtipo_mime
Por ejemplo, una imagen GIF tiene el siguiente tipo de MIME:
Tipo de contenido: image/gif

Los tipos de datos primarios, a veces denominados "tipos de datos discretos", son:

- **texto**: texto de datos legible text/rfc822 [RFC822]; text/plain [RFC2646]; text/html [RFC2854].
- imagen: datos binarios que representan imágenes digitales: image/jpeg, image/gif, image/png.
- **audio**: datos de sonido digitaal: audio/basic, audio/wav
- **video**: datos de vídeo: video/mpeg
- **aplicación**: Otros datos binarios: application/octet-stream, application/pdf

Los tipos de MIME también se usan en la web para clasificar documentos transferidos usando el protocolo HTTP. Así, durante una transacción entre un servidor web y un explorador, lo primero que hace el servidor web es enviar el tipo de MIME del archivo al explorador, para que éste sepa cómo mostrar el documento.

Formatos de codificación

Para transferir datos binarios, MIME ofrece cinco formatos de codificación que se pueden usar en el encabezado *codificación de transferencia*:

- **7 bits**: formato de texto de 7 bits (para mensajes sin caracteres acentuados);
- **8 bits**: formato de texto de 8 bits;
- **QP**: formato QP, recomendado para mensajes que usan un alfabeto de 7 bits (como cuando hay acentos);
- **base 64**:Base 64, recomendado para enviar archivos binarios como adjuntos;
- **binario**: formato binario; no recomendado.

Dado que MIME es muy abierto, puede usar formatos de codificación de terceros como:

- BinHex (un formato exclusivo que pertenece a Apple),
- uuencode,
- xxencode

Codificación del encabezado

El encabezado *codificación de transferencia* se usa para especificar un formato de codificación para el cuerpo del mensaje, pero no soluciona el problema de codificación de los encabezados en sí (como el tema del mensaje).

Para codificar encabezados con conjuntos de caracteres que usan más de 7 bits, como los que incluyen letras acentuadas en el asunto del correo electrónico, el estándar MIME ofrece el siguiente formato:

juego de caracteres codificación resultado =

- **juego de caracteres** representa el carácter usado,
- **codificación** define el código deseado con dos valores posibles:
    - Q para quoted-printable
    - B para base 64

- resultado: texto codificado con el método especificado.

A continuación hay un ejemplo de un código QP con "Building façade" como asunto del correo electrónico.
Asunto: Building fa=?ISO-8859-1?Q?=E7ade?=

Mensajes compuestos

Con el tipo de MIME "de varias partes", el estándar MIME permite mensajes compuestos, es decir mensajes que incluyen adjuntos múltiples, que incluso se pueden jerarquizar.

Para hacerlo, MIME permite un estándar llamado *frontera*. Es una cadena arbitraria definida como un atributo en el encabezado *Tipo de contenido*:

Tipo de contenido: multipart/mixed;
boundary="----------020005090303070203010601"
Cada separador delimita una porción de contenido que comienza con los encabezados *Tipo de contenido* y *Codificación de contenido*. Es esencial que el valor de este separador no se encuentre dentro del contenido del mensaje.

Existen varios tipos de separadores:

- multipart/mixed define una serie de elementos múltiples
- multipart/alternative define alternativas para la misma información, como un mensaje en formato de texto o HTML. Si el cliente de correo electrónico puede mostrar mensajes con una disposición y está configurado para hacerlo, mostrará la versión HTML; de lo contrario, mostrará la versión de texto.
- multipart/parallel define datos presentes al mismo tiempo (como sonido e imagen).
- multipart/signed define una firma digital para los datos del mensaje
- multipart/related define los datos relacionados

Lista de tipos de MIME

Los tipos de MIME están estandarizados por un grupo llamado **IANA** (*Autoridad de asignación de números de Internet*). A continuación encontrará una lista no taxativa de los tipos de MIME más comunes:

Tipo de MIME	Tipo de archivo	Extensión asociada
application/atom+xml	Archivos en formato ATOM	atom
application/iges	Archivos CAS	iges
application/javascript	Archivos JavaScript	js
application/dxf	Archivos AutoCAD	dxf
application/mp4	Archivos MPEG4	mp4
application/iges	Formato de intercambio IGES CAD	igs, iges

application/octet-stream	Archivos binarios no interpretados	bin
application/msword	Archivos de documentos Microsoft Word	doc
application/pdf	Archivos Adobe Acrobat	pdf
application/postscript	Archivos PostScript	ai, eps, ps
application/rtf	Formato de texto enriquecido	rtf
application/sgml	Archivos SGML	sgml
application/vnd.ms-excel	Archivos de hojas de cálculo Microsoft Excel	xls
application/vnd.ms-powerpoint	Archivos de presentación Microsoft Powerpoint	ppt
application/xml	Archivo XML	xml
application/x-tar	Archivos TAR comprimidos	tar
application/zip	Archivos ZIP comprimidos	man
audio/basic	Archivos de audio básicos	au, snd
audio/mpeg	Archivo de audio MPEG	mpg,mp3
audio/mp4	Archivo de audio MPEG-4	mp4
audio/x-aiff	Archivos de audio AIFF	aif, aiff, aifc
audio/x-wav	Archivos de audio Wav	wav
image/gif	Imágenes Gif	man
image/jpeg	Imágenes Jpeg	jpg, jpeg, jpe
imagen/png	Imágenes PNG	png
image/tiff	?Imágenes Tiff	tiff, tif
image/x-portable-bitmap	Archivos Bitmap PBM	pbm
image/x-portable-graymap	Archivos Graymap PBM	pgm
image/x-portable-pixmap	Archivos Pixmap PBM	ppm
multipart/x-zip	Archivos comprimidos en Zip	zip
multipart/x-gzip	Archivos comprimidos en Zip GNU	gz, gzip
text/css	Hoja de estilo	css
text/csv	Archivos de texto separados por comas	csv
text/html	Archivos HTML	htm, html
text/plain	Archivos de texto sin formato	txt, g, h, c, cc, hh, m, f90
text/richtext	Archivos de texto enriquecido	rtx
text/rtf	Archivos de texto con formato enriquecido	rtf
text/tab-separated-value	Archivos de texto separados por tabulador	tsv
text/xml	Archivos XML	xml

video/h264	Vídeos H.264	h264
video/dv	Vídeos DV	dv
video/mpeg	Vídeos MPEG	mpeg, mpg, mpe
video/quicktime	Vídeos QuickTime	qt, mov
video/msvideo	Vídeos Microsoft Windows	avi

•Monitorización y registros del servicio de correo electrónico.

Registro de actividad del servidor de correo (logs)
Ejemplo:
Para ilustrar la descripción de los logs de los servidores de correo se utilizará el siguiente mensaje. El mensaje se presenta tal cual lo ven los programas lectores de correo. Los lectores de correo formatean los mensajes para que el usuario vea en pantalla sólo la parte de interés.

From - Wed Jul 14 12:52:34 2004
X-UIDL: UID121500
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
Return-Path: <u.n.e.d.@yahoo.es>
Received: from hermes-uno.uned.es (bm103103-5.uned.es [10.103.103.5])
by nerea-nueve.uned.es (Postfix) with ESMTP id 404CC636A5
for <admin.correo@csi.uned.es>; Wed, 14 Jul 2004 12:52:00 +0200 (CEST)
Received: from hermes-uno.uned.es (localhost.localdomain [127.0.0.1])
by hermes-uno.uned.es (8.12.8/8.12.8) with ESMTP id i6EApxg6031829
for <admin.correo@csi.uned.es>; Wed, 14 Jul 2004 12:51:59 +0200
Received: from web51009.mail.yahoo.com (web51009.mail.yahoo.com
[206.190.39.128])
by hermes-uno.uned.es (8.12.8/8.12.8) with SMTP id i6EApxYb031820 for
<admin.correo@csi.uned.es>; Wed, 14 Jul 2004 12:51:59 +0200
Message-ID: <20040714115158.7790.qmail@web51009.mail.yahoo.com>
Received: from [62.204.192.73] by web51009.mail.yahoo.com via HTTP; Wed, 14
Jul 2004 12:51:58 CEST
Date: Wed, 14 Jul 2004 12:51:58 +0200 (CEST)
From: Administrador <u.n.e.d.@yahoo.es>
Subject: Prueba
To: admin.correo@csi.uned.es
MIME-Version: 1.0
Content-Type: text/plain;
charset=iso-8859-1
Content-Transfer-Encoding: 8bit
X-imss-version: 2.5
X-imss-result: Passed

X-imss-scores: Clean:4.29222 C:22 M:1 S:5 R:5
X-imss-settings: Baseline:5 C:4 M:4 S:4 R:4 (0.2500 1.0000)
Prueba.

El envío/recepción del mensaje anterior generó en los servidores de correo las siguientes entradas de registro (logs):

Jul 14 12:51:59 hermes-uno sendmail25[31820]: i6EApxYb031820:
from=<u.n.e.d.@yahoo.es>, size=555, class=0, nrcpts=1,
msgid=<20040714115158.7790.qmail@web51009.mail.yahoo.com>,
proto=SMTP, daemon=MTA, relay=web51009.mail.yahoo.com [206.190.39.128]
Jul 14 12:52:00 hermes-uno sendmail25[31828]: i6EApxYb031820:
to=<admin.correo@csi.uned.es>, delay=00:00:01, xdelay=00:00:01,
mailer=esmtp, pri=30398, relay=localhost.uned.es.
[127.0.0.1], dsn=2.0.0, stat=Sent (2.0.0 i6EApxg6031829 Message accepted for delivery)
Jul 14 12:52:00 hermes-uno sendmail19000[31829]: i6EApxg6031829:
from=<u.n.e.d.@yahoo.es>, size=916, class=0, nrcpts=1,
msgid=<20040714115158.7790.qmail@web51009.mail.yahoo.com>,
proto=ESMTP, daemon=Daemon0, relay=localhost.localdomain [127.0.0.1]
Jul 14 12:52:00 hermes-uno sendmail19000[31833]: i6EApxg6031829:
to=<admin.correo@csi.uned.es>, delay=00:00:01, xdelay=00:00:00,
mailer=esmtp, pri=30759, relay=csi.uned.es.
[62.204.192.23], dsn=2.0.0, stat=Sent (Ok: queued as 404CC636A5)
Jul 14 12:52:00 nerea-nueve postfix/smtpd[20662]: 404CC636A5:
client=bm103103-5.uned.es[10.103.103.5]
Jul 14 12:52:00 nerea-nueve postfix/cleanup[18502]: 404CC636A5:
message-id=<20040714115158.7790.qmail@web51009.mail.yahoo.com>
Jul 14 12:52:00 nerea-nueve postfix/qmgr[31460]: 404CC636A5:
from=<u.n.e.d.@yahoo.es>, size=1343, nrcpt=1 (queue active)
Jul 14 12:52:00 nerea-nueve postfix/pipe[16585]: 404CC636A5:
to=<c0000000@nerea-nueve.uned.es>, orig_to=<admin.correo@csi.uned.es>,
relay=maildrop, delay=0, status=sent (nerea-nueve.uned.es)

Explicación de las cabeceras del mensaje

Las cabeceras de interés son "Message-ID:" y "Received:".
Cada vez que se crea un mensaje se le asigna un identificador único que determina el mensaje unívocamente. Este identificador se incorpora al mensaje en el campo Message-ID.
Todos los servidores de correo por los cuales pasa el mensaje hasta llegar a su destino añaden una cabecera Received donde se especifica:
• from: el nombre con el que se presenta el ordenador que envía el mensaje y entre paréntesis la dirección IP y nombre DNS de dicho ordenador con los que le ve el servidor que recibe el mensaje.
• by: nombre del ordenador que recibe el mensaje y que añade la cabecera Received que se está leyendo.

• with: especifica el mailer con el que se recibe el mensaje. Viene a ser el subsistema dentro del software de correo que se encarga de recibir el mensaje.
• id: es el identificador local del mensaje que sirve para poder hacer un seguimiento del mensaje dentro del servidor, en la cola de correo o en los registros del sistema (logs).
Explicación de las entradas de registro
En cada servidor por el que pasa el mensaje se guardan logs de la recepción y del reenvío/entrega del mensaje. Estos registros permiten a los administradores del servicio de correo detectar si ha habido algún problema y el motivo especificado por el servidor.
En condiciones normales de entrega donde un mensaje ha sido recibido y reenviado/entregado correctamente los registros que pueden verse en los servidores de la UNED, tales como en el ejemplo, se corresponden con:
1. El software del servidor de entrada/salida de la UNED que escucha en el puerto estándar SMTP (25).
2. El software del servidor de entrada/salida de la UNED que recibe el mensaje tras pasar por el antivirus.
3. El software del servidor donde se encuentran los buzones.
Para el caso 1 se realizan dos anotaciones por el software de correo, en este caso Sendmail .

Jul 14 12:51:59 hermes-uno sendmail25[31820]: i6EApxYb031820:
from=<u.n.e.d.@yahoo.es>, size=555, class=0, nrcpts=1,
msgid=<20040714115158.7790.qmail@web51009.mail.yahoo.com>,
proto=SMTP, daemon=MTA, relay=web51009.mail.yahoo.com
[206.190.39.128]
Jul 14 12:52:00 hermes-uno sendmail25[31828]: i6EApxYb031820:
to=<admin.correo@csi.uned.es>, delay=00:00:01, xdelay=00:00:01,
mailer=esmtp, pri=30398, relay=localhost.uned.es.
[127.0.0.1], dsn=2.0.0, stat=Sent (2.0.0 i6EApxg6031829 Message
accepted for delivery)

En la primera, realizada al recibir el mensaje, se pueden ver los siguientes campos:
• Día y hora en la que se efectúa el apunte.
• Nombre del servidor donde que realiza el apunte.
• Nombre y PID del proceso que realiza el apunte.
• Identificador local del mensaje que se está procesando. Coincide con el especificado en la cabecera Received que se añade al mensaje por este software cuando le procesa.
• Dirección de correo-e que remite el mensaje.
• Tamaño del mensaje. clase. Número de destinatarios.
• Message-ID del mensaje procesado.
• Protocolo y demónio mediante el cual se recibe el mensaje.
• Dirección IP y nombre del ordenador que nos ha transmitido el mensaje (relay).
En la segunda, realizada al enviar el mensaje, se pueden ver los siguientes campos:
• Día y hora en la que se efectúa el apunte.
• Nombre del servidor donde que realiza el apunte.
• Nombre y PID del proceso que realiza el apunte.

• Identificador local del mensaje que se está procesando. Coincide con el especificado en la cabecera Received que se añade al mensaje por este software cuando le procesa.
• Dirección o direcciones de correo-e del destinatario o destinatarios del mensaje.
• Tiempo transcurrido durante el procesado del mensaje (delay, xdelay). Subsistema de correo utilizado para enviar el mensaje (mailer). Y prioridad del mensaje (pri).
• Message-ID del mensaje procesado.
• Dirección IP y nombre del ordenador al que se ha retransmitido el mensaje (relay).
• Resultado del envío del mensaje (dsn, stat). Los códigos a grosso modo son:
Si empieza con 2, todo OK. (en este caso: 2.0.0)
Si empieza con 4, ha habido algún problema transitorio/temporal y no se ha podido recepcionar el mensaje, inténtelo más tarde. A veces se notifica al origen apuntando que ha habido un problema, pero que no es necesario que reenvíe el mensaje.
Si empieza con 5, ha habido un error grave, por ejemplo el usuario o dirección de correo no existe, no vuelva a intentarlo. El mensaje se borra y se notifica al origen del problema encontrado y que su mensaje no ha sido entregado.
• Al final entre paréntesis este software añade la respuesta que le devuelve el ordenador destino. en este caso el sotware que recibe el mensaje le dice que OK y además le especifica el identificador local que ha asignado al mensaje.
El caso 2 es similar al caso 1 puesto que es el mismo software y por tanto realiza el mismo tipo de apuntes.
En el caso 3 los apuntes del registro son distintos porque el software de correo es Postfix. Este software es más modular que el anterior y cada uno de los módulos realiza un apunte del trabajo que ha realizado con el mensaje

Jul 14 12:52:00 nerea-nueve postfix/smtpd[20662]: 404CC636A5:
client=bm103103-5.uned.es[10.103.103.5]
Jul 14 12:52:00 nerea-nueve postfix/cleanup[18502]: 404CC636A5:
message-id=<20040714115158.7790.qmail@web51009.mail.yahoo.com>
Jul 14 12:52:00 nerea-nueve postfix/qmgr[31460]: 404CC636A5:
from=<u.n.e.d.@yahoo.es>, size=1343, nrcpt=1 (queue active)
Jul 14 12:52:00 nerea-nueve postfix/pipe[16585]: 404CC636A5:
to=<c0000000@nerea-nueve.uned.es>,
orig_to=<admin.correo@csi.uned.es>, relay=maildrop, delay=0,
status=sent (nerea-nueve.uned.es)
En el primer apunte, realizado al recibir el mensaje, se pueden ver los siguientes campos:
• Día y hora en la que se efectúa el apunte.
• Nombre del servidor donde que realiza el apunte.
• Nombre y PID del proceso que realiza el apunte.
• Identificador local del mensaje que se está procesando. Coincide con el especificado en la cabecera Received que se añade al mensaje por este software cuando le procesa.
• Dirección IP y nombre del ordenador que nos ha transmitido el mensaje (client).

•Servicio de correo electrónico vía web.

Casi todos los proveedores de correo dan el servicio de correo web: permiten enviar y recibir correos mediante un sitio web diseñado para ello, y por tanto usando sólo un navegador web. La alternativa es usar un programa de correo especializado. El correo web es cómodo para mucha gente, porque permite ver y almacenar los mensajes desde cualquier sitio (en un servidor remoto, accesible por el sitio web) en vez de en un ordenador personal concreto.
Como desventaja, es difícil de ampliar con otras funcionalidades, porque el sitio ofrece un conjunto de servicios concretos y no podemos cambiarlos. Además, suele ser más lento que un programa de correo, ya que hay que estar continuamente conectado a sitios web y leer los correos de uno en uno.

Para evitar la utilización de su correo electrónico a través de la web por otros usuarios y sobre todo al usar equipos compartidos por varias personas recuerde:

- Desconectar la sesión actual pulsando en enlace "Desconectarse" del menú que aparece en el sistema de webmail y posteriormente cerrar el navegador.

- Configurar su navegador para que no recuerde las contraseñas del formulario de entrada al sistema. Para ello se le indica a continuación las opciones de configuración en los navegadores más comunes:

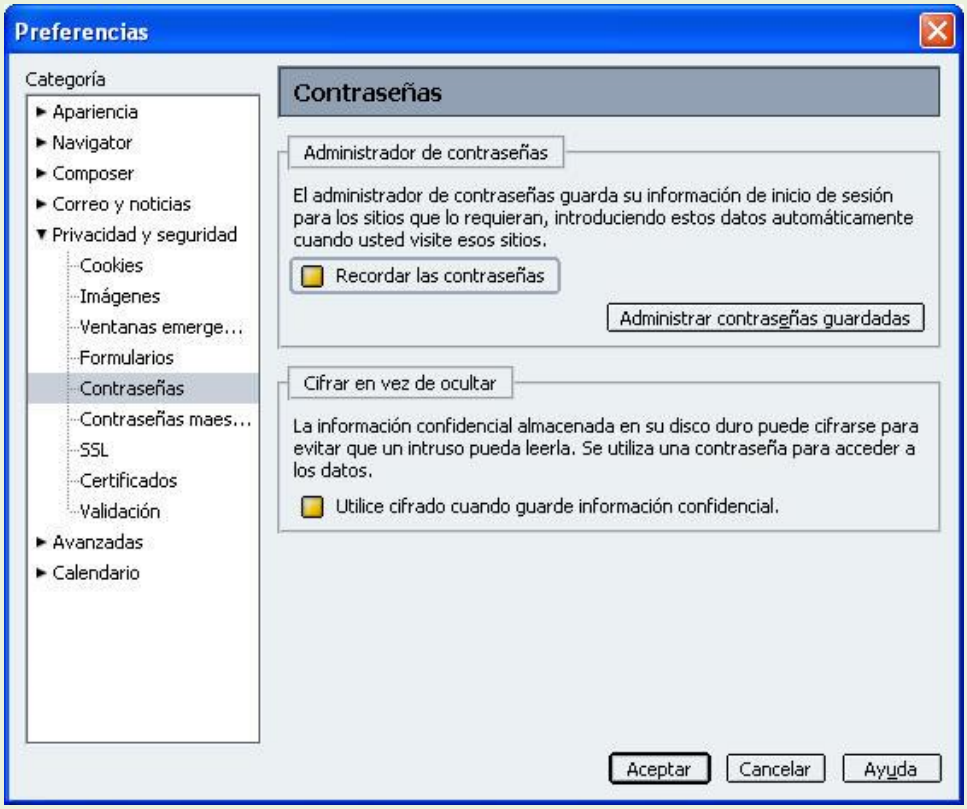
Internet Explorer

- Pulse el Menú Herramientas -> Opciones de Internet. Seleccione la pestaña "Contenido" y verá un botón "Autocompletar" en el apartado "Información Personal". Pulse este botón y desmarque la opción "Nombres de usuario y contraseñas de formulario" como se indica en la imagen siguiente. Puede opcionalmente borrar las contraseñas pulsando el botón "Borrar contraseñas". Pulse Aceptar y a partir de ese momento su navegador no le recordará la contraseña al introducir el usuario en las páginas web que visite

Mozilla 1.7

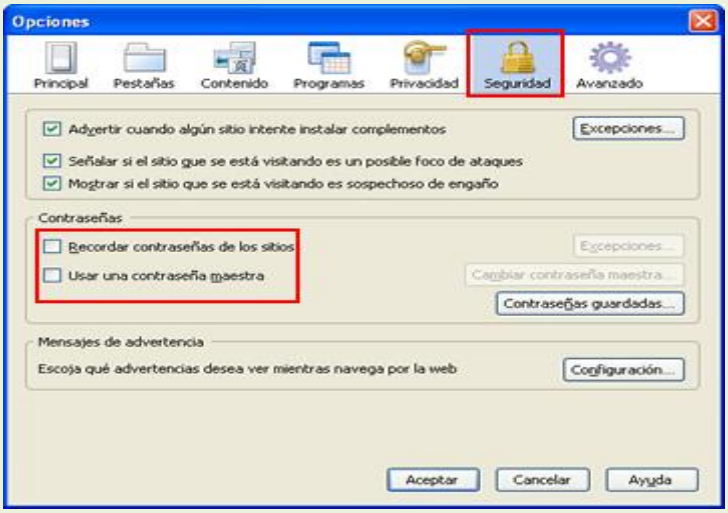
- Pulse el Menú Editar -> Preferencias. Seleccione la rama "Privacidad y seguridad" del panel izquierdo. Desmarque la opción "Recordar las

contraseñas" del apartado "Administrador de contraseñas". Pulse Aceptar y a partir de ese momento su navegador no le recordará la contraseña al introducir el usuario en las páginas web que visite.



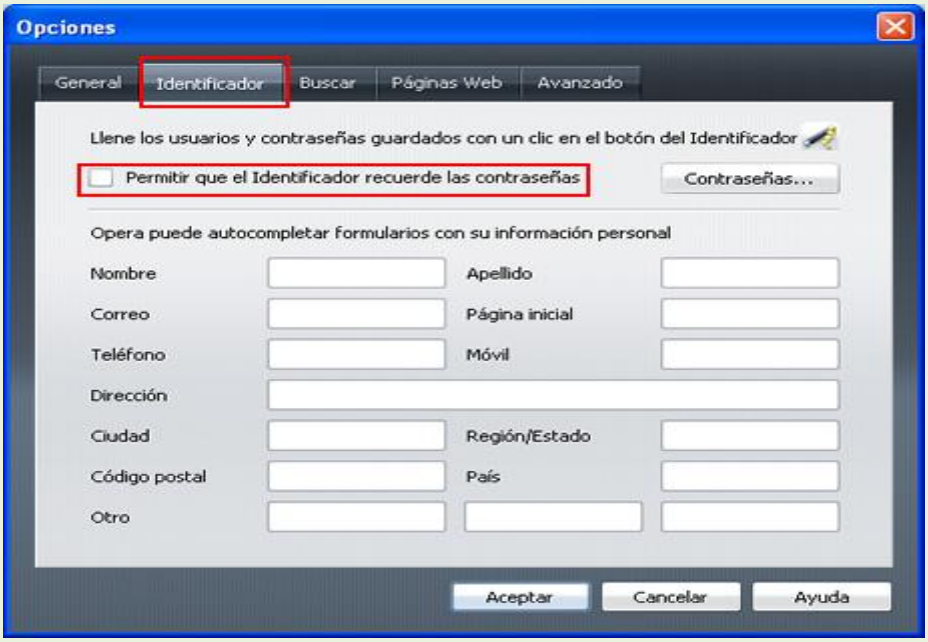
Firefox

- Pulse el Menú Herramientas -> Opciones. Seleccione el grupo de opciones "Seguridad" de la parte superior de la pantalla. Desmarque la opción "Recordar contraseñas de los sitios " del apartado "Contraseñas" y pulse Aceptar.



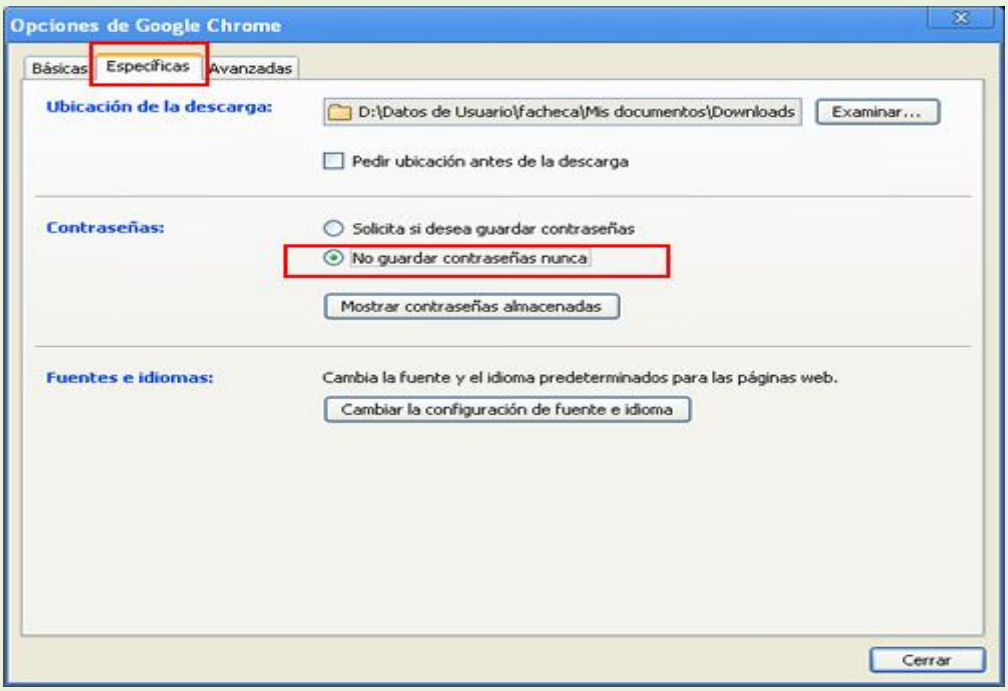
Opera

- Pulse el Menú "Herramientas -> Opciones..." Seleccione la pestaña "Identificador" de la parte superior de la pantalla. Desmarque la opción "Permitir que el Identificador recuerde las contraseñas " y pulse Aceptar.



Google Chrome

- Pulse el Menú "Herramientas -> Opciones" Seleccione la pestaña "Específicas" de la parte superior de la pantalla. Marque la opción "No guardar contraseñas nunca" de la sección "Contraseñas:" y pulse Cerrar.



Safari

- Pulse el Menú Herramientas -> Preferences. Seleccione la pestaña "Autofill". Desmarque la opción "User names anda passwords " del apartado "AutoFill web forms:". Pulse Aceptar y a partir de ese momento su navegador no le recordará la contraseña al introducir el usuario en las páginas web que visite.

•Correo seguro:

- Firma digital y cifrado de mensajes.

Para asegurar que nuestros mensajes de correo llegan sin ninguna modificación y totalmente confidenciales sin que nadie pueda leerlos más que el destinatario, podemos hacer uso de la firma y el cifrado digital de mensajes de correo electrónico mediante la extensión Enigmail y el uso de GnuPG.

¿Qué es y para qué nos sirve?

- Firma: nos permite que nuestro destinatario compruebe que el mensaje no fue modificado en el camino y que lo que lee es exactamente lo que redactamos.
- Cifrado: nos permite ocultar el contenido del mensaje para que sólo el destinatario final pueda leerlo.

No son excluyentes, se pueden usar para crear un mensaje de correo firmado y cifrado.

¿Cómo funciona?

La explicación del proceso es la parte más complicada, pero vamos a intentar verlo de forma práctica y muy gráfica.

Para que todo el proceso funcione cada usuario debe disponer de un par de claves, similar a tener dos llaves, una que daremos a la gente (clave pública) y otra que **no daremos a nadie** (clave privada).

- Clave pública: se la enviaremos a todo el mundo que la quiera, la subiremos a un servidor, o a nuestra web... Esta clave permitirá a la gente verificar nuestra firma y crear mensajes cifrados para nosotros.
- Clave privada: **no se la daremos a nadie**, ya que nos permitirá firmar y descifrar correo.

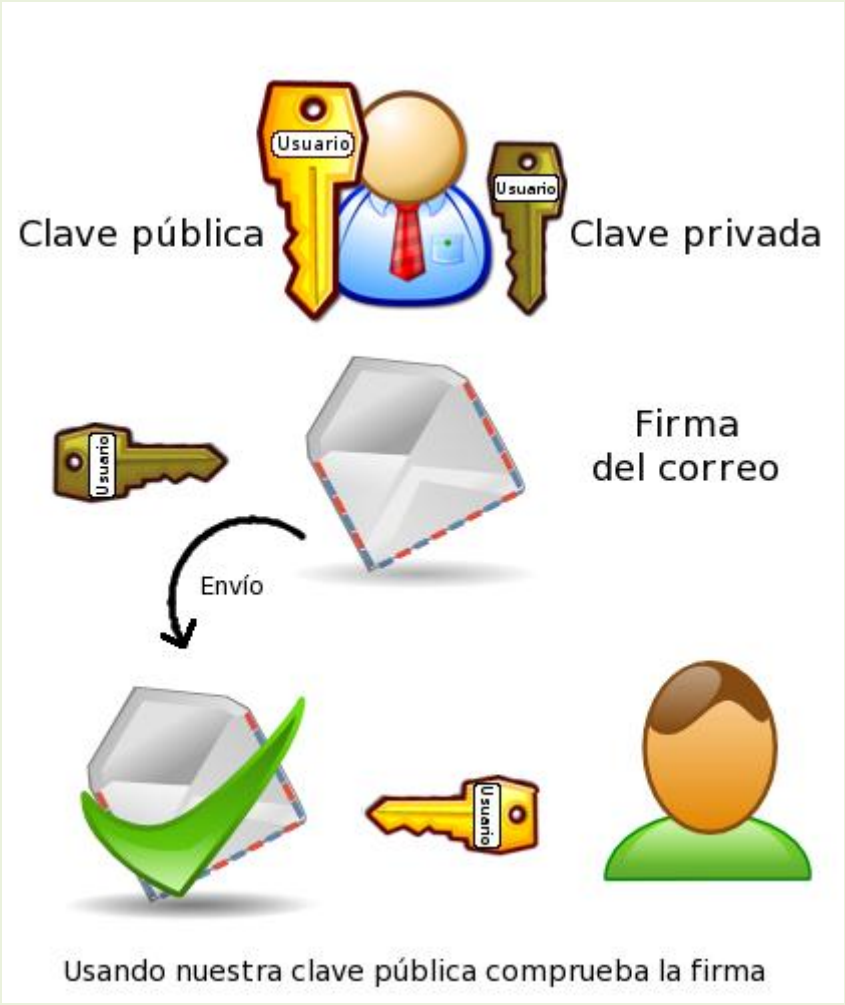
Es importante darse cuenta de que estas claves son dos archivos que se generarán en nuestro PC y que están íntimamente ligadas, pero **no se puede averiguar una a través de la otra**.

Ejemplo de firma

Supongamos que queremos mandar un mensaje firmado a nuestro amigo Pepe. Para ello, antes de nada, debemos recordar que Pepe debe tener nuestra clave pública.

- Gracias a nuestra clave privada generaremos un correo firmado.
- Pepe recibirá nuestro correo firmado.
- Pepe usará nuestra clave pública para comprobar la validez de la firma.

Gráficamente:



Ejemplo de cifrado

Ahora supondremos que queremos mandar a Pepe un mensaje cifrado para que sólo él pueda ver el contenido. Para ello, previamente, dispondremos de la clave pública de Pepe.

- Con la clave pública de Pepe cifraremos el mensaje.
- Pepe recibirá un mensaje cifrado.
- Pepe usará su clave privada para ver el contenido del mismo.

Gráficamente:

Resumen

En este apartado hemos visto qué es la firma y el cifrado digital y qué es necesario para usarlo. En los siguientes apartados aprenderás a crearte un par de claves (pública y privada) y a usarlo con tu cliente de correo.

Firma y cifrado con GPG y Enigmail

Instalación

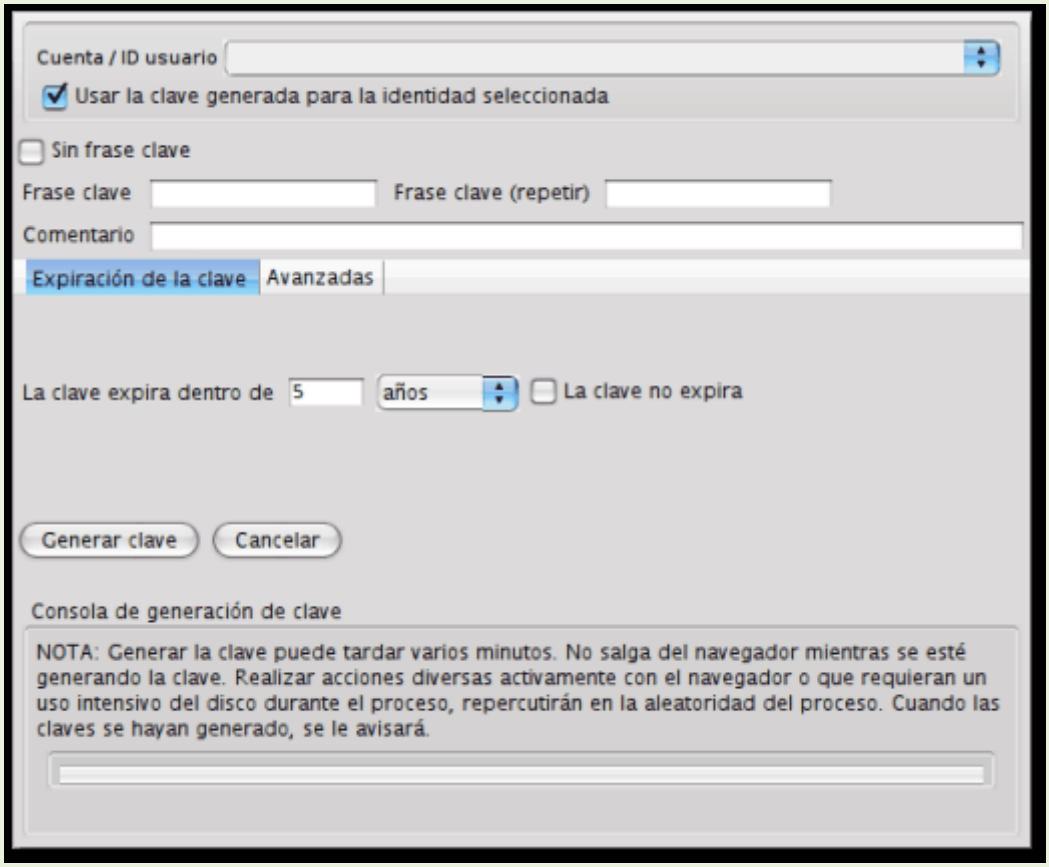
En primer lugar, debes descargar e instalar GnuPG, disponible para los sistemas operativos más usados. Es posible que necesites reiniciar el sistema para completar la instalación.

- GnuPG para windows (descarga la última versión del archivo gnupg-w32cli.exe)
- GnuPG para GNU/Linux (puedes encontrarlo en los repositorios de tu distro favorita)
- GnuPG para Mac OS

En segundo lugar, debes instalar la extensión Enigmail en tu cliente de correo, la cual puedes obtener en Mozilla Addons, entre otros sitios.

Generación del par de claves

Abre Thunderbird y verás una nueva opción en el menú superior a la izquierda de Herramientas titulado OpenGPG. Selecciona OpenPGP > Administración de claves. Se abrirá una ventana; selecciona en el menú Generar > Nuevo par de claves.



En el diálogo que aparece puedes especificar varias preferencias de la clave:

- La cuenta/identificación que quieres usar para el par de claves.
- La contraseña o frase clave del par de claves. La contraseña sirve para proteger tu clave privada contra un uso fraudulento; si alguien consigue robar tu clave privada, aún necesitará conocer la contraseña asociada para poder utilizarla.
- El tiempo de expiración de la clave, es decir, el tiempo durante el cual la clave que generes será válida. Puedes hacer pruebas con una clave con un tiempo de expiración bajo, pero más tarde puedes generar una clave que no expire nunca sin problemas, pues siempre puedes utilizar un certificado de revocación para invalidar tu clave.
- En la pestaña Avanzadas, el tamaño y el tipo de clave. Asegúrate de que seleccionas un tipo de clave DSA y El Gamal. Cuanto más grande sea la clave, más segura será, pero también requerirá más recursos el cifrado y descifrado lícito de mensajes.

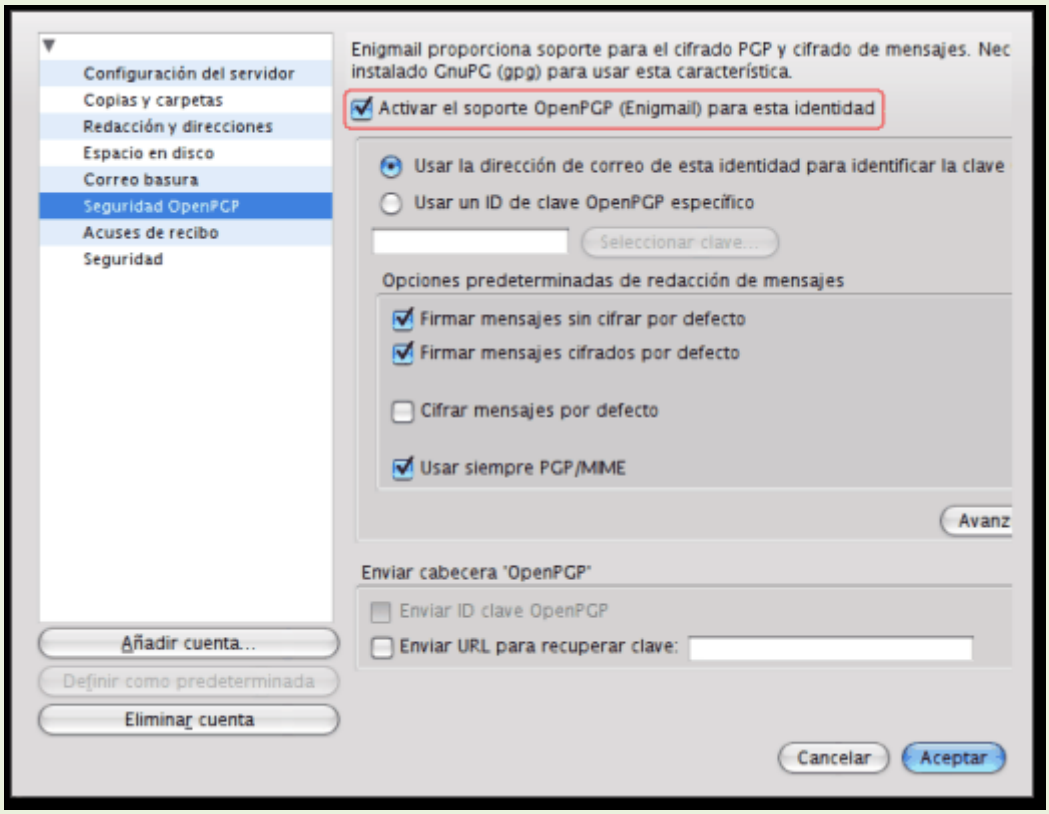
Haz clic en el botón "Generar clave". El proceso puede llegar a tardar varios minutos, como indica la nota al pie del diálogo.

Cuando haya acabado, se te preguntará si quieres generar un certificado de revocación, el cual necesitarás si pierdes tu clave privada o te la roban. Haz clic en Sí y guarda el certificado en alguna carpeta que no sea de acceso público. También puedes guardarla en un lápiz USB, en un CD-ROM o en un disquete.

Una vez guardado el certificado de revocación en un lugar seguro podrás ver tu nueva clave en la lista de claves conocidas en negrita, y, en el campo Tipo, "pub/sec", que significa "pública/secreta", es decir, que posees tanto la clave pública como la clave privada.

Configuración de las claves

Puedes utilizar tu nueva clave para firmar los correos que envíes. Para ello, abre el diálogo de configuración de las cuentas y en la sección Seguridad OpenPGP selecciona "Activar el soporte OpenGPG (Enigmail) para esta identidad".



Si sólo tienes la clave que acabas de generar, utiliza la opción "Usar la dirección de correo de esta identidad para identificar la clave OpenPGP", pero, si tienes más de una, puedes utilizar la opción "Usar un ID de clave OpenPGP específico" para elegir la que quieres usar.

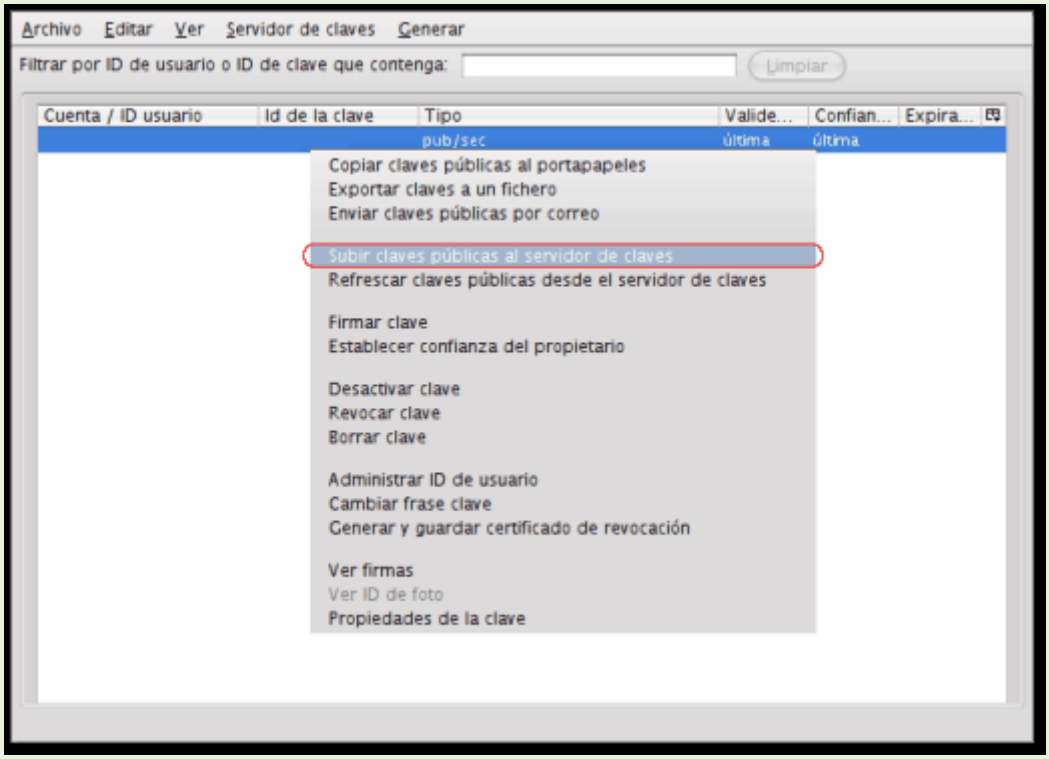
Más abajo puedes activar el firmado y/o cifrado de los mensajes por defecto. Si no lo activas, siempre puedes hacerlo mientras estés redactando un correo a través del menú OpenPGP o los botones OpenPGP y S/MIME de la ventana de redacción, que se muestran por defecto tras instalar Enigmail.

Si sólo tienes tu clave privada y pública no puedes cifrar mensajes, sólo firmarlos, ya que necesitas la clave pública del usuario al que quieres enviar el mensaje cifrado para poder hacerlo. Si el usuario al que quieres enviar mensajes cifrados ya tiene clave pública, pídele que te la proporcione; si no, pídele que genere un par de claves de la misma manera que tú lo hiciste.

Subir la clave pública a un servidor de claves

A pesar de que las claves públicas (nunca las privadas) se pueden distribuir por correo electrónico, mediante un lápiz USB, etc., lo más común es usar los llamados servidores de claves, que no son otra cosa que repositorios en Internet de claves públicas, de acceso libre, normalmente. Para publicar tu clave en uno de estos servidores, no tienes

más que hacer clic derecho en ella en la ventana de administración de claves de Enigmail y seleccionar la opción Subir claves públicas al servidor de claves. En la lista de servidores que aparece, selecciona uno, por ejemplo, pgp.mit.edu (acuérdate de la dirección) y pulsa el botón Aceptar.



El usuario al que quieras enviar correo cifrado deberá realizar el mismo proceso (o elequivalente con su gestor de claves GPG) para subir su clave pública a un servidor de su elección, cuya dirección te deberá proporcionar. En la ventana del administrador declaves de OpenPGP, selecciona en el menú Servidor de claves > Buscar claves. En el diálogo que aparece, introduce la dirección del servidor de claves que te proporcionó el otro usuario y el nombre o identidad con que registró su clave. Pulsa Aceptar y aparecerá una ventana con las claves encontradas en el servidor que coinciden con tu criterio de búsqueda. Selecciona la que quieras importar y pulsa Aceptar, tras lo cual podrás ver la clave pública del contacto en la lista de claves disponibles, esta vez con el tipo "pública" presente en la columna Tipo.

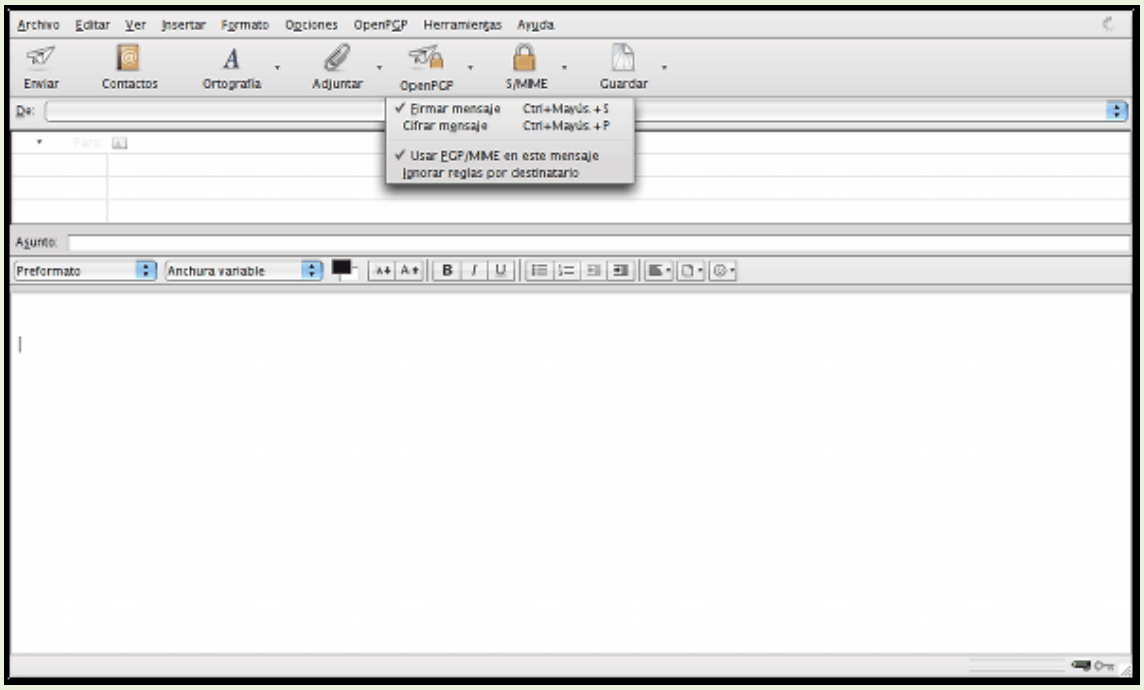
Firmar y/o cifrar mensajes

Firmar y cifrar mensajes desde la ventana de redacción es muy sencillo.

Si quieres firmar tu mensaje, selecciona en el menú superior *OpenPGP > Firmar mensaje*, o pulsa el botón *OpenPGP* de la barra de herramientas y marca la opción. Al enviar el mensaje se te pedirá la contraseña o frase de paso de tu clave privada, si la

protegiste de esta manera, y se generará un código a partir del contenido de tu mensaje que se adjuntará a éste y permitirá al destinatario verificar que el cuerpo del mensaje no ha sido alterado en su trayecto.

Si quieres cifrar tu mensaje, selecciona en el menú superior *OpenPGP > Cifrar mensaje*, o pulsa el botón *OpenPGP* de la barra de herramientas y marca la opción. Como ya se comentó, para enviar un mensaje cifrado a alguien necesitas su clave pública. Las claves de los destinatarios especificados en los campos «Para:» se buscarán en tu anillo de claves en función de su dirección de correo electrónico. Si al enviar el mensaje no se encuentra alguna clave o no es de confianza, se abrirá una ventana pidiéndote seleccionar las claves públicas que se usarán para cifrar, desde la que puedes también descargarte las claves que te falten desde los servidores de claves.



•Veracidad del correo:

El principal problema actual es el correo no deseado, que se refiere a la recepción de correos no solicitados, normalmente de publicidad engañosa, y en grandes cantidades, promoviendo pornografía y otros productos y servicios de calidad sospechosa. Usualmente los mensajes indican como remitente del correo una dirección falsa. Por esta razón, es más difícil localizar a los verdaderos remitentes, y no sirve de nada contestar a los mensajes de correo no deseado: las respuestas serán recibidas por usuarios que nada tienen que ver con ellos. Por ahora, el servicio de correo electrónico no puede identificar los mensajes de forma que se pueda discriminar la verdadera dirección de correo electrónico del remitente, de una falsa. Esta situación que puede resultar chocante en un primer momento, es semejante por ejemplo a la que ocurre con el correo postal ordinario: nada impide poner en una carta o postal una dirección de remitente aleatoria: el correo llegará en cualquier caso. No obstante, hay tecnologías desarrolladas en esta dirección: por ejemplo el remitente puede firmar sus mensajes mediante criptografía de clave pública. Además del correo no deseado, existen otros problemas que afectan a la seguridad y veracidad de este medio de comunicación:
los virus informáticos, que se propagan mediante ficheros adjuntos infectando el ordenador de quien los abre **la suplantación de identidad,** que es correo fraudulento que generalmente intenta conseguir información bancaria **los bulos** (bromas, burlas, o hoax), que difunden noticias falsas masivamente **las cadenas de correo electrónico,** que consisten en reenviar un mensaje a mucha gente; aunque parece inofensivo, la publicación de listas de direcciones de correo contribuye a la propagación a gran escala del 'correo no deseado y de mensajes con virus, suplantadores de identidad y engaños.

- Correo basura (“Spam”)fraude, engaño, cadenas y virus informáticos.

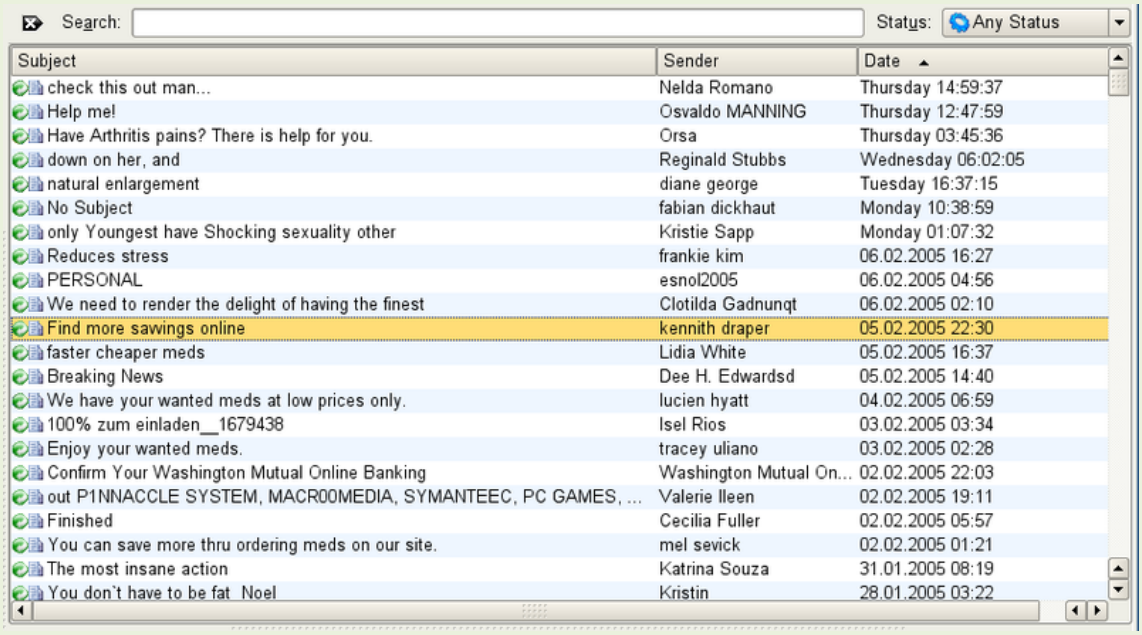
Se llama ***spam***, **correo basura** o **mensaje basura** a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina *spamming*. La palabra *spam* proviene de la segunda guerra mundial, cuando los familiares de los soldados en guerra les enviaban comida enlatada. Entre

estas comidas enlatadas estaba una carne enlatada llamada spam, que en los Estados Unidos era y es muy común.

Aunque se puede hacer *spam* por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico. Otras tecnologías de Internet que han sido objeto de correo basura incluyen grupo de noticias, usenet, motores de búsqueda, , redes sociales, wikis, foros, blogs, también a través de ventanas emergentes y todo tipo de imágenes y textos en la web.

El correo basura también puede tener como objetivo los teléfonos móviles (a través de mensajes de texto) y los sistemas de mensajería instantánea como por ejemplo Outlook, Lotus Notes, Windows live ,etc.

También se llama correo no deseado a los virus sueltos en la red y páginas filtradas (casino, sorteos, premios, viajes, drogas, software y pornografía), se activa mediante el ingreso a páginas de comunidades o grupos o acceder a enlaces en diversas páginas o inclusive sin antes acceder a ningún tipo de páginas de publicidad



Por el momento los dos mecanismos más habituales para la obtención de los datos personales de acceso, son el correo electrónico y la infección con virus de tipo gusano o troyano con funciones para la captura de las claves.

Correo electrónico.

Sin duda el correo electrónico es actualmente la técnica más utilizada en este tipo de fraude, tal vez porque resulte el más efectivo a corto plazo para el atacante.

Junto a la Ingeniería Social, el Spam es el otro gran aliado para el "phishing" debido a lo sencillo y barato que resulta para llegar hasta millones de usuarios con mensajes similares al siguiente:

".... Estimado cliente; El departamento de seguridad del banco ha detectado en las últimas fechas diversos tipos de técnicas fraudulentas en Internet por medio de las cuales es posible que las claves de acceso de algunos de nuestros clientes hayan sido capturadas para, haciendo un uso ilegal de las mismas,...."

"..... Estimado cliente; El departamento de seguridad del banco ha detectado en las últimas fechas diversos tipos de técnicas fraudulentas en Internet por medio de las cuales es posible que las claves de acceso de algunos de nuestros clientes hayan sido capturadas para, haciendo un uso ilegal de las mismas...."

"..... El único lugar donde podrá realizar el cambio de claves se encuentra tras el siguiente enlace: https://xxxxx.xx.xxxxx.. donde quedará disponible hasta el próximo día XX-XX-XXXX momento a partir del cual, se procederá a la cancelación de los accesos de todos aquellos usuarios que no hayan realizado el cambio de sus claves."
"......Muy agradecidos por su colaboración.....Don EEEEEEE (Departamento de Seguridad-CAJA DE INTERNET)

En estos mensajes, la dirección del remitente estará falsificada siendo muy parecida o incluso podrá coincidir con alguna cuenta legítima de la entidad en cuestión. No importa. El objetivo es, que alguno de los millones de receptores de ese correo sea cliente de esa entidad y pulse sobre el enlace propuesto para realizar el cambio o confirmación de sus claves, o introduzca cualquier otro dato personal.

Obviamente, la página enlazada también será falsa y estará controlada por los estafadores quienes habrán cuidado hasta el más mínimo detalle, en replicar con toda fidelidad la imagen, logotipos, colores y formatos de las páginas legítimas de la entidad. En la página, se pedirán todos los datos necesarios para poder realizar operaciones en las cuentas de la entidad: Nombre de usuario, Clave de acceso, Clave Personal, Firma, etc.

Una vez que sean confirmados los cambios, los estafadores tendrán a su disposición toda la información necesaria para acceder a las cuentas de aquellos usuarios que hayan caído en el engaño.

Una cadena de mensajes por correo electrónico es un tipo de cadena de mensajes que utiliza el correo electrónico como forma de propagación.
Debido a la facilidad de propagación del correo electrónico, estas cadenas se han convertido en mensajes masivos. Los mensajes de cadena buscan coaccionar o convencer de varias maneras a sus lectores de que dicha cadena sea reenviada a otro grupo de usuarios de correo electrónico. El nombre de "cadena" proviene del encadenamiento de pasajes que hacen estos mensajes de usuario a usuario. Son raras las cadenas que tienen que ver con dinero o que piden información confidencial. En su mayoría, no tienen nada que ver con transacciones financieras o reclutamiento de terceros. Por esa razón, encajan muy bien en la categoría de spam. Pueden también ser consideradas como rumores (hoaxes), ya que difunden mensajes falsos.
Los mayores daños que causan las cadenas son entorpecer el tráfico de Internet abarrotando los servidores con mensajes inútiles y alimentan las listas de e-mail canjeadas o vendidas entre atacantes y spammers. Las personas en general reenvían el mensaje automáticamente a su lista de amigos, ya sea porque es un pedido de ayuda o una información que les parece relevante, y difícilmente se preocupan por "esconder" las direcciones de e-mails. Así, cada vez que una cadenas es reenviada a aquella enorme lista de e-mails, nuevas direcciones caen en las manos de personas malintencionadas.

Un virus informático es un **programa de computadora**, que tiene como objetivo causar una alteración en un sistema de cómputo. Al igual que otras amenazas, un virus informático puede causar la alteración total de programas e información, o comprometer su integridad. A diferencia de otras amenazas, un virus informático puede propagarse de programa en programa, de sistema en sistema, sin intervención premeditada de las personas.

El componente esencial de un virus informático es un **conjunto de instrucciones** (programa de computadora) las cuales, cuando se ejecutan, se propagan por si mismas a otros programas o archivos, no infectados.

Un virus informático típico ejecuta dos funciones:

- Se copia a sí mismo a un programa, no infectado.

- Ejecuta cualquier instrucción que el autor del virus incluyó en él. Las instrucciones las puede ejecutar en una fecha predeterminada, o luego de un número de ejecuciones. También lo puede hacer en forma alterna e imprevista (random). Dependiendo de los motivos que tuvo el autor para crearlo, las instrucciones de un virus pueden ser de cualquier tipo. Desde desplegar un inocente mensaje en la pantalla a borrar y/o alterar completamente la información almacenada en un medio magnético (disquete, disco fijo). En algunos casos, un virus puede contener instrucciones que no sean destructivas, pero puede causar daño al replicarse a sí mismo, utilizando recursos limitados del sistema, como espacio en discos, tiempo de la memoria principal o conexiones de una red.