

The background features a decorative graphic consisting of three concentric blue circles of varying sizes in the upper right quadrant. Two thin blue lines intersect at a point near the center of these circles, extending towards the top left and bottom right corners. A large, solid blue circle is positioned in the bottom right corner.

SERVICIOS DE RED E INTERNET

INSTALACIÓN Y ADMINISTRACIÓN DE SERVICIOS DE
CORREO ELECTRÓNICO

UD 6: “Instalación y administración de servicios de correo electrónico”

- **ÍNDICE**
- **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.

- **Características del servicio de correo electrónico.**

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.



Principales características:

- **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:**

- Agentes de correo electrónico.

Los servidores de correo a menudo realizan diferentes funciones según sea el uso que se planifique para el mismo, como es leer, responder, transportar el mensaje, entregar el mensaje,... etc.

Los agentes de correo electrónico son los siguientes:

- **MUA (Mail User Agent - Agente de Usuario):** permite **leer, componer, responder y disponer** (por ejemplo borrar o archivar) de los **mensajes de correo electrónico**.

Se ocupa de inclusión de formatos esenciales, tales como **el From** y otros, como manejar **attachments (MIME Multipurpose Internet Mail Extensions)**.

Ejemplos: mail (BSD y otros), mh, pine, elm, Eudora, Thunderbir.

- **MTA (MAil Transfer Agent - Agente de Transporte):** **Recibe mensaje de MUA, interpreta destinatario**, y se encarga de que **viaje hasta su destino**.

Utiliza protocolo **estándar SMTP** (Simple Mail Transport Protocol, RFC 2821) o **ESMTP** (Extended, RFC 1869, etc), con **comandos en ASCII (EHLO, VRFY, RCPT, DATA)**.

Ejemplos: sendmail (o Postfix, Exim) en sistemas Linux.

- **MDA (Mail Delivery Agent - Agente de Entrega):** que se encarga de **entregar los mensajes** que llegan por el MTA a cada MDA de **cada usuario** dentro de una misma máquina. Entre otras cosas un **MDA puede aplicar filtros, generar respuestas automáticas**, etc...

Cada tipo de recipiente **requiere un MDA** particular. Ej: archivos locales (/var/mail/), bases de datos.

Ejemplos: /bin/mail, procmail.

MSA (Access Agent - Agentes de Envío): Permite descargar al MTA (que puede estar muy ocupado) de algunas funciones de verificación (pre-procesamiento). Esto implica:

- **Que los nombres de host parezcan válidos** (fully qualified). El término FQDN (fully qualified domain name) aplica a direcciones de máquina cuyo dominio parece correcto
- **Log de errores**, reescribiendo encabezados, etc.

- **Reconfiguración (MUAs deben comunicarse por puerto 587).**

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.

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**.

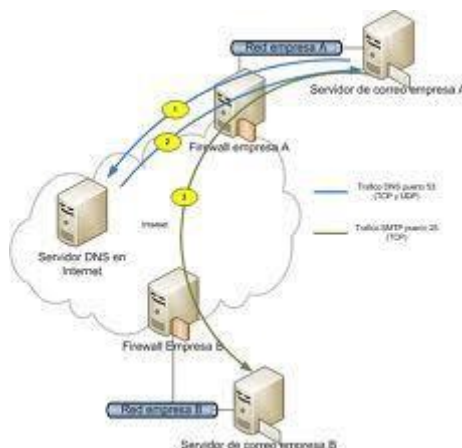
La recuperación del correo se logra a través de un programa de software llamado **MUA** (Mail User Agent [Agente Usuario de Correo]).

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**.

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

Un **servidor de correo** es una aplicación de red ubicada en un servidor en internet cuya función es parecida al Correo postal solo que en este caso los correos (otras veces llamados mensajes) que circulan, lo hacen a través de nuestras Redes de transmisión de datos y a diferencia del correo postal, por este medio solo se pueden enviar adjuntos de ficheros de cualquier extensión y no bultos o paquetes al viajar la información en formato electrónico.



Tipos de servidores de correo:

- Los **servidores POP3** (Protocolo de oficina de correos 3) retienen los mensajes de correo electrónico entrantes hasta que el usuario compruebe su correo y entonces los transfieren al equipo. POP3 es el tipo de cuenta más habitual para el correo electrónico personal. Normalmente, los mensajes se eliminan del servidor después de comprobar el correo.
- Los **servidores IMAP** (Protocolo de acceso a mensajes de Internet) permiten trabajar con los mensajes de correo electrónico sin necesidad de descargarlos antes al equipo. Puede obtener una vista previa, eliminar y organizar los mensajes directamente en el servidor de correo electrónico, donde se guardan copias de los mismos hasta que el usuario los elimina. IMAP es más frecuente en las cuentas de correo electrónico de empresas.
- Los **servidores SMTP** (Protocolo simple de transferencia de correo) administran el envío de los mensajes de correo electrónico a Internet. El servidor SMTP administra el correo electrónico saliente y se utiliza en combinación con un servidor POP3 o IMAP de correo electrónico entrante.

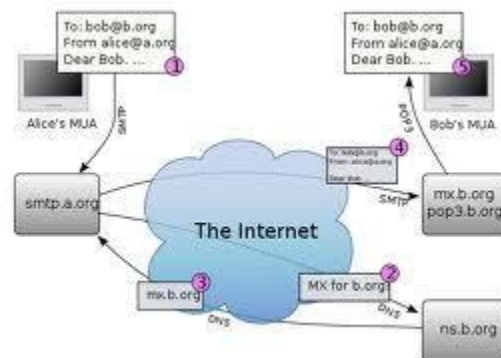
Open Relay

Un **Open Relay (Relay abierto)** es un término utilizado para describir servidores de correo que permiten a los usuarios no autorizados enviar correo. En la actualidad, los

servidores de correo no lo permiten. La mayoría de las empresas son conscientes de los problemas de seguridad relacionados y tampoco apoyan esta práctica.

Desafortunadamente, aún existen muchos servidores con relay abierto disponibles en Internet, que los hackers y spammers pueden utilizar para enviar malware y spam.

Open Relay usa 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 esté 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).

Smart Host

Un **Smart host (host inteligente)** es un tipo de servidor retransmisor de correo que permite a un servidor SMTP enrutar el correo electrónico a un servidor de correo intermedio y no directamente al servidor del destinatario.

A menudo esto requiere la autenticación de **Smart host** del remitente para verificar que el remitente tiene privilegios para obtener correos electrónicos enviados a través del host inteligente. Esta distinción es importante desde una retransmisión abierta que

reenviará los mensajes de ese remitente sin necesidad de autenticación. Las técnicas más comunes incluyen autenticación **SMTP-AUTH y POP** antes de **SMTP**.

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

Los clientes de correo electrónico, son **programas para gestionar los mensajes** recibidos y **poder escribir nuevos**. Suelen incorporar muchas más funcionalidades que el correo web, ya que todo **el control del correo pasa a estar en el ordenador del usuario**. Por ejemplo, algunos incorporan potentes filtros anti-correo no deseado.

Por el contrario, necesitan que **el proveedor de correo ofrezca este servicio**, ya que no todos permiten usar un programa especializado (algunos sólo dan correo web). En caso de que sí lo permita, el proveedor tiene que explicar detalladamente cómo hay que configurar el programa de correo. Esta información siempre está en su sitio web, ya que es imprescindible para poder hacer funcionar el programa, y es distinta en cada proveedor. Entre los datos necesarios están: **tipo de conexión (POP o IMAP), dirección del servidor de correo, nombre de usuario y contraseña**. Con estos datos, el programa ya es capaz de obtener y descargar nuestro correo.



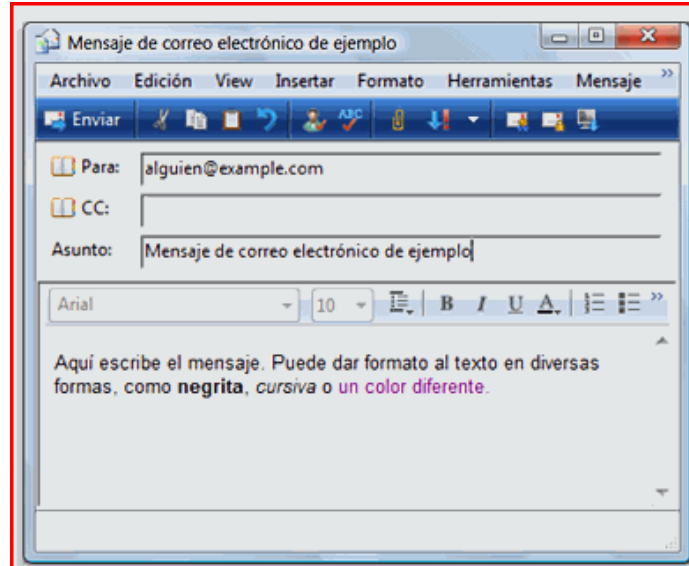
El funcionamiento de un programa de correo es muy diferente al de un correo web, ya que **un programa de correo descarga de golpe todos los mensajes que tenemos disponibles, y luego pueden ser leídos sin estar conectados a Internet** (además, se quedan grabados en el ordenador). En cambio, en un sitio web se leen de uno en uno, y hay que estar conectado a la red todo el tiempo.

Algunos ejemplos de programas que realizan las funciones de cliente de correo electrónico son **Mozilla Thunderbird, Outlook Express y Eudora**.

- 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 más 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 telefónicas gratuitas?

No es lo mismo que:

Llamadas telefónicas 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.

- Direcciones, cuentas de correo y servidores DNS.

Direcciones

Una **dirección de correo electrónico** es un **conjunto de palabras que identifican** a una persona que **puede enviar y recibir correo**. Cada dirección es única y pertenece siempre a la misma persona. Un ejemplo es **persona@servicio.com**.

Que se lee persona arroba servicio punto com. El signo @ (llamado arroba) siempre está en cada dirección de correo, y la divide en dos partes: el nombre de usuario (a la izquierda de la arroba; en este caso, persona), y el dominio en el que está (lo de la derecha de la arroba; en este caso, servicio.com). La arroba también se puede leer "en", ya que persona@servicio.com identifica al usuario persona que está en el servidor servicio.com (indica una relación de pertenencia).



Una **dirección de correo se reconoce** fácilmente porque siempre **tiene la @**, donde la **@ significa "pertenece a..."**; en cambio, una dirección de página web no. Por ejemplo, mientras que **http://www.servicio.com/** puede ser

una página web en donde hay información (como en un libro), **persona@servicio.com** es la dirección de un correo: un buzón a donde se puede escribir.

Lo que hay **a la derecha de la arroba** es precisamente **el nombre del proveedor** que da **el correo**, y por tanto es algo que el usuario no puede cambiar. Por otro lado, **lo que hay a la izquierda** depende normalmente de la elección del usuario, y **es un identificador cualquiera, que puede tener letras, números, y algunos signos**. Es aconsejable elegir en lo posible una dirección fácil de memorizar para así facilitar la transmisión correcta de ésta a quien desee escribir un correo al propietario, puesto que es necesario transmitirla de forma exacta, letra por letra. Un solo error hará que no lleguen los mensajes al destino.

Es indiferente que las letras que integran la dirección estén escritas en mayúscula o minúscula. Por ejemplo, persona@servicio.com es igual a **Persona@Servicio.Com**.

Cuentas de correo

Servicio online que **provee un espacio para la recepción, envío y almacenamiento de mensajes de correo** electrónico en internet. Una cuenta de e-mail se asocia a un único usuario, el cual puede acceder a su cuenta a través de un nombre de usuario y contraseña. **Las cuentas de e-mail suelen ser servicios que ofrecen empresas de forma gratuita** (los más populares) **o de pago**. Algunos de estos servicios populares son **Gmail de Google, Yahoo! Mail de Yahoo! Y Hotmail de Microsoft**. Los servicios mencionados anteriormente son todos del tipo webmail.

La imagen muestra una interfaz web para crear una cuenta de correo. Hay campos para 'nombre de la cuenta' y 'contraseña'. En la parte inferior, hay una sección 'opciones de espacio' con un campo de texto y un botón 'Crear cuenta'.

El servicio de cuentas de correo es ofrecido por servidores de mail, que son los encargados de recibir, almacenar y/o enviar mensajes de e-mail, empleando **POP3 y SMTP** para la recepción y envío respectivamente. No todos los proveedores de servicios de correo electrónico ofrecen acceso **por POP3**, sino que sólo admiten acceso a los e-mails por web. Algunos servicios requieren un pago por parte de sus usuarios para acceder **al POP3**.

Servidores DNS

Un Registro MX' o **Mail eXchange Record** (registro de intercambio de correo) es un tipo de registro, un recurso DNS que especifica cómo debe ser encaminado un correo electrónico en Internet. Los registros MX apuntan a los servidores a los cuales envían

un correo electrónico, y a cuál de ellos debería ser enviado en primer lugar, por prioridad.

Cuando un mensaje de correo electrónico es enviado a través de Internet, **el remitente** (el agente de transferencia de correo - **MTA** Mail Transfer Agent) **hace una petición al DNS solicitando el registro MX para los nombres de dominio de destino**. El nombre de dominio es la parte de la dirección de correo que va a continuación de la "@". Esta consulta devuelve una lista de nombres de dominios de servidores de intercambio de correo que aceptan correo entrante para dicho dominio, junto con un número de preferencia.

Entonces **el agente emisor** (o remitente) intenta establecer una **conexión SMTP** (Simple Mail Transfer Protocol - Protocolo Simple de Transferencia de Correo) hacia uno de estos **servidores**, comenzando con el que tiene el número de preferencia más pequeño, y enviando el mensaje al primer **servidor con el cual puede establecer una conexión**. Si **no hay registros MX** disponibles, una segunda petición es **solicitada al registro A** (A Record) **del dominio** en su lugar.

El mecanismo **MX permite usar múltiples servidores de correo para un solo dominio** y establece el orden en el cual deberían ser interrogados, aumentando la probabilidad que el correo pueda ser entregado y proporcionando la capacidad de distribuir el procesamiento del correo entrante a través de múltiples servidores físicos. Esta característica resulta muy útil aplicada a un cluster de alta disponibilidad con puertas de enlace de correo baratas, que son capaces de procesar cientos de mensajes por segundo (además de poner en cuarentena o quitar spam y/o virus).

El mecanismo **MX no garantiza la capacidad de proporcionar un servicio de correo en puertos TCP y UDP alternativos**, ni tampoco la del balance de carga en un conjunto de servidores de igual prioridad (mediante la asignación de valores de carga para cada uno). A fecha de 2004, algunos MTA (Mail Transfer Agent), el más notable de ellos exim, soportan el uso de SRV records para la publicación de direcciones IP, puertos, prioridad y peso de los servidores de correo.

Para **comprobar el registro MX de un dominio en Windows**, se puede abrir una ventana de línea de comandos (pulsar Inicio->Ejecutar, y escribir cmd). Al aparecer la ventana de línea de comandos se debe escribir nslookup y pulsar enter. Luego se escribe "set type=mx" sin comillas y se pulsa enter. Entonces se escribe "server <DNS>" (donde <DNS> puede ser dominioservidor.com) y se presiona enter. Por último se introduce el nombre de dominio, como wikipedia.org, se pulsa enter, y aparecerá el registro MX.

- Protocolos y servicios de descarga de correo: SMTP/ESMTP, POP, IMAP.

SMTP

Simple Mail Transfer Protocol (SMTP) Protocolo Simple de Transferencia de **Correo**, es un protocolo de la **capa de aplicación**. **Protocolo de red** basado en textos utilizados para el intercambio de mensajes de **correo electrónico** entre **computadoras** u otros dispositivos (**PDA's, teléfonos móviles, etc.**). Está definido en el **RFC 2821** y es un estándar oficial de Internet.

Funcionamiento

SMTP se basa en el modelo **cliente-servidor**, donde un cliente envía un mensaje a uno o varios receptores. La comunicación entre el cliente y el servidor consiste enteramente en líneas de texto compuestas por caracteres **ASCII**. El tamaño máximo permitido para estas líneas es de 1000 caracteres.

Las respuestas del servidor constan de un código numérico de tres dígitos, seguido de un texto explicativo. El número va dirigido a un procesamiento automático de la respuesta por autómata, mientras que el texto permite que un humano interprete la respuesta. En el protocolo SMTP todas las órdenes, réplicas o datos son líneas de texto, delimitadas por el carácter <CRLF>. Todas las réplicas tienen un código numérico al comienzo de la línea.

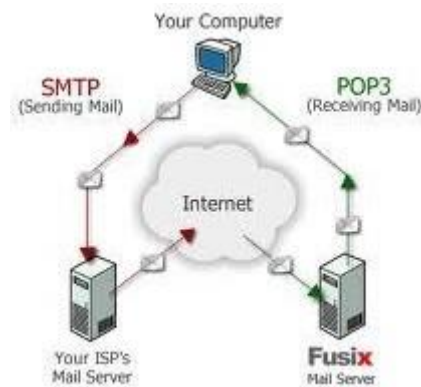
En el conjunto de protocolos **TCP/IP**, el SMTP va por encima del **TCP**, usando normalmente el puerto 25 en el servidor para establecer la conexión.

POP

El protocolo **POP** (Protocolo de oficina de correos), como su nombre lo indica, permite recoger el correo electrónico en un servidor remoto (servidor POP). Es necesario para las personas que no están permanentemente conectadas a Internet, ya que así pueden consultar sus correos electrónicos recibidos sin que ellos estén conectados.

Existen dos versiones principales de este protocolo, POP2 y POP3, a los que se le asignan los puertos 109 y 110 respectivamente, y que funcionan utilizando comandos de texto radicalmente diferentes.

Al igual que con el protocolo SMTP, el protocolo POP (POP2 y POP3) funciona con comandos de texto enviados al servidor POP. Cada uno de estos comandos enviados por el cliente (validados por la cadena CR/LF) está compuesto por una palabra clave, posiblemente acompañada por uno o varios argumentos, y está seguido por una respuesta del servidor POP compuesta por un número y un mensaje descriptivo.



IMAP

Internet Message Access Protocol, o su acrónimo **IMAP**, es un protocolo de red de acceso a mensajes electrónicos almacenados en un servidor. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet. IMAP tiene varias ventajas sobre POP, que es el otro protocolo empleado para obtener correo desde un servidor. Por ejemplo, es posible especificar en IMAP carpetas del lado servidor. Por otro lado, es más complejo que POP ya que permite visualizar los mensajes de manera remota y no descargando los mensajes como lo hace POP.

- **Funcionamiento del servicio de correo electrónico.**

Escritura del mensaje

Se pueden mandar mensajes entre computadores personales o entre dos terminales de una computadora central. Los mensajes se archivan en un buzón (una manera rápida de mandar mensajes). Cuando una persona decide escribir un correo electrónico, su programa (o correo web) le pedirá como mínimo tres cosas:

- **Destinatario:** una o varias direcciones de correo a las que ha de llegar el mensaje
- **Asunto:** una descripción corta que verá la persona que lo reciba antes de abrir el correo
- El propio **mensaje**. Puede ser sólo texto, o incluir formato, y no hay límite de tamaño

Además, se suele dar la opción de incluir **archivos adjuntos** al mensaje. Esto permite traspasar datos informáticos de cualquier tipo mediante el correo electrónico.

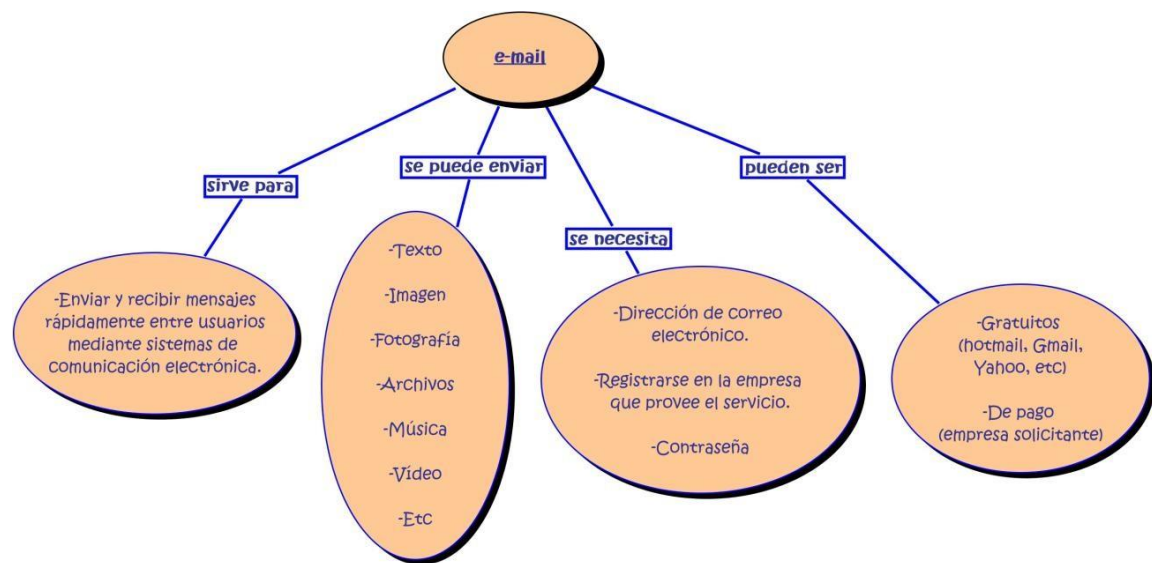
Para especificar el **destinatario** del mensaje, se escribe su dirección de correo en el campo llamado **Para** dentro de la interfaz (ver imagen de arriba). Si el destino son varias personas, normalmente se puede usar una lista con todas las direcciones, separadas por comas o punto y coma.

Además del campo **Para** existen los campos **CC** y **CCO**, que son opcionales y sirven para hacer llegar copias del mensaje a otras personas:

- **Campo CC (Copia de Carbón):** quienes estén en esta lista recibirán también el mensaje, pero verán que no va dirigido a ellos, sino a quien esté puesto en el campo **Para**. Como el campo **CC** lo ven todos los que reciben el mensaje, tanto el destinatario principal como los del campo **CC** pueden ver la lista completa.
- **Campo CCO (Copia de Carbón Oculta):** una variante del **CC**, que hace que los destinatarios reciban el mensaje sin aparecer en ninguna lista. Por tanto, el campo **CCO** nunca lo ve ningún destinatario.

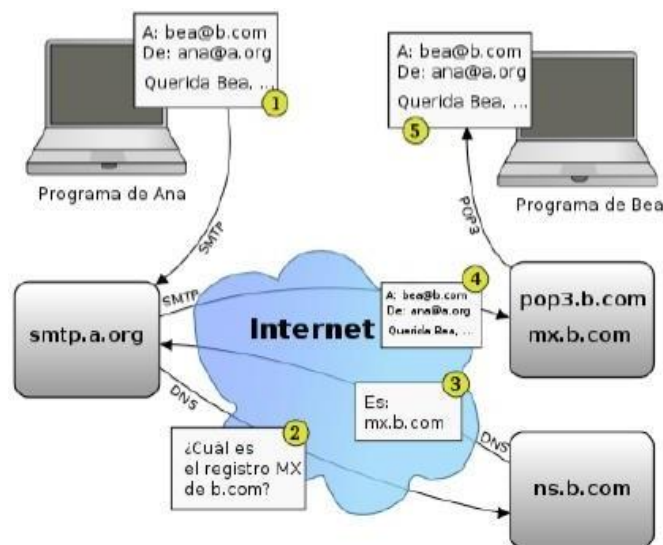
Un ejemplo: *Ana* escribe un correo electrónico a *Beatriz* (su profesora), para enviarle un trabajo. Sus compañeros de grupo, *Carlos* y *David*, quieren recibir una copia del mensaje como comprobante de que se ha enviado correctamente, así que les incluye en el campo **CC**. Por último, sabe que a su hermano *Esteban* también le gustaría ver este trabajo aunque no forma parte del grupo, así que le incluye en el campo **CCO** para que reciba una copia sin que los demás se enteren. Entonces:

- *Beatriz* recibe el mensaje dirigido a ella (sale en el campo **Para**), y ve que *Carlos* y *David* también lo han recibido.
- *Carlos* recibe un mensaje que no va dirigido a él, pero ve que aparece en el campo **CC**, y por eso lo recibe. En el campo **Para** sigue viendo a *Beatriz*.
- *David*, igual que *Carlos*, ya que estaban en la misma lista (**CC**).
- *Esteban* recibe el correo de *Ana*, que está dirigido a *Beatriz*. Ve que *Carlos* y *David* también lo han recibido (ya que salen en el **CC**), pero no se puede ver a él mismo en ninguna lista, cosa que le extraña. Al final, supone que es que *Ana* le incluyó en el campo **CCO**.



Envío

El envío de un mensaje de correo es un proceso largo y complejo. Éste es un esquema de un caso típico:



En este ejemplo ficticio, *Ana* (**ana@a.org**) envía un correo a *Bea* (**bea@b.com**). Cada persona está en un servidor distinto (una en a.org, otra en b.com), pero éstos se pondrán en contacto para transferir el mensaje. Por pasos:

- 1- *Ana* escribe el correo en su programa **cliente de correo electrónico**. Al darle a *Enviar*, el programa contacta con **el servidor de correo** usado por *Ana* (en este caso, smtp.a.org). Se comunica usando un lenguaje conocido como **protocolo SMTP**. Le transfiere el correo, y le da la orden de enviarlo.
- 2- El servidor SMTP ve que ha de entregar un correo a alguien del dominio b.com, pero no sabe con qué ordenador tiene que contactar. Por eso consulta a su **servidor DNS** (usando el protocolo **DNS**), y le pregunta quién es el encargado

de gestionar el correo del dominio b.com. Técnicamente, le está preguntando el **registro MX** asociado a ese dominio.

- 3- Como respuesta a esta petición, el servidor DNS contesta con el **nombre de dominio** del servidor de correo de *Bea*. En este caso es mx.b.com; es un ordenador gestionado por el **proveedor de Internet** de *Bea*.
- 4- El servidor SMTP (smtp.a.org) ya puede contactar con mx.b.com y transferirle el mensaje, que quedará guardado en este ordenador. Se usa otra vez el protocolo **SMTP**.
- 5- Más adelante (quizás días después), *Bea* aprieta el botón "*Recibir nuevo correo*" en su programa **cliente de correo**. Esto empieza una conexión, mediante el protocolo **POP3** o **IMAP**, al ordenador que está guardando los correos nuevos que le han llegado. Este ordenador (pop3.b.com) es el mismo que el del paso anterior (mx.b.com), ya que se encarga tanto de recibir correos del exterior como de entregárselos a sus usuarios. En el esquema, *Bea* recibe el mensaje de *Ana* mediante el protocolo POP3.

Ésta es la secuencia básica, pero pueden darse varios casos especiales:

- Si ambas personas están en la misma red (una Intranet de una empresa, por ejemplo), entonces no se pasa por Internet. También es posible que el servidor de correo de *Ana* y el de *Bea* sean el mismo ordenador.
- *Ana* podría tener instalado un servidor SMTP en su ordenador, de forma que el paso 1 se haría en su mismo ordenador. De la misma forma, *Bea* podría tener su servidor de correo en el propio ordenador.
- Una persona puede no usar un programa de correo electrónico, sino un webmail. El proceso es casi el mismo, pero se usan conexiones HTTP al webmail de cada usuario en vez de usar SMTP o IMAP/POP3.
- Normalmente existe más de un servidor de correo (MX) disponible, para que aunque uno falle, se siga pudiendo recibir correo.

Si el usuario quiere puede almacenar los mensajes que envía, bien de forma automática (con la opción correspondiente), bien sólo para los mensajes que así lo desee. Estos mensajes quedan guardados en la carpeta "Enviados".

Recepción

Cuando una persona recibe un mensaje de correo electrónico puede verse en la bandeja de entrada un resumen de él:

- **Remitente (o De o De: o From o From: -en inglés-):** esta casilla indica quién envía el mensaje. Puede aparecer el nombre de la persona o entidad que nos lo envía (o su apodo o lo que desee el remitente). Si quien envía el mensaje no ha configurado su programa o correo web al respecto aparecerá su dirección de email.
- **Asunto:** en este campo se ve el tema que trata el mensaje (o lo que el remitente de él desee). Si quien envía el mensaje ha dejado esta casilla en blanco se lee [ninguno] o [sin asunto].
 - Si el mensaje es una respuesta el asunto suele empezar por RE: o Re: (abreviatura de responder o *reply* -en inglés-, seguida de dos puntos). Aunque según de dónde proceda el mensaje pueden aparecer An: (del alemán *antwort*), Sv: (del sueco *svar*), etc.
 - Cuando el mensaje procede de un reenvío el asunto suele comenzar por RV: (abreviatura de reenviar) o Fwd: (del inglés *forward*), aunque a veces empieza por Rm: (abreviatura de remitir).
- **Fecha:** esta casilla indica cuándo fue enviado el mensaje o cuándo ha llegado a la bandeja de entrada del receptor. Puede haber dos casillas que sustituyan a este campo, una para indicar la fecha y hora de expedición del mensaje y otra para expresar el momento de su recepción

Además pueden aparecer otras casillas como:

- **Tamaño:** indica el espacio que ocupa el mensaje y, en su caso, fichero(s) adjunto(s).
- **Destinatarios (o Para o Para: o To o To: -en inglés-):** muestra a quiénes se envió el mensaje.
- **Datos adjuntos:** si aparece una marca (habitualmente un clip) significa que el mensaje viene con uno o varios ficheros anexos.
- **Prioridad:** expresa la importancia o urgencia del mensaje según el remitente (alta -se suele indicar con un signo de exclamación-, normal -no suele llevar marca alguna- o baja -suele indicarse con una flecha apuntando para abajo-).
- **Marca (de seguimiento):** si está activada (p.e. mostrando una bandera) indica que hay que tener en cuenta este mensaje (previamente lo ha marcado la persona que lo ha recibido).
- **Inspeccionar u omitir:** pinchando en esta casilla se puede marcar el mensaje para inspeccionarlo (suelen aparecer unas gafas en la casilla y ponerse de color llamativo -normalmente rojo- las letras de los demás campos). Pinchando otra

vez se puede marcar para omitirlo (suele aparecer el símbolo de "prohibido el paso" en este campo y ponerse en un tono suave -normalmente gris- las letras de las demás casillas). Pinchando una vez más volvemos a dejar el mensaje sin ninguna de las dos marcas mencionadas.

- **Cuenta:** Si utilizamos un **cliente de correo electrónico** configurado con varias cuentas de correo esta casilla indica a cuál de ellas ha llegado el mensaje en cuestión.
- **Primeras palabras del (cuerpo del) mensaje.**

Los mensajes recibidos pero sin haber sido leídos aún suelen mostrar su resumen en negrita. Después de su lectura figuran con letra normal. A veces si seleccionamos estos mensajes sin abrirlos podemos ver abajo una previsualización de su contenido.

Si el destinatario desea leer el mensaje tiene que abrirlo (normalmente haciendo (doble) clic sobre el contenido de su asunto con el puntero del ratón). Entonces el receptor puede ver un encabezado arriba seguido por el cuerpo del mensaje. En la cabecera del mensaje aparecen varias o todas las casillas de arriba mencionadas (salvo las primeras palabras del cuerpo del mensaje). Los ficheros adjuntos, si existen, pueden aparecer en el encabezado o debajo del cuerpo del mensaje.

Una vez que el destinatario ha recibido (y, normalmente, leído) el mensaje puede hacer varias cosas con él. Normalmente los sistemas de correo (tanto programas como *correo web*) ofrecen opciones como:

- **Responder:** escribir un mensaje a la persona que ha mandado el correo (que es sólo una). Existe la variante **Responder a todos**, que pone como destinatarios tanto al que lo envía como a quienes estaban en el campo CC.
- **Reenviar (o remitir):** pasar este correo a una tercera persona, que verá quién era el origen y destinatario original, junto con el cuerpo del mensaje. Opcionalmente se le puede añadir más texto al mensaje o borrar los encabezados e incluso el cuerpo (o parte de él) de anteriores envíos del mensaje.
- **Marcar como spam:** separar el correo y esconderlo para que no moleste, de paso instruyendo al programa para que intente detectar mejor mensajes parecidos a éste. Se usa para evitar la publicidad no solicitada (*spam*).
- **Archivar:** guardar el mensaje en el ordenador, pero sin borrarlo, de forma que se pueda consultar más adelante. Esta opción no está en forma explícita, ya que estos programas guardan los mensajes automáticamente.
- **Borrar:** Se envía el mensaje a una carpeta *Elementos eliminados* que puede ser vaciada posteriormente.

- **Mover a carpeta o Añadir etiquetas:** algunos sistemas permiten catalogar los mensajes en distintos apartados según el tema del que traten. Otros permiten añadir marcas definidas por el usuario (ej: "trabajo", "casa", etc.).

- **Cuentas de correo, alías y buzones de correo.**

Una **cuenta de correo** (cuenta de e-mail, e-mail account) es un servicio online que provee un espacio para la recepción, envío y almacenamiento de mensajes de correo electrónico en internet.

Una cuenta de e-mail se asocia a un único usuario, el cual puede acceder a su cuenta a través de un nombre de usuario y contraseña.



Un **buzón de correo** es un espacio donde poder almacenar correos electrónicos. Se pueden visualizar mediante un cliente de correo (Outlook) o bien vía internet mediante Webmail. Los buzones de correos tienen una limitación de espacio. Puedes crear redirecciones hacia otros buzones de correo. Puedes crear autorespondedores para cada mensaje que se reciba.

Un **alias** es la primera parte que forma un correo que esta antes de la @, por ejemplo el endavid@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.



Los alias son nombres equivalentes que tu programa de Correo (y sólo el tuyo) va a reconocer como destino de tus mensajes. Si otra persona quisiera utilizar uno de los alias que te has definido tú, tendría que definírselo antes, él también en su propia libreta.

Por ejemplo, puedes definir en tu libreta que merche a secas sea tu alias de mdura@iata.csic.es . Así, cuando envíes un mensaje a merche, tu programa de Correo sustituirá ese alias por la dirección correcta.

También puedes definir una lista: es como un alias pero que apunta a un grupo de personas en vez de a una sólo. Por ejemplo, puedes crear un alias *mus* que este dirigido a alfredo@uv.es, jaime@deptr.upv.es, rosa@agri.gv.es. Cuando mandes un mensaje a *mus*, convocando la próxima partida de naipes, tu programa de Correo lo multiplicará, enviando una copia a cada una de esas direcciones.

Aparte de esos alias y listas personales, también puede haberlos públicos, si el ordenador que sirve el correo en el destino ha sido configurado para reconocerlos. Por ejemplo, mercedes.dura@iata.csic.es también identifica a mdura@iata.csic.es . Y la lista pública iata@iata.csic.es engloba a todas las personas que tienen buzón de correo electrónico en el IATA por que así ha quedado establecido en nuestro servidor de Correo.

- **Estructura de los mensajes de correo electrónico.**

- Cabecera, Cuerpo, MIME.

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.

```
Delivered-To: [redacted]@gmail.com
Received: by 10.223.104.80 with SMTP id n16cs349411fao;
        Sun, 21 Jun 2009 13:01:18 -0700 (PDT)
Received: by 10.210.132.3 with SMTP id f3mr1298662ebd.55.1245614478194;
        Sun, 21 Jun 2009 13:01:18 -0700 (PDT)
Return-Path: <integrity@info.com>
Received: from mail.selvafile.com (159.Red-80-35-203.staticIP.rima-tde.net
[80.35.203.159])
        by mx.google.com with ESMTP id 28si239572eyg.24.2009.06.21.13.01.13;
        Sun, 21 Jun 2009 13:01:18 -0700 (PDT)
Received: from User ([80.122.29.250] RDNS failed) by mail.selvafile.com with
Microsoft SMTPSVC(6.0.3790.1830);
        Sun, 21 Jun 2009 22:02:38 +0200
From: "Paypal"<integrity@info.com>
Subject: Notification
Date: Sun, 21 Jun 2009 21:52:35 +0200
MIME-Version: 1.0
Content-Type: text/html;
        charset="Windows-1251"
Content-Transfer-Encoding: 7bit
X-Priority: 1
X-MSMail-Priority: High
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
```

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).

Todo mensaje de correo trae una cabecera y un cuerpo. Las cabeceras empiezan siempre con un **"From "** al comienzo de la línea y acaban con una línea en blanco. El cuerpo empieza y acaba siempre con una línea en blanco. Echemos un vistazo a los datos que son relevantes a Sendmail.

- **Tenemos en primer lugar el campo From.** Indica quién envía el mensaje.
- **Return-Path:** indica a sendmail, por donde debe ser enrutado el mensaje en caso de devolución.
- **Received:** indica todas y cada una de las máquinas por donde ha ido pasando el mensaje.
- **Message-ID:** es una etiqueta que identifica el mensaje y garantiza que sea único en toda la Internet. El método habitual consiste en formar dicho ID con el nombre de la máquina origen, la fecha del mensaje y el nombre asignado en la cola de envío.
- **X-Priority:** Indica al MTA la prioridad con que debe ser tratado un mensaje. El fichero de configuración de sendmail define diversos niveles de prioridad, asignando diversos valores a diversas etiquetas ("normal", "urgent", etc). Cuando sendmail procesa la cola de mensajes en espera de ser enviados, intenta enviar primero los de mayor prioridad.

- **Monitorización y registros del servicio de correo electrónico.**

Se deberá monitorizar, intervenir y examinar el contenido de los mensajes y buzones de los usuarios en alguna de las siguientes circunstancias:

- Cuando el responsable de la cuenta de correo lo pida, para detectar y corregir posibles problemas que afecten al normal funcionamiento de la cuenta.
- Cuando sucedan eventos que afecten al funcionamiento general del servicio, para detectar el origen y las causas del problema.
- Cuando la autoridad competente de la así lo solicite
- Por requerimiento legal



Registro de eventos

Se registran en archivos específicos el funcionamiento y uso del correo electrónico. En concreto se generan trazas de los siguientes eventos:

- Envío y recepción de mensajes.
- Acceso a los buzones de los usuarios.
- Alta, baja, modificación y consulta de cuentas de correo.
- Cambios de claves de acceso al buzón.
- Cambios en archivos de configuración personales de los usuarios.

Para cada uno de estos eventos se registra de manera detallada todos los datos concernientes al mismo: direcciones IP de los ordenadores, direcciones de correo del remitente y del destinatario, etc.

- **Servicio de correo electrónico vía web.**

El correo electrónico vía web o webmail es un servicio que permite gestionar el correo electrónico desde un sitio web. Es de gran utilidad para personas que tienen que desplazarse con frecuencia ya que con él se pueden enviar y recibir mensajes desde cualquier equipo conectado a Internet y lo ofrecen habitualmente los/as proveedores/as de acceso a Internet en sus páginas web.

El webmail suele estar basado en lenguaje HTML. Para acceder al correo electrónico suele ser utilizado con los navegadores más conocidos. Los mensajes y los ficheros adjuntos quedan almacenados en el servidor del/de la proveedor/a de correo, pudiendo accederse a ellos desde cualquier lugar remoto sin necesidad de descargarlos en ninguna máquina local. Para usar webmail es necesario que el navegador tenga habilitada la aceptación del JavaScripts y Cookies.

Ventajas

Dado que el webmail y los mensajes residen en la cuenta de alojamiento remota y no en un ordenador local, se evita la preocupación de localizar mensajes en el ordenador en que han sido descargados o fallos en la aplicación de correo electrónico.

Otras ventajas serían:

- **Siempre es accesible** desde cualquier ordenador con navegador gráfico y conectado a Internet.
- **Requiere muy pocos recursos** del sistema.
- Es muy **fácil de usar y gestionar**.
- **No requiere ninguna configuración**, simplemente el uso de los datos del/de la usuario/a de la cuenta, la contraseña y el nombre de su dominio.
- **Todas las actualizaciones y mejoras de la aplicación** se realizan de forma automática y transparente.
- **Se puede enviar y recibir correos** a través de los navegadores más populares (Internet Explorer, Netscape Navigator, Opera, etc.) desde los sistemas operativos más habituales (Windows, Macintosh, Linux, etc.).

Características

Básicamente permiten las mismas prestaciones que el correo electrónico (e-mail).

Destacamos:

- Envío de mensajes a múltiples destinatarios/as.
- Agenda de direcciones online.
- Envío y recepción de archivos adjuntos por mensaje.
- Adición automática de una firma personal al enviar un mensaje.

- Creación de carpetas personales para ayudarle en la gestión y categorización de sus mensajes.

Los ficheros que se quieren adjuntar deben encontrarse en el ordenador local y no en la cuenta remota de alojamiento compartido.

Ejemplos de correo webmail:

-  Hotmail
-  Yahoo
-  Gmail
-  Mixmail

- **Correo seguro:**

- Firma digital y cifrado de mensajes.

No hay nada más fácil que leer los correos de otras personas, ya que viajan desnudos por la Red. Valga la siguiente analogía. Un correo electrónico normal es como una tarjeta postal sin sobre, que puede leer todo el que tenga interés. Por consiguiente, la mejor manera de preservar la intimidad en los mensajes de correo electrónico es recurrir a la criptografía.

Por medio de potentes técnicas criptográficas, el contenido del mensaje puede ser enviado cifrado, permitiendo así que sólo el destinatario legítimo del correo sea capaz de leerlo. Con este mecanismo se garantiza la confidencialidad del correo. Sin embargo, los modernos sistemas de seguridad del correo, como PGP y otros, no se limitan a cifrar el contenido de los mensajes intercambiados, sino que también añaden otros servicios, como la integridad, que garantiza que el contenido del mensaje no ha sido alterado por el camino; la autenticación, que asegura la identidad del remitente del correo, de manera que podemos estar seguros de que fue escrito por quien lo envió y no ha sido falsificado; y el no repudio, que nos protege frente a que posteriormente el que envió el correo (o lo recibió de nosotros) alegue posteriormente no haberlo enviado (o recibido si era el destinatario). Estos últimos servicios se prestan mediante las firmas digitales.



Veamos a continuación muy brevemente cómo funcionan estas técnicas:

Cifrado

El cifrado consiste en transformar un texto en claro (inteligible por todos) mediante un mecanismo de cifrado en un texto cifrado, gracias a una información secreta o clave de cifrado. Se distinguen dos métodos generales de cifrado:

Cifrado simétrico

Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el criptosistema es simétrico o de clave secreta (v. figura). Estos sistemas son mucho más rápidos que los de clave pública, y resultan apropiados para el cifrado de grandes volúmenes de datos.

Ésta es la opción utilizada para cifrar el cuerpo del mensaje. Para ello se emplean algoritmos como IDEA, RC5, DES, TRIPLE DES, etc.

Cifrado asimétrico

Por otro lado, cuando se utiliza una pareja de claves para separar los procesos de cifrado y descifrado, se dice que el criptosistema es asimétrico o de clave pública. Una clave, la privada, se mantiene secreta, mientras que la segunda clave, la pública, es conocida por todos. De forma general, las claves públicas se utilizan para cifrar y las privadas, para descifrar (v. figura). El sistema posee la propiedad de que a partir del conocimiento de la clave pública no es posible determinar la clave privada ni descifrar el texto con ella cifrado. Los criptosistemas de clave pública, aunque más lentos que los simétricos, resultan adecuados para los servicios de autenticación, distribución de claves de sesión y firmas digitales, como se explicará posteriormente. Se utilizan los algoritmos de RSA, Diffie-Hellman, etc.

En general, el cifrado asimétrico se emplea para cifrar las claves de sesión utilizadas para cifrar el documento, de modo que puedan ser transmitidas sin peligro a través de la Red junto con el documento cifrado, para que en recepción éste pueda ser descifrado. La clave de sesión se cifra con la clave pública del destinatario del mensaje, que aparecerá normalmente en una libreta de claves públicas.

El cifrado asimétrico se emplea también para firmar documentos y autenticar entidades, como se describe a continuación en firmas digitales.

Firmas Digitales

En principio, basta con cifrar un documento con la clave privada para obtener una firma digital segura, puesto que nadie excepto el poseedor de la clave privada puede

hacerlo. Posteriormente, cualquier persona podría descifrarlo con la clave pública, demostrándose así la identidad del firmante.

En la práctica, debido a que los algoritmos de clave pública son muy ineficaces a la hora de cifrar documentos largos, los protocolos de firma digital se implementan junto con funciones unidireccionales de resumen (hash), de manera que en vez de firmar un documento, se firma un resumen del mismo.

Este mecanismo implica el cifrado, mediante la clave privada del emisor, del resumen de los datos, que serán transferidos junto con el mensaje. Éste se procesa una vez en el receptor, para verificar su integridad.

Por lo tanto, los pasos del protocolo son:

- 1) A genera un resumen del documento.
- 2) A cifra el resumen con su clave privada, firmando por tanto el documento.
- 3) A envía el documento junto con el resumen firmado a B.
- 4) B genera un resumen del documento recibido de A, usando la misma función unidireccional de resumen. Después descifra con la clave pública de A el resumen firmado. Si el resumen firmado coincide con el resumen que él ha generado, la firma es válida.

De esta forma se ofrecen conjuntamente los servicios de no repudio, ya que nadie excepto A podría haber firmado el documento, y de autenticación, ya que si el documento viene firmado por A, podemos estar seguros de su identidad, dado que sólo él ha podido firmarlo. En último lugar, mediante la firma digital se garantiza asimismo la integridad del documento, ya que en caso de ser modificado, resultaría imposible hacerlo de forma tal que se generase la misma función de resumen que había sido firmada.

- **Veracidad del correo:**

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

Spam

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 denominan **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 **grupos 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.

Fraudes

El **"scam"** es una práctica fraudulenta de origen africano que consiste en obtener fondos de los usuarios de Internet por coerción al tentarlos con una suma de dinero prometiéndoles una parte. Su uso se originó en Nigeria y se le dio el nombre de "419" en referencia al artículo del Código Penal nigeriano que castiga este tipo de práctica.

El método del fraude es clásico: usted recibe un correo electrónico del único descendiente de un africano rico que falleció recientemente. Esta persona ha depositado varios millones de dólares en una empresa de seguridad financiera y la persona que lo contacta necesita que un asociado extranjero le ayude a transferir los fondos. Además, está dispuesto a pagarle un porcentaje nada despreciable si usted proporciona una cuenta donde transferir los fondos.



Al responder a un mensaje de fraude, el usuario de Internet se ve atrapado en un círculo vicioso que puede costarle cientos de dólares o hasta su vida si cae en la trampa.

Por lo general, existen dos situaciones posibles:

- El intercambio con el delincuente se hace virtualmente, en cuyo caso éste enviará a la víctima algunos "documentos oficiales" para ganarse su confianza y le solicitará un anticipo de los fondos para los honorarios del abogado, impuestos de aduana, tarifas bancarias, etc.
- O bien, presionado por el delincuente cibernético, la víctima acepta viajar a su país y llevar efectivo, en cuyo caso tendrá que gastar dinero en la estancia, en tarifas bancarias, en sobornos a empresarios y así sucesivamente.

En el mejor de los casos, la víctima regresa a su hogar habiendo perdido una cantidad de dinero considerable y, en el peor de los casos, nadie lo vuelve a ver.

Phishing es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.



Es realizado por medio de **e-mails que aparentan venir de fuentes legítimas, como bancos, empresas conocidas, universidades, tiendas, u otras**. Ellas piden que usted haga click en algún link o ingrese a determinado sitio web para "actualizar" sus datos o participar de alguna promoción. El objetivo, claro, es robar sus datos bancarios.

Cadenas

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 cadena es reenviada a aquella enorme lista de e-mails, nuevas direcciones caen en las manos de personas malintencionadas.

Virus

Debido al auge de Internet los creadores de virus han encontrado una forma de propagación masiva y espectacular de sus creaciones a través mensajes de correo electrónico, que contienen archivos Visual Basic Scripts, anexados, los cuales tienen la extensión .VBS

Los virus informáticos se extienden más fácilmente mediante los datos adjuntos en mensajes de correo electrónico o mediante mensajes de mensajería instantánea. Por tanto, nunca debe abrir un archivo adjunto de correo electrónico a menos que sepa quién envió el mensaje o a menos que esté esperando el archivo adjunto de correo electrónico. Los virus informáticos se pueden camuflar como datos adjuntos de imágenes divertidas, tarjetas de felicitación o archivos de audio y vídeo.

