IES N1 Gijón

Principado de Asturias
Consejería de Educación

# UNIDAD DE TRABAJO 5

# Servicio de correo electrónico

*Celia C. Pellico Llera*

Cofinanciado por la Unión Europea

# Contenidos

1. Introducción
2. Funcionamiento
3. Estructura de los mensajes de correo electrónico
4. Clientes de correo electrónico (MUA)
5. Servidores de correo
6. Servicio de correo electrónico vía web
7. Protocolo de transferencia de mensajes. SMTP
8. Protocolos de entrega de correo. POP/IMAP
9. SPAM
10. Seguridad

# 1. Introducción

El servicio de correo electrónico (e-mail) es uno de los más usados en Internet.
Ha sustituido en gran medida al correo tradicional, especialmente en las comunicaciones de empresa ya que, entre otras cosas, reduce notablemente los costes y agiliza las comunicaciones. Incluso el correo electrónico puede sustituir al envío de correo certificado, ya que permite el acuse de recibo que certifica la recepción de un correo por un usuario.

El servicio de correo electrónico ya se comenzó a usar en los **años 60** del siglo pasado. Mucho antes de que se desarrollara Internet ya existían una gran cantidad de usuarios de correo electrónico. En sus orígenes, el correo electrónico sólo permitía enviar mensajes de texto codificados en **ASCII**. Desde que, en los años 90, se comenzaron a desarrollar los tipos **MIME**, el correo electrónico permite adjuntar en los mensajes archivos de diversos tipos.



El servicio de correo electrónico ofrece la posibilidad de enviar mensajes a través de una red TCP/IP y, basados en el correo electrónico, han surgido otros servicios de comunicación como las listas de distribución, mensajería instantánea, software colaborativo, etc.

El correo electrónico es un servicio fácil de usar, pero su administración y configuración pueden llegar a ser muy complejas.

## Ventajas

- **Fácil de utilizar**.
- Permite el intercambio de mensajes entre usuario sin necesidad del que el emisor y receptor establezcan una conexión previa.
- **Asíncrono**: Los receptores pueden leer y responder los mensajes cuando deseen (no es una comunicación síncrona como, por ejemplo, una llamada telefónica).
- **Adjuntos**: Se intercambian mensajes de texto que pueden incluir otros objetos adjuntos, como pueden ser documentos, imágenes, programas, archivos de audio, vídeo, etc.).
- **Rapidez en la entrega**: un mensaje de correo electrónico puede llegar a su destinatario prácticamente en el momento de ser enviado.
- **Coste económico**: teniendo conexión a Internet se pueden enviar mensajes de correo electrónico sin ningún coste. Para las empresas, supone importantes ahorros en gastos de envío de cartas por correo tradicional a clientes, proveedores, trabajadores, etc.
- **Multidifusión**: es posible enviar un mismo correo a muchos destinatarios a la vez.
- **Seguridad**: sobre los mensajes se pueden establecer medidas de seguridad que eviten que puedan ser interpretados si son interceptados, que aseguran que el receptor los ha leído, y que aseguran la identidad del autor del correo.

## Desventajas

- No garantiza que el mensaje llegue a destino ni la autoría del mensaje.
- Spam, suplantación de identidad, no confidencialidad, adjuntos con software malicioso (puede ser vía de entrada de virus), etc.

# Componentes del servicio de correo electrónico

- **Mensaje**: más conocido como correo o e-mail, es la información que transmite el servicio de correo electrónico. Permiten adjuntar archivos de diversos tipos.
- **Cuentas de correo**: las identificaciones para los remitentes del correo electrónico y los destinatarios. Un usuario puede tener muchas cuentas de correo y cada cuenta de correo está registrada en un servidor de correo. Es el nombre de usuario del sistema y el dominio al que pertenece, por ejemplo: admin@asir100.net.
- **Alias**: son cuentas a las que se asocia un buzón de otra cuenta del mismo dominio.
- **Cuentas de correo redirigidas**: son cuentas a las que se asocia un buzón perteneciente a otra cuenta de otro dominio.
- **Buzón**: espacio de almacenamiento de un servidor donde guarda los mensajes destinados a usuarios para que éstos los puedan obtener. Cada usuario tiene asignado un buzón de usuario similar al buzón de nuestro domicilio donde el cartero deja las cartas dirigidas a nosotros.
- **Protocolos:**

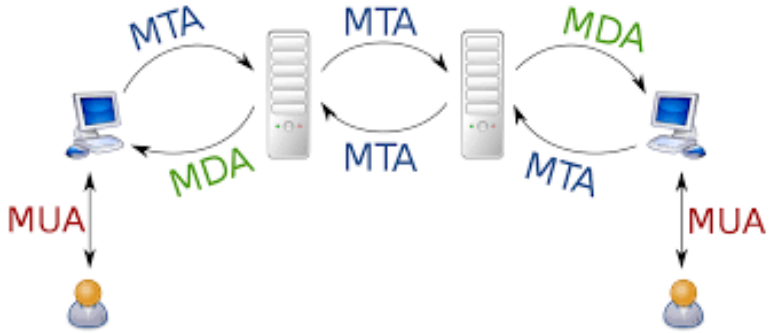
  – De transferencia: SMTP (propagación de mensajes de correo entre servidores).

  – De entrega de correo: POP3, IMAP (acceso a los buzones de correo por parte de los clientes).

- **Clientes de correo o agentes de usuario (MUA)**: programa de usuario que permiten a los usuarios enviar, recibir, manipular, archivar, borrar mensajes. Pueden actuar como clientes **POP/IMAP** en el acceso a los buzones.
- **Servidores de correo** : software que se encarga de recibir correos de un cliente o de otro servidor funcionando como cliente y de enviarlos hacia otro servidor o transferirlos hacia el usuario destino.
  - **Buzones de correo (mailbox):** Carpetas y archivos que contienen los mensajes de correo asociados a un usuario del sistema.
  - **Agentes de transferencia de correo (MTA).** Procesos encargados de recibir/enviar mensajes de correo (propagar hacia su destino) entre servidores mediante SMTP.
  - **Agentes de entrega de correo (MDA).** Procesos encargados de almacenar los mensajes de correo en los buzones de usuario (mailbox).
  - **Servidores POP/IMAP.** Procesos que permiten a los clientes de correo (MUA), acceder a los mensajes del buzón y leerlos, extraerlos, borrarlos, etc.
  - **Componentes adicionales**. Añaden funcionalidades integrándose con el MTA y el MDA. Por ejemplo serían filtros antispam que archivan mensajes sospechosos en carpetas de spam, antivirus que escanean los archivos adjuntos a los mensajes, listas de distribución, etc.

# Agentes de correo

Un agente de correo es un software que se encarga de realizar alguna operación con los mensajes de correo.




En la transmisión del correo electrónico fundamentalmente intervienen tres agentes:

- **MTA (Mail Transfer Agent)**: es el sistema que se encarga de tomar el email de un MUA o de otro MTA y entregarlo a otro MTA o a un MDA, en caso de que el email pertenezca al dominio propio del MTA. Ejemplos de MTA son postfix, exim, courier... Un agente MTA debe tener asociado un registro **MX** en una zona de un dominio para que se pueda conocer a qué equipo se tiene que enviar el correo destinado a cuentas de ese dominio. Los agentes MTA usan el protocolo SMTP cuando transfieren o reciben correo.
- **MDA (Mail Delivery Agent)**: es un software que se comunica con los MUA para entregarles el correo almacenado en los buzones de los usuarios que estén utilizando los MUA. Un MDA accede a los buzones de los usuarios y entrega los correos a los MUA utilizando el protocolo POP3 o el protocolo IMAP.
- **MUA (Mail User Agent)**: es un software de usuario donde un usuario puede enviar y recibir correos. En una MUA un usuario puede iniciar sesión con una o con varias de sus cuentas. Para cada cuenta el usuario tiene configurado cual va a ser el MTA que se encarga de la transferencia de los correos que vaya a enviar y cuál va a ser el MDA que se encarga de entregarle el correo almacenado en el buzón de usuario.

# 2. Funcionamiento

## Direcciones y cuentas de correo

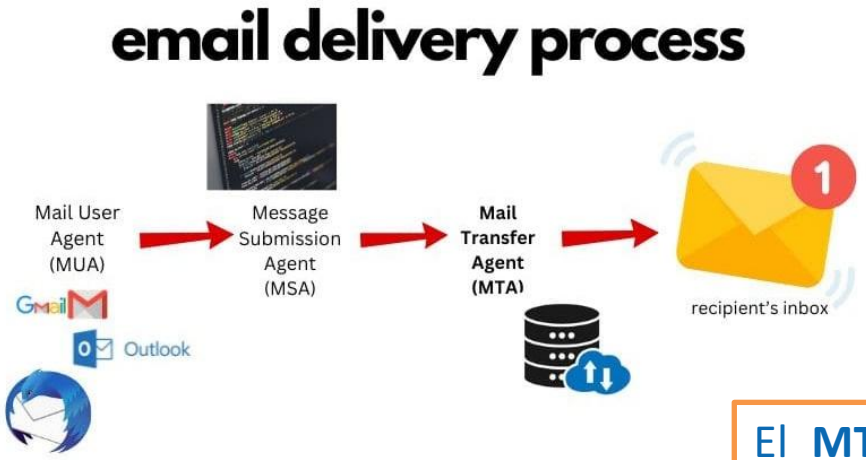
- Lo habitual es que cada dirección tenga asociada una cuenta con contraseña en un servidor de correo electrónico donde se depositan y almacenan los mensajes.
- Una dirección de correo es una cadena de caracteres en la que se permiten letras números guiones bajos y puntos separadores.
- Consta de dos partes separadas por el carácter **@** (arroba).
- La segunda parte de la dirección indica el dominio al que pertenece. Por ejemplo, en la dirección t*yrion123@educastur.es* el usuario es ***tyrion123*** y el dominio ***educastur.es***.
- Un usuario puede tener varias direcciones de correo.
- Una dirección de correo puede tener uno o varios **alias**.

Un **alias** de correo es una cuenta aparentemente normal pero que internamente no tiene asociado un buzón. Los mensajes enviados a esa dirección se redirigen a otra cuenta.
Por ejemplo, t*yrion123@educastur.es* puede tener un alias que sea t*yrion.Lanister@educastur.es.* Los mensajes enviados a esta segunda dirección se archivan en el buzón de " t*yrion123* ". La segunda dirección es un alias de la primera.

Una opción es tener dos cuentas de correo, con dos buzones separados, pero que una de ellas "*propague*" todos los mensajes a la otra. Por ejemplo, *tyrion123@educastur.es* puede **redirigir** (forward) los mensajes a *tyrion123@gmail.com.* En este caso existen dos cuentas con sus buzones respectivos, pero la primera reenvía los mensajes a la segunda y no los almacena en su buzón.

# Envío de mensajes

1. El usuario escribe un mensaje de correo utilizando un cliente de correo (de texto, gráfico o mediante navegador). Incluye un destinatario, puede incluir copia (vista u oculta) a otros destinatarios, habitualmente se indica un asunto y opcionalmente archivos adjuntos.
2. El cliente de correo (MUA) envía el mensaje al Agente de Envío de Mensajes (MSA) también software. Entonces, el MSA envía el mensaje a su servidor MTA que lo propagará al MTA de destino.
3. En destino existen varias posibilidades
   - Que se archive en el buzón de un usuario local (y llegue a destino).
   - Que no exista usuario de destino.
   - Que sea redirigido a otro buzón de correo.




El **MTA**, el **MUA** y el **MSA** son componentes del Protocolo Simple de Transferencia de Correo (**SMTP**).

**Entre dos cuentas del mismo dominio**

- Un usuario ***ana@aula.com*** utiliza un MUA para editar un correo destinado a la cuenta de usuario ***jorge@aula.com*** perteneciente al mismo dominio. Cuando Ana envía el correo, el MUA actúa como cliente SMTP para enviar el correo al MTA que actúa como servidor SMTP en el dominio **aula.com**.
- Dado que el destinatario pertenece al dominio del MTA, éste comprueba que ese destinatario tiene cuenta de usuario en el dominio. Si es así, deposita el correo en el buzón de usuario.

**Entre dos cuentas de distinto dominio**

- Un usuario ***ana@aula.com*** utiliza un MUA para editar un correo destinado a la cuenta de usuario ***luis@aulaubuntu.com*** perteneciente a otro dominio. Cuando Ana envía el correo, el MUA actúa como cliente SMTP para enviar el correo al MTA que actúa como servidor SMTP en el dominio **aula.com.**
- Dado que el destinatario no pertenece al dominio del MTA, éste envía una consulta al **servidor DNS** para averiguar a que MTA debe enviar el correo para que llegue a su destinatario. Consulta los registros **MX** del dominio **aulaubuntu.com** para obtener el nombre del servidor SMTP al que debe enviar el correo y después consulta cuál es la IP de ese servidor.
- El MTA de **aula.com** actuando como cliente SMTP envía el correo al MTA de **aulaubuntu.com** actuando como servidor SMTP.
- El MTA de **aulaubuntu.com** comprueba que el destinatario ***jorge@aulaubuntu.com*** tiene cuenta de usuario en el dominio. Si es así, deposita el correo en el buzón de usuario.

# Envío de correos y DNS

Existe una fuerte relación entre el protocolo **SMTP** de transferencia de mensajes de correo y el protocolo **DNS** de resolución de nombres, ya que una parte muy importante la dirección de correo es el domino DNS de emisor y receptor(es).

Hay que recordar que uno de los registros de recursos de los servidores DNS era del tipo **MX** que indicaba qué direcciones IP estaban asociadas a los servidores de correo de un dominio DNS.

```
..
srein.local.          IN  MX 10   smtp1.srein.local.
srein.local.          IN  MX 20   smtp2.srein.local.

smtp1.srein.local.    IN  A       172.22.0.241
smtp1.srein.local.    IN  A       172.22.0.242
..
```




# Recogida de mensajes

Cuando un usuario quiere consultar su buzón de correo para examinar los mensajes que ha recibido puede:

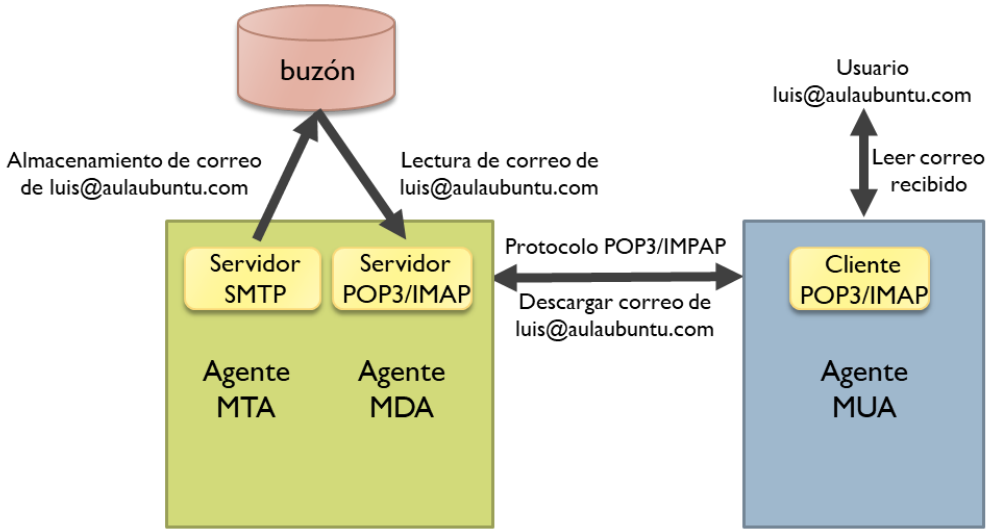
- Iniciar sesión en el servidor de correo y acceder al correo directamente o utilizando un cliente de correo local en modo texto (no es lo habitual).
- Utilizar un cliente de correo que, utilizando el protocolo POP3 o bien IMAP, consulte de forma remota el buzón de correo y le permita ver los mensajes leídos, no leídos, consultarlos, archivarlos, etc.

Como dijimos, hay dos protocolos que son utilizados para que un MUA pueda obtener el correo almacenado en los buzones de usuario y entregárselo a sus destinatarios:

- **POP3.**
- **IMAP.**

El proceso de descarga de correo se desarrolla de la siguiente forma:

- Un usuario ***luis@aulaubuntu.com*** inicia una sesión en el MUA de su equipo.
- El MUA actúa como cliente POP3 y/o IMAP y contacta con el MDA o servidor POP3/IMAP que tenga configurado usando el protocolo correspondiente.
- El MUA solicita descargar el correo de ***luis@aulaubuntu.com***.
- EL MDA del dominio **aulaubuntu.com** lee el buzón del usuario ***luis@aulaubuntu.com***, obtiene los mensajes almacenados y se los entrega al MUA.
- El MUA muestra los mensajes recibidos al usuario.




Descarga de correo desde un buzón de usuario

# 3. Estructura de los mensajes de correo electrónico

Un mensaje está dividido en tres **partes**:

- **Cabecera** o ***head*** que contiene varios campos con la información necesaria para que se pueda transmitir correctamente el mensaje. Compuesta por líneas de texto ASCII en formato ***nombre: valor*** con información que es usada para análisis, transferencia y clasificación del mensaje. Las cabeceras son incluidas y consultadas por los componentes que intervienen en la transferencia.
- **Cuerpo** o ***body*** que contiene el texto del mensaje. En un principio sólo se permitían mensajes codificados en **ASCII** (código de 7 bits). Actualmente (gracias a las extensiones MIME) se pueden incluir otro tipo de contenidos.
- **Extensiones MIME** (Multipurpose Internet Mail Extensions) 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. De esta forma se pueden usar en el cuerpo del mensaje caracteres especiales (ñ, tildes, etc.), alfabetos no latinos (árabe, chino, hebreo) y archivos de diferentes tipos (audio, video, imágenes, software, etc.)

**S/MIME** (Secure/Multipurpose Internet Mail Extensions) es un estándar para criptografía de clave pública y firmado de correo electrónico encapsulado en MIME. Desarrollado originalmente por RSA, la especificación original usó la especificación MIME. Haz clic aquí para saber más…

## Cabeceras

Contienen varias y cada una de ellas da una información relativa al mensaje de correo. Las que se utilizan con más frecuencia en los mensajes son:

- **To**: especifica la cuenta de correo del usuario destinatario del correo.
- **From**: identifica la cuenta de correo del usuario remitente.
- **CC**: indica un conjunto de destinatarios de una copia del mensaje que se envía al destinatario especificado en ***To***. Todos los destinatarios podrán ver las direcciones de las cuentas de correo de los otros destinatarios.
- **CCO** o BCC: igual que la anterior, pero en este caso cada destinatario no puede ver las direcciones de correo de los otros destinatarios.
- **Subject**: es el asunto del mensaje. Es un texto corto que describe el contenido del mensaje.
- **Reply-To**: especifica la dirección de correo electrónico en la que el remitente indica al destinatario que quiere recibir la respuesta al mensaje enviado.
- **Received**: Incluye la identidad del MTA, fecha, hora de recepción y otra información que agrega cada MTA por el que pase el mensaje.
- **Date**: indica la fecha y hora en que se ha enviado el mensaje.
- **Delivered-to**: Dirección real (sin alias) a la que se entrega el mensaje.
- **Message-id**: Identificador del mensaje
- **In-Reply-to**: Identificador del mensaje al que se responde.
- **Return-Path**: Agregada por el MTA, indica el emisor real del mensaje de correo

# 4. Clientes de correo electrónico (MUA)

Es un programa de usuario que permite que los usuarios editen y envíen mensajes de correo y obtengan el correo recibido leyendo los buzones de usuario.

Por el aumento del uso de la web para gestionar el correo, cada vez son menos utilizados.

## Funciones

- Escribir y enviar mensajes de texto, texto enriquecido, adjuntar archivos de varios tipos.
- Revisar y leer los mensajes de correo recibidos, aplicar reglas de archivado, organizar los mensajes en carpetas, etc.
- Otras funciones como firma digital, verificación de firmas, enviar/recibir mensajes cifrados, añadir firma de texto, gestionar múltiples buzones, incluir reglas de clasificación, reenvío, borrado, etc.
- Actúan como clientes SMTP y POP/IMAP para enviar y recibir mensajes. La mayoría pueden actuar como clientes con los tres protocolos, aunque algunos solo pueden actuar como clientes de un solo protocolo.

## Agentes de recuperación de correo (MRAs)

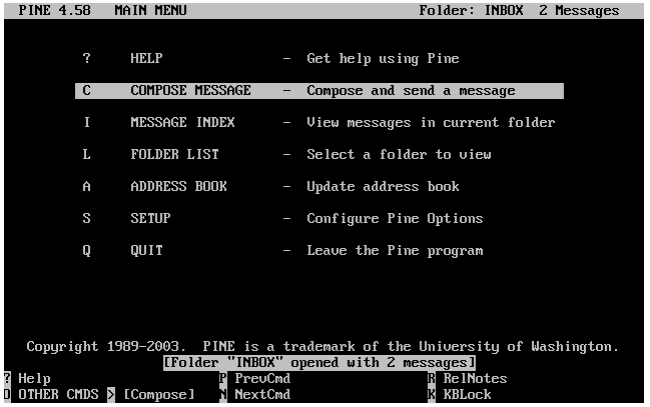
Término utilizado (poco extendido) para referirse al software que permite recuperar mensajes de correo de buzones remotos (usando POP o IMAP). Puede ser un programa aislado o estar integrado en un cliente de correo con más funcionalidades.

Existen soluciones software para flexibilizar la distribución de correo entre diferentes servidores y buzones, que permiten recuperar mensajes de buzones remotos sin la intervención directa del usuario y, almacenarlos en local o bien enviarlos mediante SMTP a otros servidores. Algunos ejemplos son Fetchmail o Getmail.

# Tipos

- **Clientes en modo texto**

Poco utilizados. Ofrecen un interfaz en modo texto a la persona usuaria. En sistemas Unix/Linux nos permiten acceder directamente al buzón del usuario (sin necesidad de servidor POP/IMAP) si están en la misma máquina que los buzones.
De este tipo son **mail**, **mutt** o **pine**.




- **Clientes gráficos**

Ofrecen un interfaz gráfico a la persona usuaria y múltiples utilidades adicionales.
Ejemplos son **Mozilla Thunderbird**, **Microsoft Outlook**, **Windows Live mail** o **Evolution, Eudora**.



- **Clientes web**

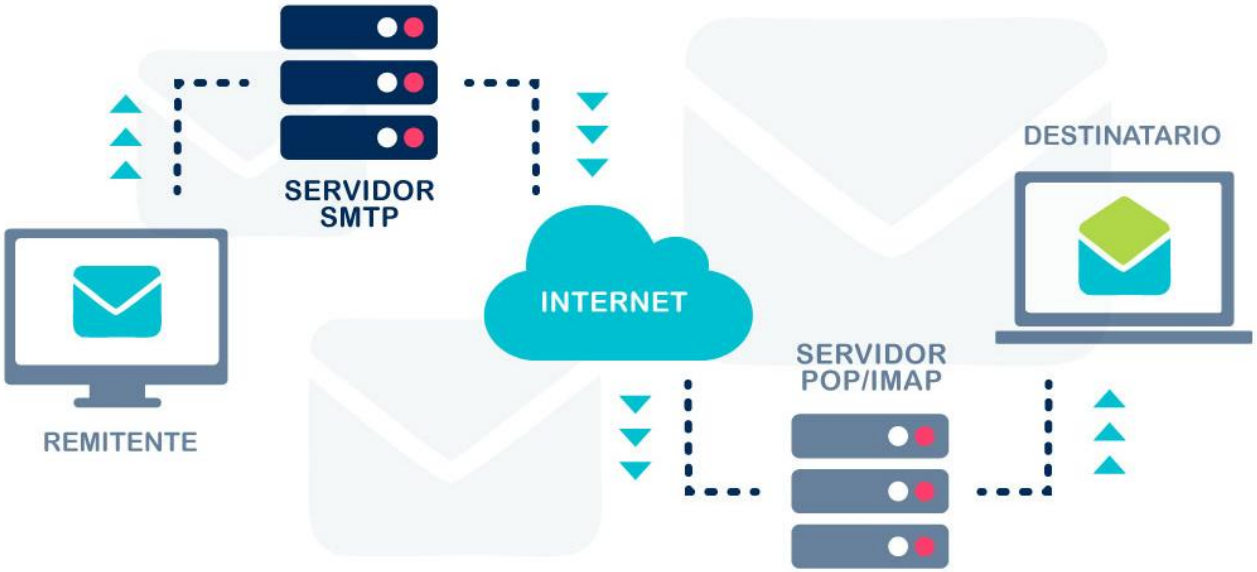
Son aplicaciones web que se ejecutan sobre un servidor web.
Facilitan la gestión del correo gracias a la flexibilidad que proporciona el acceso desde un navegador.
Algunos ejemplos son **RoundCube,** , **Horde**, **ProtonMail…**




Muchos proveedores de correo gratuito (**Google**, **Microsoft**, **Yahoo**, **gmx**) ofrecen un servicio web para gestionar sus cuentas.

# 5. Servidores de correo

Un servidor de correo es un conjunto de aplicaciones y procesos que permiten el almacenamiento y reenvío de mensajes de correo electrónico.




El componente principal de un servidor de correo es el MTA (Agente de transferencia de correo) como vimos antes. Es habitual utilizar los términos "servidor de correo" y "MTA" como sinónimos.

Aparte del MTA, los servidores de correo, pueden integrar una serie de componentes adicionales para ampliar y mejorar su funcionalidad. Pueden ejecutarse en uno o múltiples equipos, y verse como un único software integrado o como un conjunto de programas independientes que se comunican para gestionar adecuadamente el correo.

Son complejos de configurar y hay que integrarlos con otros servicios de red

# Agentes de transferencia de correo (MTA)

Son procesos encargados de la transferencia de los mensajes de correo entre equipos de una red mediante el protocolo SMTP. Permiten la recepción y envío/reenvío de mensajes de correo electrónico. Por tanto, son los responsables del encaminamiento del correo entre diferentes sistemas. Actúan como:

– Cliente SMTP para enviar correos a otros MTAs.

– Servidor SMTP para recibir correo de otros MTAs o de MUAs. Por defecto escuchan peticiones en el puerto 25/TCP.

## Recepción y reenvío de correo

Simplificando, la labor de un MTA es la recepción de correo y la retransmisión (***Relay***).

- **Recepción de correo** (almacenamiento)
  - – Se produce cuando el MTA recibe un mensaje que corresponde a un usuario local.
  - – Almacena el mensaje en el buzón (*mailbox*) del usuario.
- **Retransmisión o reenvío** (Relay).
  - – Si se recibe un mensaje cuyo destinatario no pertenece a alguno de los dominios gestionados por el servidor.
  - – Se reenvía a otro MTA que puede ser el destinatario final u otro servidor intermedio (*smart host*).

El reenvío debe estar controlado y restringido, ya que en otro caso, puede ser un origen de correo incontrolado de usuarios no legítimos. Para este control se suele requerir autenticación previa al reenvío y "*listas negras*" de direcciones, segmentos o dominios sospechosos.

## Servidores open relay

Se dice que un servidor de transferencia de correo (MTA) es **open relay** cuando permite reenviar a través de él cualquier correo recibido desde otro servidor MTA o desde un MUA. Un servidor de este tipo puede ser usado para enviar indiscriminadamente a través de él spam, virus, etc., debido a que no controlan el acceso de los remitentes.

Muchas veces estos servidores de correo pueden estar configurados en modo open relay por descuido, por desconocimiento, por error de configuración o por modificación en su configuración por un atacante, pero en otros muchos casos se instalan servidores en modo open relay para facilitar el envío de spam, de virus y de otros agentes maliciosos.

Hay elaboradas **listas negras** de servidores de correo open relay sobre los que se han detectado usos maliciosos. Las listas negras sirven a otros servidores para detectar automáticamente el correo basura o spam.

## Servidores smart host

Un servidor de correo se considera que actúa como **smart host** cuando recibe mensajes de otros MTAs que van dirigidos a destinatarios que no tienen cuentas en él. Su función es por lo tanto reenviarlos, o bien directamente al servidor del destinatario o a otro servidor que actúa como smart host.
Debe estar configurado para permitir sólo el reenvío de correos de determinados usuarios, IPs, dominios, etc. Si no es así, se consideraría *open relay*.

## Agentes de entrega de correo (MDA)

Los agentes de entrega de correo (Mail Delivery Agent) son programas invocados por los agentes de transmisión de correo (MTA) para realizar el trabajo de depositar los mensajes de correo en los buzones del usuario que es destinatario final del mensaje.

- Estos programas realizan funciones de clasificación, filtrado y distribución de correo.
- Pueden estar integrados en el MTA o ser una pieza de software adicional.
- Su labor no es transportar mensajes entre sistemas ni proporcionan un interfaz de usuario.

## Servidores POP/IMAP

Permiten a los clientes de correo (MUA) acceder a los buzones desde equipos remotos mediante los protocolos POP o IMAP.

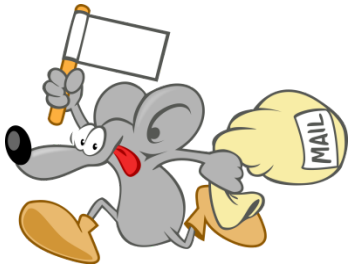
- Los servidores POP (por defecto) escuchan peticiones en el puerto **110/TCP**.
- Los servidores IMAP (por defecto) escuchan peticiones en el puerto **143/TCP**

Pueden estar integrados en el propio MTA o ser un módulo de software adicional.

## Elegir el servidor de correo

En la elección de un software servidor de correo electrónico se tendrá en cuenta que sea fácilmente configurable, que tenga muchas opciones de configuración, la gestión de cuentas de usuario y buzones, el filtrado de correos, la seguridad que implemente, etc. También se debe tener en cuenta el S.O. sobre el que se va a instalar, el consumo de recursos o la rapidez de respuesta.

Existen múltiples servidores tanto para sistemas libres como propietarios.




Algunos ejemplos son:

**Servidores SMTP (Agentes MTA)**

- **Postfix**: tiene sólo distribución para Linux con licencia IBM Public License (ir a Postfix)
- **Sendmail**: distribución para Linux con licencia GNU GPL (ir a Sendmail)

**Servidores POP3/IMAP (Agentes MDA)**

- **Dovecot**: tiene sólo distribución para Linux con licencia MIT y LGPL (ir a Dovecot)
- **Cyrus IMAP server**: tiene sólo distribución para Linux con licencia BSD (ir a Cyrus IMAP Server)

**Servidores SMTP y POP3/IMAP**

- **hMailServer**: es un servidor para sistemas Windows gratuito y de licencia GPL (ir a hMailServer)
- **Zymbra**: Es un servidor para sistemas Windows, Linux y MacOS. Tiene distribuciones de código abierto y de código cerrado. Se distribuye con licencia Yahoo Public License (ir a Zymbra)

# Componentes adicionales

En los servidores de correo es habitual añadir otro software que pueda ofrecer más funcionalidades, como pueden ser:

– **Filtros anti Spam** que, en base a examen de cabeceras y/o listas negras, redirijan correos a carpetas específicas.

– **AntiVirus**. Programas que examinen los mensajes y sus archivos adjuntos en busca de contenido malicioso.

– **Sistemas de autenticación**. Basados en cifrado de contraseñas, doble factor de autenticación, etc.

– **Gestión de listas de distribución**. Listas de correo en las que los miembros reciben mensajes de un tema concreto. Últimamente usadas para enviar publicidad o avisos a clientes de empresas, afiliados o simpatizantes de sindicatos, grupos de interés, etc.




Filtros contra spam y phishing



Protección contra malware




Accesos seguros



Política de privacidad



Cifrado de extremo a extremo



Cifrado de conocimiento cero




Protocolos de autenticación

# Integración de servidores en DNS

Para enviar un mensaje de correo y que llegue al buzón del usuario destinatario, es necesario conocer el servidor de correo encargado del buzón de usuario y su dirección IP. Será el servidor de correo del dominio al que pertenece la cuenta de correo del destinatario, el que deberá estar integrado en la zona **DNS**.

Antes de enviar un mensaje a *destino@mimail.com* desde una cuenta de correo de un dominio diferente se hace una consulta al servidor DNS responsable de la zona *mimail.com*. En este servidor se consulta:

- **Registro MX** que indique el nombre de un servidor MTA de correo para el dominio.
- **Registro A** que indique la dirección IP del servidor de correo.

Obtenida la dirección IP del servidor, se establecerá una conexión SMTP con el equipo que tiene esa dirección y se le enviará el mensaje de correo.

Aunque no es obligatorio se debe añadir un registro **PTR** en la **zona inversa** para resolver la dirección IP del servidor de correo. Esto es así porque algunos servidores de correo, al recibirlo desde otro servidor, verifican que la dirección IP corresponde al servidor remitente mediante el registro PTR (si no hay registro PTR o es incoherente con el registro A, el mensaje de correo se rechaza).

# Servidores principales y secundarios

Al igual que otros servicios (DNS, DHCP, etc.), para aumentar rendimiento, seguridad y disponibilidad, es habitual configurar múltiples servidores de correo para el mismo dominio que se puedan repartir la carga de trabajo o simplemente ofrecer alta disponibilidad caso que el servidor principal no pueda dar respuesta.

Es posible definir varios registros MX en un dominio DNS y, esta definición, va acompañada de una prioridad que indica la precedencia del servidor asociado a la IP correspondiente. Si el servidor principal no puede atender la petición, se redirige al siguiente.

```
..
srein.local.    IN      MX      10      smtp1.srein.local.
srein.local.    IN      MX      20      smtp2.srein.local.

smtp1.srein.local.      IN      A       172.22.0.241
smtp2.srein.local.      IN      A       172.22.0.242
..
```

## Servidores de primer y segundo nivel

Según el tamaño de la organización, puede ser habitual configurar varios servidores para gestionar el servicio de correo electrónico.

Una arquitectura (sin incluir servicios añadidos) es en servidores de primer y segundo nivel.

**Servidores de correo (estafetas) de primer nivel.**

– Gestionan correo entrante y saliente de la organización
– Incluyen mecanismos de seguridad (antiSpam, antivirus, filtros, etc.)
– Reciben correo de internet y lo reenvían a los servidores de segundo nivel
– Reciben correo de los servidores de segundo nivel y lo reenvían (actúan como *smarthost*) hacia Internet.
– Ofrecen acceso a los buzones desde clientes de correo mediante POP/IMAP.

**Servidores de correo (estafetas) de segundo nivel.**

– Proporcionan servicio a los usuarios de la organización (pueden tenerlos configurados como servidores SMTP en sus clientes de correo).
– Reciben mensajes de los clientes de correo de la organización y los reenvían, según el destinatario, a otros servidores de segundo nivel internos o bien a los servidores de primer nivel.
– No establecen conexiones directamente al exterior.

Esta arquitectura es flexible y en base a ella se pueden crear múltiples configuraciones que incluyen más niveles, servidores de autenticación, buzones centralizados, filtros, balanceo de carga y alta disponibilidad con servidores redundantes.

# 6. Servicio de correo electrónico vía web

Cuando queremos tener un servidor de correo para nuestro dominio podemos instalar nuestro propio servidor o contratar el servicio a un servidor de correo electrónico vía web.

Normalmente, las empresas de ***hosting*** suelen proporcionar este servicio.

El servicio contratado se dará en unas determinadas condiciones, entre otras:

- Espacio total de disco disponible para los buzones de usuarios.
- Máximo número de cuentas de usuario y tamaño máximo de los buzones de usuario.
- Sistemas de seguridad.
- Acceso a aplicaciones por los clientes que accedan al servicio.
- Tipo de asistencia.



# 7. Protocolo de transferencia de mensajes. SMTP

- Mediante el protocolo SMTP (Simple Mail Transfer Protocol) se produce el transporte de los mensajes de correo electrónico desde el ordenador del remitente hasta que se deposita en el buzón del usuario destinatario. Es el protocolo que define las reglas que utilizan los MTAs para intercambiar correos y los MUAs para enviar mensajes a los MTAs.
- El protocolo SMTP establece conexiones cliente-servidor, en las que el cliente solicita el envío de un mensaje de correo al servidor, y éste se encarga de transportarlo hacia otro servidor o bien de almacenarlo en buzones de usuario.
- Utiliza TCP como protocolo de transporte y se comunica con los clientes en el puerto **TCP 25**. Los clientes pueden usar cualquier puerto **mayor que 1024**.
- SMTP es un protocolo **inseguro** porqué transmite la información en **texto plano y no requiere autenticación**. Ahora es bastante normal que SMTP trabaje sobre conexiones seguras en las que se cifra la información. El no requerir autenticación puede ocasionar graves problemas ya que cualquier usuario podría solicitar el envío de correos a través de un servidor SMTP.
- Se han desarrollado varias mejoras en el funcionamiento del protocolo que han sido recogidas en varios ***RFC***, por ejemplo para mejorar la seguridad en el envío de correos. El protocolo establece un conjunto de comandos que los clientes pueden enviar a los servidores y los formatos de las posibles respuestas a los comandos.

# Funcionamiento básico

– El cliente (MUA o MTA) establece una conexión TCP con el servidor.

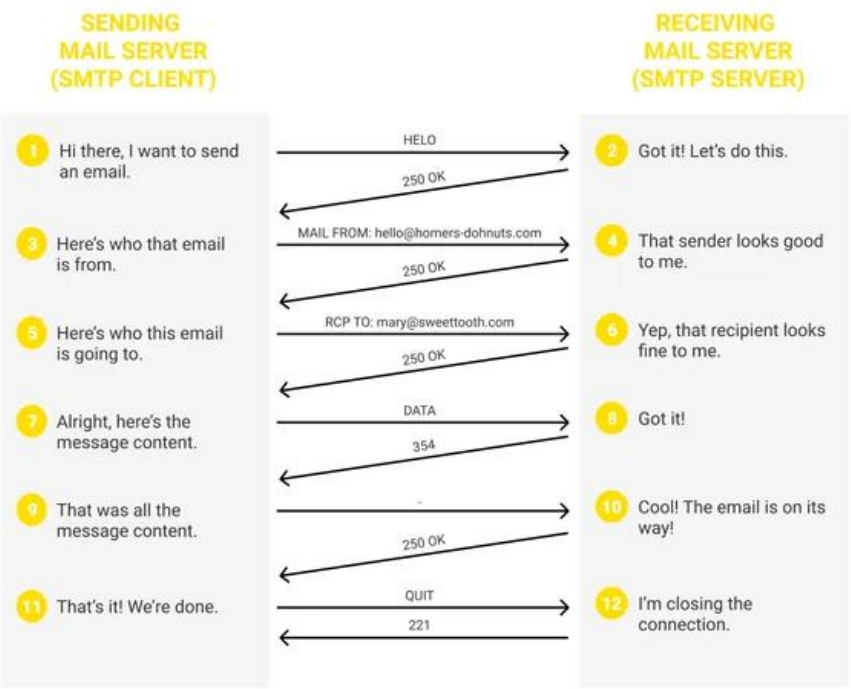
– El servidor envía la respuesta (por ejemplo código 220).

– El cliente saluda al servidor con el comando "HELO".

– El servidor acepta y responde (por ejemplo 250).

– Se siguen enviando comandos y recibiendo respuestas para enviar mensajes de correo (uno o varios).

– Una vez que se ha intercambiado el correo, se finaliza la conexión con el comando "QUIT"




[Todo lo que necesitas saber sobre SMTP]

# Comandos SMTP

Son utilizados por los clientes SMTP para realizar peticiones y enviar información.

Admiten parámetros y se terminan con ***<CR><LF>*** (retorno de carro y avance de línea).

- **HELO *nombre_máquina*** lo envía el cliente para identificarse. Aunque es válido cualquier valor en nombre_máquina, se debería escribir el nombre real.
- **MAIL FROM**: ***dirección*** para identificar al remitente del correo. En dirección hay que escribir la dirección de correo electrónico del remitente.
- **RCPT TO**: ***dirección*** para identificar al destinatario del correo. En dirección hay que escribir la dirección de correo electrónico del destinatario. Se puede enviar varias veces seguidas este comando cuando se quiere enviar un correo a varios destinatarios.
- **DATA** para indicar que se va a comenzar a enviar el mensaje.
- **SUBJECT**: ***asunto*** permite especificar el asunto del mensaje. Es obligatorio que este comando se envíe a continuación de DATA, que después se envíe una línea en blanco y después el contenido o cuerpo del mensaje. El mensaje tiene que terminar con una línea que tenga sólo un punto y pulsando después ENTER.
- **QUIT** cierra la conexión cliente servidor.
- **RSET**: Se envía para abortar la comunicación .

# Códigos de respuesta

El servidor SMTP envía respuestas al cliente para indicarle como ha sido procesado un comando. En las respuestas SMTP el servidor envía un código numérico de **3 dígitos** (por ejemplo: *250 Ok, 551 User not local*, etc.) con el que indica como ha sido procesado el comando al que corresponde la respuesta. El primero de los dígitos indica si el comando ha sido o no procesado con éxito. Los otros dos dígitos dan mayor detalle del contenido de la respuesta.

| Código | Descripción |
|---|---|
| 2xy | Respuesta positiva. La acción se realizó con éxito. Puede enviarse otro comando. |
| 3xy | Respuesta positiva temporal. Se está esperando que el cliente envíe información adicional necesaria para poder completar la acción. |
| 4xy | Respuesta pendiente. Se indica que se ha producido un error temporal y que podría enviarse el comando nuevamente para posiblemente procesarse con éxito. |
| 5xy | Respuesta negativa. Se indica que se ha producido un error permanente, se seguirá produciendo aunque se siga enviando el comando. |

Haz clic aquí para ver la lista de los códigos de respuesta SMTP

# Protocolo ESMTP

ESMTP (Extended Simple Mail Transfer Protocol) define un conjunto de extensiones del protocolo SMTP que solucionan problemas e incorporan nuevas funcionalidades y comandos.
Una de las funcionalidades destacadas es la posibilidad de utilizar autenticación (comando AUTH) entre clientes y servidores, algo fundamental para evitar el spam.

Los clientes que quieran utilizar ESMTP deben utilizar el comando EHLO (Extended HELLO) en vez de HELO en la fase de saludo.
Un servidor puede responder con éxito (código 250) o con fallo/error (código 5xx).

- Si el saludo es rechazado, se continuará la comunicación mediante SMTP.
- Si el saludo es aceptado por un servidor ESMTP, responderá el código 250 OK en una respuesta de varias líneas con su dominio y una lista de palabras clave para indicar las extensiones soportadas.

Haz clic aquí para saber más de ESMTP

# 8. Protocolos de entrega de correo. POP/IMAP

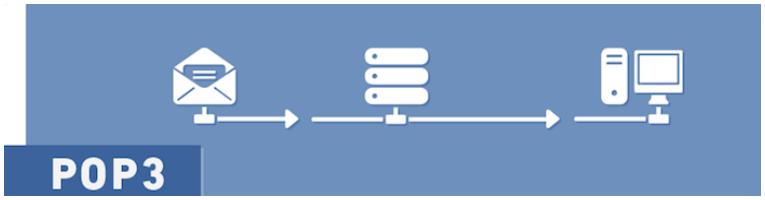
Hemos visto que los servidores SMTP se encargan de transportar los mensajes de correo desde el cliente SMTP del remitente hasta el buzón del usuario destinatario. En este buzón quedan almacenados los mensajes como archivos. Un usuario podría consultar los mensajes recibidos accediendo a su buzón (una carpeta en el disco del servidor donde el usuario tiene la cuenta de correo) y editando los archivos, pero evidentemente esto no es realizable en la práctica cuando el usuario no tiene acceso al ordenador servidor.

Además del protocolo SMTP de transferencia de mensajes de correo electrónico, existen dos protocolos para la descarga de correo por los usuarios receptores desde sus buzones de usuario. Estos protocolos son **POP3** e **IMAP**.
Para ambos protocolos, un cliente del protocolo establece una conexión autentificada con un servidor y una vez establecida la conexión permite que el usuario, desde el cliente, pueda acceder al correo de su buzón, solicitar su entrega y gestionarlo.

Cuando un usuario ha iniciado un programa cliente de correo y solicita acceder al correo recibido en una de sus cuentas, el programa cliente le pide una contraseña que será la correspondiente a la cuenta de correo que esté usando. El cliente de correo enviará la dirección de correo de la cuenta y la contraseña al servidor que validará éstos para iniciar la conexión cliente-servidor.

# Características y funcionamiento de POP

El protocolo **POP** (**P**ost **O**ffice **P**rotocol) es un protocolo **cliente/servidor** para la entrega o descarga de correo desde los buzones de usuario en los servidores a los programas clientes de usuario. Actualmente se usa **POP3** (versión 3 del protocolo) y escucha a los clientes en el puerto **TCP 110**.




Permite:

– Conectarse al servidor de correo
– Listar los mensajes del buzón.
– Descargar los mensajes (eliminándolos o manteniendo una copia en el servidor).
– Cerrar la conexión

Es necesario que el usuario tenga una cuenta de correo en un servidor para que pueda tener un buzón de correo y, por tanto, para que pueda acceder a ese buzón. Además, para usar POP3 como protocolo de descarga, será necesario que el cliente de correo pueda usar el protocolo POP3, que el servidor de descarga sea un servidor POP3 y que el cliente envíe al servidor la dirección de cuenta y la contraseña correcta.

Al igual que SMTP, utiliza TCP en la capa de Transporte y se basa en el envío de comandos y respuestas en formato ASCII entre cliente y servidor.

El protocolo POP3 es un protocolo **inseguro** ya que, aunque utiliza autentificación, todo el intercambio de información se realiza en texto plano (sin cifrar) incluidas la dirección de correo y la contraseña. El protocolo **POP3S** mejora la seguridad encriptando o cifrando mediante **SSL** la información transmitida. El protocolo POP3S usa el puerto **995**.

Una conexión cliente/servidor POP3 se desarrolla de la siguiente forma:

- **Conexión**: el cliente solicita establecer una conexión de transporte con el puerto TCP 110.
- **Fase de autorización**: tras establecerse la conexión TCP, el cliente se autentifica ante el servidor enviando la dirección de correo y la contraseña del usuario mediante los comandos POP3 ***USER*** y ***PASS***.
- **Fase de transacción**: desde el cliente ya se pueden enviar comandos al servidor para gestionar el correo y listarlo, descargarlo, eliminarlo, etc.
- **Fase de actualización**: se inicia cuando el cliente solicita cerrar la conexión POP3 enviando el comando ***QUIT***. Es en esta fase cuando el servidor elimina realmente mensajes que habían sido marcados para ser borrados.
- En una conexión POP3 el cliente envía comandos y el servidor devuelve respuestas. Los comandos de POP3 se describen en el **RFC 1939**.

# Características y funcionamiento de IMAP

Al igual que POP3, el protocolo **IMAP** (**I**nternet **M**essage **A**ccess **P**rotocol) es un protocolo para la descarga de correos desde los buzones de usuario a los clientes del servicio. Actualmente se trabaja con **IMAP4** la versión 4 de este protocolo.

Permite:

– Operar en modo desconectado (*offline*) estableciendo conexiones para listar y descargar mensajes, de forma parecida a POP3.

– Operar en modo conectado (*online*), donde el cliente puede estar conectado al servidor mientras su interfaz esté activa, permitiendo así la manipulación de buzones como si fueran locales (buscar, consultar, renombrar, mover, borrar mensajes y cambiar su estado).

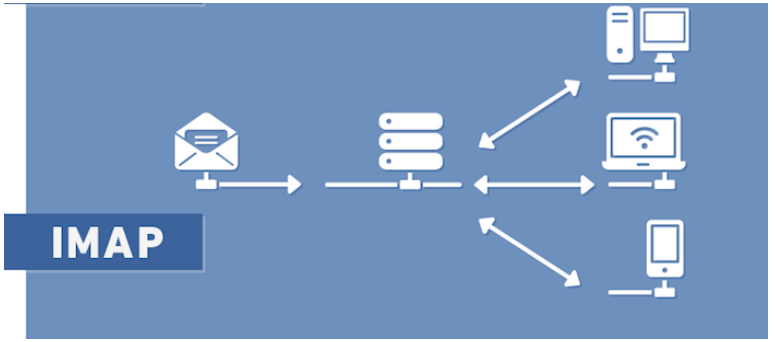
– Acceso a partes de los mensajes (por ejemplo, leerlos pero no descargar sus adjuntos).

– Acceso concurrente de varios usuarios al mismo buzón.

– Crear, borrar y manipular buzones.

Usa TCP como protocolo de transporte y como el resto de protocolos, se basa en el intercambio de mensajes de texto en ASCII entre cliente y servidor.

Un servidor IMAP establece las conexiones con los clientes en el puerto **TCP 143** y si se usa el protocolo **IMAP seguro** para transmitir la información cifrada, utiliza el puerto **TCP 993**.




Ofrece mecanismos de autenticación entre cliente y servidor (*AUTHENTICATE*, *LOGIN*, *SASL*, …). El usuario debe autenticarse para acceder a su buzón.

El funcionamiento de IMAP presenta varias diferencias con respecto a POP3:

- **Mantenimiento de conexiones**: con POP3 se mantiene la conexión mientras se descarga el correo. Con IMAP se mantiene la conexión mientras el cliente está activo. Se trabaja en línea y, por tanto, el usuario puede ver al momento cada nuevo correo recibido.
- **Acceso a partes de los mensajes**: IMAP permite obtener parte de los mensajes o algunos de los objetos MIME incluidos sin tener que descargar todo el correo.
- **Soporte para acceso simultáneo a varios buzones**: IMAP permite que un usuario pueda acceder a varios buzones simultáneamente e incluso mover mensajes de un buzón a otro.
- **Respaldo para búsquedas**: IMAP permite que el usuario pueda realizar búsquedas de mensajes que cumplan determinados criterios.
- **Acceso simultáneo a un buzón**: IMAP permite que se esté accediendo a un mismo buzón desde varios clientes. Esto es adecuado cuando un buzón corresponde a una cuenta de usuario utilizada por varias personas.
- **Correo permanente en el servidor**: IMAP permite que el correo permanezca hasta que el usuario decida eliminarlo. Con POP3, por defecto, el correo se elimina del servidor cuando ha sido descargado por el cliente.

# 9. SPAM



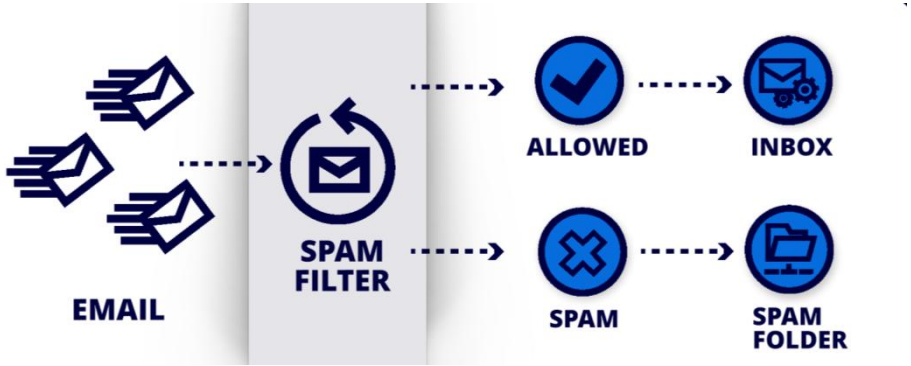

El término **SPAM** se utiliza para referirse a mensajes de correo no deseados, no solicitados, o de remitentes desconocidos o falsos.

- Existen muchos tipos de SPAM según el medio usado para su transmisión: Redes sociales, SMS, chats, telefónico, etc.
- El SPAM de correo electrónico, normalmente son mensajes enviados de forma masiva, a muchos destinatarios, conteniendo publicidad, información falsa, códigos maliciosos o información cuyo objetivo es engañar al receptor para obtener un provecho (es muy utilizado en técnicas de ingeniería social).
- La acción de enviarlo se llama *spamming* y quienes lo hacen son *spammers*.
- El SPAM es perjudicial para usuarios y empresas por la pérdida de tiempo y recursos que supone. Tiene un gran impacto económico y social y es uno de los problemas de Internet.

Evita el spam con unas sencillas pautas

# Filtros y métodos antispam

Los MTAs combinan sus propios métodos con filtros antispam para determinar si un correo es marcado como spam o no.
Estos métodos pueden ser **preventivos** o **correctivos**.




## MÉTODOS PREVENTIVOS

– Concienciación y educación digital del usuario.
- Usar el campo CCO para no mostrar la lista de receptores en los mensajes.
- Explicar los peligros de los adjuntos, enlaces en mensajes.
- Etc.

– Medidas legales de atención al **RGPD** y no enviar mensajes de publicidad no explícitamente autorizados ni revelar datos personales que puedan ser aprovechados por terceros.

– Enmascaramiento de direcciones en sitios web, chats y redes sociales para evitar ***spambots*** (robots que escanean la web en búsqueda de direcciones de correo).

Normativa sobre datos personales

## MÉTODOS CORRECTIVOS

Implantados en MTAs, MUAs y filtros antispam

– Basados en el contenido de los mensajes.
  - Filtros básicos de cabeceras y contenidos (definidos en reglas en los MTAs).
  - Filtros basados en OCR (Lectura óptica de caracteres) sobre las imágenes de los mensajes.
  - Filtros heurísticos basados en palabras claves habituales en el spam. (“viagra”, “free”, etc.)
  - Filtros bayesianos basados en análisis estadísticos y probabilidades.

– No basados en el contenido de los mensajes.
  - Listas públicas o comerciales (blancas/negras/grises) de dominios y direcciones marcados como orígenes legítimos, spam o sospechosos.
  - Esquema de autorización (autorización de MTAs)
    - **SPF** (Sender Policy Framework). Los DNS almacenan información de Ips autorizadas para envío de correo. Los MTA consultan los dns para averiguar si es correo autorizado (Comando MAIL FROM en SMTP).
    - **Sender ID**. Evolución de SPF realizada por Microsoft que con comprobaciones adicionales.
    - **DKIM** (***DomainKeys*** Identified Mail). Uso de algoritmos de clave pública y funciones HASH para firmar los correos y verificarlos en destino. Los DNS de la organización almacenan las claves públicas.

# Software antispam para MUAs

Los clientes de correo (MUAs) también pueden integrar filtros antispam y/o se pueden configurar para usar filtros antispam externos.




El gran problema de los filtros antispam son los falsos negativos y positivos en el filtro de mensajes.

Algunos ejemplos de software antispam son:

- Apache SpamAssasin
- Zimbra
- Spamfighter
- Spamihilator
- Barracuda
- E-Securemail



Apache SpamAssassin

zimbra
A SYNACOR PRODUCT

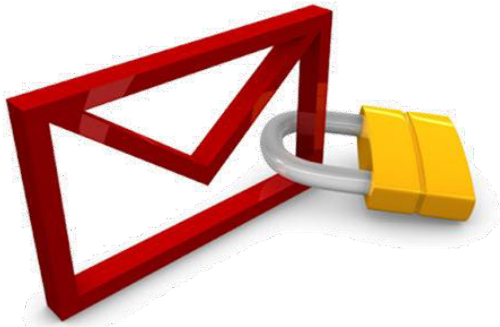
Spamihilator
Anti-Spam-Filter

SPAMfighter

secuserve
Collaboration as a service

Barracuda

# 10. Seguridad



El servicio de correo se basa en protocolos muy antiguos y en sus especificaciones **no** se incluyó la seguridad (SMTP se desarrolló en 1984).
La seguridad en el servicio de correo electrónico es muy compleja, ya que intervienen múltiples componentes y protocolos.

Los principales problemas de seguridad son:

- Los clientes y servidores de correo son sistemas complejos y con múltiples funcionalidades.
- En SMTP el intercambio de información se realiza en texto plano y originalmente no proporciona mecanismos de autenticación ni de clientes ni de servidores.
- Los mensajes pueden contener información falsa, códigos maliciosos, publicidad, engaños.
- Los protocolos IMAP y POP si incluyen originalmente mecanismos de autenticación para acceder a los buzones, pero el intercambio de información se realiza en texto plano y tampoco está clara la autenticación de servidores.

## Autenticación SASL y SPA

- **SASL** (Simple Authentication and Security Layer) es un *framework* de autenticación para protocolos orientados a conexión (SMTP, POP3, IMAP4, LDAP, …)
  – Permite distintos tipos de autenticación (Anonymous, CRAM-MD5, GSSAPI, PLAIN o NTLM, entre otros).
  – Se suele integrar con protocolos SSL/TLS para aumentar la seguridad.
- **SPA** (Secure Password Authentication) es un método de autenticación de Microsoft para protocolos SMTP, POP e IMAP.

## Autenticación SMTP

Para aumentar la seguridad y controlar quién usa el servidor para enviar correos se han definido extensiones del protocolo SMTP para autenticar a usuarios finales y MTAs.

Algunos estándares de autenticación SMTP son:

– **POP (o IMAP) before SMTP**: Método obsoleto que consiste en autenticarse en el servidor POP o IMAP (que sí soportan autenticación). El servidor SMTP se comunica con el servidor POP/IMAP que le indica si ha tenido éxito la autenticación.

– **SMTP AUTH**: Es una extensión de SASL para SMTP que forma parte del conjunto de extensiones del protocolo ESMTP y permite a los usuarios autenticarse en el servidor SMTP antes de enviar el correo.

- Se implementa a través del comando AUTH
- Se integra con los protocolos SSL/TLS para aumentar su seguridad.

– **Autenticación mediante certificado** (si se usa SMTPS).

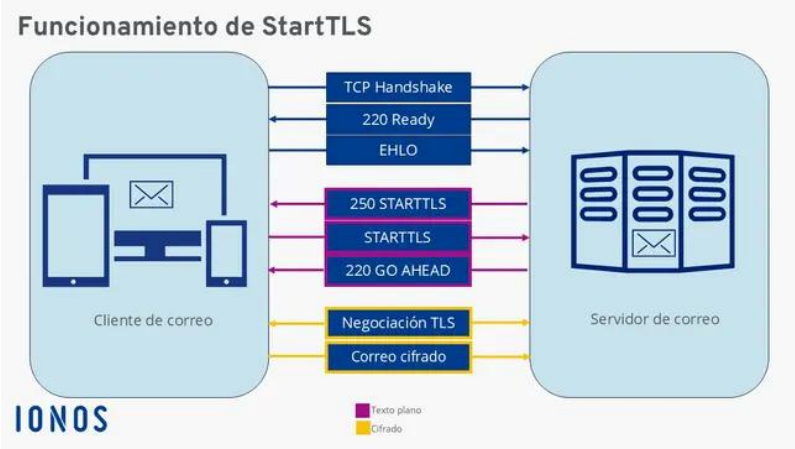
# Protocolos seguros. SMTPS, POPS, IMAPS

Al igual que otros protocolos como HTTP y FTP, los protocolos de correo SMTP, POP, e IMAP, que originalmente transmiten en texto plano sin cifrar, se pueden encapsular en SSL/TLS para garantizar la confidencialidad, integridad de la comunicación, y autenticación de los servidores involucrados.

- El protocolo **SMTPS** es un conjunto de especificaciones que indican cómo encapsular el protocolo no seguro SMTP en SSL/TLS para ofrecer comunicaciones seguras. SMTPS usa los puertos 465/TCP y 587/TCP.

- Los protocolos **POPS** e **IMAPS** son especificaciones de encapsulamiento de POP e IMAP mediante SSL/TLS. Usan los puertos 995/TCP y 993/TCP respectivamente.

**STARTTLS** es un mecanismo para negociar conexiones SSL/TLS sobre protocolos de texto plano. Hay extensiones STARTTLS para SMTP, POP e IMAP.
Es habitual encontrar MTAs configurados con SMTP AUTH (SASL) y STARTTLS escuchando peticiones SMTPS en el puerto 25/TCP.



# Antivírus



Los servidores de correo pueden establecer reglas para filtrar y restringir el envío de correos o “marcar” mensajes que cumplan determinadas características (contenido inapropiado, spam, malware, etc.).
Estas funcionalidades pueden estar integradas en los MTA o bien ser módulos o complementos.

Los Antivirus analizan los mensajes de correo en búsqueda de malware y aprueban, devuelven, descartan o marcan mensajes sospechosos. Pueden estar integrados en los servidores de correo y/o en los programas cliente.

Algunos ejemplos de antivirus son:

- **ClamAV**
- **Kaspersky**
- **Avast**
- **eset**
- **McAfee**

# Firma y cifrado de mensajes. PGP y S/MIME

Los protocolos seguros no garantizan que los mensajes no sean leídos, interceptados o manipulados por terceros durante la comunicación.

Para prevenir estas situaciones, se pueden cifrar y/o firmar los mensajes mediante algoritmos criptográficos. Los dos principales métodos son:

– **S/MIME** (Secure/Multipurpose Internet Mail Extensions)

Conjunto de algoritmos, protocolos e infraestructura de clave pública (certificados digitales y autoridades de certificación) para firmar y cifrar mensajes de correo. Implementado en muchos clientes de correo como Thunderbird, Outlook, Eudora, etc.

– **PGP** (Pretty Good Privacy) y **OpenPGP**

Software criptográfico para firmar y cifrar datos de forma segura. OpenPGP es la versión abierta de PGP (software con licencia). Se caracterizan porque no existe una autoridad de certificación central, se basan en “anillos de confianza” y servidores de claves públicas.

Versiones de OpenPGP son ***GPG*** (Gnu Privacy Guard), ***GPA*** (Gnu Privacy Assistant) o ***Gpg4***.



# REFERENCIAS

## Bibliografía

***Servicios de red e internet***. García Sánchez, Álvaro. Sanz Rodríguez, Javier. González Sotillo, Álvaro. Enamorado Sarmiento, Luis. Garceta Grupo Editorial.

***Servicios en Red***. Andreu Gómez, Joaquín . Editorial Editex

## Webgrafía

***Wikipedia***

***www.freepik.es***

***recursostic.educacion.es***

***Otros…***

