

# Servicios en red

Joaquin Andreu



<b>Unidad 1. Servicios DHCP</b>	ISBN 978-84-9003-083-7
<b>Unidad 2. Servicios DNS</b>	ISBN 978-84-9003-084-4
<b>Unidad 3. Servicios de acceso remoto</b>	ISBN 978-84-9003-085-1
<b>Unidad 4. Servicios FTP</b>	ISBN 978-84-9003-086-8
<b>Unidad 5. Gestión de servicios de correo electrónico</b>	ISBN 978-84-9003-087-5
<b>Unidad 6. Gestión de servidores web</b>	ISBN 978-84-9003-088-2
<b>Unidad 7. Interconexión de red</b>	ISBN 978-84-9003-089-9
<b>Unidad 8. Redes inalámbricas</b>	ISBN 978-84-9003-090-5
<b>Unidad 9. Voz IP</b>	ISBN 978-84-9003-091-2
<b>Servicios en red (obra completa)</b>	ISBN 978-84-9771-760-1

# 5

# Gestión de servicios de correo electrónico

## vamos a conocer...

1. Cuentas de correo, alias y buzones de usuario
2. Elementos del servicio de correo electrónico
3. Formato de los mensajes de correo electrónico
4. Protocolos y servicios de descarga de correo electrónico
5. Protocolos y servicios de envío de correo electrónico
6. Tipos MIME
7. Vulnerabilidades de los servicios de correo electrónico
8. Clientes de correo electrónico
9. Servidores de correo electrónico
10. Correo seguro
11. Webmail

### PRÁCTICA PROFESIONAL

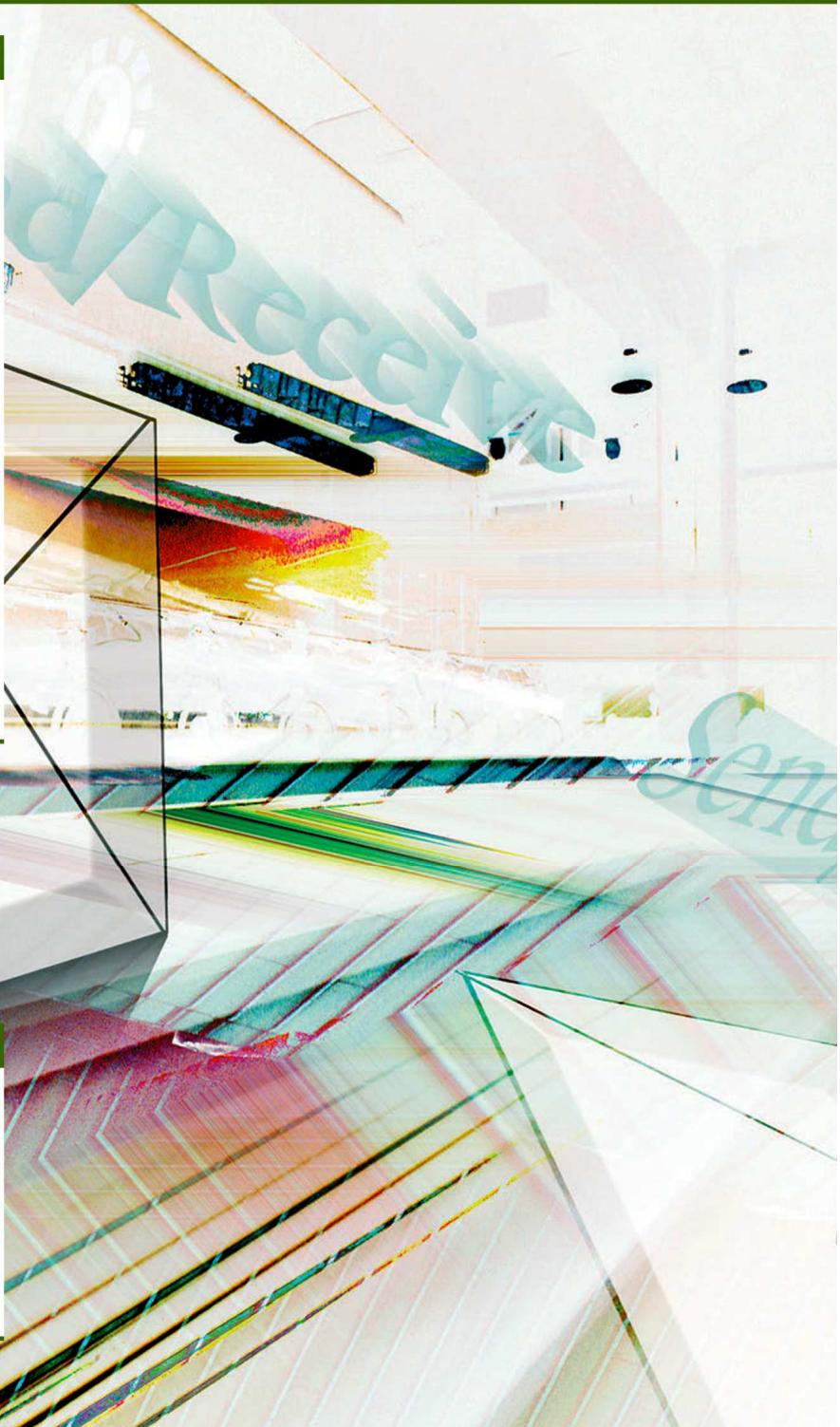
Instalación y configuración de un servidor de correo en Linux y un cliente en Windows

### MUNDO LABORAL

Administrar el correo de tu dominio  
DynDNS con Gmail

## y al finalizar esta unidad...

- Describirás los protocolos de envío y recogida de correo electrónico.
- Aplicarás clientes webmail.
- Instalarás clientes mail.
- Instalarás servidores de mail.
- Crearás usuarios y verificarás su acceso.
- Configurarás los alias para el correo electrónico.
- Sabrás tratar el spam.



## CASO PRÁCTICO INICIAL

### situación de partida

Xavi trabaja en una empresa llamada Tomates Rizados y ha decidido alquilar el dominio «tomatesrizados.eu».

Hasta el momento, los administrativos utilizaban como herramientas de trabajo el fax, el teléfono, la mensajería de paquetes y el correo ordinario.

Cada vez más, para ahorrar costes y agilizar trámites, tanto los proveedores como los clientes solicitaban correos electrónicos a través de los que poder enviar presupuestos, ofertas, etc.

El gerente de esta empresa es un señor muy tradicional reacio a invertir en nueva tecnología, aunque conoce y utiliza la informática e incluso tiene autómatas en el proceso de envasado de tomates, los cuales tienen asociados ordenadores a través de los que consulta la producción, el rendimiento, etc.

Hasta ahora, cuando algún empleado tenía que comunicarse por correo electrónico utilizaba su correo particular, hecho que da una impresión de poca profesionalidad. Por lo que un empleado decide crear la cuenta «tomatesrizados@hotmail.com» para utilizarla en el trabajo.

El gerente ya le ha dado permiso a Xavi para que use las cinco cuentas de correo que tienen con el dominio y Xavi tiene que decidir qué alias debe crear.

A nivel local, quiere establecer un servidor de correo electrónico y configurar los clientes de correo para los administrativos.

También pretende hacer un pequeño manual para que los comerciales puedan consultar su correo electrónico por webmail sin tener que desplazarse a la empresa.

### estudio del caso

Analiza cada punto de la Unidad de Trabajo, con el objetivo de contestar las preguntas de este caso práctico.

1. ¿Qué protocolos le interesa instalar a Xavi en su servidor (POP3, POP3S, IMAP, SMTP, SMTPS...)?
2. Si a Xavi le gusta más Windows que Linux, ¿qué servidor de correo electrónico le interesa instalar?
3. ¿Cuántas cuentas de correo electrónico debe crear, si el gerente quiere una propia, la jefa de administración otra y existen cinco departamentos más?
4. ¿Cómo debe crear las cuentas de correo electrónico?
5. ¿Cómo creará el alias y de qué tipo deberá ser?
6. ¿Cómo puede impedir usos indebidos del servidor de correo?
7. ¿Qué clientes de correo electrónico le aconsejas instalar?
8. ¿Qué servicio de webmail le aconsejarías?
9. ¿Qué recomendaciones para el envío de correo debe hacer a los empleados?
10. ¿Qué actitud deben tener frente al spam?

## 1. Cuentas de correo, alias y buzones de usuario



Para referirnos al correo electrónico el término que se suele utilizar es el anglicismo **e-mail**, que proviene de la construcción inglesa *electronic mail*, pero podemos encontrar muchas más formas para referirnos al correo electrónico, tales como *correo-e*, *e-correo*, simplemente *correo* o *mail*; o incluso hay gente que utiliza la palabra *messenger* como genérico, confundiéndolo con el servicio de correo de Messenger. Este servicio fue el más usado desde el inicio de internet hasta que la Web 2.0 facilitó, desde páginas web, simular o consultar servicios mail/correo, news/foros, blogs/bitácoras, wikis, redes sociales, irc/chats, etc. El correo electrónico ha sustituido a la mayoría de correo ordinario no administrativo y a casi todos los envíos de fax, aunque el fax sobrevive gracias a que las empresas tienen un hardware muy antiguo y a la dificultad que supone para algunos escanear o enviar un correo electrónico.

Las **ventajas** del correo electrónico sobre el tradicional son muchísimas:

- **Precio:** casi todas las empresas tienen internet, por lo que el coste del correo electrónico es cero; en el correo tradicional necesitamos hojas, sobres, sellos, etc.
- **Rapidez:** un correo electrónico puede tardar entre medio segundo o unos minutos en llegar a su destino; en España, una carta puede tardar días o semanas (depende desde dónde se envíe).
- **Seguridad:** el correo electrónico ofrece una mayor seguridad, incluso hay tipos específicos de correo con seguridad extra (SMTSP, POP3S, etc.); en cambio las cartas están más expuestas a diversos riesgos que hacen peligrar su seguridad (pérdidas, daños causados por el transporte, etc.).
- **Eficiencia:** el correo electrónico puede llegar a muchas más personas (un mismo e-mail puede ir destinado hasta a 256 destinatarios) en menor tiempo y ahorrando costes (algo de lo que ya hemos hablado anteriormente), lo que nos proporciona una mayor eficiencia.

Las desventajas del correo electrónico son muy subjetivas, y son los valores añadidos del correo tradicional:

- La personalización a través de la escritura manual, escritura y dibujos a mano, que suelen tener mucho valor sentimental.
- El sobre del correo físico permite incluir elementos tangibles: fotos, postales, algún detalle...
- Al receptor no le hace falta tener conexión a internet, ordenador, impresora, etc.

Hoy en día es crucial, por ejemplo, tener una cuenta de correo electrónico, hasta el punto de que, incluso en los procesos de selección, muchas empresas no leen currículos en los que no aparezca una cuenta de correo de la persona que opta al puesto; nos lo solicitan en las fichas de los centros educativos para ponerse en contacto de forma más rápida y eficaz; también a la hora de mandarnos información sobre temas que nos interesen; podemos gestionar multitud de trámites sin movernos de casa a través de una cuenta de correo; hacer reservas de hotel; adquirir y facturar nuestro equipaje y recibir a través del correo electrónico la documentación necesaria; registrarnos en páginas de empresas que nos interesen; comunicarnos con familiares y amigos, etc. En definitiva, es una herramienta indispensable en nuestro día a día.

En 2007, el 67% de los estadounidenses tenían e-mail; en España, en febrero de 2009 casi la mitad de los que leían el correo tenían solo webmail, y de estos el 60% lo tenían con las cuentas de Microsoft (Live, Hotmail, MSN, etc.).

La mayoría de los usuarios recibe entre 25 y 50 correos semanales y envía de 1 a 5. Todos reciben publicidad sin permiso y más de un tercio de los usuarios la prohibiría (de hecho lo está).

El correo electrónico funciona enviando texto, pero permite adjuntar archivos de cualquier naturaleza (imágenes, vídeos, programas...).

Se inventó antes que internet (a la vez que la red ARPA) y fue crucial para su creación. Empezó a utilizarse en 1965 y en 1966 ya había crecido exponencialmente. En 1971, Ray Tomlinson incorporó el uso de la arroba (@) para separar el nombre de usuario del servidor que recibía (y alojaba) el correo. En 1980 se sugirió la norma del SMTP, en 1984 se creó el RFC del POP y, por fin, en 1992 se incluyeron los tipos MIME, que permiten adjuntar casi cualquier formato de archivo y texto encriptado.

El correo electrónico es un tipo de comunicación escrita en diferido: no requiere que el receptor esté conectado a la red y puede leerlo cuando quiera, tiene un retardo.

No debemos confundirlo con otros tipos de comunicación:



Nombre	Tipo	Tiempo	Necesidad	Software
<b>mail</b>	escrito	en diferido	una cuenta de usuario	cliente de correo
<b>news</b>	escrito	en diferido	una cuenta de usuario	cliente de correo
<b>irc/chat</b>	escrito	tiempo real	un nick	cliente de irc
<b>mensajería instantánea</b>	escrito	tiempo real	una cuenta de usuario, normalmente en el mismo servidor	cliente de mensajería instantánea
<b>VoIP</b>	voz	tiempo real	IP o DNS del servidor	cliente de VoIP
<b>videoconferencia</b>	imagen y voz	tiempo real	IP o DNS del servidor	cliente videoconferencia

Uno de los problemas que siguen teniendo los servicios de correo electrónico es que los mensajes son texto plano ASCII, y por ello muchas veces no se visualizan bien algunos caracteres. Muchos usuarios añaden un mensaje al final affirmando que no tildan y no usan la letra ñ, ni la cedilla ç, etc. a propósito, para evitar que esto les ocurra.

Las antiguas versiones de correo no aseguraban la recepción del correo (algo que sigue pasando de forma muy excepcional), y dejaban enviarlo con una cuenta de correo de otra persona, hecho que supone un delito, ya que se considera suplantación de personalidad. Los correos electrónicos se utilizan incluso como pruebas en procesos judiciales.

## 1.1. Cuentas de correo

### saber más

Para saber más sobre nombres de cuentas de correo lee el RFC 5322.

### EJEMPLO

Se han internacionalizado nuevos dominios y con ellos los correos, pero aún no son aconsejables.

Ahora pueden existir correos como:

Pedro.ñiguez@españa.es

eric@barça.cat

μελλοεαρλ@θνεστον.χομ

Para la representación de los códigos UTF-8 lee los RFC 4952 y el experimental 5335.

### recuerda

Algunos sistemas también permiten símbolos como el de exclamación (!), el número o la almohadilla (#), el dólar (\$), el porcentaje o por ciento (%), la y o ampersand (&), la comilla simple o apóstrofo ('), el asterisco (\*), el más (+), el menos (-), la barra oblicua o de división (/), el igual (=), la interrogación de cierre (?), el acento circunflejo (^), el acento grave (`), las llaves ({ }), la barra vertical u operador lógico () y la virgulilla o equivalencia (~). El carácter punto(.) solo debe usarse, en el nombre de usuario, sin poder repetirse de forma seguida (dos puntos uno junto a otro) y nunca al final del nombre.

### saber más

A la virgulilla los anglosajones la llaman también la tilde de la ñ, como si la ñ no fuese una letra, sino la n con una tilde distinta.

Para enviar y recibir un correo es necesario tener una cuenta de usuario en un servidor de correo o una dirección de correo electrónico.

Normalmente el proveedor de correo electrónico, el ISP, o el proveedor de hosting ofrecen la posibilidad de tener una cuenta en sus servidores desde un programa de lectura de correo, lo que se llama cliente o agente de correo, **MUA** (*Mail User Agent*), por ejemplo Microsoft Outlook Express.

Las cuentas de correo tienen dos partes:

- El **nombre de usuario**, que no debe superar los 64 caracteres y que debe cumplir las restricciones que estos nombres tengan en el sistema operativo, normalmente solo acepta letras anglosajonas (diferencia entre mayúsculas y minúsculas), los dígitos, el guion (-), el subrayado o barra baja (\_), y el punto (.).
- Y el **nombre o dirección IP del servidor** de correo electrónico, con un máximo de 256 caracteres.

Ambas partes tienen que estar separadas por el símbolo arroba (@) y, en total, el correo no debe sobrepasar los 256 caracteres.

### EJEMPLO

Correctos	Incorrectos
joaquin@hotmail.com	Hola..como.@nose.es
amigos-cocina@216.239.59.147	Maria@rodriguez#torres@mi dominio.eu info@
mi-casa.-__768@msn.es	buintierradefrutashermosasrosasbue nosvinosairepuroyverdescampos.com
Jose.garcia@usuarios.es.lapagina.de	

## 1.2. Alias de buzón

Un alias es un apodo o sobrenombre que se utiliza por razones estéticas o para dar un matiz familiar y cariñoso. En el caso de la informática se utilizan mucho para nombres de usuarios, etc. Los alias de correo electrónico se emplean, principalmente, para el **reenvío** de correo. Podemos poner un alias a una dirección que ya tenemos en ese mismo servidor (por ejemplo: si tenemos una cuenta llamada «Manuel@dominio.com», podemos crear los alias «manu@dominio.com» o «manolo@dominio.com»), a otro correo de otro servidor («manu@dominio.com» a «manu@dominio.es») o a varios correos («manu@dominio.com» a «gerente@dominio.com», «miempresa@hotmail.es» y «666999666@movistar.es»).

Existen dos tipos de alias para correo electrónico, los que sustituyen a uno o varios correos concretos y los llamados universales, «de sistema» o «sumidero», que recogen el correo de todas las direcciones posibles que no estén asignadas a ningún usuario dado de alta (como si fuese una dirección comodín).

### 1.3. Buzones de usuario

Muchas personas llaman buzón de correo a las direcciones de correo electrónico, sin embargo, los buzones son subcarpetas (*folders*, en inglés) del sistema de correo electrónico del usuario, donde se almacenan los mensajes recibidos, por lo que pueden ser distintas cuentas de un mismo usuario, carpetas de una misma cuenta, o distintos usuarios en un servidor de correo concreto. Dichas carpetas pueden ser reales o virtuales.

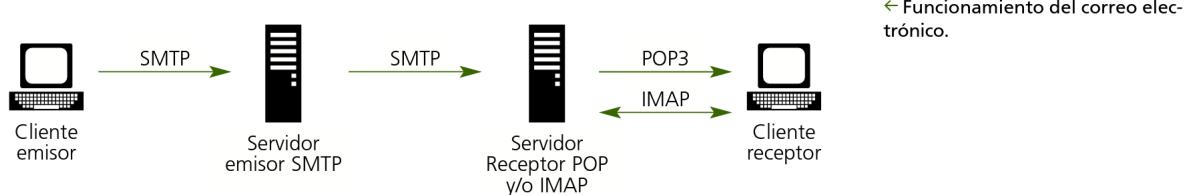
#### **Caso práctico inicial**

Xavi tiene que crear buzones de correo para distintos usuarios.

## 2. Elementos del servicio de correo electrónico

Los servicios de correo electrónico se basan en un modelo cliente-servidor y pueden utilizarse en cualquier tipo de red TCP/IP. En el proceso de envío y recepción de correo electrónico participan tres tipos de programas:

- **MTA:** el Agente de Transferencia de Correo (*Mail Transport Agent* o *Message Transport Agent*, Agente de Transporte de Mensajes) es un software que transfiere correo electrónico de una computadora a otra, es el servidor SMTP el que envía el correo o el mensaje.
- **MDA:** el Agente de Entrega de Correo (*Mail Delivery Agent*) es un software que acepta correo entrante y lo distribuye a los buzones de los destinatarios (si la cuenta de destino está en la máquina local), o lo reenvía a un servidor MTA.
- **MUA:** el Cliente de Correo Electrónico (*Mailer* o *Mail User Agent*) es el que permite enviar, recibir y editar correos.



El software más utilizado es:

Tipo	SO	Aplicaciones
<b>MTA</b>	Multiplataforma	Sendmail; Postfix y Sun Java System Messaging
	Unix	Qmail
	Windows	Microsoft Exchange Server
<b>MDA</b>	Multiplataforma	Postfix-maildrop y Sun Communication Suite
	Unix	Procmail y Maildrop
	Windows	Microsoft Exchange Server
<b>MUA</b>	Multiplataforma	Mozilla Thunderbird
	Unix	Eudora, Opera, ml y Mutt
	Windows	Microsoft Outlook

### 3. Formato de los mensajes de correo electrónico

El protocolo SMTP fija que los mensajes de correo electrónico deben llevar una cabecera y un cuerpo.

La **cabecera** tiene que llevar una serie de campos. Los básicos son:

- **REMITENTE (DE o FROM):** quién envía el correo, cuenta de correo electrónico del emisor del mensaje. Algunos clientes solo aceptan configurar una cuenta de correo emisora y ocultan este campo; otros aceptan varias, pero tienen una por defecto; y los menos permiten ponerla «a mano», permitiendo la suplantación (en Europa es delito esta práctica). Es un campo de cumplimentación obligatoria.
- **DESTINATARIO (PARA o To):** correo electrónico del destinatario. Es un campo obligatorio y debe tener estrictamente un solo destinatario; no debemos confundirlo con el webmail, que trataremos más adelante.
- **DESTINATARIO DE COPIA (CC):** campo opcional que permite que enviemos correos electrónicos hasta a 256 destinatarios, separados por coma (,) o punto y coma (;) y seguidos de un espacio en blanco. Envía el mismo correo electrónico a todos los destinatarios del **PARA** y del **CC**, pero cuidado, ya que informa a todos de quién los recibe porque los destinatarios son visibles. Es aconsejable usarlo solo para enviar correos a familiares o amigos ya que, si alguno de los destinatarios no quiere que publicites su correo, podría denunciarte y las multas son de hasta 30.000 euros. Esta opción permite al remitente enviar una respuesta al emisor o a **TODOS** los destinatarios iniciales.

#### caso práctico inicial

Xavi debe recomendar a los trabajadores la utilización del campo CCO para envíos grupales.

- **DESTINATARIO DE COPIA OCULTA (CCO o BCC):** tiene la misma utilidad que el campo **CC**, solo que envía los correos a los destinatarios sin que estos puedan ver las demás direcciones. Esto es recomendable para comunicaciones de empresa, publicidad permitida, etc.
- **RESPONDER (REPLY TO):** campo opcional que lleva la dirección a la que queremos que nos respondan. Si está vacío utiliza el campo **DE**, si contiene una dirección es la que se escribe al pulsar **RESPONDER**.
- **FECHA (DATE):** en este campo se reflejan la fecha y la hora del sistema emisor del mensaje.
- **TEMA (ASUNTO o SUBJECT):** campo que resume el texto del mensaje. Se aconseja usar la lengua materna, pues los virus suelen escribir mensajes en inglés. Algunos filtros de correo desechan mensajes del tipo «i love you», «viagra»... Si no lo rellenamos suele aparecer «Sin asunto» o «No subject» y algunos filtros lo descartan.

En el **cuerpo** del mensaje escribiremos el texto que queramos hacer llegar a nuestros destinatarios.

#### recuerda

Para preservar las direcciones de nuestros destinatarios utilizaremos el campo CCO.

The screenshot shows a Windows-based email client interface. At the top, there are dropdown menus for 'Archivo', 'Nuevo', 'Comunicación', 'Búsqueda', 'Ayuda'. Below the menu bar, there's a toolbar with icons for 'Nuevo', 'Responde', 'Responde todo', 'Envía', 'Imprimir', 'Copiar', 'Cortar', 'Pegar', 'Borrar', 'Recuperar', 'Reenviar', 'Filtrar', 'Formato', 'Formato de fuente', 'Formato de párrafo', and 'Formato de lista'.

The main area contains the following fields:

- De:** tomatesrizados@hotmail.com \*
- Para:** tomatesfritosverdes@tomatesfritosverdes.es \*
- CC:**
- CCO:** info@envasedetomates.com ✖ | comercial@tomates.cn ✖
- Asunto:** Oferta tomates rizados

Below the fields, there's a preview pane showing the message content: "Estimado cliente, para la campaña de tomates 2011-2012, tenemos una oferta para compradores de múltiples de 10 toneladas, con un rapel de 10+2."

## 4. Protocolos y servicios de descarga de correo electrónico

Existen diversos servicios de recepción de e-mail. Los más utilizados son:

- **POP**, *Post Office Protocol* (Protocolo de Oficina Postal): protocolo de recepción de correo que permite la gestión, el acceso y la transferencia entre el servidor y el cliente local. Usa el puerto 110 (en su versión POP3, la más usada actualmente), el 995 para POP3S, y algún servidor utiliza el 1109. Está definido en el RFC 5321.
- **IMAP**, *Internet Message Access Protocol* (Protocolo de Acceso a Mensajes de Internet): protocolo de acceso a mensajes almacenados en el servidor. Usa el puerto 143, el 220 para su versión IMAP3 y 993 para IMAPS. El IMAP4.1 está especificado en el RFC 3501. Los proveedores gratuitos de correo AOL y Gmail soportan IMAP.

El protocolo POP nos permite realizar un telnet al puerto 110 y utilizar las siguientes órdenes:

- **USER [nombre]**: para identificar al usuario.
- **PASS [password]**: para introducir la contraseña de usuario.
- **STAT**: informa de cuántos mensajes hay en el buzón (los que no están borrados) y de su longitud total.
- **LIST**: muestra todos los mensajes con su longitud.
- **RETR [núm]**: solicita el envío del mensaje especificado con un número de mensaje.
- **TOP [núm] [líneas]**: muestra la cabecera y el número de líneas requerido del mensaje especificado con el número.
- **DELE [núm]**: borra el mensaje especificado con el número.
- **RSET**: recupera los mensajes borrados (solo de la conexión actual).
- **UIDL [núm]**: lista la cadena identificativa de cada uno de los mensajes y sus números; si se especifica un número solo lista ese mensaje.
- **QUIT**: salir.

## 5. Protocolos y servicios de envío de correo electrónico

Existen distintos tipos de servicios de envío de correo electrónico. Los más usados son los **SMTP**, *Simple Mail Transfer Protocol* (Protocolo Simple de Transferencia de Correo), que utiliza el puerto 25. Está definido en el RFC 821, 2821 y 5321. Se comunica con otros servidores o clientes con líneas de texto «plano» o codificado en ASCII, con un máximo de 1.000 caracteres. Existe la versión segura SMTP sobre SSL, que usa el puerto 465 (no oficial) y que puede utilizar el 587 en algunos programas.

Los servidores SMTP son los más importantes, son los que permiten el envío de correo. Muchas empresas y particulares configuran la recepción de distintos buzones (y sus servidores de recepción) en un mismo programa, pero tan solo uno de SMTP como buzón de salida predeterminada o como único servidor de envío.

### caso práctico inicial

Xavi necesita decidirse entre POP3 e IMAP.

### saber más

Para saber más sobre protocolos de correo lee los RFC:

- POP 1725.
- POP3 1939 y 1957.
- Autenticación 2195.
- POP webmail 2384.
- POPS 2595.
- Otros POP: 3206 y 5034.
- IMAP: 1064, 2060, 2177.
- IMAPS: 2595.
- IMAP4.1: 3501.

### saber más

Si programas en C++ es interesante conocer la clase SmtpClient, ya que contiene funciones que permiten a las aplicaciones enviar mensajes de correo electrónico mediante el protocolo SMTP.

## EJEMPLO

### Comunicación:

```
S: Espera conexión TCP 25.
C: Abre una conexión.
S: 220 sigurd.innosoft.com
C: EHLO ymir.claremont.edu
S: 250-sigurd.innosoft.com
S: 250-EXPN
S: 250-HELP
S: 250 SIZE 1000000
C: MAIL FROM:<ned@thor.inno
soft.com> SIZE= 500000
S: 250 Address Ok.
C: RCPT TO:<ned@hmcvax
.claremont.edu>
S: 452 Insufficient channel
storage: ned@hmcvax.CLA
REMONT.EDU
C: DATA
S: 354 Send message, ending
in CRLF.CRLF.
...
C: .
S: 250 Some recipients OK
C: QUIT
S: 221 Goodbye
```

El funcionamiento del servicio SMTP es el siguiente:

- El cliente establece una conexión con el servidor SMTP y espera un mensaje «220 Service ready» o «421 Service non available».
- Si el mensaje es exitoso (220), el cliente envía la orden **HELO**, pidiendo que se identifique el servidor e iniciar así una sesión.
- Una vez identificado, el cliente empieza el envío de correo con la **MAIL**. El servidor contesta «250 OK».
- Con la orden **RCPT To:<user@host>** el cliente indica para quién es el correo, si el envío es para varios se envían distintos **RCPT To**. El servidor contestará para cada orden **RCPT** «250 OK» o «550 No such user here», si no encuentra al destinatario.
- El cliente envía la orden **DATA** para especificar los contenidos del mensaje. El servidor responde «354 Start mail input, end with CRLF+CRLF». Esta es la notificación acordada para el fin del mensaje.
- El cliente envía el cuerpo del mensaje, línea a línea, siendo la última un punto (.). Si todo ha ido bien, el servidor enviará un «250 Some recipients OK», o un mensaje de error acorde con el problema.
- Si no se van a enviar más correos, el cliente cierra la conexión con **QUIT**. El servidor contesta «221 Goodbye».

En el ejemplo pueden verse las órdenes básicas del SMTP:

- **HELO**: para abrir una sesión con el servidor.
- **MAIL FROM**: para indicar quién envía el mensaje (**DE/FROM**).
- **RCPT To**: para indicar el destinatario del mensaje (**PARA/CC**).
- **DATA**: para indicar el comienzo del mensaje (este finalizará cuando haya una línea únicamente con un punto [.]).
- **QUIT**: para cerrar la sesión.
- **RSET**: para abortar la transacción en curso y borrar todos los registros.
- **SEND**: inicia una transacción en la que el receptor es un terminal.
- **SOML**: el mensaje se entrega a un terminal o a un buzón.
- **SAML**: el mensaje se entrega a un terminal y a un buzón.
- **VRFY**: solicita al servidor la verificación del argumento.
- **EXPN**: solicita al servidor la confirmación del argumento.
- **HELP**: ayuda o información de un comando y sus parámetros.
- **NOOP**: se emplea para reiniciar los temporizadores.
- **TURN**: solicita al servidor que se intercambien los paquetes.

De los tres dígitos del código numérico, el primero indica la categoría de la respuesta (como la mayoría de servicios). Las categorías son las siguientes:

- **2XX**: códigos de éxito.
- **3XX**: el servidor espera que el cliente envíe nuevos datos, necesarios para terminar la operación.
- **4XX**: error temporal, se espera a que se repita la instrucción.
- **5XX**: indica una condición de error permanente.

## saber más

Para saber más sobre protocolos de correo lee los RFC:

- SMTP 1870, 5321 y 5322.
- SMTP SPAM 2505.
- SMTP Seguro 2920, 3207.
- SMTP notificaciones 3461.
- Autorrespondedores 3834.
- Internacionalización 5336, 5504.
- Adjuntos 3030.
- SMTP Autenticación 2554.
- Otros: SMTP 3462, 4409, 5068.
- SMTP obsoletos 821, 822, 974, 1653, 1869, 1891, 1892, 1893, 2476, 2487, 2554, 2821, 2822 y 4952.

## 6. Tipos MIME

Los tipos **MIME**, *Multipurpose Internet Mail Extensions* (Extensiones de Correo de Internet Multipropósito) son unas especificaciones de intercambio, a través de internet, de todo tipo de archivos (audio, vídeo, documentos en pdf, en word, etc.) de forma transparente para el usuario. El correo electrónico y las páginas web nacieron en modo exclusivamente de texto, las nuevas necesidades obligaron a crear un sistema que permitiese el intercambio de todo tipo de archivos. El correo es texto puro (en ASCII), mientras que los navegadores solo aceptan de forma nativa el texto (ASCII) y las imágenes (en formatos JPG y GIF). La evolución e internacionalización de internet han hecho que los tipos MIME sean capaces de soportar:

- Textos en caracteres no ASCII (España, Barça, Rodríguez, etc.).
- Ficheros adjuntos que no son del tipo texto.
- Cuerpos de mensajes con múltiples partes (varios megas).
- Internacionalización de las nuevas DNS.

Los tipos MIME son una norma del IETF (*Internet Engineering Task Force*), y están especificados en los RFC 2045, 2046, 2047, 2077, 4288 y 4289.

Existe una lista de los tipos MIME donde se especifica los que soporta cada programa, cada navegador, cada servidor SMTP y cada servidor HTTP. Con programas como MIME Edit podemos modificar el comportamiento del navegador Firefox ante diferentes extensiones de archivos, asociándolos a distintas aplicaciones (pero solo a una a la vez) o simplemente guardándolo en una carpeta. También se pueden añadir nuevos tipos MIME en algunos programas (como por ejemplo en el servidor HTTP Apache).

Extensión	Tipo MIME	Aplicación
323	text/h323	Videoconferencia
AI, PS, EPS	application/postscript	Adobe PS
AVI	video/x-msvideo	Vídeo AVI
BMP	image/bmp	Imagen BMP
CSS	text/css	Estilos web
DOC	application/msword	Microsoft Word
EPS	application/postscript	Adobe PS
GIF	image/gif	Imagen GIF
HTM, HTML	text/html	Texto ASCII HTML
JPE, JPG, JPEG	image/jpeg	Imagen JPEG
JS	application/x-javascript	Java
MOV	video/quicktime	Apple Video Quicktime
PPS	application/vnd.ms-powerpoint	Microsoft Power Point
PDF	application/pdf	Adobe Acrobat
SWF	application/x-shockwave-flash	Flash
ZIP	application/zip	Archivo comprimido

### saber más

Para saber más tipos MIME, consulta los RFC:

- 1426 – 8 bits.
- 1521 – Formatos del cuerpo de mensaje.
- 1847 – Correo multiparte seguro (firmado y encriptado).
- 2045 – Formato de los cuerpos de mensaje.
- 2046 – Tipos de archivos multimedia.
- 2047 – Cabezas de mensaje con texto no ASCII.
- 2049 – Criterios y ejemplos.
- 2183 – Cabeza de mensajes.
- 2231 – Codificación de caracteres.
- 2387 – Tipos de contenido multiparte.
- 3156 – Con seguridad OpenPGP.
- 4288 – Especificaciones.
- 4289 – Procesos de registro.

### saber más

Las listas completas de tipos de MIME están publicadas en internet. Una de las páginas donde las puedes encontrar es:

<http://www.iana.org/assignments/media-types>

## 7. Vulnerabilidades de los servicios de correo electrónico

### recuerda

Un **hacker** es aquella persona que modifica un programa o máquina para alterar su funcionamiento. Los que lo hacen para perjudicar a otros u obtener un beneficio particular se llaman **crackers** o criminales informáticos.

Como todo tipo de software, los servidores tienen vulnerabilidades. Este es un aspecto muy crítico para la seguridad, la confidencialidad y la suplantación, por lo que se aconseja la constante actualización del software, informarse en los foros, listas de distribución o estar dado de alta en news que hablen de este tema (por ejemplo en Google Groups).

Los problemas típicos de un servidor de correo electrónico son:

- **Backdoor** (puerta trasera): secuencia especial del código de programación que usa el programador para acceder o escapar en caso de emergencia, excepción, etc. Terceras personas pueden utilizar las *backdoors* con fines maliciosos y/o espionaje.
- **Bug**: error o defecto de software, estos pueden actuar como «puertas traseras» para los hackers.
- **Exploit** (explotar): forma de automatizar el aprovechamiento de un error o de un fallo para causar un comportamiento no deseado.
- **Malware**: software dañino. Engloba virus, troyanos, automarcadores, spyware (espías), adware (programas publicitarios), keyloggers (secuestraclaves), etc.
- **Hoax** (bulo): correo con contenido falso y atrayente. Se suele distribuir en cadena para captar direcciones de correo electrónico, revelar contraseñas o instalar malware (virus, troyanos, etc.).
- **Phishing**: delito tipo estafa para conseguir, de forma fraudulenta y con «ingeniería social» (engaños o suplantación de personalidad), información confidencial (contraseñas, cuentas o tarjetas bancarias, etc.).
- **Troyano**: programa que lleva en su interior un programa malicioso o un virus.
- **Ataques de denegación de servicio**: bombardeo de mensajes que provoca una respuesta del servidor, saturando los recursos e incluso dejándolo inaccesible durante un tiempo.
- **Spam** (correo basura): mensajes no solicitados, normalmente de publicidad y enviados a gran cantidad de gente a la vez. Muchos proveedores de correo ya consideran spam los mensajes para unos pocos usuarios, otros usan listas, etc.

### caso práctico inicial

Xavi debe recomendar a los trabajadores que no envíen spam.

### caso práctico inicial

Es crucial para Xavi conocer las vulnerabilidades y las precauciones que ha de seguir.

### 7.1. Tipos de spam

Existen dos tipos de correo basura:

- La publicidad encubierta: normalmente son mensajes de relaciones públicas diseñados para promocionar una empresa, producto o individuo. Utilizan un lenguaje comercial y tienen enlaces a páginas comerciales.
- Phishing, virus y otros dañinos.

Hay una categorización dentro de lo que es el spam: pornografía, salud, tecnologías informáticas, finanzas, educación, etc. También existe spam en foros, blogs, wikis, etc.

El spam aumenta el tráfico en internet, ralentiza los equipos, impide a los usuarios la fácil identificación de sus correos, etc. Para evitar problemas, es interesante que el servidor de correo tenga software original y actualizado, un buen antivirus, un eficiente y configurable cortafuegos y un filtro de spam.

Recuerda que estos delitos están contemplados en la LSSI y en la LOPD con multas de hasta 150.000 euros. Según la LSSI (Ley de Servicios de la Sociedad de Información y Comercio Electrónico), el envío de publicidad sin permiso tiene las siguientes clasificaciones:

Infracción	Multa
El envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente [...].	Hasta <b>30.000</b> euros.
El envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente o el envío, en el plazo de 1 año, de más de tres comunicaciones comerciales por los medios aludidos a un mismo destinatario [...].	De <b>30.001</b> hasta <b>150.000</b> euros.

## 7.2. Precauciones

También es más que aconsejable estar informado de las vulnerabilidades del software de correo electrónico en foros y news, por ejemplo:

- SendMail es inseguro en versiones anteriores a la 8.12.10.
- Microsoft Exchange Server es inseguro para IMAP y en general se presta a ataques de denegación de servicios antes de las versiones 2000 SP3, 2003 SP2 y 2007 SP1.
- Google Chrome tiene un buen antivirus y una lista de servidores potencialmente peligrosos, avisándote antes de entrar en esas páginas.
- Internet Explorer es uno de los navegadores que más parches por inseguridad necesita, porque muchos piratas atacan constantemente a Microsoft.

## ACTIVIDADES

1. Crea tu propia lista de ventajas e inconvenientes del correo tradicional, el correo electrónico y el webmail. Si no se te ocurre nada, lo mejor es que lo hagáis en grupos de cinco personas.
2. Busca en internet información, a fecha de hoy, sobre el uso del correo electrónico. ¿Cuántas personas tienen correo? ¿Cuántos mensajes mandan? ¿Qué cantidad de spam reciben?, etc.
3. Localiza la definición de lista de correo o lista de distribución.
4. Diferencia entre correo, foro y Messenger.
5. Busca comparativas entre clientes de correo (Internet Explorer, Thunderbird, etc.).
6. En internet, busca las últimas vulnerabilidades detectadas de los servidores de correo electrónico.
7. Diferencia entre los campos del correo electrónico CC y CCO.
8. ¿Qué son las listas de Robinson? ¿Qué te parecen?
9. En EE. UU. no han tenido mucho éxito las leyes antispam. Busca jurisprudencia o noticias de juicios en España sobre el spam. ¿Te parecen útiles las leyes que existen si el spam ronda el 40% de todos los mensajes del mundo? ¿Qué solución darías?
10. Debatid en clase posibles medidas para evitar el spam.
11. Haz una lista de cinco familiares y cinco amigos. ¿Cuántos tienen correo? ¿A cuántos los tienes en tu agenda de correo?

## 8. Clientes de correo electrónico

### 8.1. Linux

#### Texto

Las órdenes mail desde el terminal de Linux y ml desde UNIX permiten enviar y recibir correo electrónico. Las versiones de escritorio (*Desktop*) no tienen estas órdenes por defecto, por ello recomendamos instalar el paquete mutt.

Para configurar el cliente con nuestra cuenta de correo como las de Gmail, editamos el archivo oculto `.muttrc`. Para una cuenta como por ejemplo `tomatesrizados@gmail.com` por IMAP, quedaría así (los comentarios van detrás de la almohadilla `[#]`):

```
set from="tomatesrizados@gmail.com" #Dirección de correo.
set realname="Tomates Rizados SL" #Nombre real.
set imap_user="tomatesrizados@gmail.com" #Usuario IMAP.
set imap_pass="tupass" #Contraseña.
set folder="imaps://imap.gmail.com:993" #Buzón seguro.
set spoolfile="+INBOX"
set postponed="+[Gmail]/Drafts"
set trash="imaps://imap.gmail.com/[Gmail]/Trash"
set header_cache=~/.mutt/cache/headers
set message_cachedir=~/.mutt/cache/bodies
set certificate_file=~/.mutt/certificates
set check_new # Revisa el correo electrónico.
set mail_check=60 # Lo revisa cada x segundos, en este caso 60.
set beep_new # Suena un beep si se recibe correo nuevo.
set move=no # Para que no mueva los mensajes al salir.
set include=yes # Al responder incluye el mensaje recibido.
set reply_to=yes # Activa el responder.
set pager_index_lines=6
set sendmail=/usr/bin/msmtp # Para enviar correo.
```

Ahora ya podemos ejecutar `mutt`, pero de momento solo recibiremos correos. Para poder enviar debemos instalar y configurar el SMTP (paquete `msmtprc`). Editamos el archivo de configuración oculto `.msmtprc`:

```
defaults
tls on
account default
host smtp.gmail.com # Pon el servidor SMTP.
from tomatesrizados@gmail.com # Pon tu mail.
auth on # Publicita el autor.
tls_certcheck off # Desactiva certificados.
user tomatesrizados@gmail.com # Usuario.
password tupass # Tu contraseña.
port 587 # El puerto (en este caso el de smtp.gmail.com).
```

Debemos cambiarle los permisos a este archivo a 600.

Ahora ya podemos escribir el mensaje en cualquier editor (nano, gedit, joe, vi, etc.) y enviarlo desde `msmtprc`.

#### saber más

Los comandos más importantes de `msmtprc` son:

- m** – nuevo correo.
- y** – confirmar el envío.
- r** – responder.
- a** – adjuntar un archivo.

Tanto para Linux como para Windows, podemos descargar Mozilla Thunderbird, cliente de correo gratuito que soporta IMAP/POP/Webmail, news, RSS, corrector ortográfico, cifrado PGP, antispam... Linux ya tiene instalado un cliente gráfico llamado Evolution.

Descargamos el programa desde <http://www.mozilla-europe.org> (la web detecta tu sistema operativo y el idioma), la instalación es muy intuitiva (debe descomprimirse). Es más sencillo hacerlo desde el gestor de paquetes.



Para configurar una cuenta de correo electrónico debemos conocer los servidores POP (o IMAP o Webmail para la recepción) y el SMTP (para el envío), si hemos alquilado un dominio, estarán expresados en el contrato; si es gratuito podemos consultarlos en internet (por defecto solo acepta webmail de Gmail, pero pueden instalarse parches para soportar otros como Hotmail). Para ello iremos a **APLICACIONES > INTERNET > THUNDERBIRD MAIL** donde la primera vez que entremos aparecerá el asistente de cuentas. Si quisieramos añadir deberíamos ir a **EDITAR > CONFIGURACIÓN DE LAS CUENTAS**, seleccionaríamos **CUENTA DE CORREO ELECTRÓNICO**, pulsaríamos **SIGUIENTE**; completaríamos el nombre (un alias que aparecerá al enviar el correo y el correo electrónico) y pulsaríamos **SIGUIENTE**; introduciríamos el nombre de los servidores (POP o IMAP y SMTP) y pulsaríamos **SIGUIENTE**.

Después tendríamos que poner el nombre de usuario (que suele ser la parte anterior a la arroba, o el correo completo, pero puede ser de otra forma. Ejemplos: «usuario», «usuario\$terra.es», «usuario@gmail.com», etc.).

Pulsaríamos **SIGUIENTE**, añadiríamos el nombre de cuenta y pulsaríamos **TERMINAR**.

Para recibir correo debemos pulsar **RECIBIR MENSAJES**.



Para enviar un correo nuevo debemos pulsar **REDACTAR**.



Para adjuntar archivos, **ADJUNTAR**.



Para configurar el filtro de mensajes spam debemos ir a **HERRAMIENTAS > CONTROLES DE CORREO BASURA**.

Existe la posibilidad de activar el acuse de recibo al crear una cuenta.

## saber más

Para poder leer correo electrónico de Gmail con cualquier cliente, debemos entrar en [gmail.com](http://gmail.com) y en **CONFIGURACIÓN > REENVÍO Y CORREO POP/IMAP**.



## vocabulario

**Acuse de recibo:** El acuse de recibo fuerza al destinatario a enviarte un correo (lo hace automáticamente su cliente de correo) si quiere ver el contenido del e-mail. Esto es muy interesante para las empresas, porque por ejemplo, se ahorran dinero en burofax, en el caso de que necesitasen una prueba válida judicialmente, el acuse de recibo les serviría.

## 8.2. Windows

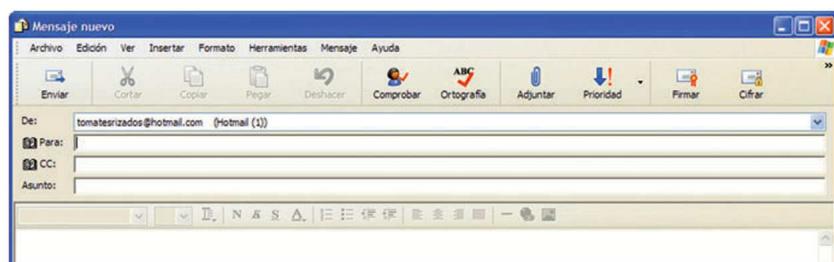
### caso práctico inicial

Debemos aconsejar a Xavi que elija entre Outlook y Thunderbird.



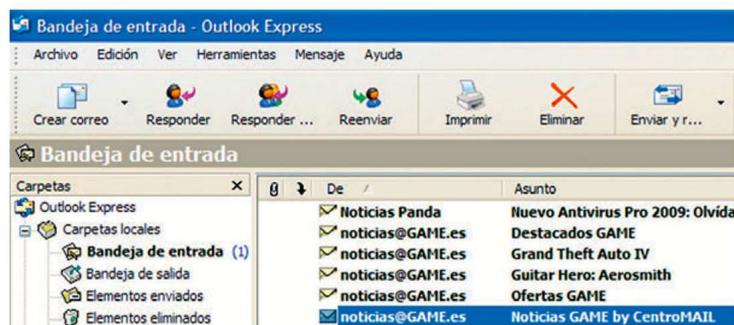
Windows instala, por defecto, Outlook Express (algunos prefieren Microsoft Office Outlook, del paquete Office). Windows 98 tiene accesos directos en el escritorio; Windows XP los tiene en el menú de inicio; Windows Vista también, pero el nombre es Windows Mail; en Windows 7 aparece un ícono en el extremo izquierdo de la barra de tareas (junto a Internet Explorer). Como todos los clientes, requiere una configuración inicial de los servidores que, en todas sus versiones, aparece en **HERRAMIENTAS > CUENTAS**. Pulsamos **AGREGAR > CORREO**, escribimos el **NOMBRE PARA MOSTRAR** (el que verá el destinatario) y pulsamos **SIGUIENTE**. Introducimos la **DIRECCIÓN DE CORREO ELECTRÓNICO** y pinchamos en **SIGUIENTE**. En **MI SERVIDOR DE CORREO ENTRANTE ES** seleccionamos **POP3, IMAP o HTTP** según corresponda (**HTTP** solo soporta Hotmail, MSN y los de Microsoft; el servicio es de pago para nuevos usuarios y gratuito para los que ya tienen cuentas. Usamos el servidor **HTTP http://services.msn.com/svcs/hotmail/httpmail.asp**). Pulsamos **SIGUIENTE** y completamos el **NOMBRE DE CUENTA** (con el correo electrónico), la **CONTRASEÑA** (podemos activar la casilla **RECORDAR CONTRASEÑA** solo si al equipo no tiene acceso nadie) y/o **INICIAR SESIÓN USANDO AUTENTICACIÓN DE CONTRASEÑA SEGURA (SPA)** (algunos servidores lo requieren). Pulsamos **FINALIZAR**.

Para recibir correo (y enviarlo después de escribirlo) debemos pulsar **ENVIAR Y RECIBIR TODO**. Cuando queramos escribir un mensaje nuevo pulsaremos **CREAR CORREO** y nos aparecerá la siguiente ventana:



Los elementos **DE**, **PARA**, **CC**, **ASUNTO** y **CUERPO** se ven directamente. Al terminar de redactar el correo pulsamos **ENVIAR** (no lo envía directamente, lo pasa a la **BANDEJA DE SALIDA**, esperando que marquemos **ENVIAR Y RECIBIR TODO**). Para añadir archivos debemos pulsar **ADJUNTAR**. Si queremos elevar la prioridad del mensaje lo seleccionaremos pulsando **PRIORIDAD**.

En **HERRAMIENTAS > SOLICITAR CONFIRMACIÓN DE LECTURA** podremos forzar el acuse de recibo.



Desde la **BANDEJA DE ENTRADA**, pulsando sobre un mensaje, podemos leerlo o realizar las siguientes acciones: **ELIMINAR** (pasa a la **BANDEJA DE ELIMINADOS**), **RESPONDER** (crea un mensaje con el nombre del emisor como destinatario y copia el cuerpo del mensaje), **RESPONDER A TODOS** (responde a todos los destinatarios del campo **DE** y **CC**) o **REENVIAR** (copia el cuerpo y los archivos adjuntos, con el campo **PARA** vacío).

## 9. Servidores de correo electrónico

En todos los servicios de internet existe un servidor que es el más usado con diferencia. Este no es el caso del correo electrónico, ya que se emplean mucho tanto Sendmail (que es el más usado aunque con poca diferencia, y el más versátil, y por ello el más difícil) como Postfix para Linux, aunque algunos prefieren Qmail, Exim, World Group Mail, etc. En el caso de Windows, el servidor más usado es Microsoft Mail Exchange. Parece que la solución más profesional es Sendmail sobre Linux Open Susse, acompañado de Spamassassin, MailScanner y Clamav (e incluso WhiteBox, Dovecot y Horde, que evitan el spam, los virus, no limitan las cuentas...). Nosotros veremos Postfix sobre Ubuntu, por ser el más fácil. Lo único claro es que no es muy recomendable usar servidores de correo electrónico con Linux Cent OS.

Instalamos el paquete de Postfix. Lo arrancamos con `/etc/init.d/postfix start`. Sería interesante probarlo con un `telnet localhost 25`, si nos contesta con un mensaje 220 ponemos `helo localhost`. Si nos contesta un 250, probamos `mail from: root` (este usuario debe existir y tenemos que estar en una de sus sesiones). Se lo enviamos a un usuario que exista en este servidor: `rcpt to: xavi`. Empezamos a enviar con `data`, seguimos con `subject: primer correo de prueba`, luego escribimos las líneas que queramos enviar (la última debe tener solo un punto [.]). Abandonamos la sesión con `quit`. Ahora entramos con el usuario destinatario (Xavi en nuestro ejemplo), y si todo ha ido bien nos aparecerá un mensaje tipo «*You have mail in /var/spool/mail/xavi*». Ahora, para que el servidor no sea solo local, debemos editar el archivo `/etc/postfix/main.cf`:

```
myhostname = smtp.tomatesrizados.eu          # Nombre del servidor.
mydomain = tomatesrizados.eu                  # Nombre del dominio.
mynetworks = 192.168.0.0/24                   # Red desde donde
                                                # enviarán correo.
defer_transports = smtp                      # Crea una cola, por
                                                # si no conectamos el
                                                # servidor las 24 horas.
relayhost = smtp.gmail.com                   # Delega el envío a
                                                # otro servidor SMTP.
myorigin = tomatesrizados.eu                 # Enmascara el correo
                                                # local (LAN e internet).
masquerade_domain = tomatesrizados.eu       # Enmascara el correo local
                                                # (aconsejado solo internet,
                                                # no para LAN e internet).
inet_interfaces = all                        # Interfaces que escuchará
                                                # (all/eth0/eth1/localhost...).
mailbox_size_limit = 51200000                 # Límite del buzón en KB
                                                # (por defecto 50 MB).
message_size_limit = 10240000                 # Límite del mensaje en KB
                                                # (por defecto 10 MB).
smtpd_banner = $myhostname                   # Identificación.
                                                # (Tomates Rizados SL)
mydestination = localhost, $myhostname,
                localhost.$mydomain, $mydomain
```

### saber más

Para más información visita:

- [sendmail.org](http://sendmail.org)
- [postfix.org](http://postfix.org)
- [qmail.org](http://qmail.org)
- [Group-Mail.com](http://Group-Mail.com)
- [microsoft.com/exchange](http://microsoft.com/exchange)
- [linuxparatodos.net](http://linuxparatodos.net)
- [qmailtoaster.com](http://qmailtoaster.com)
- [forosdelweb.com](http://forosdelweb.com)
- [apache.org/spamassassin](http://apache.org/spamassassin)
- [mailscanner.info](http://mailscanner.info)
- [ubuntuforums.org](http://ubuntuforums.org)
- [jacobs-university.de](http://jacobs-university.de)

### saber más

Servidores más frecuentes:

- [pop.gmail.com:995](http://pop.gmail.com:995) con SSL
- [smtp.gmail.com:465](http://smtp.gmail.com:465) con SSL /TLS
- [imap.gmail.com:993](http://imap.gmail.com:993) con SSL
- [pop3.live.com:995](http://pop3.live.com:995) con SPA
- [smtp.live.com:25](http://smtp.live.com:25) con SSL
- [pop.mail.yahoo.com:110](http://pop.mail.yahoo.com:110)
- [smtp.mail.yahoo.com:25](http://smtp.mail.yahoo.com:25)
- [pop3.email.msn.com:110](http://pop3.email.msn.com:110) con SPA
- [smtp.email.msn.com:25](http://smtp.email.msn.com:25) con SSL
- [smtp.terra.es:25](http://smtp.terra.es:25)
- [smtp.wanadoo.es:25](http://smtp.wanadoo.es:25)

### caso práctico inicial

Aunque Xavi prefiere los servidores Windows (sobre los de la familia Unix), debe elegir un servidor de correo compatible con el sistema operativo y su versión (incluido si es de 32 o 64 bits).

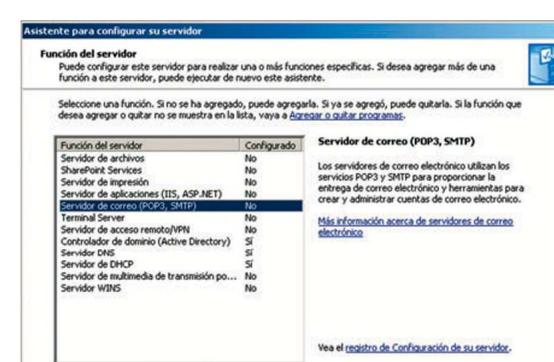
Para Windows, Microsoft Exchange Server 2010 permite gestionar el correo, pero está preparado para Windows Server 2010 con un procesador de 64 bits. Según el sistema operativo que vayamos a utilizar, se recomienda un servidor de correo distinto:

Versión + Procesador	Programas
95, 98, 98 SE, Me	ArGoSoft Mail Server (gratuito)
NT 4 SP6, NT 5, NT 6, Server 2000, XP Professional x32	MailEnable
Server 2000 SP4 Server 2003 32 XP Professional SP1	Microsoft Exchange Server 2003 SmarterMail Correo POP3 y SMTP de Active Directory
Server 2003 x64 Server 2008 x64	Microsoft Exchanger Server 2007 SP1 Correo POP3 y SMTP de Active Directory
Server 2010 x64	Microsoft Exchange Server 2010 Correo POP3 y SMTP de Active Directory



La pantalla de **CONFIGURAR EL SERVICIO POP3** no da la opción (mediante menú desplegable) de utilizar el **INTEGRADO EN ACTIVE DIRECTORY** o **ARCHIVO DE CONTRASEÑA CIFRADA** (es mejor este último si no hemos instalado más servicios o no deseamos correo local). En **NOMBRE DE DOMINIO DE CORREO ELECTRÓNICO** debemos escribir el nombre que tengamos alquilado (tomatesrizados .eu en nuestro caso).

<b>Configurar el servicio POP3</b>	Debe especificar cómo se autenticarán en el servidor los clientes de correo electrónico, así como el nombre de dominio de correo electrónico.
Selección del tipo de autenticación de usuario:	<input checked="" type="radio"/> Integrado en Active Directory <input type="radio"/> Integrado en Active Directory <input type="radio"/> Archivo de contraseña cifrada
Nombre de dominio de correo electrónico:	<input type="text"/>



### recuerda

Si al instalar el servidor POP3 en Active Directory, este no encuentra el archivo issapp.vbs podrás bajártelo desde Microsoft.com, para el 2003 valdría el SP1. Para NT, 2003 y XP Professional, busca el paquete *Administration Tools Pack*.

Existen distintas versiones de este paquete, asegúrate de la versión que tienes (el 2003 o el 2003 R2), porque quizás te convenga bajarte el SP2.

Pulsamos **SIGUIENTE** y esperamos a la instalación del servidor POP3 (nos pedirá el CD de instalación de Windows). Para terminar, pulsamos **FINALIZAR**.

Antes de configurar debemos repasar los siguientes aspectos:

- Disponemos de una partición NTFS para poder establecer cuotas de disco para el correo electrónico.
- Tenemos alquilado un nombre de dominio (a no ser que solo queramos servicio local para la LAN, para lo que usamos localhost@localdomain).
- Podemos alterar el servidor de nombres en nuestra LAN o si nuestro ISP nos lo permite (registros MX).
- Poseemos una IP estática, o podemos configurarla con noIP, etc.
- Hemos configurado correctamente el direccionamiento inverso en el servidor DNS (si no, se marcarán nuestros correos como spam).
- Tenemos un buen cortafuegos y los puertos de correo abiertos.

Ahora debemos crear buzones de correo (para cada usuario cada buzón debe ser distinto), para ello podemos usar el complemento **Microsoft Management Console** (MMC) del servicio POP3 de Windows, que es gráfico, o la orden **winpop** (desde la línea de comandos). Para el MMC pulsamos **INICIO > PANEL DE CONTROL > SERVICIO POP3**, en la parte izquierda, en el árbol desplegable, pulsamos con el botón secundario del ratón sobre el dominio en el que deseamos crear las cuentas. Pulsamos **NUEVO > BUZÓN** y completamos en el formulario los siguientes datos:

- **NOMBRE DE BUZÓN**: suele ser el nombre de usuario, si no existe se debe crear. La longitud máxima es 20 caracteres para cuentas locales y 64 para otras.
- **CONTRASEÑA** y **CONFIRMAR CONTRASEÑA**: aquí se introduce la contraseña.

En línea de comandos, podemos dar de alta un buzón con esta sintaxis:

```
winpop add dominio\usuario@dominio [/createuser contraseña]
```

### EJEMPLO

```
winpop add tomatesrizados.eu
winpop add xavi@tomatesrizados.eu
winpop add xavi@tomatesrizados.eu /createuser 123456javi++
```

## 9.1. Configuración de alias

Como ya hemos indicado anteriormente, solemos usar los alias para nombrar al mismo buzón de correo de distintas maneras y que así parezcan varias cuentas. Es como si Xavi usase indistintamente los nombres Xavi, Javier, Xabi, Sabih, etc. (dependiendo de con quién hable o en qué comunidad esté). Pero también existe la posibilidad de utilizar los alias para distintos servidores de correo (pero es el mismo buzón de correo, no son distintos correos, están redirigidos desde el servidor DNS con registros MX y/o CNAME) o para correo local (`xavi@localhost`, `xavi@tomatesrizados.eu`, `xavi@gmail.com`), este caso sería como utilizar Xavi en el instituto, Don Andréu en el trabajo, etc.

En el caso del `localhost`, si el emisor y el destinatario están en la misma red o dependen del mismo servidor, los mensajes no llegan a salir a internet, evitando el tráfico innecesario.

### caso práctico inicial

Para los buzones de correo de Windows, Xavi necesita conocer estas restricciones.

### recuerda

El servidor de correo está relacionado con el IIS, si se borrase un dominio eliminaríamos todos sus buzones de correo y sus correos electrónicos.

### recuerda

No podemos usar para nombres de buzón los caracteres: `@()`/`[]``:``;``<>``*``=``?``+`.

### saber más

Para las opciones de **winpop**:  
**createquotofile**: crear cuotas de disco,  
**delete**: eliminar usuarios,  
**changepwd**: cambiar contraseña,  
etc., consulta la ayuda de Windows Server o entra en <http://technet.microsoft.com/es-es>

### caso práctico inicial

Para los departamentos, Xavi puede de que necesite crear alias de correo emisor.

## vocabulario

**Correo local:** Correo de la LAN, que gestiona un mismo servidor.

**Correo externo:** Correo de una WAN que gestiona un servidor externo o varios.

## saber más

Todos estos alias se mencionan en el RFC 5321.

Configurar alias en Linux (con Postfix) requiere añadir en el archivo /etc/postfix/main.cf la línea:

```
alias_maps = hash:/etc/postfix/aliases
```

Entonces ya podemos editar /etc/aliases (que también se suele encontrar en /etc/postfix/aliases) y añadir una línea por cada alias. Imaginemos que a Xavi le queremos poner tres alias (como si tuviese tres correos, pero todos son el buzón xavi):

```
root      xavi
webmaster xavi
compras   xavi
```

Algunas versiones añaden dos puntos después del nombre de usuario:

```
root:      xavi
```

Para que estos cambios surtan efecto debemos ejecutar el comando newaliases. Aunque no sean alias, a veces necesitamos enviar archivos con una cuenta local, pero queremos que se refleje con un dominio que hemos alquilado. Para ello editamos (o creamos, según corresponda) el archivo /etc/postfix/sender\_canonical, que contiene las correspondencias entre buzones locales y externos:

```
xavi@localdomain      xavi@tomatesrizados.eu
Juan@localdomain       Juan@gmail.com
```

Para que se cree la base de datos indexada (que crea un archivo más veloz), ejecutamos:

```
postalias hash:sender_canonical
```

Y añadimos en el archivo /etc/postfix/main.cf la siguiente línea:

```
sender_canonical_maps
hash:/etc/postfix/sender_canonical
```

Los cambios surtirán efecto al reiniciar el servidor:

```
postfix reload
```

Ahora solo nos queda hacer lo mismo para recibir, con la salvedad de que en el archivo /etc/postfix/recipient\_canonical invertimos el orden de las columnas:

```
xavi@tomatesrizados.eu      xavi@localdomain
```

## 9.2. Usos indebidos

En cuanto configuremos un servidor de correo electrónico nos «lloverán» los ataques para usar el servidor como *open-relay* (retransmisor de correo spam).

Gestionar un correo requiere mucha responsabilidad, no solo para evitar virus o el ser receptores de miles de correos spam, sino también para evitar que consiga ejecutar un proceso *zombie* que envíe correo spam y que eso provoque que nos incluyan en «listas negras», no pudiendo usar el servicio de correo adecuadamente.

Otros usos indebidos son delitos, como:

- La suplantación de personalidad: que puede demostrarse con los registros de direcciones IP de los accesos al servidor.
- La lectura del correo de ex empleados en las empresas: en estos casos se recomienda cambiar las contraseñas cada vez que entra un empleado nuevo o cada 6 meses.
- El acceso a nuestro correo por parte de personas no autorizadas: debido a que muchas veces dejamos las cuentas abiertas y cualquiera puede acceder.

### **caso práctico** inicial

Es crucial para Xavi tener en cuenta las conexiones *open-relay*.

### **recuerda**

El derecho a la intimidad y el secreto de las comunicaciones está amparado en la Constitución española. El correo electrónico junto con las redes sociales, los chat, SMS y MMS están incluidos en este derecho, por lo que según el Código Civil, leer sin permiso un correo, puede penarse hasta con 1 año de cárcel.

## ACTIVIDADES

12. Configura una cuenta de correo en Thunderbird.
13. Configura una cuenta de correo en Outlook.
14. Envíate un correo con una imagen JPG adjunta desde Thunderbird. Abre el mensaje, ¿ves la imagen o necesitas abrirla?
15. Envíate un correo con una imagen TIF o PNG adjunta desde Outlook. Abre el mensaje, ¿ves la imagen o necesitas abrirla?
16. Envía a tus compañeros (al menos a dos) un correo con copia oculta desde Thunderbird.
  - a) ¿Cómo les ha llegado?
  - b) ¿Pueden contestarte?
  - c) ¿Pueden contestarse entre ellos?
17. Envía a tus compañeros (al menos a dos) un correo con copia oculta desde Outlook. ¿Es más fácil la configuración en Thunderbird o en Outlook?
18. Envíate un correo con confirmación desde Thunderbird, comprueba si se ejecuta. ¿Para qué (o cuándo) crees que se puede usar esta opción?
19. Envíate un correo con confirmación desde Outlook. Comprueba si se ejecuta.
20. Envíate un correo de alta prioridad desde Thunderbird. Comprueba que ha llegado, ¿qué símbolo aparece junto al correo?
21. Envíate un correo de alta prioridad desde Outlook. Comprueba que ha llegado, ¿qué símbolo aparece junto al correo?
22. Para una cuenta de correo electrónico de la LAN, configura el cliente de correo mutt en modo texto para Linux. Comprueba que funciona enviándote un correo a ti y a un compañero.
23. ¿Qué servidor de POP3 y SMTP te conviene para el sistema operativo para servidores que tienes instalado?
24. Configura en Thunderbird la opción de evitar correo basura.

## 10. Correo seguro

El correo electrónico viaja por internet «sin sobre», puede leerse como si fuese una postal, no tiene ningún tipo de protección. Existen distintas alternativas para autenticar al emisor y para evitar que se visualicen los mensajes. Ya vimos la posibilidad que tenía el servicio SSH de crear túneles, incluso para el correo; pero existen otras alternativas, como la firma digital, que permite conocer al emisor, y el cifrado de mensajes, para evitar que sean leídos por quien no es el receptor (que el código solo sea compartido por el emisor y el receptor será lo que protegerá al correo). Actualmente algunos programas añaden la posibilidad de saber si el mensaje fue manipulado por el camino, además de otras características del SSH.

### 10.1. Firma digital

#### recuerda

La **criptografía** es una ciencia (y un arte) que cifra (y descifra) los mensajes con determinados algoritmos matemáticos para que solo el emisor y el receptor entiendan la información.

La firma digital es, en la transmisión de mensajes telemáticos (digitales, informáticos) y en la gestión de documentos electrónicos, un método criptográfico que asocia la identidad de una persona o un sistema informático a ese mensaje o documento. Es, a todos los efectos, como una firma autógrafa. Algunos tipos de firma pueden asegurar que el mensaje no ha sido manipulado. La firma digital se basa en dos claves, una pública y otra privada. Algunas características son:

- Atribuye de forma irrefutable la identidad del usuario (mientras guarde la clave).
- Asegura la integridad del mensaje (en los algoritmos actuales).
- Garantiza su origen, evitando que el emisor pueda repudiarlo.
- Es confidencial (de momento y con la tecnología actual).

Para obtener las claves hace falta acudir a una **Autoridad Certificadora (AC)**. En Europa, las AC están listadas como **Prestadores de Servicios de Certificación**, aunque existen **Autoridades Locales de Registro**, por ejemplo, muchas Comunidades Autónomas tienen sus propias certificaciones y suelen delegar en los ayuntamientos.

En el ámbito estatal, la Fábrica Nacional de Moneda y Timbre (FNMT) delega en todas las oficinas de Hacienda, la ACE (Agencia de Certificación Electrónica) delega en los bancos y cajas, la FESTE (Fundación para el Estudio de la Seguridad de las Telecomunicaciones) delega en notarios, registradores, etc. Estas firmas se entregan en disquete, CD, pendrive o en el **DNI-e** (nuevo DNI en España, Documento Nacional de Identidad Electrónico).

Internacionalmente, existe una autoridad certificadora de la comunidad de internet llamada CAcert.org.

#### saber más

Los Prestadores de Servicios de Certificación españoles más conocidos son:

- CERES (FNMT).
- ANCERT (notarios).
- ACCV-GVA (Gobierno valenciano).
- BANESTO (banco).
- CAMERFIRMA (c. de comercio).
- CATCert (Gobierno catalán).
- C. O. Arquitectos de Sevilla
- D. G. de la Policía y de la G. C.
- Ministerio de Defensa.
- Registradores de España.
- Santander (banco).
- Telefónica Empresas.

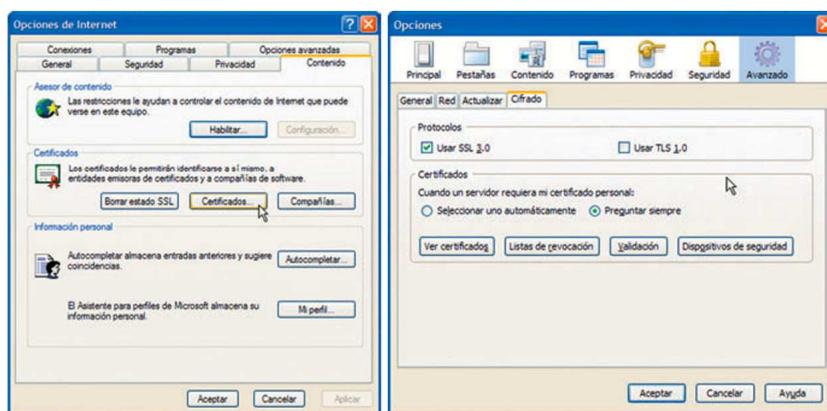


Para leer el DNI-e hace falta un periférico llamado lector de DNI-e que cuesta, aproximadamente, 40 euros. Muchos usuarios usan un lector ISO 7816 que sirve para EMV (Europay, MasterCard y Visa) y GSM (para tarjetas SIM de móviles) y que cuesta la mitad.

Cuando se requiere la utilización de una firma digital lo único que hay que hacer es introducir el soporte de almacenamiento que las contiene. Se pueden instalar en la mayoría de los navegadores. En el caso de que queramos que solo se instale en el navegador que tenemos predeterminado únicamente tendremos que hacer doble clic sobre el certificado.

### recuerda

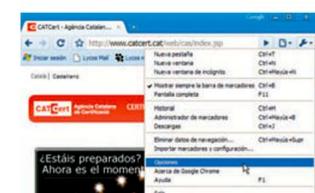
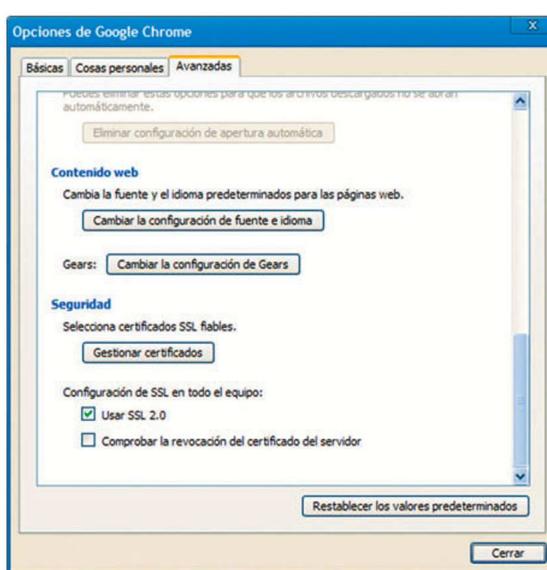
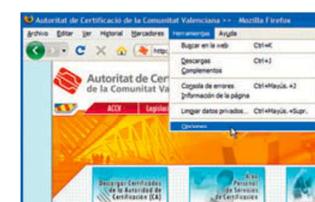
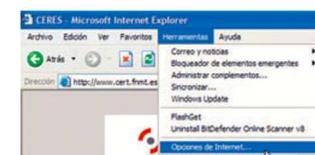
La firma digital tiene la misma vigencia legal que la firma autógrafa, por lo que es muy necesario proteger los archivos de las claves. También se puede usar para comunicaciones burocráticas.



Podemos forzarlo para Internet Explorer: en el menú **HERRAMIENTAS > OPCIONES DE INTERNET**, pulsamos en la pestaña **CONTENIDO**, después en el botón **CERTIFICADOS** y, por último, en **IMPORTAR**.

En Firefox **HERRAMIENTAS > PREFERENCIAS > AVANZADAS > CERTIFICADOS > ADMINISTRAR CERTIFICADOS... > IMPORTAR**.

En Google Chrome pulsamos sobre el icono de la llave inglesa, después en **OPCIONES**, y en la solapa de **AVANZADAS** pulsamos el botón **GESTIONAR CERTIFICADOS > IMPORTAR**.



## 10.2. Cifrado de mensajes

### saber más

Existen algoritmos de encriptación que pueden romperse con ataques de fuerza bruta o bombardeo de claves, por ello debemos tener en cuenta:

Tipo	Reventable	Aconsejado
RSA	512 bits	2.048 bits
DSA	64 bits	2.048 bits
AES	64 bits	128 bits
IDEA	64 bits	128 bits
SSL	40 bits	1.024 bits
TLS	40 bits	128 bits

Cuando hablamos del cifrado de los mensajes nos referimos al proceso por el cual se encriptan, se codifican los textos. La encriptación, la criptografía para «escribir oculto», codifica la información mediante algoritmos matemáticos, de tal manera, que solo el emisor y el receptor puedan descodificarla. Existen muchísimos algoritmos de codificación (RSA, DSA, SPA, PGP, SSL, etc.), pero en el caso del correo electrónico nos limitaremos a los que usan los servidores. Lo primero que tenemos que hacer es instalar programas que nos permitan soportar SASL (método de autenticación) y TLS (cifrado e integridad para los correos) como vemos en el *saber más* del lateral.

Creamos el archivo `/etc/postfix/ssl` y ejecutamos:

```
# openssl genrsa -des3 -rand /etc/hosts -out smtpd.key 1024
      (Asignamos la longitud de clave)
# chmod 600 smtpd.key
# openssl req -new -key smtpd.key -out smtpd.csr
# openssl x509 -req -days 3650 -in smtpd.csr -signkey
      smtpd.key -out smtpd.crt
# openssl rsa -in smtpd.key -out smtpd.key.unencrypted
# mv -f smtpd.keyunencrypted smtpd.key
# openssl req -new -x509 -extensions v3_ca -keyout cakey.
      pem -out cacert.pem -days 3650
```

### saber más

Para instalar en Linux los programas que nos permitan soportar SASL y TLS usamos como administrador:

```
#apt-get install
cyrus-sasl libssl2
libssl2-devel
libssl2-plug-plain
libssl2-plug-anonymous
libssl2-plug-crammd5
libssl2-plug-digestmd5
libssl2-plug-gssapi
libssl2-plug-login
```

Entonces debemos modificar el archivo `/etc/postfix/main.cf`:

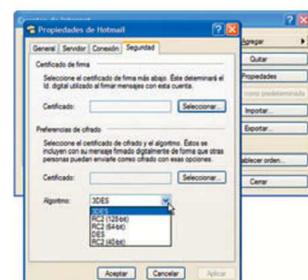
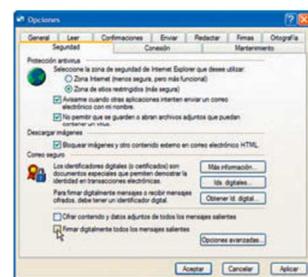
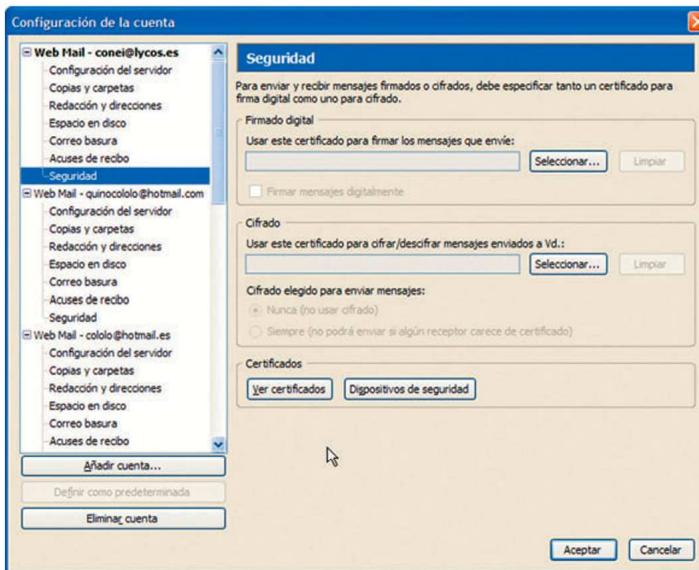
```
smtpd_sasl_path = /etc/postfix/sasl:/usr/lib/sasl2
smtpd_sasl_auth_enable = yes
smtpd_sasl_local_domain = $myhostname
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtp_use_tls = yes
smtp_tls_note_starttls_offer = yes
smtpd_use_tls = yes
smtpd_tls_auth_only = yes
smtpd_tls_key_file = /etc/postfix/ssl/smtpd.key
smtpd_tls_cert_file = /etc/postfix/ssl/smtpd.crt
smtpd_tls_CAfile = /etc/postfix/ssl/cacert.pem
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s          #Segundos de cache.
tls_random_source = dev:/dev/urandom
smtpd_helo_required = yes
strict_rfc821_envelopes = yes
smtpd_sender_restrictions=
check_sender_access hash:/etc/postfix/lista_blanca
smtpd_recipient_restrictions = reject_invalid_hostname,
reject_non_fqdn_hostname, reject_non_fqdn_sender,
reject_unknown_sender_domain, reject_unknown_recipient_domain,
permit_mynetworks, permit_sasl_authenticated,
reject_unauth_destination, reject_rbl_client tomatesrizados.eu
```

En el caso de los servidores Windows, para activar la posibilidad del correo seguro debemos abrir el servicio POP3: en el árbol de la consola pulsamos con el botón secundario del ratón en el nombre del equipo (no del dominio) y pulsamos PROPIEDADES. Seleccionamos REQUERIR AUTENTICACIÓN DE CONTRASEÑA SEGURA (SPA) PARA LAS CONEXIONES DE CLIENTE.

En línea de comandos podemos usar el comando `winpop`, asignándole el valor 1 para activar la autenticación SPA o 0 para desactivarlo:

```
winpop set sparequired 1
```

Para configurar la autenticación en el cliente de una cuenta existente (podemos hacerlo al crear una nueva cuenta) para Thunderbird pulsamos en el menú HERRAMIENTAS > CONFIGURACIÓN DE CUENTAS; para cada buzón de correo POP3 que hayamos configurado debemos ir a la opción de SEGURIDAD. Pulsaremos en SELECCIONAR, en FIRMA DIGITAL y/o CIFRADO (según deseemos) y buscaremos el certificado de cifrado o firma (según corresponda). En el caso de seleccionar un certificado para el cifrado, seleccionaremos CIFRADO ELEGIDO PARA ENVIAR MENSAJES, pulsando al botón de elección SIEMPRE.



Para Outlook pulsamos en el menú HERRAMIENTAS > OPCIONES y en la solapa de SEGURIDAD activamos CIFRAR CONTENIDO Y DATOS ADJUNTOS DE TODOS LOS MENSAJES SALIENTES y/o FIRMAR DIGITALMENTE LOS MENSAJES SALIENTES.

Para el servidor SMTP (de IE), desde HERRAMIENTAS > CUENTAS nos vamos a la solapa SEGURIDAD y podemos cargar los certificados, para el cifrado podemos seleccionar varios algoritmos de distintas longitudes.

En Thunderbird, el servidor SMTP puede modificarse con el botón editar (del administrador de cuentas) y seleccionaremos SSL o TLS.

Si no queremos utilizar las claves de una AC, podemos usar el sistema PGP (*Pretty Good Privacy*), que permite asegurar la confidencialidad, la autenticación e integridad del correo.

## saber más

PGP está explicado en los RFC 2440 y 4880. Países como China lo prohíben (este algoritmo y toda la criptografía), y EE. UU. y Francia limitan la longitud de las claves.

### saber más

Para mostrar la ayuda de PGP, ejecuta pgp -h en línea de comandos.



Para todos los sistemas operativos (Amiga, Atari, BeOS, EPOC, Mac OS X, MS-DOS, Newton, OS/2, Palm OS, Unix, Windows 9x, Windows Me y Windows 2000/XP/Vista) tenemos una versión gratuita para línea de comandos en <http://www.pgp.org> y una versión de evaluación gráfica (cliente y servidor solo para Windows y Unix, está especialmente diseñado para las versiones Red Hat y Suse de Linux) en <http://www.pgp.com>. Algunas personas no utilizan PGP como cliente, sino solo para crear las claves que se generan en los archivos PUBRING.PKR y SECRING.SKR. También es posible cifrar archivos o particiones con este programa o crear particiones virtuales cifradas.

Para Windows bajamos el archivo, lo descomprimimos y creamos las claves pgp -kg.

Para cifrar un mensaje, primero lo escribimos en un archivo de texto ASCII y luego ejecutamos la sintaxis:

```
pgp -e archivo userid
```

### EJEMPLO

```
pgp -e mensaje1.txt Alicia
```

Para desencriptar usamos la sintaxis:

```
pgp mensaje.pgp
```

## 11. Webmail

### caso práctico inicial

Debemos ayudar a Xavi para seleccionar un buen webmail (ver la tabla de la siguiente página).



Aunque el SMTP y POP3 son los servidores más utilizados, la mayoría de personas utilizan webmail, que es una forma de acceso al correo electrónico desde página web, sin necesidad de instalar un programa adicional cliente de correo, ni tener que configurar los servidores, claves, etc.

El correo electrónico puede permitir exclusivamente acceso webmail, puede permitir acceso a servidores POP3 (y/o IMAP) y SMTP o puede combinar ambas formas de acceso. La mayoría de proveedores de hosting ofrecen webmail y SMTP al alquilar un dominio.

Las ventajas e inconvenientes del correo webmail frente al SMTP son:

	Ventajas	Inconvenientes
Webmail	Puede consultarse en cualquier ordenador introduciendo el nombre de usuario y contraseña.	Algunos proveedores leen y filtran los mensajes y los denuncian en algunas autoridades estadounidenses. Suele llevar publicidad.
SMTP	Más fiable. Más seguro.	Requiere configuración y un programa cliente.

El funcionamiento del webmail está basado en que, tanto el cliente del emisor como el del receptor usan páginas web para el acceso. Los servidores de correo traducen esos campos de formulario al protocolo SMTP, lo envían y luego el servidor receptor lo traduce otra vez a HTTP.

Muchos servidores de correo gratuitos ofrecen cuentas webmail:

	GMAIL	YAHOO	LYCOS	HOTMAIL	AOL	TERRA	MIXMAIL
<b>Capacidad</b>	7.000 MB	1.024 MB	300 MB	25 MB	Ilimitada	250 MB	10 MB
<b>Seguridad (puntuada de 1 a 5)</b>	4	4	3	4	3	3	2
<b>Prestaciones</b>	5	5	4	4	4	4	3
<b>Pago / Publicidad</b>	No	Sí	Sí	Sí	Sí	Sí	Sí
<b>Antivirus</b>	Bueno	Bueno	Bueno en recepción, no en envío	Bueno	Bueno	Regular o bueno, de pago	Opcional
<b>Antispam</b>	95%	70%	70%	70%	70%	70%	70%
<b>Tamaño de adjuntos</b>	10 MB	10 MB	10 MB	10 MB	16 MB	20 MB	1 MB
<b>Fiabilidad de entrega</b>	80-95%	80-95%	80-95%	80-95%	80-95%	80-95%	80-95%
<b>Acceso POP</b>	Sí	Con condiciones	De pago	De pago	Sí	Sí	No
<b>Reenvío automático</b>	Sí	Con condiciones	No	No	No	Sí	No
<b>Búsqueda en mensajes</b>	Sí	Sí	Solo cabeceras	Solo cabeceras	Solo cabeceras	No	No
<b>Baja por inactividad</b>	9 meses	A discreción	3 meses	30 días	90 días	45 días	
<b>Máximo de destinatarios</b>	100	20	50	De 5 a 50, según agenda	Discreción	50	50
<b>Dominio</b>	Gmail.com	Yahoo.es Yahoo.com	Lycos.com	Hotmail.com Hotmail.es Msn.com Live.com	Aol.com	Aol.es Terra.es	Mixmail.es

## ACTIVIDADES

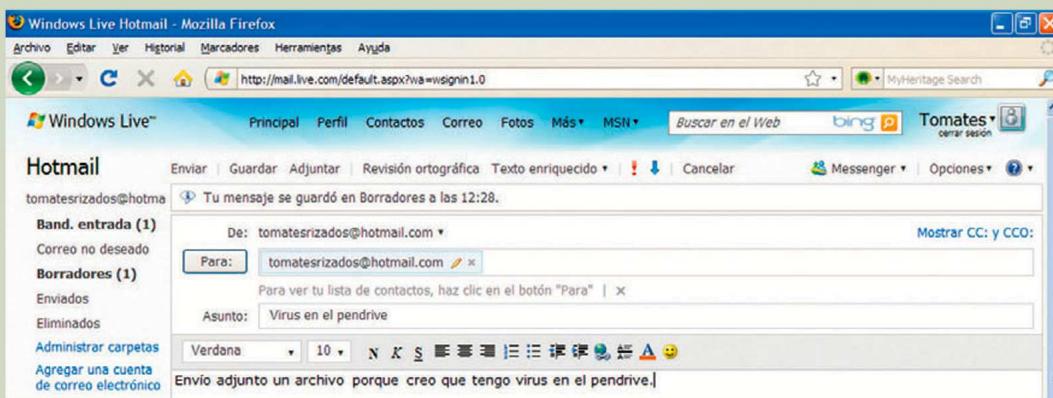
25. Haz una lista de Autoridades Certificadoras cercanas, al menos con una estatal y una de tu Comunidad Autónoma (si la tiene). Escribe el procedimiento necesario para que te concedan las claves y las direcciones más cercanas a tu casa para recogerlas (intenta que sean gratuitas).
26. Consigue los certificados de alguna Autoridad Certificadora e instálalos en Internet Explorer y Firefox. Expórtalos con contraseña a otro dispositivo. No olvides quitarlos al terminar el ejercicio, alguien podría usarlos en tu nombre.
27. Si tienes una cuenta webmail, prueba la copia oculta, el envío de adjuntos, la prioridad, etc. (si no la tienes créate una cuenta en Live.com, Hotmail.com o Gmail.com).
28. Prueba a cifrar un mensaje con Thunderbird y envíáselo a un compañero (debe tener tu clave pública, pero no tu clave privada).
29. Instala PGP en línea de comandos y crea un par de claves.

## ACTIVIDADES FINALES

- 1. Completa el siguiente cuadro:

Protocolo	Uso	Puerto	Puerto Seguro	RFC
POP3				
	143			
	Envío de correo			

- 2. Busca las características de tu cuenta de correo electrónico (capacidad, antispam, antivirus, máximo de destinatarios, si permite POP3, etc.).
- 3. Haz una lista de los servidores de correo webmail que conozcas.
- 4. Busca más información sobre vulnerabilidades del correo.
- 5. ¿Te parece una buena idea enviarte un correo con archivos adjuntos cuando no tienes un medio de almacenamiento a mano, o presumes que está infectado por virus?
- 6. Describe las partes de esta pantalla:



- 7. Instala un servidor POP3 y SMTP en una versión de Windows Server.
- 8. Crea, en Linux, un alias para una cuenta de correo local.
  - Comprueba que funciona al enviar.
  - Realiza pruebas a ver si funciona para recibir correo.
- 9. Configura un servidor DNS de tal manera que puedas comprobar si funciona el direccionamiento inverso a la IP de tu servidor de correo (si el servidor de correo tiene la IP 192.168.0.1, realiza un ping 1.0.168.192.in-addr.arpa).
- 10. Para una cuenta de correo electrónico de internet (Hotmail, MSN, Live, Gmail, etc.), configura el cliente de correo mutt en modo texto para Linux.
  - Comprueba que funciona enviándote un correo.
  - Envía un correo a un compañero.

- 11. Configura una cuenta de correo electrónico de internet (Hotmail, MSN, Live, Gmail, etc.) en Thunderbird.
- 12. Configura una cuenta de correo electrónico de webmail en Microsoft Outlook Express.
- 13. Instala un servidor SMTP para Linux.
  - Comprueba que envía correo en la LAN.
  - Comprueba si funciona en una cuenta de internet.
- 14. Instala un servidor POP3 para Linux.
  - Comprueba que envía y recibe en la LAN.
  - Comprueba si funciona en una cuenta de internet.
- 15. Instala un servidor POP3/SMTP en Windows.
  - Comprueba que te permite enviar correo electrónico a la LAN e internet.
  - Comprueba que te permite recibir correo electrónico desde la LAN e internet.
- 16. Haz un resumen de lo que no se debe hacer según la LSSI en cuanto a envío de spam y qué multas existen dependiendo de la gravedad o la reincidencia.
  - ¿Por qué crees que sigue existiendo spam? ¿Te molesta el spam?
  - ¿Has recibido alguna vez correo en nombre de un banco pidiéndote contraseñas?
- 17. Desde Linux (con los servidores de correo instalados) crea un alias de envío y prueba si funciona.
- 18. Desde Linux (con los servidores de correo instalados) crea un alias de recepción y prueba si funciona.
- 19. Instala PGP (si aún no lo has hecho), crea un par de claves e impórtalas desde Outlook y Thunderbird.
- 20. Si conoces el lenguaje de programación PHP, documéntate sobre cómo usarlo enlazado con Postfix de Linux y sobre lo que necesitas para enviar y recibir correo desde un formulario de web (como si fuese tu propio servidor de webmail).
- 21. Los ficheros de clave se entregan en disquete, mini-CD y pendrive. Debatid en clase sobre las ventajas e inconvenientes derivados del uso de los disquetes y de los pendrive.
- 22. Los certificados ahorrarán costes a las instituciones públicas y al usuario. Debatid en clase las ventajas e inconvenientes de que las instituciones públicas paguen los sistemas de almacenamiento (para potenciar su uso) o de que los paguen los usuarios (para fomentar la austeridad).
- 23. Algunas empresas privadas aceptan archivos públicos, otras solo los suyos propios y otras ambos. Debatid en clase las ventajas e inconvenientes de que existan muchas AC o de que exista una única AC estatal o europea (tipo DNI-e).
- 24. Instala un certificado de la FNMT (Fábrica Nacional de Moneda y Timbre) y entra en 060.es:
  - Consulta tu vida laboral.
  - Consulta las becas que se ofertan.
  - Consulta cómo se pueden pagar impuestos sin salir de casa.
  - Consulta los servicios online que ofrece tu comunidad y requieren autenticación.
- 25. Instala en Linux los antivirus, cortafuegos y todo programa recomendado para la seguridad del servidor.
- 26. Configura los clientes de correo para poder leer el correo del servidor de tu LAN.

## PRÁCTICA PROFESIONAL

### material

- PC con Linux Ubuntu, última versión (o máquina virtual, mínimo Ubuntu con kernel 2.6).
- Ordenadores con Windows.
- Conexión LAN.

### Instalación y configuración de un servidor de correo en Linux y un cliente en Windows

#### Objetivo:

Instalar un servidor de correo electrónico (POP3 y SMTP) en un servidor Linux, configurando un usuario y creándole un alias, así como un cliente de correo en Windows, con las técnicas que hemos estudiado en la unidad.

#### Desarrollo:

Supongamos que trabajamos en una empresa que quiere minimizar costes utilizando freeware.

**1.** Instalaremos Postfix en Linux:

- a) Instalaremos el paquete correspondiente:

```
#apt-get install postfix
```

**2.** Editaremos el archivo de configuración /etc/postfix/main.cf para configurar:

```
myhostname = alumno-desktop          # Nombre del servidor.
mydomain = localdomain              # Nombre del dominio.
mynetworks = 127.0.0.0/8      # Red desde donde enviarán correo.
mydestination = localhost,
$myhostname, localhost.
$mydomain, $mydomain
```

**3.** Una vez realizados estos pasos crearemos un usuario.

**4.** Postfix retomará los usuarios del servidor, por lo que la creación de usuarios se debe hacer en el sistema con adduser o useradd (depende de la versión de Linux).

**5.** Para crear los alias añadiremos en el archivo /etc/postfix/main.cf las líneas:

```
alias_maps = hash:/etc/postfix/aliases
sender_canonical_maps = hash:/etc/postfix/sender_canonical
```

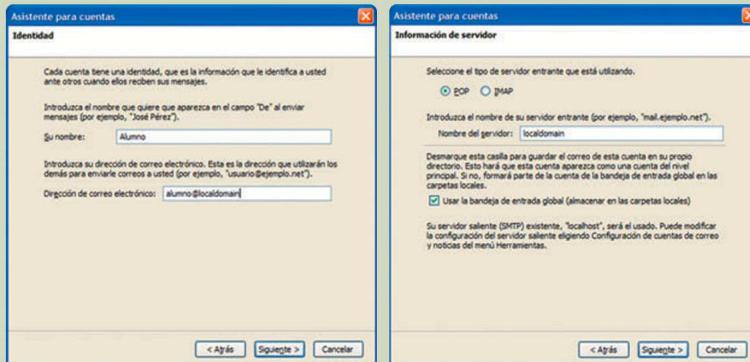
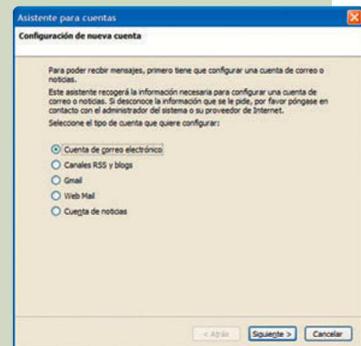
**6.** Crearemos los alias en el archivo de alias (para la recepción) /etc/postfix/aliases:

root:	info
compras:	info

7. Crearemos los alias también en el archivo de envío /etc/postfix/sender\_canonical:

Info:	root
-------	------

8. Ahora instalaremos el cliente en Windows: descargamos el programa desde <http://www.mozilla-europe.org> (la web detecta tu sistema operativo y el idioma). Ejecutamos el programa. En el Asistente para cuentas, configuraremos la cuenta, seleccionando CUENTA DE CORREO ELECTRÓNICO y pulsamos SIGUIENTE.
9. Configuraremos el nombre de usuario. En la dirección de correo electrónico tenemos que poner la dirección que hayamos configurado en el servidor de correo (alumno@localdomain, alumno@127.0.0.1 si estamos en el mismo ordenador o alumno@192.168.0.2 si esa fuese la IP del servidor).



10. Para comprobar si el servidor funciona nos enviaremos (a alumno@localdomain) un correo electrónico y lo descargaremos para leerlo.
11. Probaremos si funciona el alias enviando un correo de alumno a compras.

## Actividades

1. ¿Te ha parecido muy complicado el proceso de instalación y configuración?
2. ¿Qué utilidades le ves a un correo solo de LAN?
3. Prueba a hacerlo con el servidor Sendmail en vez de Postfix.

## MUNDO LABORAL

**Ejemplo genérico de configuración de registros MX, en un dominio particular, para gestionar el correo con Gmail:**

1. Elimina todas las entradas MX existentes.
2. Introduce los siguientes registros MX.  
Define los valores TTL en una hora (valor = 3.600).  
Prioridad: 1  
Servidor de correo: ASPMX.L.GOOGLE.COM.
3. Guarda los cambios.

### Administrar el correo de tu dominio DynDNS con Gmail

Ayuda de Google Apps. Admin.: Configuración de registros MX.



1. Accede a tu cuenta en DynDNS.com.
2. Haz clic en **My Services** (Mis servicios) debajo de tu nombre de usuario.
3. En **Zone Level Services** (Servicios de Nivel de Zona), haz clic en **Custom DNS** (DNS personalizado) junto al dominio que vas a utilizar con Google Apps.
4. En **Mail eXchanger (MX) Records** [Registros Mail eXchanger (MX)], selecciona todos los dominios existentes y haz clic en **Delete MX** (Eliminar MX).
5. Junto a **Mail eXchanger (MX) Records** [Registros Mail eXchanger (MX)], haz clic en **Add New MX** (Añadir MX nuevo).
6. En **Preference** (Preferencia), selecciona **5 -- Highest** (5 -- Máxima).
7. En **Mail Exchanger**, introduce **ASPMX.L.GOOGLE.COM**.
8. Haz clic en **Modify MX** (Modificar MX).
9. En la parte superior derecha, haz clic en **Return to...** (Regresar a...).

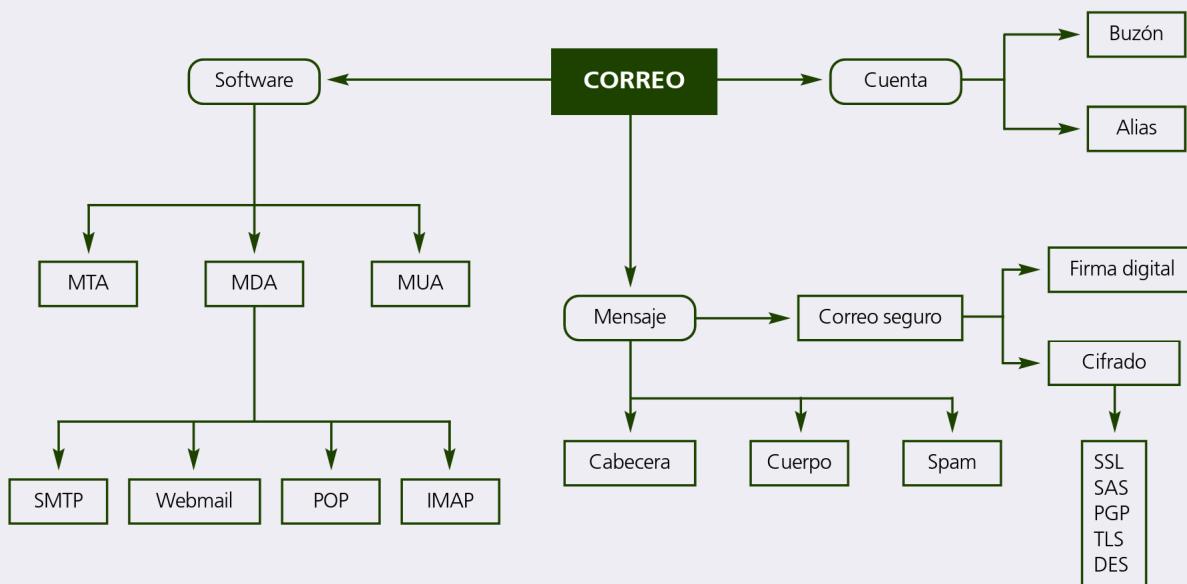
Has configurado los registros MX para que apunten a Google. Recuerda que los cambios que se realicen en los registros MX pueden tardar hasta 48 horas en transferirse a través de internet.

Google.com, actualizado el 27/07/2009.

### Actividades

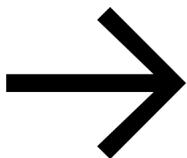
1. ¿Has entendido correctamente todos los pasos de la **Ayuda de Google Apps**?
2. ¿Serías capaz de realizar lo que te indican? ¿Y el caso genérico?
3. Este servicio era gratuito para empresas, ahora solo lo es para las ONG. Compara el precio de Google (unos 40 euros/usuario/año) con otros proveedores de correo.
  - ¿Sería interesante plantearte la contratación de este servicio en el caso de que tu empresa tuviese 20 empleados?
  - ¿Y te lo plantearías teniendo en cuenta las herramientas de antivirus, antispam, etc. que ofrece Google?

## EN RESUMEN



## EVALÚA TUS CONOCIMIENTOS

1. Los clientes de correo electrónico también se llaman:
  - a) MUA.
  - b) MDA.
  - c) MTA.
  - d) MIA.
2. Para enviar un correo a varias personas que no se conocen lo ideal es meter sus direcciones en:
  - a) Para.
  - b) CC.
  - c) CCO.
  - d) De.
3. El puerto por defecto del protocolo POP3 es:
  - a) 25.
  - b) 110.
  - c) 143.
  - d) 995.
4. Si enviamos spam en España, podremos ser multados con:
  - a) Hasta 600 euros.
  - b) Hasta 30.000 euros.
  - c) Hasta 150.000 euros.
  - d) En Europa no está prohibido.
5. Las claves de la firma digital son:
  - a) Una clave privada.
  - b) Una clave asíncrona PGP.
  - c) Una clave privada y otra pública.
  - d) Una clave síncrona SPA.
6. El código que identifica que en el envío del correo electrónico todo va bien es el:
  - a) 200.
  - b) 250.
  - c) 402.
  - d) Ninguno.



**Redacción y selección de contenidos:** Joaquín Andreu

**Edición:** Montserrat Sánchez

**Diseño de cubierta:** Paso de Zebra

**Fotocomposición, maquetación**

**y realización de gráficos:** MT Color & Diseño, S. L.

**Fotografías:** Microsoft Corporation; Canonical Ltd.; Apple Inc.; Bind, licencia BSD; ICANN; PuTTY, Simon Tatham; OpenSSH, OpenBSD; Webmin; TeamViewer GMBH; RealVNC Limited; Medialogic; Google; Google Inc.; Mozilla Foundation; Filezilla-project.org; gFTP, Brian Masney ; GNU.org; OpenSight Software, LLC; cPanel Inc.; Cuerpo Nacional de Policía, Ministerio del Interior, Gobierno de España; Fábrica Nacional de Moneda y Timbre, Ministerio de Economía y Hacienda, Gobierno de España; Conselleria de Justicia i Administracions Públiques, Generalitat Valenciana; Agència Catalana de Certificació, Generalitat de Catalunya; Yahoo!; Adobe Systems Incorporated; Romain Bourdon; The Apache Software Foundation; Oracle Corporation; The PHP Group; GNU; 3Com Corporation; PLANET Technology Corporation; GSMA; Telefónica Móviles España, SAU; France Télécom; The Information Technology & Innovation Foundation; TeleAtlas; HISPAKSAT, SA; SES ASTRA, Grupo SES; NEO-SKY 2002, SA; Euskaltel, SA; Xfera Móviles, SA; EDIMAX Technology Co.; Check Point Software Technologies Ltd.; Agnitum Ltd.; Bluetooth SIG.; Wi-Fi Alliance; IEEE; D-LINK Europe Ltd.; Jinx, Inc.; Medion Iberia, SL; Sony Computer Entertainment Europe; Symantec Corporation; Bratel Co., Ltd.; Technicolor; Koninklijke Philips Electronics N.V.; Accton Technology Corporation; Skype Limited; Cisco System, Inc.; ITU; ISOC; Digium, Inc.; Peoplecall the callshop Co.; Vonage Marketing LLC; AOL Inc.; Telefonica USA Inc.; Jajah, Inc.; CounterPath Corporation; Internap Network Services Corporation; iDATE FR; Getty Images (Photos.com) y archivo Editex

**Dibujos:** Ángel Ovejero

**Dirección producción:** Teresa del Arco

**Preimpresión:** José Ciria

**Producción editorial:** Francisco Antón

**Dirección editorial:** Carlos Rodríguez

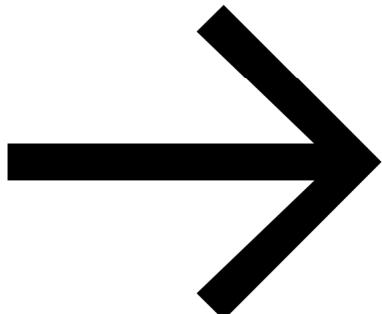
**Editorial Editex, S. A.** ha puesto todos los medios a su alcance para reconocer en citas y referencias los eventuales derechos de terceros y cumplir todos los requisitos establecidos por la Ley de Propiedad Intelectual. Por las posibles omisiones o errores, se excusa anticipadamente y está dispuesta a introducir las correcciones precisas en posteriores ediciones o reimpresiones de esta obra.



El presente material didáctico ha sido creado por iniciativa y bajo la coordinación de **Editorial Editex, S. A.**, conforme a su propio proyecto editorial.

© **Editorial Editex, S. A.**

Vía Dos Castillas, 33. C.E. Ática 7, edificio 3, planta 3<sup>a</sup>, oficina B  
28224 Pozuelo de Alarcón (Madrid)



Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra solo puede ser realizada con la autorización de sus titulares, salvo excepción prevista por la ley. Diríjase a CEDRO (Centro Español de Derechos Reprográficos, [www.cedro.org](http://www.cedro.org)) si necesita fotocopiar o escanear algún fragmento de esta obra.