

UNIDAD 7

Correo electrónico

1. Correo electrónico

1.1. ¿Qué es el correo electrónico?

El correo electrónico permite el intercambio de mensajes mediante el uso de sistemas de comunicación electrónicos. Se basa en el protocolo SMTP (*Simple Mail Transfer Protocol*) o protocolo simple de transferencia de correo.

La idea de que diferentes usuarios accedan a un ordenador de forma remota y guarden datos se remonta al año 1971 en el Instituto Tecnológico de Massachusetts (MIT, Massachusetts Institute of Technology). Si bien el concepto de correo electrónico dentro de una red informática no se empezó a generalizar hasta el año 1975.

Puedes ver un poco de historia en el fichero llamado *Historia*.

El correo electrónico y el correo postal funcionan de manera análoga: los dos permiten enviar y recibir mensajes que llegan a un buzón destino gracias al uso de direcciones personales. En el caso del correo electrónico, la función de buzón la realiza un servidor de correo.

El correo electrónico presenta algunas desventajas. Por ejemplo, no garantiza que los mensajes lleguen a su destino, no asegura que el remitente sea quien dice ser, no está obligado a avisar de cualquier anomalía ocurrida durante el envío o la recepción del mensaje, y facilita la transmisión de virus o malware.

Cuentas de correo

La cuenta de correo es nuestra identificación dentro del servicio para poder recibir y enviar de manera única los mensajes.

Normalmente el proveedor de servicio de Internet (ISP) dará la posibilidad de obtener una cuenta de correo electrónico en sus servidores a través de un agente de correo MUA (*Mail User Agent*).

Las cuentas de correo están formadas por dos partes separadas por el símbolo arroba (@):

- La primera parte indica el nombre del usuario de la cuenta.
- La segunda especifica el dominio del servidor de correo donde está alojada la cuenta.

Por ejemplo, *javier@servidor1.com* indica que es la dirección de correo del usuario "Javier" que se encuentra en el servidor "servidor1". Dentro de este servidor no se pueden tener dos direcciones iguales, pero el usuario Javier puede tener más de una dirección de correo en diferentes servidores (como por ejemplo *javier@servidor2.com* o *javier@servidor3.com*).

Existen dos formas básicas de configurar las descargas de las cuentas de correo electrónico según el protocolo:

- IMAP (*Internet Message Access Protocol*) o protocolo de acceso a mensajes de Internet: en este caso los mensajes se guardan en el servidor de correo.
- POP (*Post Office Protocol*) o protocolo de oficina de correos: en este caso los mensajes se guardan en el ordenador del usuario.

El símbolo arroba (@) fue introducido en el año 1971 para separar el nombre del usuario y del servidor. Se escogió, entre otras cosas, porque en inglés se lee -at- (en español -en-) y no forma parte de ningún nombre o apellido.

Alias

Un alias es una dirección de correo electrónico alternativa que apunta a una cuenta de correo principal.

Un alias intenta suministrar una dirección más significativa.

Buzón de usuario

Los buzones de correo electrónico son carpetas donde se guardan los mensajes de correo.

1.2. Funcionamiento del servicio de correo

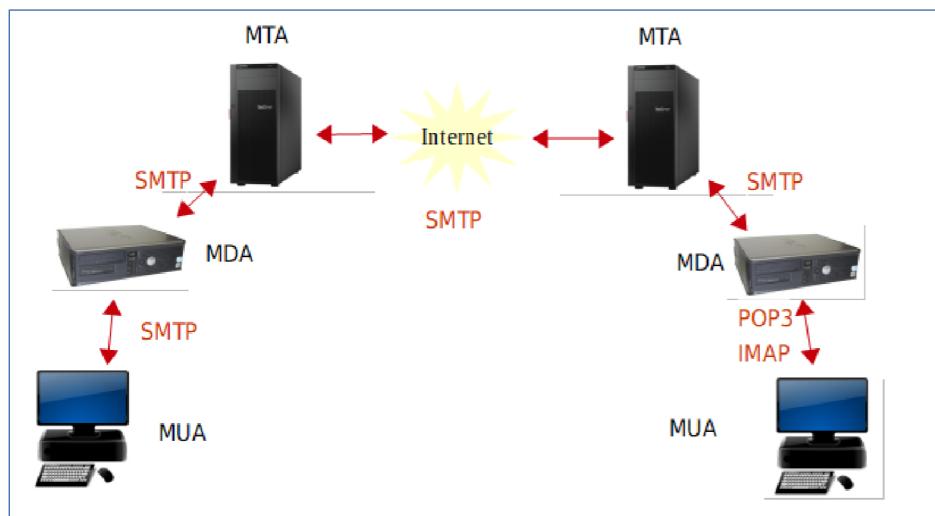
El servicio de correo opera siguiendo el modelo cliente-servidor. Cuando se envía un correo, el mensaje se dirige a través de diferentes servidores hasta que llega al del receptor.

Agentes del servicio

Los diferentes agentes que intervienen en el envío de un correo electrónico entre dos usuarios son:

- **MUA** (*Mail User Agent*) o agente de usuario de correo: es un programa de ordenador usado para enviar y recibir correos.
- **MTA** (*Mail Transfer Agent*) o agente de transferencia de correo: es el servidor de correo. Se comunica con otros servidores mediante el protocolo simple de transferencia de correo SMTP. En su viaje desde el origen hasta su destino final, un mensaje puede pasar por varios MTA de forma transparente para el usuario.
- **MDA** (*Mail Delivery Agent*) o agente de entrega de correo: es un programa que gestiona los buzones de la lista local de correo.

Veamos cómo se desarrolla el envío de un mensaje entre dos usuarios: el MTA del usuario se comunica con otros MTA hasta llegar al destino. Éste último, entrega el mensaje al MDA, que lo almacena esperando que el destinatario lo descargue mediante el uso de POP o IMAP.



Formato del mensaje

El protocolo SMTP indica que los mensajes deben incluir:

- **Cabecera**: incluye, entre otros, los siguientes campos:

- **De o remitente:** indica el usuario que envía el mensaje.
 - **Para o destinatario:** indica el usuario al que va dirigido el correo.
 - **CC o copia carbón:** destinatario de copia. Los usuarios que estén en la lista recibirán el correo, pero verán que no está dirigido solo a ellos. Este campo es visible para todos.
 - **CCO o copia carbón oculta:** destinatario de copia oculta. En este caso, no se agregan a la lista de destinatarios los usuarios que se añaden a este campo. Permanecerán ocultos para todos los destinatarios, incluidos los que estén en este campo.
 - **Fecha:** especifica la fecha y la hora de envío del mensaje.
 - **Asunto:** breve descripción del contenido del mensaje.
- **Cuerpo:** contiene el mensaje. Puede ser solo texto plano o tener algún tipo de formato.

Extensiones MIME

Las MIME (*Multipurpose Internet Mail Extensions*) o extensiones multipropósito de correo de Internet son un conjunto de especificaciones que fijan el intercambio de todo tipo de archivos de forma transparente para el usuario.

Tipos MIME

Las extensiones MIME soportan:

- Texto con caracteres distintos de ASCII, como la –ñ- o la –ç-.
- Adjuntos que no son del tipo texto, como imágenes.
- Cuerpos de mensajes con múltiples partes.
- Información de encabezados con caracteres distintos ASCII.

1.3. Protocolos de descarga de correo

POP e IMAP son los dos protocolos que prevalecen en la descarga de correo electrónico.

POP

POP (*Post Office Protocol*) o protocolo de oficina de correos se utiliza para recibir correos. Permite que el usuario se descargue en su ordenador los correos recibidos para revisarlos posteriormente sin necesidad de estar conectados a Internet.

POP se desarrolló en los años 80 y, desde entonces, ha tenido una serie de mejoras. Actualmente se utiliza la versión POP3; las anteriores versiones de este protocolo se consideran obsoletas.

El usuario que utiliza POP3 se conecta al servidor, descarga todos los mensajes, los graba en el ordenador local, los marca como nuevos, los borra del servidor y se desconecta.

POP3 utiliza una autenticación sin cifrado. Para aumentar el nivel de seguridad existe la extensión APOP (*Authenticated POP*) o POP autenticado. Esta extensión permite que el emisor cifre la contraseña y que esta sea descifrada por el receptor.

POP3 permite conectar al usuario y al servidor mediante *telnet* a través del puerto 110.

Niveles del protocolo POP3	
Aplicación	Transporte
POP3	TCP (110) TCP cifrado (995)

IMAP

IMAP (*Internet Message Access Protocol*) o protocolo de acceso a mensajes de Internet. Se utiliza

para recibir correos. Permite al usuario acceder al servidor de correo desde cualquier ordenador con acceso a Internet y definir carpetas en el servidor para guardar los mensajes. Fue creado en el año 1984 como alternativa al protocolo POP.

Actualmente se utiliza la versión IMAP4.

Los usuarios de IMAP4 permanecen conectados el tiempo que su enlace esté activo y se descargan los mensajes bajo demanda. De esta manera se mejoran los tiempos de respuesta si se recibe un número elevado de mensajes o si estos son de gran tamaño respecto a usuarios que utilicen POP3, que se conectan el tiempo necesario para descargar los correos.

Con IMAP4 disminuye la incidencia de los virus. Al poder definir carpetas en el servidor, los mensajes no se guardan en el ordenador del usuario hasta que sean descargados.

El término IMAPS hace referencia al protocolo IMAP cifrado utilizando SSL (*Secure Sockets*) o capa de conexión segura.

Niveles del protocolo IMAP	
Aplicación	Transporte
IMAP4	TCP (143) TCP cifrado (993)

1.4. Protocolo de envío de correo SMTP

SMTP (*Simple Mail Transfer Protocol*) o protocolo de transferencia de correo simple es un protocolo que define una serie de comandos y procedimientos para que dos dispositivos puedan intercambiar mensajes de correo electrónico.

Se definió en las RFC 821 y 822, en las que se establece el formato de los mensajes, el MTA y el procedimiento para almacenar y reenviar correo.

Este protocolo fue diseñado en 1982 únicamente para transferir mensajes de texto ASCII. Desde entonces se han incorporado diversas mejoras, algunas de las cuales se detallan a continuación:

- Las RFC 2821 define es ESMTP o SMTP extendido, que permite gestionar mensajes con un tamaño mayor a 64Kb, trabajar con temporizaciones diferentes del cliente y del servidor y evitar las tormentas de correo infinitas al reenviar mensajes entre servidores.
- La RFC 2920 mejora la productividad del servidor SMTP al aceptar varios comandos dentro de un único envío TCP.
- La RFC 3030 permite el uso de mensajes MIME.

Funcionamiento del protocolo

La finalidad de este protocolo es entregar un mensaje de correo a su destinatario. Para ello se deben realizar los siguientes pasos:

1. El cliente compone el mensaje de correo y lo envía al puerto 25 de su servidor SMTP, llamado **servidor de correo saliente**.
2. Dicho servidor SMTP saliente realiza una petición a un servidor DNS. Este le proporciona el registro MX donde se asocia la dirección IP del servidor SMTP del receptor con el nombre de dominio correspondiente a la dirección de correo electrónico del destinatario.
3. El servidor SMTP saliente reenvía el mensaje al servidor de correo SMTP del receptor.
4. El servidor SMTP destinatario recibe el correo, lo procesa y lo deja en el buzón de entrada del usuario.

Sabías que...

En el correo web o webmail se usan conexiones HTTP para acceder a los diferentes servidores de correo en lugar de SMTP.

Comandos

SMTP tiene sus orígenes en los protocolos de capa de aplicación precedentes, incluido el FTP, de ahí que también utilice comandos. Algunos de los más empleados se muestran a continuación:

Comandos SMTP	
Comando	Explicación
HELO/EHLO	Identifica al cliente, quien se encarga de enviarlo seguido de un nombre de dominio.
MAIL FROM	Identifica al remitente del mensaje.
RCPT TO	Identifica a los destinatarios del mensaje.
DATA	El cliente lo genera para indicar que inicia el envío del contenido del mensaje.

Temporizaciones

Si los servidores de correo asumen intervalos de tiempo de trabajo diferentes, uno de ellos puede haber acabado mientras el otro continúa con su tarea, de forma que se interrumpe inesperadamente la conexión.

Tormentas de correo infinitas

Supongamos que el servidor DistribUSA tiene una lista de correo, ListaUSA, con las distribuidoras de cine en EEUU y que el servidor DistribEspaña tiene una lista de correo, ListaEspaña, con las distribuidoras de España, donde cada lista contiene una entrada a la otra, por ejemplo:

```

SERVIDOR DistribUSA
ListaUSA = (Disney, ListaEspaña, Fox)
SERVIDOR DistribEspaña
ListaEspaña = (Lolafilms, ListaUSA, DeAPlaneta)

```

Si se envía un mensaje a una de las listas, se puede generar un bucle infinito de envíos de correos electrónicos, a menos que se introduzca algún proceso que evite esta situación.

Sabías que...

Un emisor de correo que utilice SMTP extendido envía un comando EHLO en vez del antiguo HELO. Si el receptor responde con un código de error significa que utiliza el protocolo SMTP original.

Códigos de respuesta

La respuesta del servidor incluye un código compuesto por tres dígitos. El primero puede tomar cinco valores con los siguientes significados:

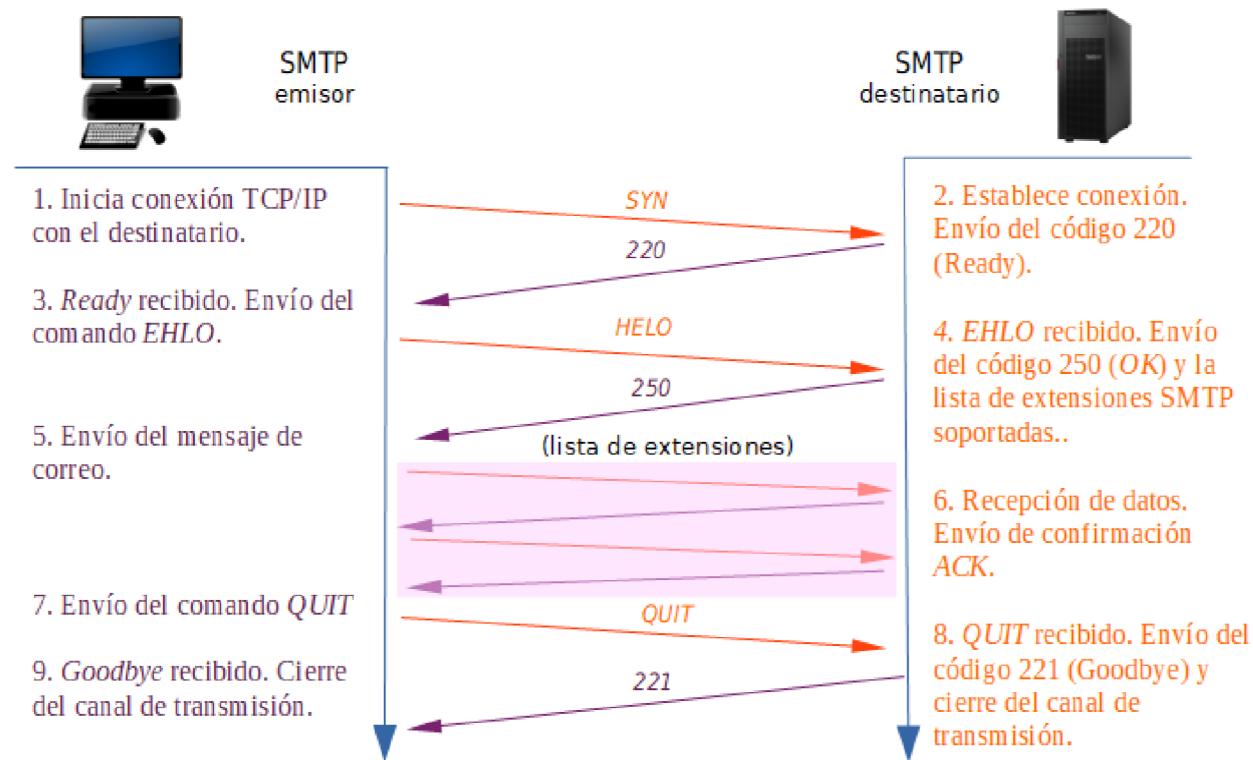
Códigos de respuesta SMTP	
Dígito Xyz	Explicación
1yz	El comando es aceptado, pero la acción queda suspendida a la espera de saber si el cliente desea continuar o abortar.
2yz	La acción se ha realizado con éxito.
3yz	El comando es aceptado, pero la acción queda pendiente hasta que el cliente envíe otro comando con más información.
4yz	El comando no es aceptado. El cliente puede volver a iniciar la secuencia de comandos.
5yz	El comando no es aceptado y se necesita la intervención humana para corregir la petición.

Procedimiento

Un mensaje de correo electrónico se transmite en tres fases:

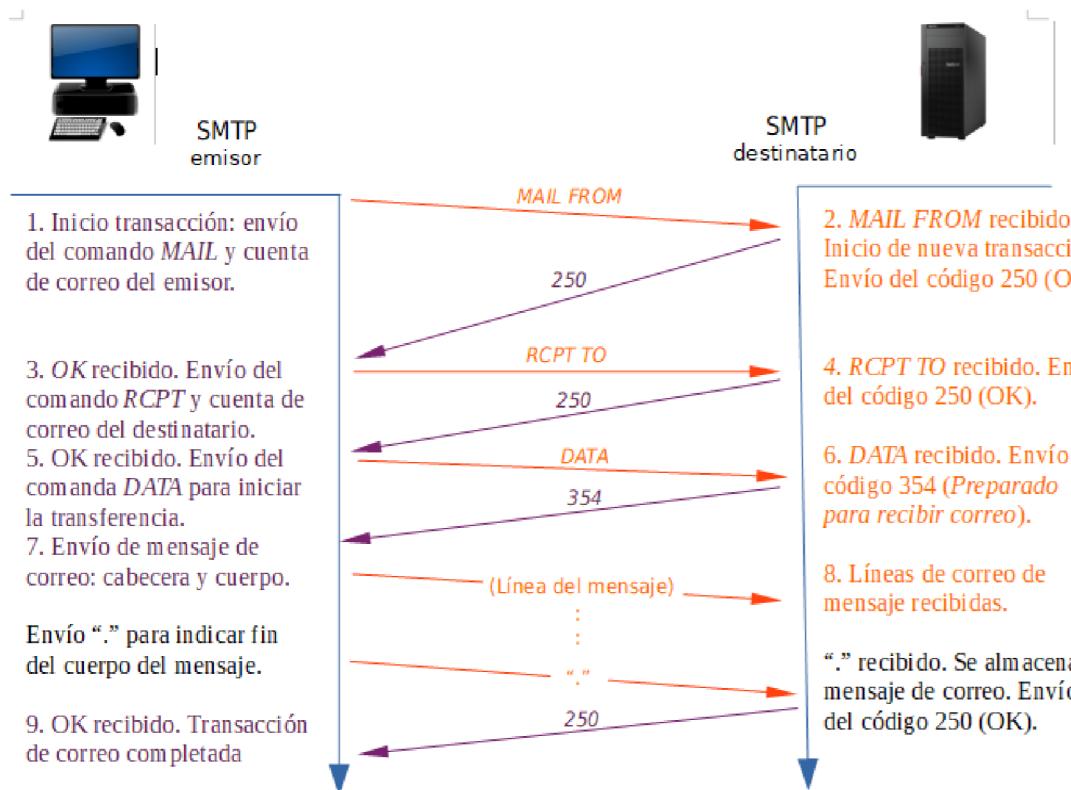
1. Se establece una conexión SMTP y se inicia la sesión.
2. Se realiza el proceso de transacción SMTP, es decir, se envía el mensaje de correo electrónico propiamente dicho.
3. Se cierra la sesión y se finaliza la conexión SMTP.

Una vez realizada la conexión e iniciada la sesión, el cliente SMTP empieza la transacción de correo formada por una serie de comandos que permiten identificar tanto al remitente y destinatario del correo como la transmisión del contenido del mensaje, incluidas las cabeceras.



Para cada comando, el destinatario SMTP genera una respuesta que informará de si el comando fue aceptado, si está a la espera de nuevos comandos o qué condiciones de error existen.

La siguiente figura muestra el proceso de transacción SMTP. El contenido del mensaje de correo se envía a través del comando *DATA*. Si el receptor lo acepta, remite un código de respuesta 354 que considera el resto de líneas como texto del mensaje. El final del envío se identifica mediante una línea con un único punto <CRLF>.<CRLF>. Al recibirse el fin del mensaje, este es almacenado y se confirma su recepción.



CR/LF

Carriage Return/Line Feed son dos caracteres especiales, cuyos valores en formato ASCII son 13 y 10. Representan "retorno de carro" y "nueva línea", respectivamente.

Cliente/servidor y emisor/destinatario

Los servidores SMTP envían y reciben correos electrónicos. El dispositivo que envía actúa como cliente para esa transacción mientras que el receptor tiene el rol de servidor. Para evitar confusiones, se ha elegido nombrar como emisor al dispositivo SMTP que envía correos y como destinatario al que los recibe.

Actividad resuelta 7.1

Instalación de MTA y MUA para enviar correo

Objetivo: tener un primer contacto con un cliente de correo para enviar mensajes desde la consola a través de un servidor SMTP preconfigurado. Instalar y utilizar el MUA para escribir el correo y el MTA para enviártelo a tu cuenta de correo externa de Gmail u otra.

Material y herramientas: el servidor que utilizaremos como cliente y servidor de correo.

Utilidades: la orden *mail* del paquete mailx para el cliente MUA y el paquete postfix para el servidor MTA.

Consideraciones previas: se requiere instalar y utilizar la configuración preestablecida como sitio de Internet del servidor de correo con Postfix, así como un cliente de consola.

Desarrollo:

Instalación del servidor MTA Postfix

En esta ocasión vas a instalar el servidor de correo saliente Postfix y el servidor de correo entrante Dovecot. Así se podrán ofrecer los servicios SMTP y POP3. Sigue estas instrucciones para instalar estos programas:

1. Inicia el gestor de paquetes Synaptic.
2. Haz clic en el botón Recargar para actualizar la lista de paquetes disponibles en los repositorios de Internet.
3. Accede a la herramienta de búsqueda.
4. Escribe postfix en el cuadro de texto y, a continuación, haz clic sobre el botón Buscar.
5. Haz doble clic en la casilla de verificación del paquete postfix. Si la instalación requiere otros paquetes, haz clic sobre el botón Marcar.
6. Repite los pasos 3, 4 y 5 para el paquete dovecot-pop3d. Así habrás marcado todos los paquetes necesarios para instalar el servidor.
7. Haz clic en el botón Aplicar para iniciar la instalación.
8. Se abrirá la ventana con el resumen de la instalación que vas a realizar. Léela y haz clic sobre el botón Aplicar.
9. Mientras continúa la instalación se muestra la ventana de diálogo *Aplicando los cambios*. Esta ventana se cerrará automáticamente cuando termine este proceso.
10. Antes de finalizar, se abre otra ventana llamada *Debconf en servidor* que te permitirá configurar algún parámetro del servidor de correo Postfix. Selecciona *Sitio de Internet* en la lista desplegable *Tipo genérico de configuración de correo*.
11. Haz clic en el botón *Adelante*.
12. De nuevo, se abre la ventana *Debconf en servidor*. Teclea el dominio de hayas elegido (en nuestro caso *cieloazul.com*) en el cuadro de texto *Nombre del sistema de correo*. Así indicas que a los usuarios de correo electrónico se les añada la cadena @cieloazul.com al final de su nombre.
13. Luego, haz clic en el botón *Adelante*.
14. Cuando finaliza la instalación se abre la ventana *Cambios Aplicados*. Haz clic sobre el botón *Cerrar* para retornar a la ventana principal de la aplicación.
15. Haz clic sobre el botón *Cerrar* de la ventana Synaptic para salir de este programa.

Instalación del cliente MUA mailx

1. Instala el paquete desde consola con la orden:
`$sudo apt-get install mailutils`
2. A continuación, tendrás que conocer la sintaxis de esta nueva herramienta. Consulta su propio manual con la orden *man*.
`$man mailx`
3. Envía un primer mensaje a ti y al profesor. Quizás aparezca en el buzón de spam, ya que tu dominio y servidor no son de fiar.
`$sudo echo "Cuerpo del correo electrónico" | mail -s "Asunto" cuenta_profesor@gmail.com tu_cuenta_de_correo@gmail.com`
4. Entra en tu cuenta de correo y verifica si Postfix se ha puesto en contacto con el servidor MTA de tu cuenta y entrega el mensaje.
5. Por el contrario, si no se dispone de un dominio real, no habrá posibilidad de responder al mensaje, ya que Gmail no indica el motivo.

Actividad resuelta 7.2

Cómo ver la cabecera de un mensaje

Objetivo: saber qué se debe hacer para ver el contenido completo de la cabecera de un mensaje en algunos servicios de correo electrónico.

Desarrollo:

Las cabeceras de los mensajes no se muestran en los lectores de correo. Hay que mirar el código. La manera de hacerlo depende del programa cliente que se utilice. En este ejercicio se indicarán los pasos que debes seguir en un cliente de correo para ver el contenido completo de la cabecera. Si quieres verlos en otros clientes puedes buscarlos tú mismo.

En el cliente de Gmail

Haz clic en el cuadro con la flecha situada al lado de la opción *Responder*, en la parte superior derecha. Selecciona de la lista la opción *Mostrar original*.

Actividad resuelta 7.3

Emulación del funcionamiento del SMTP con el telnet en local

Objetivo: ver un ejemplo de comunicación de bajo nivel entre un cliente y un servidor de correo electrónico en local mediante comandos SMTP.

Material y herramientas: el servidor con el servidor de correo electrónico ya instalado y configurado, como se ha hecho en la actividad resuelta 7.1

Utilidades: la orden *telnet* desde la línea de comandos.

Desarrollo:

1. Se inicia la conexión vía telnet por el puerto 25 de SMTP:
`$telnet localhost 25`
2. El emisor se presenta al servidor y el servidor lo acepta indicándole lo siguiente:

HELO localhost

250 ubuntuserver.localdomain

3. Escribe un mensaje utilizando los comandos SMTP necesarios, equivalentes a la actividad resuelta 7.1, para indicarle al servidor quién eres tú y a quién te diriges:

MAIL FROM: yomismo@cieloazul.com

250 2.1.0 Ok

RCPT TO: correo_del_profesor@gmail.com

250 2.1.5 Ok

RCPT TO: correo_de_quien_quiera@gmail.com

250 2.1.5 Ok

DATA

354 End data with <CR><LF>,<CR><LF>

SUBJECT: Prueba de correo SMTP de la actividad resuelta 7.3

Tras dejar la línea en blanco requerida para separar el asunto (*subject*) del cuerpo (*body*) del correo, escribe “Hola Mundo”. Deja una nueva línea en blanco y, por último, escribe un punto y pulsa la tecla **Enter** para intercalar los caracteres especiales <CR> de retorno de carro más <LF> de fin de línea.

250 2.0.0 Ok: queued as 7E1EB4AC60

QUIT

221 2.0.0 Bye

Connection closed by foreign host.

Como resumen se puede decir lo siguiente:

Se establece la conexión mediante telnet al puerto 25. El mensaje recorre tres fases (del emisor al receptor): comando MAIL para indicar quién envía el mensaje, comando RCPT para indicar los destinatarios, comando DATA para enviar el cuerpo del mensaje. Respuesta de aceptación o rechazo por parte de cada destinatario.

Lógicamente, al disponer de un servidor MTA de SMTP instalado y configurado, se enviará este mensaje de ejemplo, ilustrando bien la secuencia real de comandos SMTP que llevó a cabo la orden MAIL en la actividad resuelta 7.1

1.5. Servidores de correo

Un servidor de correo es un MTA que emplea un protocolo de transferencia de correo, como por ejemplo SMTP, o un MDA que utiliza un protocolo de descarga de correo como POP3 o IMAP.

El servicio de correo electrónico está estrechamente relacionado con los servidores DNS, que permiten localizar el servidor SMTP del destinatario, y con los cortafuegos, que filtran los mensajes de salida para controlar que solo puedan realizar envíos los clientes autorizados. En muchas ocasiones los servidores de correo se deben combinar con aplicaciones que ofrezcan algún tipo de seguridad en la red, como un antivirus, mecanismos de cifrado e, incluso, el empleo de un proxy, lo que hace que este servicio sea uno de los más complejos de implantar en una empresa.

Microsoft Exchange es el servidor de correo de transferencia y descarga más popular para Windows, mientras que Postfix, Sendmail o qmail son los servidores de transferencia de correo más conocidos en GNU/Linux.

1.6. Clientes de correo

Instalados en el cliente

Son aquellos UA (*User Agents*-Agentes de Usuario) o aplicaciones que, instaladas en el ordenador del usuario, permiten componer, enviar y recibir y descargar mensajes de correo electrónico, así como gestionar buzones de correo. Los programas cliente más conocidos son: Microsoft Outlook, disponible únicamente para Windows, y Mozilla Thunderbird, que es multiplataforma.

Webmail

Una forma de acceder al correo electrónico sin necesidad de instalar un cliente específico es hacerlo a través de un navegador web. Esto implica componer mensajes directamente en el servidor.

Las principales ventajas de este tipo de cliente son las siguientes:

- Permite acceder al servicio de correo con independencia del lugar y del tipo de dispositivo desde el que se conecta y evitar, así, descargar los correos electrónicos.
- No hay que instalar ni actualizar un cliente de correo.
- Se puede acceder al correo, aunque no se permita configurar la aplicación cliente (por ejemplo, en lugares públicos como hoteles y cafeterías).

También tiene sus inconvenientes:

- Hay que disponer de una conexión a Internet para poder acceder al correo, aunque sea para leer mensajes antiguos.
- Si la cuenta es gratuita, se estará expuesto a anuncios no deseados.
- Cuando se pierde el servicio por cierre del proveedor, olvido de la contraseña o incumplimiento del contrato.

Sabías que...

Los clientes webmail se hicieron populares gracias a Hotmail, que en el año 1998 fue comprada por Microsoft para añadir una nueva característica, el servicio de correo electrónico, a su portal MSN (Microsoft Network), creado en 1995

Instalados en el servidor

Muchas veces suele instalarse un cliente de correo en el servidor SMTP que proporciona ese servicio con la finalidad de permitir al administrador del sistema enviar y recibir correos desde la propia máquina.

1.7. Seguridad y vulnerabilidades

Cuando se diseñaron los protocolos de correo electrónico no era primordial implementar mecanismos de seguridad, es más, el modelo de comunicación SMTP original requería que los servidores de correo reenviaran mensajes a otros y así sucesivamente hasta encontrar el servidor SMTP destinatario, lo que implicaba que cualquier servidor aceptará peticiones desde cualquier origen. Esta es la razón por la cual SMTP no requería autenticación, la particularidad que hace posible el **spam** o correo no solicitado.

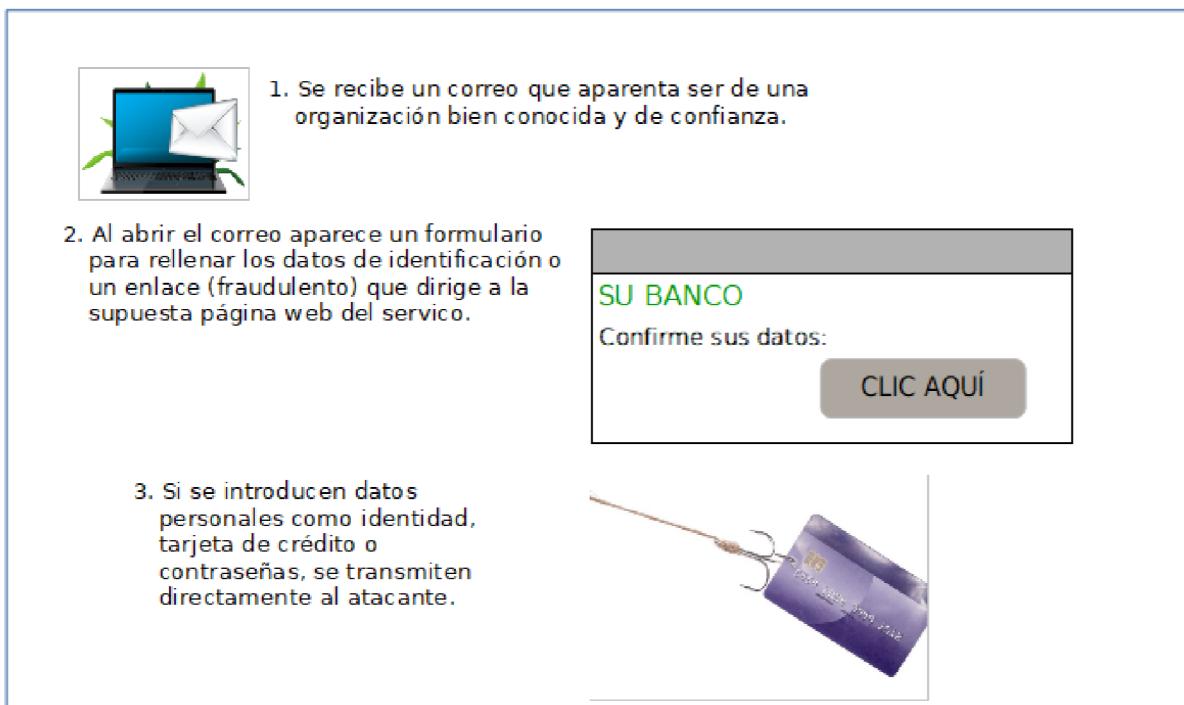
El spam se caracteriza por ser:

- **Anónimo:** no remite la dirección de correo real del emisor o utiliza la de otra persona para ocultar su identidad.
- **Duplicativo:** el correo recibido forma parte de un envío masivo cuyo contenido es similar. Por ejemplo, si de todo el texto cambian el nombre y los apellidos no se considera contenido

diferente.

Estas son formas de spam:

- **Publicidad no deseada:** son mensajes que se caracterizan por tener fines comerciales, como publicitar un producto (a veces prohibido) o una organización. No suelen producir daños ni robo de información.
- **Hoax (bulo):** son mensajes que incluyen noticias falsas en los que se solicita la colaboración del usuario para reenviarlo al mayor número de contactos posible. Su objetivo es recopilar direcciones de correo electrónico. Algunos ejemplos son la recogida de firmas, recibir un vídeo, una canción la respuesta a un acertijo si se manada un correo a un número determinado de personas, ganar premios como un viaje o un destino paradisiaco, etc.
- **Phising:** engaño que consiste en hacer creer a un usuario que el correo que se le envía proviene, por su apariencia, de una entidad legítima, por ejemplo, de una red social, una entidad financiera o una institución pública. Normalmente se apoya en mecanismos de ingeniería social y su fin es capturar información sensible. En la siguiente figura se muestran los pasos que se suelen dar en un ataque de *phising*.



Para evitar caer en la trampa del spam, hay que tener en cuenta que:

- No se debe responder a ninguna solicitud de información personal recibida a través del correo electrónico.
- No se debe hacer clic sobre los hiperenlaces de ningún correo, aunque provenga de un usuario conocido. Puedes teclearlo directamente en la barra de direcciones.
- No hay que hacer pública la dirección de correo y, si se hace, se puede sustituir la arroba por una palabra significativa, por ejemplo "at", para evitar que sea recopilada por robots o programas diseñados para reconocer direcciones de correo incluidas en páginas web.
- Se deben ignorar los mensajes que solicitan ser reenviados.
- No se debe contestar al correo basura o spam.

- Se debe comprobar si la conexión es segura mediante la aparición de *https* en la barra de direcciones del navegador.

Vocabulario

Ingeniería social: consiste en manipular a un usuario para que, de forma voluntaria, realice acciones que normalmente no haría. El objetivo es obtener datos personales como claves o cuentas bancarias, números de tarjetas de crédito, contraseñas, etc.

Scam: significa estafa en inglés y se refiere al spam que tiene por objeto el empleo fraudulento de mensajes de correo electrónico.

Pharming: es la técnica que, en vez de la ingeniería social, emplea vulnerabilidades del servicio DNS para redirigir las peticiones web del usuario hacia sitios falsos que suplantan a los originales.

Grupo de delitos telemáticos (GDT)

Perteneciente al cuerpo de la Guardia Civil, se encarga de perseguir las conductas ilegales relacionadas con las TIC. En su página web se puede encontrar el "Decálogo de navegación segura" con los últimos consejos para realizar un uso seguro de Internet.

Reenviar mensaje con CCO

Para evitar publicar las direcciones de los destinatarios de un correo electrónico cuyo campo CC (copia de carbón) está mal usado, es buena costumbre animar a familiares, amigos, clientes, etc; a usar el campo CCO (copia de carbón oculta).

2. Correo electrónico en sistemas GNULinux

Son varias las herramientas libres, y gratuitas, que nos ofrece estos sistemas para montar un servicio de este tipo. Por su facilidad de uso y gran aceptación, vamos a utilizar:

- Servidor de envío de correo electrónico Postfix. Sus características más destacables son la rapidez, la sencillez de las tareas de administración y la seguridad.
- Servidor de recepción de correo electrónico Dovecot. Este programa de código abierto es rápido, flexible, fácil de configurar y no consume muchos recursos. Y además puede trabajar con los protocolos IMAP y POP3.
- Cliente de correo electrónico Thunderbird, desarrollado por Mozilla. Es uno de los clientes de correo más populares y seguros. Además, está disponible para la mayoría de plataformas.

2.1. Instalación del servidor

Ya se ha llevado a cabo durante el ejercicio resuelto 7.1.

2.2. Configuración del servidor

Aunque hayas instalado dos programas de una sola vez en el servidor, solo vas a tener que configurar uno de ellos: Dovecot. Este proceso se centrará en indicar en qué carpetas del servidor se alojarán los archivos del correo electrónico, entre ellos la bandeja de entrada de los usuarios.

Durante la instalación ya has introducido los parámetros necesarios para la configuración de Postfix: el tipo de servidor de correo y el nombre del sistema de correo.

Acceso a los módulos de los servidores

Realizamos una actualización de los módulos que reconoce Webmin mediante la opción *Refresh modules*, tal y como hemos visto en capítulos anteriores.

Ya podemos ver los enlaces a los módulos de las aplicaciones que acabamos de instalar:

- Configuración de Postfix.
- Dovecot: servidor de IMAP/POP3.

Configuración de Dovecot

Sigue estos pasos para configurar Dovecot:

1. Abre una sesión en el servidor.
2. Inicia Webmin y accede al enlace *Dovecot: Servidor de IMAP/POP3* de la sección *Servidores* del menú principal.
3. Haz clic en el enlace *Archivos de correo*.
4. Selecciona la opción *Bandeja de entrada bajo /var/mail carpetas en ~/mail* de la lista *Localización de archivo de correo*. Así indicas que:
 - Las carpetas de correo de cada usuario, como por ejemplo *Enviados* y *Papelera*, se almacenarán en el servidor, concretamente en la carpeta *mail* del directorio personal de cada uno de ellos.
 - Todas las bandejas de entrada de los usuarios también se guardarán en el servidor, pero esta vez en archivos dentro de la carpeta */var/mail*. Cada archivo se llamará como su propietario.
5. Despliega la lista *Formato UIDL* y selecciona *Mensajero 2*. No es necesario que escribas nada en el correspondiente cuadro de texto. Con esta acción estás indicando el formato del

- identificador de mensaje que usará el servidor POP3 para saber qué mensajes aún no han sido descargados por un cliente de correo.
6. Haz clic sobre el botón *Salvar* para guardar los cambios.
 7. Haz clic en el botón *Aplicar configuración*.

Preparación del usuario

Para que un cliente de correo pueda configurar una cuenta con un determinado usuario, la bandeja de entrada de ese usuario ya debe existir en el sistema de archivos del servidor. El fichero que contiene esta bandeja se crea automáticamente cuando el usuario recibe el primer correo. ¿Qué significa eso exactamente? Vamos a comprobarlo.

Accede, dentro de la sección *Servidores*, al enlace *Lectura de Correo de Usuarios*. En la lista de buzones de usuario busca el usuario *alumno2smr*. Al pinchar nos da un error ya que no está creada la carpeta para la bandeja de entrada. Evidentemente tenemos que crearla. Así con todos los usuarios de correo. Una vez creadas las carpetas comprueba que no da error. Puedes incluso componer correos y enviarlos para ver que no da ningún error.

Configuración del cliente

Cada usuario del sistema tiene que poder ejecutar un cliente de correo manteniendo la privacidad de los mensajes que mande o que reciba. Por eso, cada usuario debe configurarlo con sus propias cuentas de correo:

1. Entras en Thunderbird del cliente correspondiente. Te va a pedir los datos para configurar la cuenta de correo.
2. Introduce los datos correctos.
3. Como es la primera vez que el cliente se conecta al servidor POP3, se muestra una excepción de seguridad.
4. Le das a *Aceptar* y ya lo tienes configurado.

Caso práctico 1

Objetivo: mostrar el funcionamiento del servidor de correo.

Descripción: vas a crear una cuenta de correo operativa para cada uno de los trabajadores de la empresa (cliente1, cliente2, cliente3 y cliente4). Las direcciones de correo serán: *cliente1@cieloazul.com* para el primero, y así sucesivamente.

Para comprobar el correcto funcionamiento se realizará el envío desde un cliente a otro, y deberá llegar el mensaje correctamente.

Peso de la nota: 30% de la nota del tema.

Se evaluará:

- Funcionamiento de la práctica (5 puntos).
- Conocimiento de los cambios realizados en el servidor para el correcto funcionamiento (3 puntos).
- Integración con el servidor DNS (2 puntos).

Caso práctico 2

Objetivo: mostrar el funcionamiento del servidor de correo con varias copias.

Descripción: una vez que funciona el caso práctico anterior, se trata de realizar un envío de un cliente al resto de clientes.

Peso de la nota: 30% de la nota del tema.

Se evaluará:

- Funcionamiento de la práctica (5 puntos).
- Conocimiento de los cambios realizados en el servidor para el correcto funcionamiento (3 puntos).
- Integración con el servidor DNS (2 puntos).