UD5. Instalación y administración del servicio de correo electrónico.

- - Características generales del servicio de correo electrónico.
- - Elementos del servicio de correo electrónico. Agentes.
- - Estructura de los mensajes de correo electrónico.
- - Protocolo de transferencia de mensajes.
- - Clientes de correo electrónico.
- - Cuentas de correo, alias y buzones de usuario.
- - Servicio de correo electrónico vía web.
- - Instalación y configuración de un servidor de correo electrónico.
- - Correo seguro: firma digital y cifrado de mensajes.
- - Reenvío de correo.
- - Técnicas para evitar correo no deseado. Filtros.
- - Protocolos y servicios de descarga de correo.
- - Diagnóstico y resolución de incidencias en el servicio.
- - Documentación de las configuraciones establecidas.

Características generales del servicio de correo electrónico.

Correo electrónico (e-mail), es un servicio de red que permite a los usuarios enviar y recibir mensajes (también denominados mensajes electrónicos o cartas digitales) mediante sistemas de comunicación electrónica. Principalmente se usa este nombre para denominar al sistema que provee este servicio en Internet, mediante el protocolo SMTP, aunque por extensión también puede verse aplicado a sistemas análogos que usen otras tecnologías. Por medio de mensajes de correo electrónico se puede enviar, no solamente texto, sino todo tipo de documentos digitales dependiendo del sistema que se use.

Características:

- Permite enviar correos desde un remitente a varios destinatarios.
- No se espera respuesta inmediata.
- La entrega es prácticamente inmediata.

- El coste es casi nulo.
- Se puede leer en cualquier momento y almacenar en formato digital y en cualquier dispositivo digital.
- Permite generar el mensaje y enviarlo a posterior.
- Sigue el modelo cliente servidor.

Inconvenientes:

- Permite la propagación de malware.
- No garantiza la recepción.
- No asegura que el remitente sea quien dice ser.
- No avisa si ha habido problemas con el mensaje o el envío.

Elementos del servicio de correo electrónico. Agentes.

Elementos del Correo Electrónico:

- Buzón de Usuario. Espacio en el servidor asociado a una cuenta, es donde se almacenan los mensajes.
- Cuenta de Correo. Identificador de la cuenta asociada al buzón.
- Cuenta de Correo Redirigida. Cuenta no asociada a un buzón, sino que está asociada a una cuenta de otro dominio a la que se reenvían los correos.
- Alias. Especie de redireccionamiento de cuentas dentro de un dominio.
- Listas de distribución. Es una cuenta virtual que engloba a varias cuentas de correo que pueden pertenecer al mismo usuario o a diferentes.

Agentes del Servicio de Correo:

MUA (Mail User Agent). Es un programa que se instala en el ordenador del usuario y que permite leer y enviar correo (Outlook, Thunderbird, Mailx, The Bat, etc).

Características:

- Dispone de un interfaz de usuario local que permite editar, componer, leer el correo.
- Es el cliente de correo tradicional.
- Permite almacenar mensajes en el ordenador local y mantener la libreta de direcciones.

MDA (Mail Delivery Agent). Se encarga de copiar los mensajes desde el servidor de correo hasta el buzón de usuario. Algunos de los más usados son:

- Qpopper y Cyrus.
- Maildrop (Unix).
- Dovecot.

MTA (Mail Transfer Agent). Transfiere los mensajes entre servidores, empleando el protocolo SMTP.

Los más comunes son:

- Sendmail.
- Postfix.
- Microsoft Exchange.
- Qmail.
- Exim.

Funciones:

- Realiza el encaminamiento del correo.
- Trabajan como servidores de correo.
- Envía el correo saliente y chequea el entrante.

Estructura de los mensajes de correo electrónico.

Escritura del mensaje

No se pueden mandar mensajes entre computadores personales o entre dos terminales de una

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

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

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

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

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

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

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

Entonces:

- ✔ Beatriz recibe el mensaje dirigido a ella (sale en el campo Para), y ve que Carlos y David también lo han recibido
- ✔ Carlos recibe un mensaje que no va dirigido a él, pero ve que aparece en el campo CC, y por eso lo recibe. En el campo “Para” sigue viendo a Beatriz

- ✔ David, igual que Carlos, ya que estaban en la misma lista (CC)
- ✔ Esteban recibe el correo de Ana, que está dirigido a Beatriz. Ve que Carlos y David también lo han recibido (ya que salen en el CC), pero no se puede ver a él mismo en ninguna lista, cosa que le extraña. Al final, supone que es que Ana le incluyó en el campo CCO.

- Campo Reply-To (responder) Dirección dónde el emisor quiere que se le conteste. Muy útil si el emisor dispone de varias cuentas.
- Campo Date (fecha, y hora, del mensaje) Fecha y hora de cuando se envío del mensaje. Si el sistema que envía el mensaje tiene la fecha y/u hora equivocadas, puede generar confusión.

Otros campos, menos importantes son:

- Sender: Sistema o persona que lo envía
- Received: Lista de los MTA que lo transportaron
- Message-Id: Número único para referencia
- In-Reply-to: Id. del mensaje que se contesta
- References: Otros Id del mensaje
- Keywords: Palabras claves de usuario
- X-Usuario: Definibles por el usuario

La cabecera del mensaje normalmente, se muestra resumida. Para ver todos los detalles bastará con expandir, mediante la opción oportuna, dicha cabecera.

Protocolo de transferencia de mensajes.

Principales protocolos usados en el correo electrónico:

- MIME
- SMTP
- POP3
- IMAP

MIME

Multipurpose Internet Mail Extensions o MIME (en español "extensiones multipropósito de correo de internet") son una serie de convenciones o especificaciones dirigidas al intercambio a través de Internet de todo tipo de archivos (texto, audio, vídeo, etc.) de forma transparente para el usuario. Una parte importante del MIME está dedicada a mejorar las posibilidades de transferencia de texto en distintos idiomas y alfabetos. En sentido general las extensiones de MIME van encaminadas a soportar:

- Texto en conjuntos de caracteres distintos de US-ASCII;
- adjuntos que no son de tipo texto;
- cuerpos de mensajes con múltiples partes (multi-part);
- información de encabezados con conjuntos de caracteres distintos de ASCII.

Prácticamente todos los mensajes de correo electrónico escritos por personas en Internet y una proporción considerable de estos mensajes generados automáticamente son transmitidos en formato MIME a través de SMTP. Los mensajes de correo electrónico en Internet están tan cercanamente asociados con el SMTP y MIME que usualmente se les llama mensaje SMTP/MIME.1

Los tipos de contenido definidos por el estándar MIME tienen gran importancia también fuera del contexto de los mensajes electrónicos. Ejemplo de esto son algunos protocolos de red tales como HTTP de la Web. HTTP requiere que los datos sean transmitidos en un contexto de mensajes tipo e-mail aunque los datos pueden no ser un e-mail propiamente dicho.

En la actualidad ningún programa de correo electrónico o navegador de Internet puede considerarse completo si no acepta MIME en sus diferentes facetas (texto y formatos de archivo).

SMTP

El Simple Mail Transfer Protocol (SMTP) (“protocolo para transferencia simple de correo”), es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA, teléfonos móviles, etcétera). Fue definido en el RFC 2821 y es un estándar oficial de Internet.1

El funcionamiento de este protocolo se da en línea, de manera que opera en los servicios de correo electrónico. Sin embargo, este protocolo posee algunas limitaciones en cuanto a la recepción de mensajes en el servidor de destino (cola de mensajes recibidos). Como alternativa a esta limitación se asocia normalmente a este protocolo con otros, como el POP o IMAP, otorgando a SMTP la tarea

específica de enviar correo, y recibirlos empleando los otros protocolos antes mencionados (POP O IMAP).

POP3

En informática se utiliza el Post Office Protocol (POP3, Protocolo de Oficina de Correo o "Protocolo de Oficina Postal") en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto. Es un protocolo de nivel de aplicación en el Modelo OSI.

Características de POP3

POP3 está diseñado para recibir correo, no para enviarlo; le permite a los usuarios con conexiones intermitentes o muy lentas (tales como las conexiones por módem), descargar su correo electrónico mientras tienen conexión y revisarlo posteriormente incluso estando desconectados. Cabe mencionar que la mayoría de los clientes de correo incluyen la opción de dejar los mensajes en el servidor, de manera tal que, un cliente que utilice POP3 se conecta, obtiene todos los mensajes, los almacena en la computadora del usuario como mensajes nuevos, los elimina del servidor y finalmente se desconecta. En contraste, el protocolo IMAP permite los modos de operación conectado y desconectado.

Los clientes de correo electrónico que utilizan IMAP dejan por lo general los mensajes en el servidor hasta que el usuario los elimina directamente. Esto y otros factores hacen que la operación de IMAP permita a múltiples clientes acceder al mismo buzón de correo.

Al igual que otros viejos protocolos de internet, POP3 utilizaba un mecanismo de firmado sin cifrado. La transmisión de contraseñas de POP3 en texto plano aún se da. En la actualidad POP3 cuenta con diversos métodos de autenticación que ofrecen una diversa gama de niveles de protección contra los accesos ilegales al buzón de correo de los usuarios. Uno de estos es APOP, el cual utiliza funciones MD5 para evitar los ataques de contraseñas. Mozilla, Eudora, Novell Evolution así como Mozilla Thunderbird implementan funciones APP.

IMAP

Internet Message Access Protocol (IMAP, Protocolo de acceso a mensajes de internet), es un

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

IMAP y POP3 (Post Office Protocol versión 3) son los dos protocolos que prevalecen en la obtención de correo electrónico. Todos los servidores y clientes de correo electrónico están virtualmente soportados por ambos, aunque en algunos casos hay algunas interfaces específicas del fabricante típicamente propietarias.

IMAP fue diseñado como una moderna alternativa a POP por Mark Crispin en el año 1986. Fundamentalmente, los dos protocolos les permiten a los clientes de correo acceder a los mensajes almacenados en un servidor de correo.

Ya sea empleando POP3 o IMAP4 para obtener los mensajes, los clientes utilizan SMTP para enviar mensajes. Los clientes de correo electrónico son comúnmente denominados clientes POP o IMAP, pero en ambos casos se utiliza SMTP.

Comparativa POP3 e IMAP

En la siguiente tabla se recogen las principales ventajas de IMAP con respecto a POP3:

Protocolo	Ventajas	Desventajas
IMAP4	• Trabaja en modo de conexión permanente, por lo que avisa inmediatamente de la llegada de nuevo correo • Transmite solo las cabeceras por lo que el usuario puede decidir su borrado inmediato • La bajada del mensaje se produce solo cuando el usuario quiere leerlo • El almacenamiento local del mensaje es opcional (una opción del	• No todos los clientes de correo soporta la extensión IMAP IDLE (aviso de nuevos correos) • Necesita una transacción por cada correo que se quiera leer • Hay un retraso en la aparición del mensaje en la pantalla del usuario, mientras se descarga • Si se pierde la conexión, no se podrá ver el mensaje salvo si el cliente de correo lo haya

	cliente de correo) • Gestiona carpetas, plantillas y borradores en el servidor • El almacenamiento de mensajes y carpetas en el servidor permite su uso desde múltiples dispositivos y de forma simultánea • Permite la búsqueda de mensajes por medio de palabras claves • Los mensajes se pueden etiquetar. El marcado queda en el servidor • Se pueden crear carpetas compartidas con otros usuarios (depende del servidor)	almacenado en local • Las carpetas, plantillas y borradores no podrán ser leídos usando POP (excepto la Bandeja de entrada)
POP3	• Los correos aparecen inmediatamente porque quedan residentes en el dispositivo (una vez descargados)	• Sólo se conecta periódicamente cada X minutos para buscar por nuevo correo • La conexión periódica provoca un aumento del tráfico y un retraso en la respuesta del cliente (esperar la descarga completa) • En cada conexión, se baja todos los correos nuevos, vayan a ser después leídos o no • Los correos ocupan espacio local del dispositivo • Por defecto, elimina los mensajes del servidor, haciendo imposible el acceso a ellos desde otro

Clientes de correo electrónico.

Un cliente de correo electrónico es un programa de ordenador usado para leer y enviar mensajes de correo electrónico.
Originalmente, los clientes de correo electrónico fueron pensados para ser programas simples para leer los mensajes del correo de usuario, enviados por el agente de reparto de correo (MDA) conjuntamente con el agente de transferencia de correo (MTA) a un buzón local.

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

Los mensajes de correo electrónico pendientes de envío serán entregados al MTA, tal vez a través de un agente de correo saliente, de forma que el cliente de correo electrónico no necesita proporcionar ninguna clase de función de transporte.

Dado que las diferentes versiones de Microsoft Windows para uso doméstico nunca han proporcionado un agente de transferencia de correo, los clientes de correo más modernos deben soportar protocolos como POP3 e Internet Message Access Protocol (IMAP) para comunicarse con un MTA remoto localizado en la máquina de proveedores de correo electrónico.

IMAP está optimizado para almacenar correos electrónicos en el servidor, mientras que el protocolo POP3 asume generalmente que los mensajes de correo electrónico se descargan al cliente. La gran mayoría de clientes de correo electrónico emplean el Protocolo de Transferencia Simple de Correo (Simple Mail Transfer Protocol, SMTP) para enviar los mensajes de correo electrónico.

Además de los clientes de correo electrónico de "cliente grueso" y de los pequeños clientes de correo que cooperan con un MDA/MTA local, aquí presentados, existen también programas de correo electrónicos basados en la Web, denominados webmail o correo web.

Un importante estándar soportado por la mayoría de los clientes de correo electrónico es MIME, que se emplea para el envío de archivos binarios adjuntos al correo. Los adjuntos son ficheros que no forman parte del correo electrónico propiamente dicho, pero que se envían junto con éste.

Messaging Application Programming Interface (MAPI) es una interfaz de programación de aplicaciones (API) privativa de Microsoft Windows que puede emplearse para acceder al servidor de correo Microsoft Exchange o para interactuar con el cliente Microsoft Outlook.

Programas cliente de correo

Mozilla Thunderbird es un cliente de correo electrónico de la Fundación Mozilla. Su objetivo es desarrollar un Mozilla más liviano y rápido mediante la extracción y rediseño del gestor de correo del Mozilla *oficial*. Es multiplataforma, utiliza el lenguaje de interfaz XUL y es software libre.

Outlook Express es un cliente de correo electrónico y de noticias de red producido por Microsoft para sus plataformas Windows, también con versiones para otras plataformas.

Es un programa especializado en correo electrónico y noticias de red, por lo que no incluye las características de groupware. En cambio, permite un mejor manejo de algunas características comunes en grupos de correo electrónico y noticias de red, como el manejo de texto.

Fue reemplazado por el cliente Windows Mail y luego Windows Live Mail.

Microsoft Outlook es un programa de pago que se incluye dentro de la *suite* Microsoft Office. Su funcionamiento es parecido al Outlook Express, aunque varían temas de configuración, creación de identidades, así como, incluye algunas funcionalidades extras como la agenda.

Microsoft Outlook es una aplicación de gestión de correo, así como agenda personal, que nos permite la comunicación con miles de personas en todo el mundo a través de mensajes electrónicos.

Cuentas de correo, alias y buzones de usuario.

Cuentas de correo

Una cuenta de correo se asocia a un único usuario, el cual puede acceder a su cuenta a través de un nombre de usuario y contraseña. Las cuentas de correo suelen ser servicios que ofrecen empresas de forma gratuita (los más populares) o de pago. Algunos de estos servicios populares son Gmail de Google, Yahoo! Mail de Yahoo! y Hotmail de Microsoft. Los servicios mencionados anteriormente son todos del tipo webmail. El servicio de cuentas de correo es ofrecido por servidores de mail, que son los encargados de recibir, almacenar y/o enviar mensajes de e-mail, empleando POP3 y SMTP para la recepción y envío respectivamente. No todos los proveedores de servicios de correo electrónico ofrecen acceso por POP3, sino que sólo admiten acceso a los e-mails por web. Algunos servicios requieren un pago por parte de sus usuarios para acceder al POP3

Alias de correo

Un alias de correo es una dirección especial en tu dominio que redirige todos los mensajes que recibe a otra cuenta.

Las cuentas de alojamiento en servers soportan dos tipos de alias de correo:

- Alias específico a otra(s) dirección(es): Puede ser una cuenta de tu dominio o a una dirección externa. Un alias puede tener uno o varios destinos.
- Alias universal que recibe cualquier dirección de tu dominio.

En un inicio, los aliases universales eran formas populares y útiles de tener varias direcciones de correo. Hoy en día no recomendamos su uso debido a la cantidad de spam (correo no solicitado) que llega al momento de configurarlo.

Buzón de correo electrónico

Un buzón puede pertenecer a un usuario o a un grupo de usuarios, o puede ser el lugar donde acumular el correo de alguien con una función específica. No hay ninguna convención estándar sobre como es o debe ser el nombre que tenga un buzón de correo para un usuario en particular. Normalmente éste suele ser el identificador con el que el usuario accede a la máquina que le gestiona el correo; y suele estar formado por las siglas de su nombre, o alguna combinación de la letras que identifican su apellido y nombre. Sin embargo, sí que existe una especie de acuerdo estándar sobre el nombre de un buzón cuando se le va a destinar a algún tipo.

Servicio de correo electrónico vía web.

Webmail

Un correo web es un cliente de correo electrónico, que provee una interfaz web por la que accede al correo electrónico. Otras formas de acceder al correo electrónico pueden ser:

- Conectándose con un cliente de correo local a un servidor de correo remoto utilizando un protocolo ad hoc de transporte de correo, como IMAP o POP, descargar los correos y almacenarlos localmente.

- Utilizando un cliente de correo por consola, por ejemplo Mutt.

El webmail permite listar, desplegar y borrar vía un navegador web los correos almacenados en el servidor remoto. Los correos pueden ser consultados posteriormente desde otro computador conectado a la misma red (por ejemplo Internet) y que disponga de un navegador web.

Generalmente también permite la redacción y envío de correos mediante esta modalidad y no está limitado a la lectura de correo electrónico.

Veamos algunos ejemplos de correo web libres:

RoundCube es un cliente de correo que nos permite visualizar los mensajes de nuestras cuentas de email a través de una página web. Pudiendo acceder desde cualquier navegador con acceso a internet. Desde él podremos realizar todas las operaciones necesarias para gestionar nuestros correos e incluso usarlo como agenda de contactos y calendario.

RoundCube esta liberado bajo la licencia GPL, RoundCube es software libre.

Zimbra ('**Zimbra Collaboration Suite**' o **ZCS**) es un programa informático colaborativo o Groupware que consta de un servicio de correo electronico creado por Zimbra Inc. compañía ubicada en San Mateo, California. La compañía fue adquirida por Yahoo! Inc. por aproximadamente 350 millones de dólares en septiembre de 2007, acordando mantener sus estándares de código abierto. El 12 de enero de 2010 fue nuevamente vendida por Yahoo a VMware. En Julio de 2013 Telligent adquirió la suite de VMware.

Posee tanto el componente de servidor como su respectivo cliente. Existen varias versiones de Zimbra disponibles: unas versiones de código abierto soportadas por la comunidad, y otras con parte del código cerrado y soportadas comercialmente que contiene algunas mejoras.

Empresas que dan servicio de correo web:

Gmail, llamado en otros lugares **Google Mail** por problemas legales, es un servicio de correo electrónico con posibilidades POP3 e IMAP gratuito proporcionado por la empresa estadounidense Google, ha captado la atención de los medios de información por sus innovaciones tecnológicas y su capacidad. El servicio de Gmail, junto con Google Calendar, Google Docs, Hangouts.. es hoy día de los más utilizados. Los documentos sobre el entramado de vigilancia mundial filtrados en 2013 y 2014 apuntan a que Gmail es uno de los objetivos de las agencias de inteligencia para la captación

masiva de datos.

Yahoo! Mail es el servicio de correo electrónico gratuito de Yahoo!. Es otro de los mayores proveedores de correo electrónico de Internet, que sirve a millones de usuarios.

Instalación y configuración de un servidor de correo electrónico.

Servidor de correo electrónico Postfix.

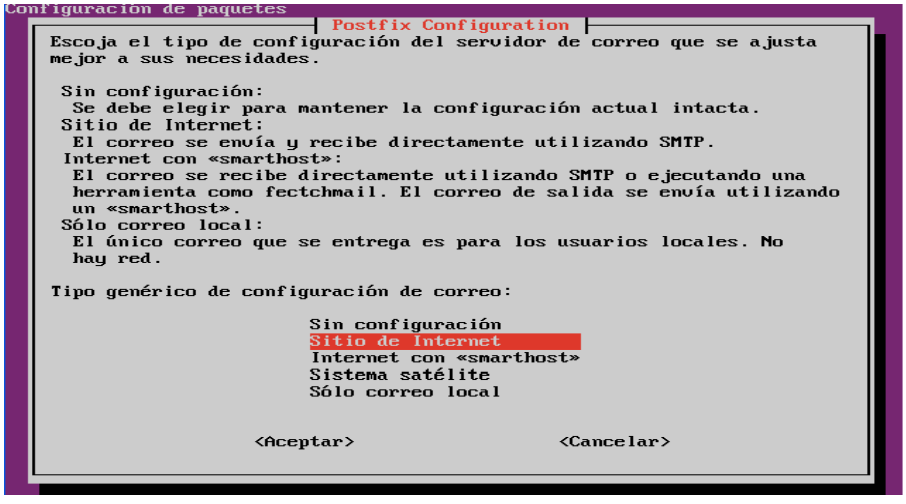
Normalmente el servidor de correo electrónico que se instala por defecto en los sistemas GNU/Linux es sendmail. Hemos elegido proceder con la instalación y configuración de Postfix porque es mucho más versátil, fácil de instalar y configurar, además es el servidor que viene predeterminado en la instalación de Ubuntu Server.

Instalación de Postfix.

mediante apt-get:

apt-get install postfix

Una vez realizada la instalación se inicia un asistente que nos ayuda a configurar el servidor de correo donde debemos indicar el tipo de servicio que deseamos instalar (normalmente Sitio de Internet) e indicamos el nombre FQDN del sitio de Internet (p.ej., servidorcorreoiescamp.es)



Iniciando el servcio

Después de la instalación, podemos consultar que está activo con el comando

service postfix status

y si no lo está iniciar el servicio ejecutando

service postfix start

Postfix tiene varios logs donde nos indica su actividad y posibles errores que hayan surgido, estos ficheros de registro son:

/var/log/mail.log

/var/log/mail.err

Cuando *Postfix* se inicia correctamente en el fichero **/var/log/mail.log** genera los siguientes mensajes:

```
Mar 22 18:40:57 ServidorCep dovecot: ssl-params: Generating SSL parameters
Mar 22 18:41:04 ServidorCep dovecot: ssl-params: SSL parameters regeneration co$
Mar 22 18:41:05 ServidorCep postfix/master[878]: daemon started -- version 2.8.$
```

Archivos de configuración.

Los ficheros de configuración de *Postfix* se encuentran en el directorio ***/etc/postfix***. Los ficheros más importantes de configuración son:

- **main.cf.** Contiene las opciones generales de configuración del servidor de correo. Existe un archivo **usr/share/postfix/main.cf.dist** donde aparecen las opciones de este archivo con mayor detalle.

- **master.cf.** Controla cómo se conectan los clientes al servidor y cómo están configurados los servicios para que el servidor funcione correctamente.

- Las opciones más importares del fichero de configuración *main.cf* son:
    - **Directorios de trabajo.** En los directorios de trabajo se indica el directorio donde se almacenan los mensajes (*queue_directory*), donde se encuentran los comandos de root (*command_directory*), el servidor (*daemon_directory*) y dónde se guardan los

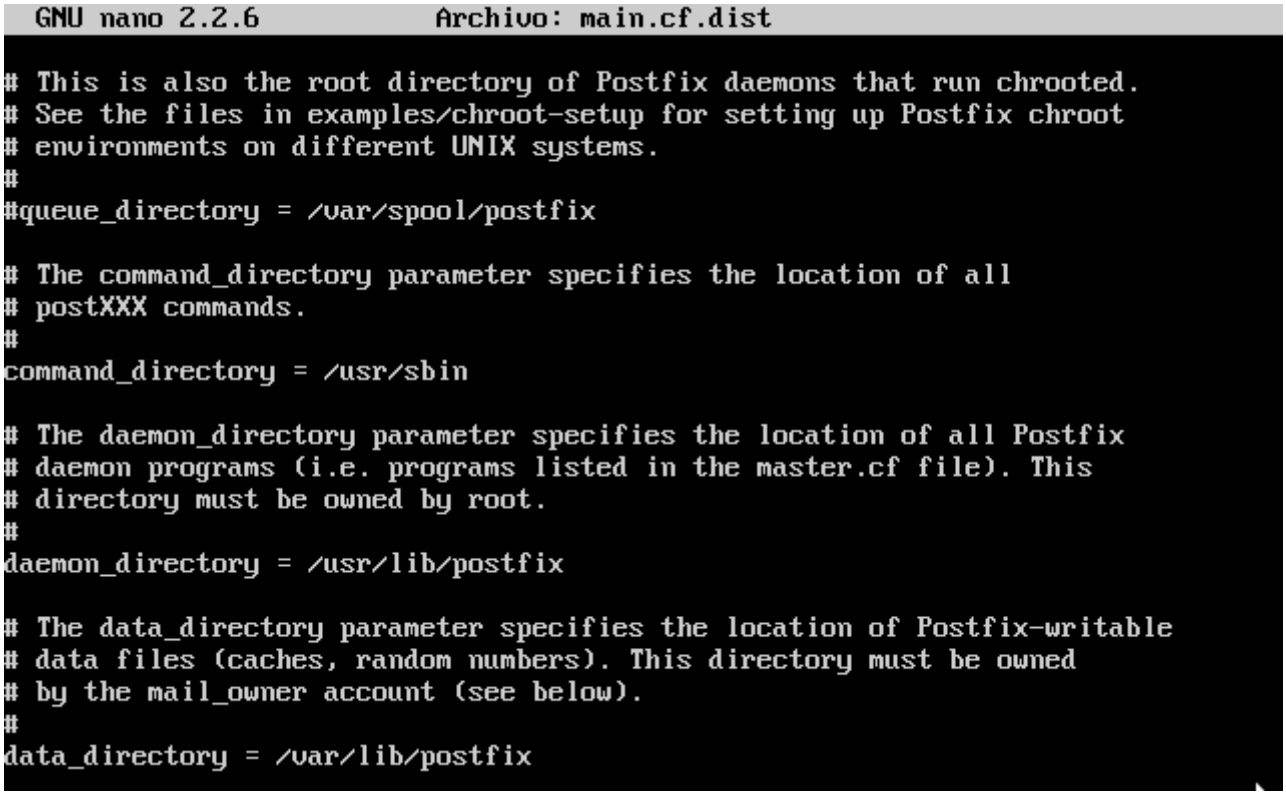
datos del servidor (*data_directory*). Por defecto:

queue_directory = /var/spool/postfix

command_directory = /usr/sbin

daemon_directory = /usr/libexec/postfix

data_directory = /var/lib/postfix



inet_interfaces. Indica las interfaces por donde el servidor recibe los correos electrónicos.

inet_interfaces = eth0

Para recibir los correos por cualquier interfaz de red escribimos

inet_interfaces = all

- **mynetworks.** Permite indicar nuestra dirección de red local.

Mynetworks = 127.0.0.0/8, 192.168.2.0/24

- **mydestination.** Permite indicar qué dominios debe utilizar para administrar el correo. Por ejemplo, si desea gestionar el dominio servidorcep.es escribimos:
  mydestination= servidorcep.es, localhost.localdomain, localhost

  En el archivo *master.cf* podemos ver una lista estructurada de los dominios, servicios y procesos que pueden activarse y configurarse en *Postfix*. A continuación, a modo de ejemplo, vemos las líneas referentes al proceso *smtp*.

```
#
==========================================================
=
#service type private unpriv chroot wakeup maxproc command + args
# (yes) (yes) (yes) (never) (100)
#
==========================================================
=
smtp inet n - n - - smtpd
```

  En este caso, el servicio *smtp* es el servicio **SMTP** básico que recibe correos por el **puerto 25/tcp.**

Configurando Postfix

Existen varias formas de configurar *Postfix*, mediante un editor de textos (p.ej., *nano)*, mediante el comando *postconf* o mediante Webmin que es una interfaz gráfica para administrar servidores remotamente.

vamos a configurarlo mediante el comando

sudo dpkg-reconfigure postfix

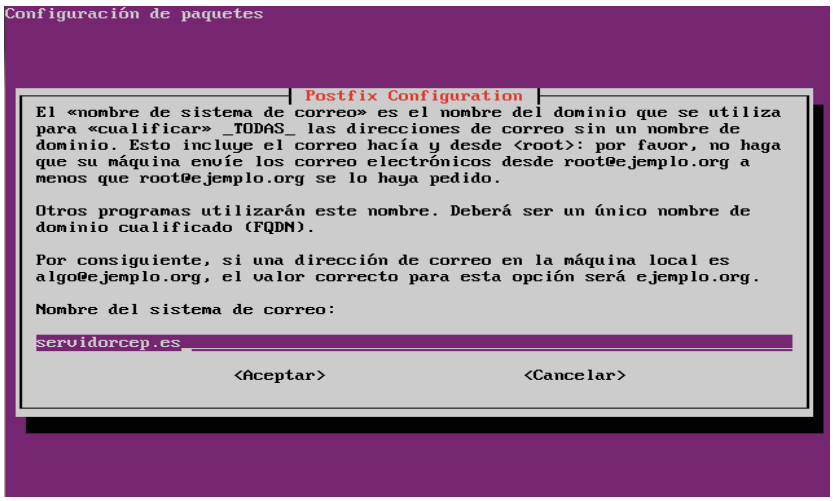
En Postfix podemos determinar que tipo de sitio vamos a tener en nuestro servidor:

- **Sin Configuración**: Esta opción no hace ninguna modificación al servidor de correo Postfix.
- **Sitio de Internet**: Se caracteriza porque el propio servidor se encarga de enviar/recibir correo electrónico utilizando SMTP, esta es la opción por default.
- **Internet con <<smarthost>>**: Se caracteriza porque el servidor no envía los correo directamente a los destinatarios, sino que los envía a otros servidores de correo y ellos se encargan de enviarlos.
- **Sistema Satélite**: Todo correo saliente se envia a otra máquina, llamada host, el correo de root y postmaster se envía de acuerdo a /etc/aliases, solamente se recibe correo localmente.
- **Solo Correo Local**: Solo entrega correo a los usuarios locales que tiene registrado el servidor de correo y no hay red.

En nuestro caso seleccionaremos la opción de **Sitios de Internet,** ya que nuestro servidor sera el encargado de administrar los usuarios y el envío/recepción de correo electrónico.

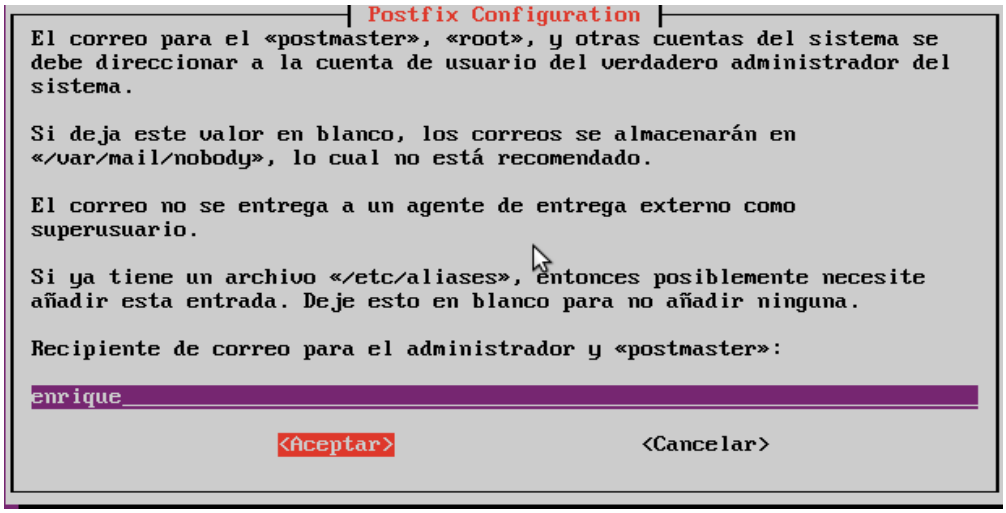
Nombre del servidor

En esta parte de la configuración solamente agregamos el nombre del servidor, o del dominio.



Alias

Solamente tomará la configuración del archivo /etc/aliases para poder enviar correo al administrador del sistema.

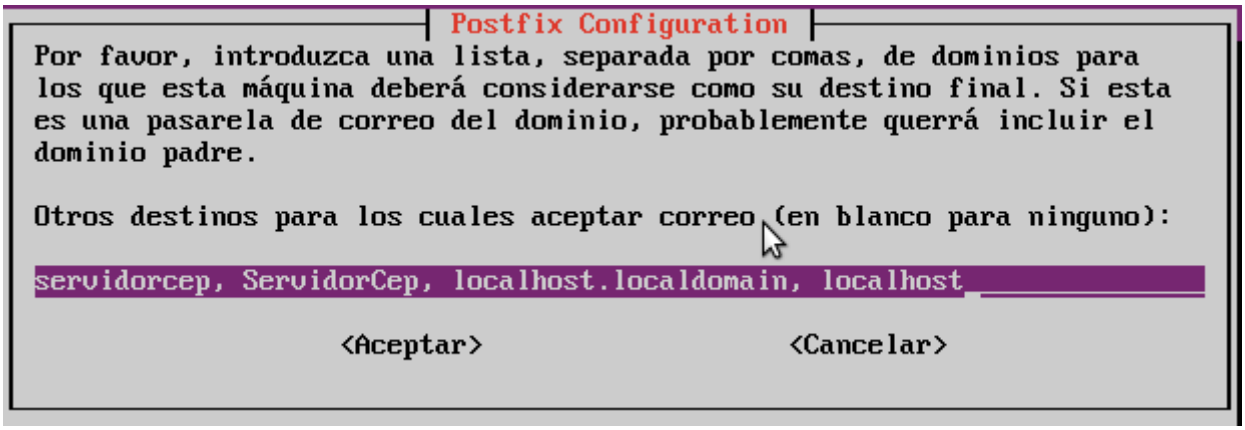


Recipiente del root/postmaster

Se personaliza a que usuario le va llegar el correo del administrador root y postmaster.

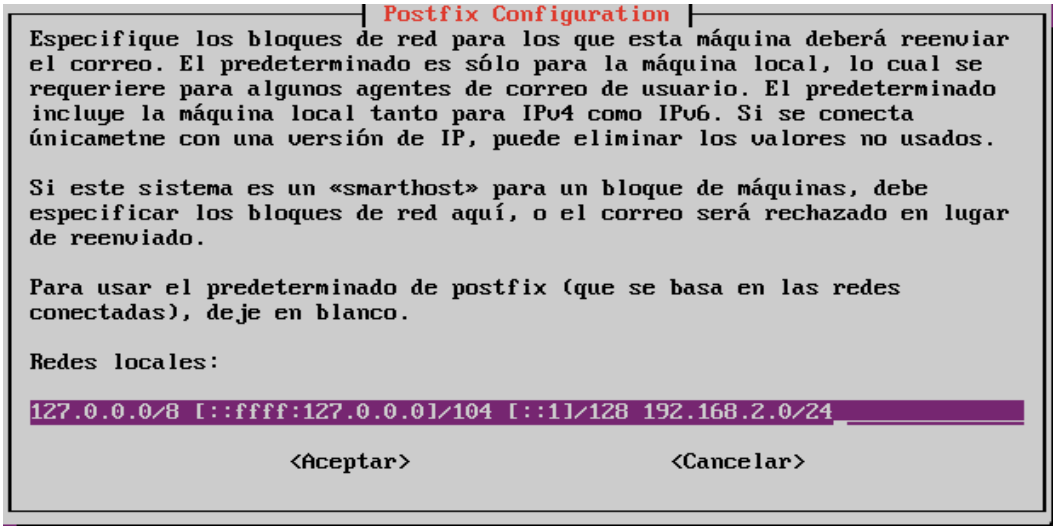
Dominios a Administrar.

Aquí agregamos los dominios que va administrar nuestro servidor de correo, los datos van separados por comas.



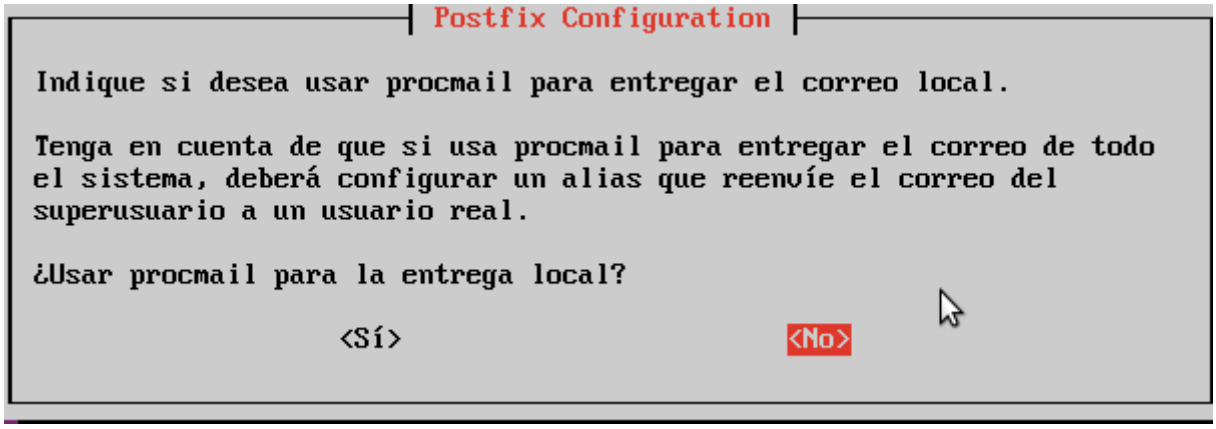
Redes Permitidas.

En esta configuración solamente permitimos las redes que tendrán acceso a nuestro servidor de correo.



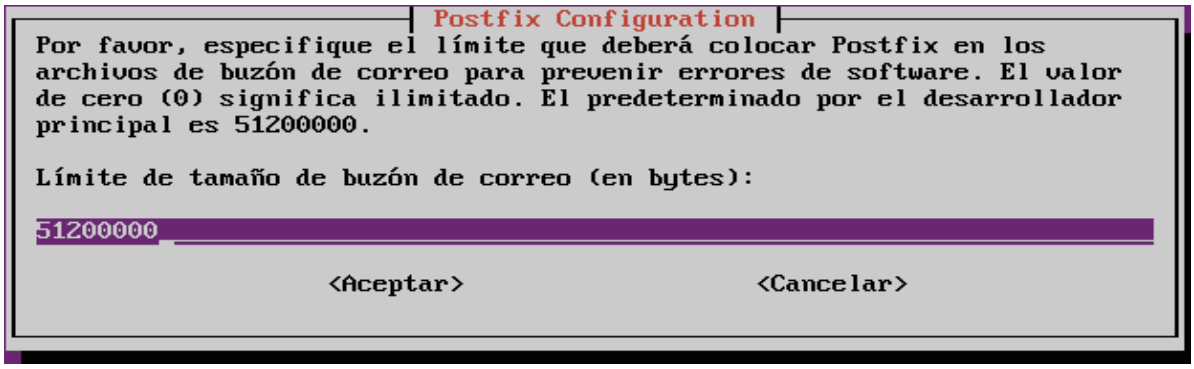
Configuración Procmail

Aquí indica que si Procmail va a ser el encargado de entregar correo localmente, seleccionamos la opción NO.



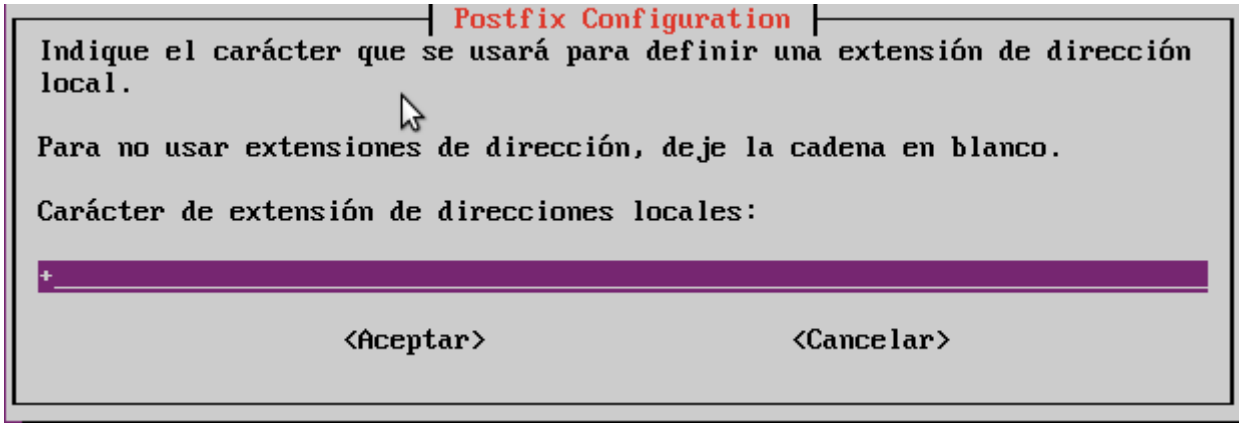
Tamaño de los Buzones.

Especificamos el tamaño de los buzones, por default viene con 51200000 bytes. Lo dejamos como está.



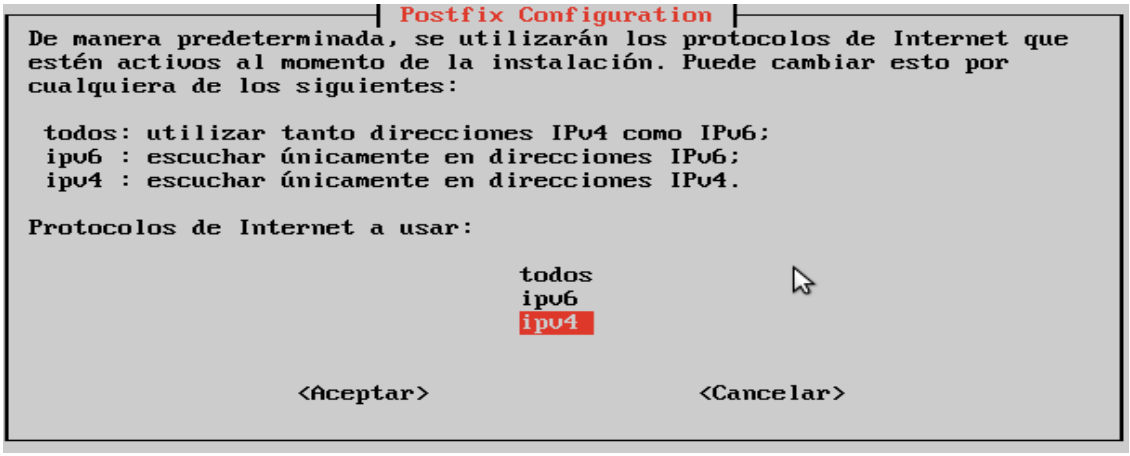
Extensiones.

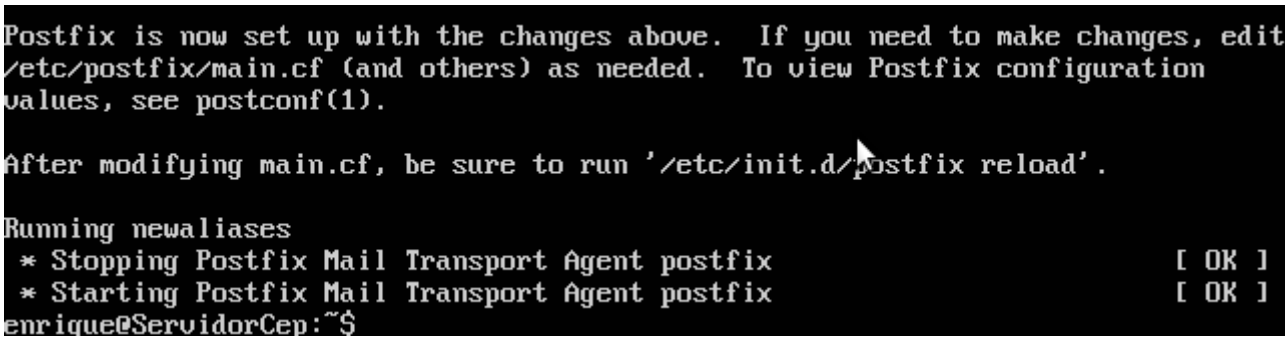
Dejamos el dato por default y damos enter para seguir.



Protocolos.

Solamente seleccionamos que protocolo queremos que utilice.





Ya tendríamos configurados la mayoría de los parámetros necesarios para usar Postfix.

Alias.

Algo que debe configurarse son los alias o redirecciones que correo. El superusuario *root* va a recibir muchos mensajes que, por seguridad, nunca recibirá.. La idea es que el administrador nunca se conecte como *root*, sino como un usuario normal y corriente.

Todo ello se consigue a través del archivo */etc/aliases* y del comando *newaliases*. Vamos al archivo de alias mencionado y allí introducimos la línea

root nombre_usuario

Una vez configurado reiniciaríamos el servidor ejecutando:

service postfix restart

Podremos ver todos los parámetros de la configuración de nuestro Postfix instalado usando el comando:

postconf

Seguridad.

Para evitar que nuestro servidor de correo electrónico se utilice de forma indebida es recomendable configurar el servidor para que lo utilicen los usuarios autorizados y evitar el correo spam.

Listas de bloqueo basadas en DNS.

Las listas de bloqueo son unas listas de servidores que supuestamente envían spam. Al configurar *Postfix* para que use estas listas significa que cada vez que llega un correo al servidor, *Postfix* comprueba que la IP del servidor que envía el mensaje no se encuentra en esas listas.

A continuación puede ver un ejemplo de lista de bloqueo que se especifica en el fichero *main.cf:*

```
maps_rbl_domains =
relays.ordb.org
list.dsbl.org
blackholes.mail-abuse.org
dialups.mail-abuse.org
relays.mail-abuse.org

smtpd_client_restrictions =
permit_mynetworks
reject_maps_rbl
check_relay_domains
```

En http://www.declude.com/JunkMail/Support/ip4r.htm podemos obtener un completo listado de bloqueo.

Control de envíos

Para indicar a *Postfix* los equipos o redes que pueden enviar correos a través del servidor se utiliza la directiva *mynetworks.* Por ejemplo, a continuación se indica que la red interna 192.168.2.0/24 puede enviar correos:

```
mynetworks = 127.0.0.0/8, 192.168.2.0/24
```

veamos algunos comandos que nos permitirán manejar postfix.

Postfix En este comando nos permite la administración del servicio postfix, teniendo

stop/start/reload/check/status	las opciones básicas de apagado, encendido, recargar, estatus del servicio y chequeo de configuración de postfix.
postfix flush	Esta es otra opción del comando postfix, el cual nos permite enviar a la fuerza correo a la cola.
mailq	Comando que nos permite ver la cola de mensajes.
postmap	Este comando nos ayuda crear ficheros de configuración auxiliares de Postfix.
postconf	Muestra la configuración actual de Postfix.
newaliases	Reconstruye la base de datos de alias.
Postqueue	Se utiliza para el manejo de las colas de correo.
-f	Manda el correo a la fuerza a cola.
-i	Envía inmediatamente un correo.
-p	Lista el contenido de las colas.
-s	Manda de golpe todos los correos a la cola.
Postsuper	Provee acceso a nivel de superusuario a la cola de correo. Permite al administrador borrar mensajes, retener o liberar mensajes o incluso reparar la estructura de la cola
-d #	Borra mensaje en la cola
-d all	Borra todos los mensajes en la cola.
-r #	Encola un mensaje.
-r all	Encola todos los mensajes.
postalias	Crea o consulta la Bds de los alias.
postcat	Muestra el contenidos de los archivos en cola, permite al administrador ver el contenido de los mensajes.

postdrop	Inyecta un mensaje dentro de la cola de salida para que Postfix lo entregue.
postkick	Se utiliza para comunicarse mediante linea de comandos con los distintos servicios de Postfix.
postlock	Bloquea una carpeta de correo para uso exclusivo.
postlog	Una interfaz de registro compatible con Postfix para usar, por ejemplo, en guiones del intérprete de comandos.

Probando el funcionamiento del correo

Primero vamos a crear otro usuario en el sistema para hacer las pruebas, para esto usaremos el comando

useradd -m nombre_usuario

lo siguiente es darle un password al usuario creado

passwd nombre_usuario

Ahora empezaremos conectando a nuestro servidor de correo mediante un **telnet** al puerto 25 usado para el correo SMTP, nos haremos pasar por un usuario **“**enrique” y le enviaremos un correo a otro usuario “paco” (ambos son usuarios del sistema donde se ha instalado *postfix*). Esto hará que se cree en el directorio ***/var/spool/mail/*** un fichero llamado paco que contendrá ese correo. Éste es el buzón de correo del usuario, y tal como está configurado *postfix* ahora, ahí vendrán a parar todos los correos añadiéndose al final del archivo de cada usuario, engordando ilimitadamente si no vamos borrando los sucesivos mensajes que recibamos, y si no configuramos cuotas.

Usamos el comando (telnet no viene por defecto hay que instalar)

telnet localhost 25

luego saludamos al servidor de correo con

helo localhost

y vamos especificando los usuarios emisor y receptor del mensaje además de los valores de los campos de nuestro email

mail from: usuario_remitente

rcpt to: usuario_receptor

data

subject: asunto_del_email

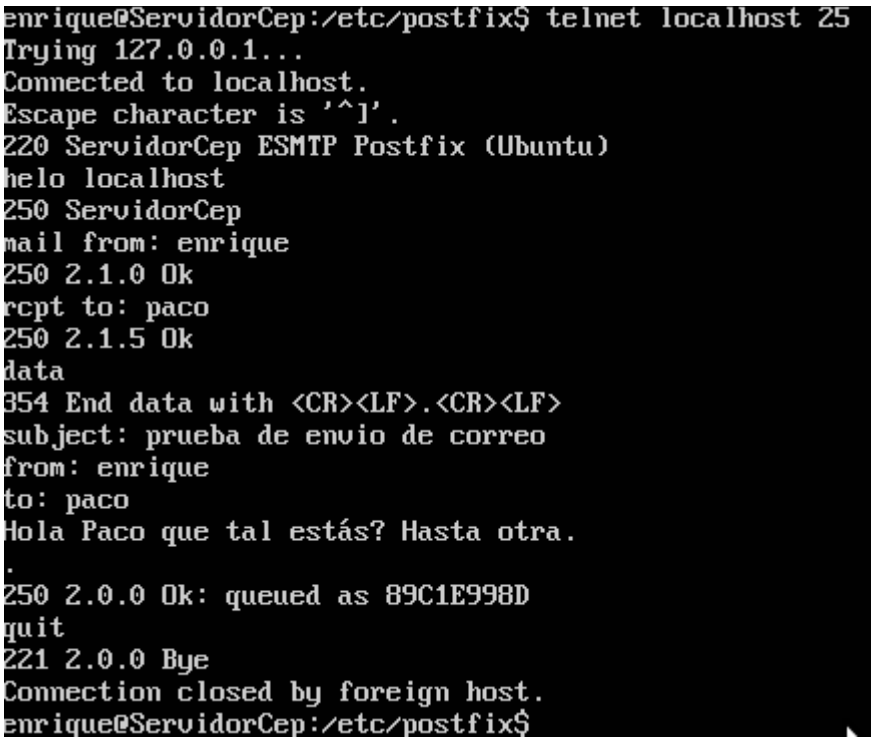
from: remitente

to: receptor

cuerpo_del_email

.

quit



Ahora se conectaría paco y leería el correo.

cat /var/spool/mail/paco

```
$ cat /var/spool/mail/paco
From enrique@ServidorCep  Thu Mar 22 19:27:33 2012
Return-Path: <enrique@ServidorCep>
X-Original-To: paco
Delivered-To: paco@ServidorCep
Received: from localhost (localhost [127.0.0.1])
        by ServidorCep (Postfix) with SMTP id 89C1E998D
        for <paco>; Thu, 22 Mar 2012 19:25:41 +0100 (CET)
subject: prueba de envio de correo
from: enrique@ServidorCep
to: paco@ServidorCep
Message-Id: <20120322182552.89C1E998D@ServidorCep>
Date: Thu, 22 Mar 2012 19:25:41 +0100 (CET)

Hola Paco que tal estás? Hasta otra.
```

Correo seguro: firma digital y cifrado de mensajes.

Concepto de criptografía

El uso del correo electrónico por medios habituales mediante canales inseguros, como por ejemplo la red Internet, no proporcionan confidencialidad ni autenticidad en los mensajes intercambiados entre los destinatarios.

Para asegurar la confidencialidad de la información es posible codificar la información intercambiada mediante el uso de la criptografía de mensajes. Los mensajes son cifrados por el remitente y descifrados por el destinatario, utilizando claves que solamente ellos conocen. De esta manera, los datos de los correos electrónicos que transitan por las redes y servidores de Internet están codificados, y son totalmente ininteligibles para terceras personas que pudieran hacer un uso fraudulento de tales datos.

Si los dos interlocutores utilizan la misma clave para cifrar y descifrar (claves simétricas), el procedimiento por el cual se intercambian las claves representa un punto débil en el esquema de seguridad. Esto se debe a que no existe ningún medio totalmente fiable para que la clave utilizada para codificar llegue al receptor con la seguridad de que no ha sido interceptada por terceros. Para solucionar este inconveniente de la criptografía simétrica, se hace uso de la criptografía de clave pública o asimétrica.

Criptografía de clave pública o asimétrica.

La criptografía de clave pública o asimétrica utiliza claves diferentes para codificar y descodificar. Se basa en la utilización de pares de claves complementarias por cada interlocutor que cumplen la propiedad de que la información cifrada con una, solamente puede ser descifrada con la otra, y viceversa. Una de estas claves es privada y la otra es pública. La clave privada debe conservarse en lugar seguro, ya que solamente puede tener acceso a ella el propietario de la clave. En cambio, la clave pública se puede distribuir, y debe comunicarse a las personas con las que se quiera intercambiar correo seguro.

La criptografía de clave pública no solamente permite la codificación, sino también la autenticación o firma de los mensajes. Mediante la autenticación o firma se puede tener la certeza de que el autor de un mensaje es quien dice ser, y el mensaje no ha sido modificado.

La criptografía simétrica es más eficiente en términos de rendimiento que la criptografía de clave pública debido a que requiere menos operaciones matemáticas. Por esto, se suele utilizar la criptografía de clave pública solamente en el punto débil del intercambio de información, que es en la comunicación de la contraseña que posteriormente utilizarán los interlocutores para cifrar y descifrar el contenido del mensaje.

Certificados digitales

La distribución de la clave pública entre varios interlocutores constituye un paso conflictivo por el problema de verificar correctamente la propiedad real de las claves públicas, ya que un intruso podría suplantar una determinada clave pública y con ello se infiltraría en comunicaciones codificadas. Las Autoridades de Certificación (AC) verifican y certifican que la propiedad de las claves públicas es de sus legítimos propietarios. El certificado digital de usuario emitido por la AC sirve para garantizar que una determinada clave pública corresponde a su propietario.

La Fábrica Nacional de Moneda y Timbre (FNMT) es una AC de la Administración Pública Española. La FNMT otorga de forma gratuita certificados digitales de usuario para la utilización de correo electrónico seguro. Los certificados para estos usos son los de la clase 2CA, válidos igualmente para operar vía Internet con Hacienda y otras administraciones.

Conceptos de firma y cifrado

Los certificados de la clase 2CA que otorga la FNMT utilizan el par de claves de cada usuario para firmar/verificar firmas y codificar/descodificar mensajes. Las claves son generadas por los navegadores y, posteriormente, la clave pública es incorporada al certificado cuando éste es descargado al navegador del cliente.

Si un usuario envía un mensaje solamente firmado, se incluye un resumen de firma de varios caracteres obtenido en función del texto del mensaje y de su propia clave privada. Para realizar la verificación de la firma, el destinatario aplica al mensaje la clave pública del remitente. Si de esta verificación se obtienen los mismos caracteres, el mensaje no ha sido manipulado, y se puede asegurar la autenticidad del mensaje. Un mensaje que está solamente firmado transita por la red totalmente legible y puede ser leído por terceras personas.

Si solamente se realiza la codificación del mensaje, el remitente utiliza la clave pública del destinatario para cifrar una clave de sesión simétrica. Con esta clave, el remitente cifra el mensaje. El destinatario utiliza su clave privada para descifrar la clave simétrica que utilizó el remitente para cifrar. En este caso, como el mensaje va codificado, transita ilegible por las redes, pero no se puede asegurar la autenticidad del emisor, debido a que cualquiera puede cifrar con la clave pública de un determinado usuario.

Los mensajes se cifran con la intención de que si algún tercero capta el mensaje no lo pueda entender, antes tendría que descifrarlo. Los mensajes se firman con el propósito de que no puedan ser alterados y de que el emisor no pueda negar luego el envío de dicho mensaje. Es posible enviar mensajes cifrados pero no firmados y viceversa.

Si un usuario posee su certificado, puede enviar correo firmado por él a cualquier persona, aunque ésta última no posea su certificado personal. Sin embargo, el receptor necesitará tener instalado en su navegador el certificado de la FNMT de clase 2CA. En primer lugar, el certificado raíz valida la clave pública del remitente, y esta clave verifica su firma.

Por lo tanto, para garantizar la confidencialidad y la autenticidad de los mensajes de correo electrónico intercambiados, es preciso codificar y firmar dichos mensajes. Para poder utilizar conjuntamente estas dos opciones, cada usuario tiene que poseer su propio certificado de usuario.

Procedimiento de obtención de certificado

Los pasos para conseguir el certificado de usuario para usos de correo electrónico seguro se describen en las páginas web de la FNMT. Se encuentran a su disposición en

http://www.cert.fnmt.es/index.php?cha=cit&sec=obtain_cert.

En el apartado “Obtener certificado”, puede ver información relativa a cómo instalarse el certificado en su navegador.

Utilización de los certificados con distintos programas de correo electrónico

Para poder utilizar los programas de correo electrónico para envío y recepción de correo electrónico seguro, es necesario incorporar al cliente de correo los certificados o identificadores digitales de las personas con las que se intercambia correo. Esta acción se realiza de diferente forma según el programa que se utilice:

Ejemplo Mozilla Thunderbird

Al recibir mensajes firmados de sus contactos, los certificados digitales se incorporan automáticamente al programa. Para comprobar su validez, hay que ir a:

Herramientas →Preferencias→“Avanzadas”-> sección de “Certificados”

botón de “Administrar certificados” del apartado “Administrar certificados” y pestaña “De otras personas”.

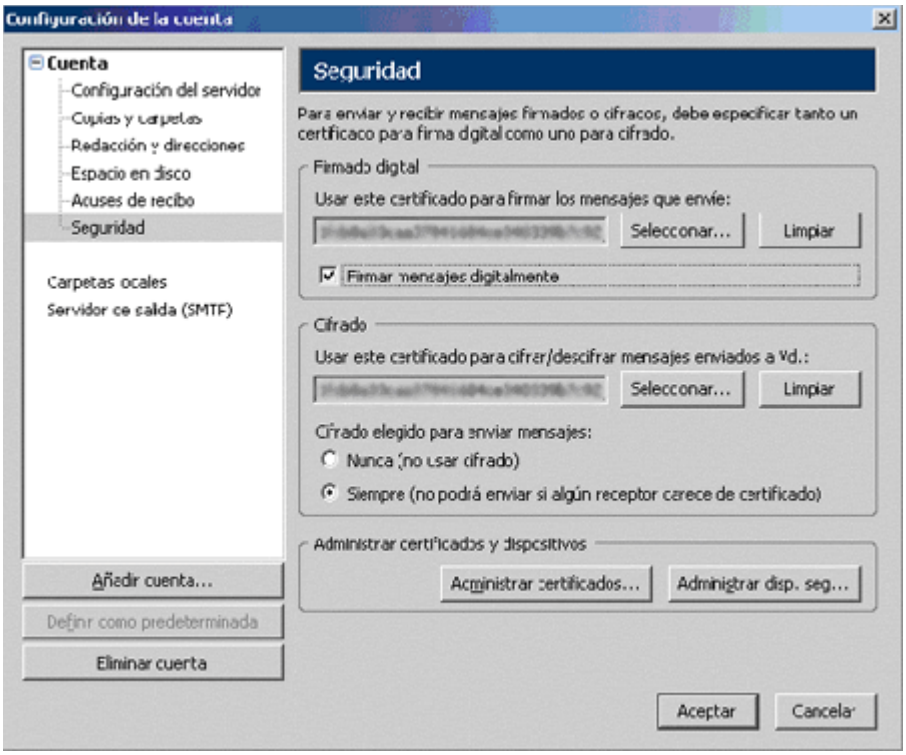
Si el certificado es válido, aparecerá en la ventana indicando que la validación se efectuó correctamente.

Con los identificadores digitales de otros usuarios ya incorporados, el programa puede comprobar la firma de los mensajes recibidos por estos usuarios y enviarles mensajes cifrados con su clave pública, que posteriormente ellos podrán descodificar con su clave privada.

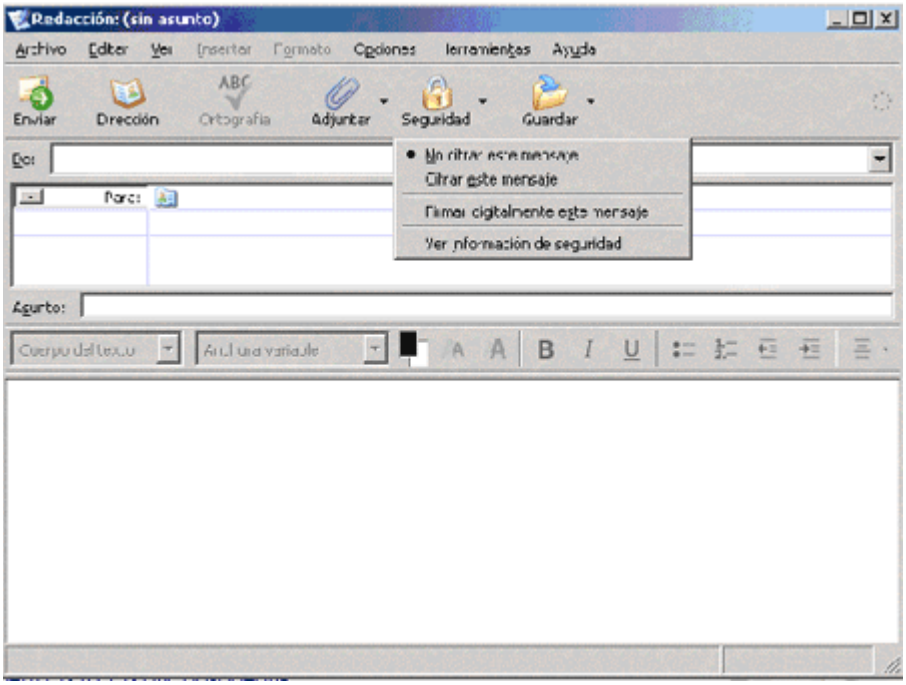
Para poder trabajar con nuestro certificado digital es necesario, en el programa de correo, ir a:

Herramientas->Configuración de cuentas.

Escoger la cuenta en la que se quiera utilizar el certificado digital e ir a la opción de “Seguridad”. En la nueva ventana, escoger si se quiere firmar los mensajes, cifrarlos o ambas cosas y seleccionar el certificado que se desea utilizar.

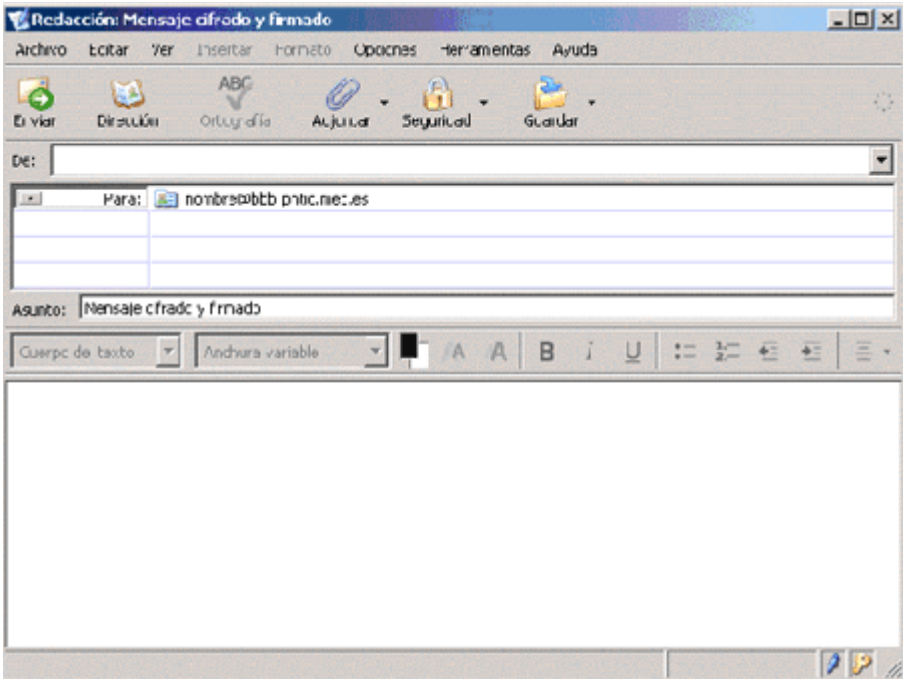


Para poder mandar un mensaje cifrado y/o firmado hay que estar en el modo de componer un mensaje nuevo y pulsar en el icono de “Seguridad” del menú superior.



Este icono da acceso a la ventana de seguridad dentro de la cual se podrá escoger las opciones de firmar, cifrar o ambas para la dirección de correo electrónico especificada en el campo de destinatario del mensaje. Solamente se podrá activar la opción de cifrar el mensaje para las direcciones de correo electrónico cuyo certificado digital se haya verificado de forma válida.

Si el mensaje se envía firmado y/o codificado, en la esquina inferior derecha del mensaje aparecerán dos iconos, el dibujo de la estilográfica indica que el mensaje se envía firmado, mientras que el icono de la llave muestra que el mensaje se está enviando codificado.

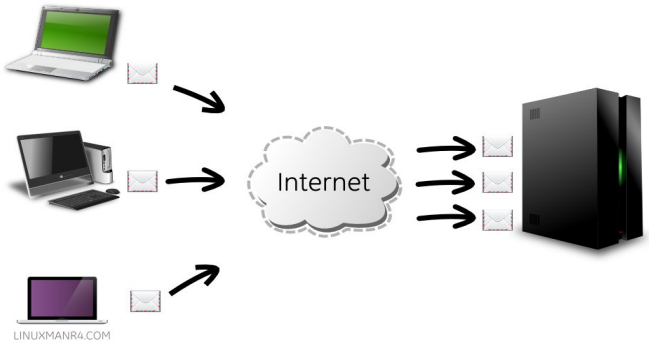


Cuando el destinatario recibe un correo firmado y/o cifrado le aparecerán unos iconos cerca de la esquina superior derecha del encabezado que muestran que la información se envió cifrada y firmada.

Los iconos son los siguientes para el firmado  y para el cifrado  .

Reenvío de correo.

Envío tradicional de correo electrónico

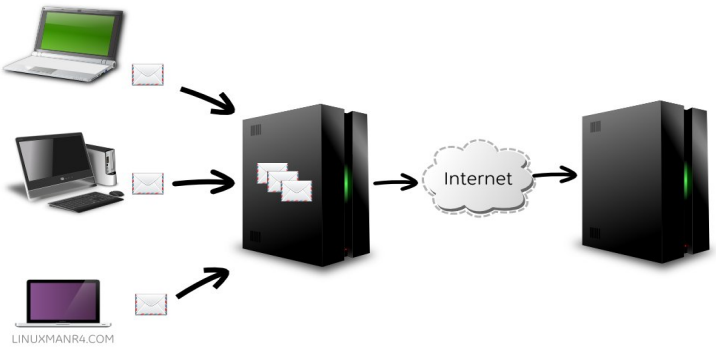


Este es el envío tradicional, cada cliente tiene configurado el servidor de correo de nuestro proveedor y por lo tanto cada usuario tiene su propio nombre de usuario y contraseña para poder enviar correo electrónico.

Si el tamaño de los adjuntos a enviar es considerable, entonces se puede tardar unos segundos (o minutos) extras hasta que da el mensaje de **enviado con éxito**. Si en esos momentos la conexión a Internet es inestable entonces dará uno o varios errores hasta que se complete el envío.

Envío con Relay

En este caso un servidor interno funciona como intermediario, podemos pensar en él como el mensajero de la oficina, le entregamos el correo y se encarga de hacer los trámites necesarios para que llegue a su destino.



Todos los correos llegan a este servidor y él se encarga de formarlos en una fila y entregarlos al servidor de correo de nuestro proveedor.
La ventaja es que solo tenemos que configurar una cuenta de correo electrónico con su nombre de usuario y contraseña para que la use el servidor que funciona como **Relay**, la configuración de los clientes de correo no necesitan estas credenciales.

Además la entrega de los clientes es prácticamente inmediata, a la velocidad de la red local, lo que da la sensación de un envío inmediato.

¿Porqué no configurar Postfix para que entregue el correo directamente?, es posible hacerlo y tampoco es complicado, el problema son las validaciones y comprobaciones que se tienen que hacer para que no se clasifique un correo como **spam**.

En la actualidad los correos que salen de un servidor de correo incluyen varios mecanismos para confirmar que son de una fuente confiable y eso si es mucho más complicado de hacer (pero no imposible).

Configurando Postfix con reenvío de correo.

Antes de comenzar hemos de crear una cuenta de correo con el proveedor que les esta proporcionando el servicio, el nombre de usuario y contraseña es la que va a utilizar el servidor con relay. Usaremos **relay@midominio.com** como ejemplo.

Para hacer los ajustes necesarios se tiene que modificar el archivo **/etc/postfix/main.cf** , este ejemplo puede servir de guía.

Archivo /etc/postfix/main.cf

mydestination =

1.
2. myhostname = midominio.com
3. mydomain = midominio.com
4.
5. #Opciones de seguridad
6. relayhost = [mail.midominio.com]:587
7. smtp_sasl_auth_enable = yes
8. smtp_sasl_password_maps = hash:/etc/postfix/smtp_pass

```
9. smtp_sasl_security_options =
10.
11.#Redes validas
12.#En este caso, localhost y toda la red local.
13.mynetworks = 127.0.0.0/8, 192.168.10.0/24
14.inet_interfaces = all

15.#Tamaño máximo del mensaje 20MB aprox.
16.message_size_limit = 27262976
```

Notamos que en la línea que dice **relayhost** el dominio está entre corchetes y además se especifica el puerto utilizado (en este caso 587).

Se hace referencia a un archivo llamado **smtp_pass** en la línea que dice **smtp_sasl_password_maps** en ese archivo se almacena el nombre de usuario y contraseña que vamos a usar para mandar los correos y es muy similar a este ejemplo:

Archivo /etc/postfix/smtp_pass

[mail.midominio.com]:587 relay@midominio.com:contraseña

Revisamos que el servidor de correo esté entre corchetes y el número de puerto. Debe de ser idéntico a como se especificó en relayhost. Como podemos ver lo que sigue es la cuenta de usuario y la contraseña.

Para que Postfix pueda usar esta información hay que preparar un archivo especial con esta instrucción…

```
postmap /etc/postfix/smtp_pass
```

Para aplicar los cambios reiniciar el servicio, en Debian es así:

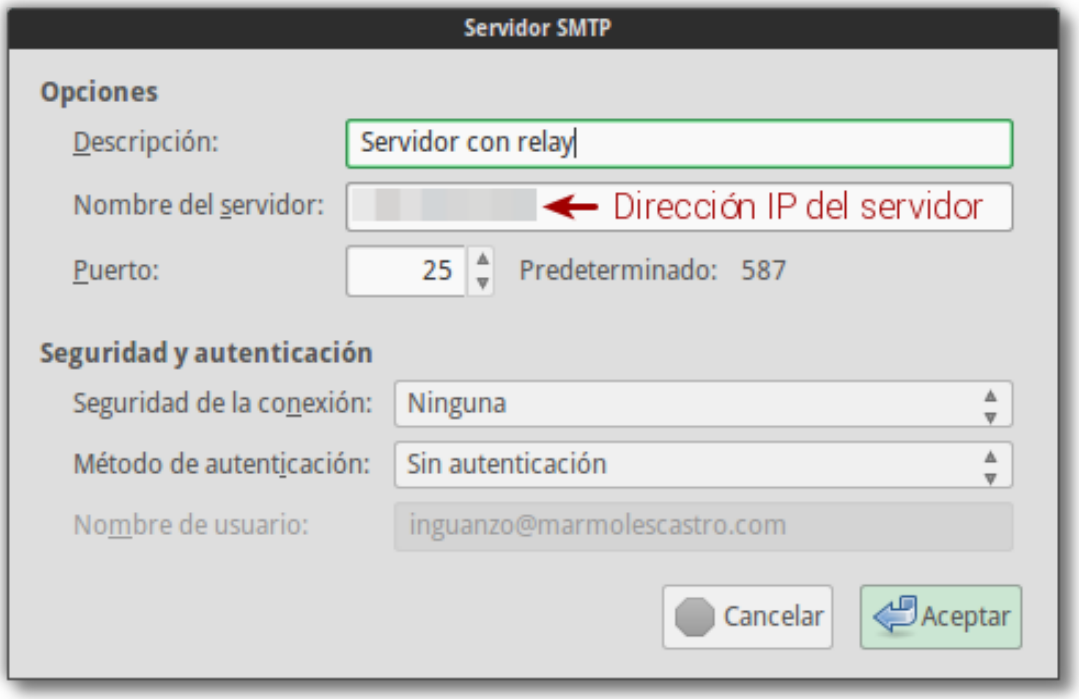
```
sudo /etc/init.d/postfix restart
```

y se verán estos mensajes.

```
Stopping Postfix Mail Transport Agent: postfix.
Starting Postfix Mail Transport Agent: postfix.
```

Para realizar las pruebas solo resta configurar un cliente de correo electrónico, en Thunderbird en el menú Preferencias – Configuración de cuentas…

Y se agrega la información de nuestro nuevo servidor.



Por default Postfix utiliza el puerto **25** y no requiere identificación alguna.
Si todo salió bien, dentro de pocos instantes debes ver que llegó correctamente el correo electrónico a tu bandeja de entrada.

Técnicas para evitar correo no deseado. Filtros.

Cómo evitar el "spam"

Los usuarios de Internet están expuestos a frecuentes ataques de "spam" (o mensajes de correo electrónico no deseados o "correos basura"). Por eso, es necesario estar preparados y aprender a enfrentarlos.

Estas son algunas **recomendaciones** para evitar la proliferación de "spam":

• *No responda los mensajes electrónicos sospechosos*. Una contestación confirma la exactitud de su

dirección y, como resultado, recibirá más mensajes que llenen su buzón de correo.

• *Si recibe mensajes que le ordenen pulsar sobre un enlace para sacar su dirección de una lista y, supuestamente, no volver a recibirlos, no lo haga*. Muchos "spammers" -personas u organizaciones que generan "spam"- usan a menudo este método como una táctica para confirmar la dirección del destinatario y así producirle más mensajes de correo indeseado.

• *Nunca dé los datos de su tarjeta de crédito u otra información personal a sitios no fiables en la red*.

• *Evite rellenar formularios en sitios web*, incluso seguros, que declaren que venderán la información a terceros.

• *Use software de filtrado* o un bloqueador de "spam".

• *No envíe su dirección de correo electrónico a través de las salas de conversación, sistemas de mensajería instantánea, tablones de anuncios o grupos de noticias*.

• *No ponga su dirección de correo electrónico principal en registros en línea o en sitios de comercio electrónico*. Use una dirección diferente para la difusión pública.

• *Escoja una dirección de correo electrónico poco común*. Algunos "spammers" usan programas que producen aleatoriamente millones de direcciones potenciales. Estos programas vinculan diferentes combinaciones o palabras a los nombres del dominio de proveedores grandes, como Hotmail, para alcanzar el máximo número de posibles cuentas del correo electrónico activas.

• *Nunca escriba su dirección electrónica en una página web para que le manden mensajes*. Muchas empresas de "spam", recopilan direcciones de las páginas web. Si es imprescindible que escriba su dirección, cambie algunos caracteres o añada caracteres nuevos, por ejemplo: *nombre*-arroba-*dominio* (arroba escrito con palabras).

Protocolos y servicios de descarga de correo.

POP3 e IMAP desarrollados en el apartado Protocolos de transferencia de mensajes.

Diagnóstico y resolución de incidencias en el servicio.

El principal problema actual es el ***correo no deseado***, que se refiere a la recepción de correos no solicitados, normalmente de publicidad engañosa, y en grandes cantidades, promoviendo *pornografía* y otros productos y servicios de calidad sospechosa.
Usualmente los mensajes indican como remitente del correo una dirección falsa. Por esta razón, es más difícil localizar a los verdaderos remitentes, y no sirve de nada contestar a los mensajes de correo no deseado: las respuestas serán recibidas por usuarios que nada tienen que ver con ellos. Por ahora, el servicio de correo electrónico no puede identificar los mensajes de forma que se pueda discriminar la verdadera dirección de correo electrónico del remitente, de una falsa. Esta situación que puede resultar chocante en un primer momento, es semejante por ejemplo a la que ocurre con el correo postal ordinario: nada impide poner en una carta o postal una dirección de remitente aleatoria: el correo llegará en cualquier caso. No obstante, hay tecnologías desarrolladas en esta dirección: por ejemplo el remitente puede firmar sus mensajes mediante criptografía de clave pública.

Además del *correo no deseado*, existen otros problemas que afectan a la seguridad y veracidad de este medio de comunicación:

- los **virus informáticos**, que se propagan mediante ficheros adjuntos infectando el ordenador de quien los abre
- la **suplantación de identidad**, que es correo fraudulento que generalmente intenta conseguir información bancaria
- los **bulos** (bromas, burlas, o hoax), que difunden noticias falsas masivamente
- las **cadenas de correo electrónico**, que consisten en reenviar un mensaje a mucha gente; aunque parece inofensivo, la publicación de listas de direcciones de correo contribuye a la propagación a gran escala del *correo no deseado* y de mensajes con virus, *suplantadores de identidad* y *engaños*.

Pérdida progresiva de la privacidad

En 2014 los principales proveedores de correo web como Google, Hotmail o Yahoo exigen como requisito proveer datos personales como un **número de teléfono obligatorio** o una dirección de correo alternativa obligatoria para así impedir las altas anónimas o de personas que no puedan tener acceso a la compra de un teléfono móvil.