# Servidores de correo

Capítulo destinado a configuraciones específicas para mitigar/solucionar vulnerabilidades, errores de configuración en servidores de correo.

- Deshabilitar Open Relay interno y externo en Postfix

# Deshabilitar Open Relay interno y externo en Postfix

Guía para evitar que personas no autorizadas envíen correos electrónicos a nombre del dominio de una entidad.

Esta solución es para postfix con autenticación mediante dovecot.

En caso de no tener instalado dovecot procedemos a su instalación:

```
apt install dovecot-core dovecot-imapd
```

Instalamos el plugin pcre de postfix:

```
apt install postfix-pcre
```

Configuramos el archivo /etc/postfix/main.cf de la siguiente manera:

```
# See /usr/share/postfix/main.cf.dist for a commented, more complete version



# Debian specific:  Specifying a file name will cause the first
# line of that file to be used as the name.  The Debian default
# is /etc/mailname.
#myorigin = /etc/mailname

smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)
biff = no

# appending .domain is the MUA's job.
append_dot_mydomain = no

# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h
```

```
readme_directory = no

# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
smtpd_tls_auth_only = yes


## SASL implementation
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_tls_security_options = $smtpd_sasl_security_options


# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
# information on enabling SSL in the smtp client.

myhostname = dominio.gob.bo
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = $myhostname, localhost.dominio.gob.bo, localhost, dominio.gob.bo
relayhost =
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 [IP servidor de correo]


disable_vrfy_command = yes
```

```
# Restricciones


smtpd_helo_required = yes
smtpd_sender_login_maps = pcre:/etc/postfix/controlled_envelope_senders.pcre
smtpd_client_restrictions = permit_mynetworks, reject_unknown_client_hostname,
reject_unknown_reverse_client_hostname, permit
smtpd_recipient_restrictions = permit_mynetworks, permit_sasl_authenticated
,reject_unauth_destination,reject_unknown_sender_domain, reject_sender_login_mismatch, permit
```

Los parámetros a considerar son los siguientes:

- **smtpd_sasl_auth_enable = yes** : Habilitar la autenticación SASL en postfix.
- **smtpd_sasl_type = dovecot** : utilizar dovecot para la autenticación SASL.
- **myhostname = dominio.gob.bo** : Declaran los dominios a los que se autorizará mandar mensajes a través del servidor de correo.
- **mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 [IP servidor de correo]** : Configurar la lista de direcciones IPs que pueden mandar correos. (Típicamente solo la IP interna del servidor de correo).
- **smtpd_helo_required = yes** : Exige que un cliente SMTP remoto se presente con el comando HELO o EHLO antes de enviar el comando MAIL u otros comandos que requieran negociación EHLO.
- **smtpd_sender_login_maps = pcre:/etc/postfix/controlled_envelope_senders.pcre** : Filtro de búsqueda opcional con el dominio de inicio de sesión SASL que poseen las direcciones del remitente (MAIL FROM).
- **smtpd_client_restrictions** : Restricciones de cliente
  - permit_mynetworks .- Permite el envío de correo a clientes que coincidan con las direcciones descritas en mynetworks.
  - reject_unknown_client_hostname .- Hace una comparación con la IP y nombre del cliente para verificar que coincidan, en caso de no coincidir rechaza la solicitud.
  - reject_unknown_reverse_client_hostname .- Rechaza la solicitud cuando la dirección IP del cliente no tiene asignación de dirección-> nombre.
  - permit : Permitir en caso de no ser rechazado en sentencias anteriores.
- smtpd_recipient_restrictions: Restricciones del recipiente (RCPT)
  - permit_mynetworks .- Permite la solicitud a clientes que coincidan con las direcciones descritas en mynetworks.
  - permit_sasl_authenticated .- Permite la solicitud cuando el cliente se haya autenticado correctamente a través del protocolo RFC 4954 (AUTH).
  - reject_unauth_destination .- Rechaza la solicitud si el que envía no es un retransmisor permitido, ó si el receptor del mensaje no es un destino válido.
  - reject_unknown_sender_domain .- Rechaza la solicitud cuando Postfix no es el destino final para la dirección del remitente y el dominio MAIL FROM tiene 1) ningún registro DNS MX ni DNS A, o 2) un registro MX con formato incorrecto, como un registro con un

nombre de host MX de longitud cero.
- reject_sender_login_mismatch .- Rechaza la solicitud cuando $ smtpd_sender_login_maps especifica un propietario para la dirección MAIL FROM, pero el cliente no está (SASL) conectado como propietario de la dirección MAIL FROM.
- permit .- Permitir en caso de no ser rechazado en sentencias anteriores.

Adicionalmente es necesario añadir el archivo controlled_envelope_senders.pcre en la dirección establecida, en este caso /etc/postfix/:

```
 #envelop sender       owners (SASL login names)
/^(.*)@dominio\.gob\.bo$/   ${1}
```

Por último es necesario hacer una configuración en dovecot:

Para versiones de dovecot que corresponden a postfix 2.7 se edita el archivo /etc/dovecot/dovecot.conf:

```
client {
    # The client socket is generally safe to export to everyone. Typical use
    # is to export it to your SMTP server so it can do SMTP AUTH lookups
    # using it.
    #path = /var/run/dovecot/auth-client
    path = /var/spool/postfix/private/auth
    mode = 0660
    user = postfix
    group = postfix
  }
```

Para versiones posteriores se edita el archivo /etc/dovecot/conf.d/10-master.conf:

```
service auth {
  # auth_socket_path points to this userdb socket by default. It's typically
  # used by dovecot-lda, doveadm, possibly imap process, etc. Its default
  # permissions make it readable only by root, but you may need to relax these
  # permissions. Users that have access to this socket are able to get a list
  # of all usernames and get results of everyone's userdb lookups.
  unix_listener auth-userdb {
    #mode = 0600
    #user =
    #group =
```

```
}

# Postfix smtp-auth
unix_listener /var/spool/postfix/private/auth {
  mode = 0660
  user = postfix
  group = postfix
}
```