

CONFIGURACION DE SERVIDOR DE CORREO SEGURO BAJO SSL

Crear el certificado para la página web antes de eso crear la carpeta localcerts dentro de ssl

```
root@debian-serv:/etc/ssl/localcerts# openssl req -x509 -nodes -days 3000 -newkey rsa:1024 -out /etc/ssl/localcerts/mail.crt -keyout /etc/ssl/localcerts/mail.key
```

Añadimos la ruta en el fichero /etc/postfix/main.cf

```
GNU nano 2.2.6 Fichero: /etc/postfix/main.cf Modificado

# 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/localcerts/mail.crt
smtpd_tls_key_file=/etc/ssl/localcerts/mail.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

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

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_un$
myhostname = debian-serv.local

^G Ver ayuda ^O Guardar ^R Leer Fich ^Y Pág Ant ^K CortarTxt ^C Pos actual
^X Salir ^J Justificar ^W Buscar ^V Pág Sig ^U PegarTxt ^T Ortografía
```

En el fichero master modificamos las siguientes líneas (descomentamos)

```
smtps inet n - - - smtpd
-o syslog_name=postfix/smtps
-o smtpd_tls_wrappermode=yes
-o smtpd_sasl_auth_enable=yes
-o smtpd_client_restrictions=permit_sasl_authenticated,reject
-o milter_macro_daemon_name=ORIGINATING
```

```
GNU nano 2.2.6 Fichero: /etc/postfix/master.cf

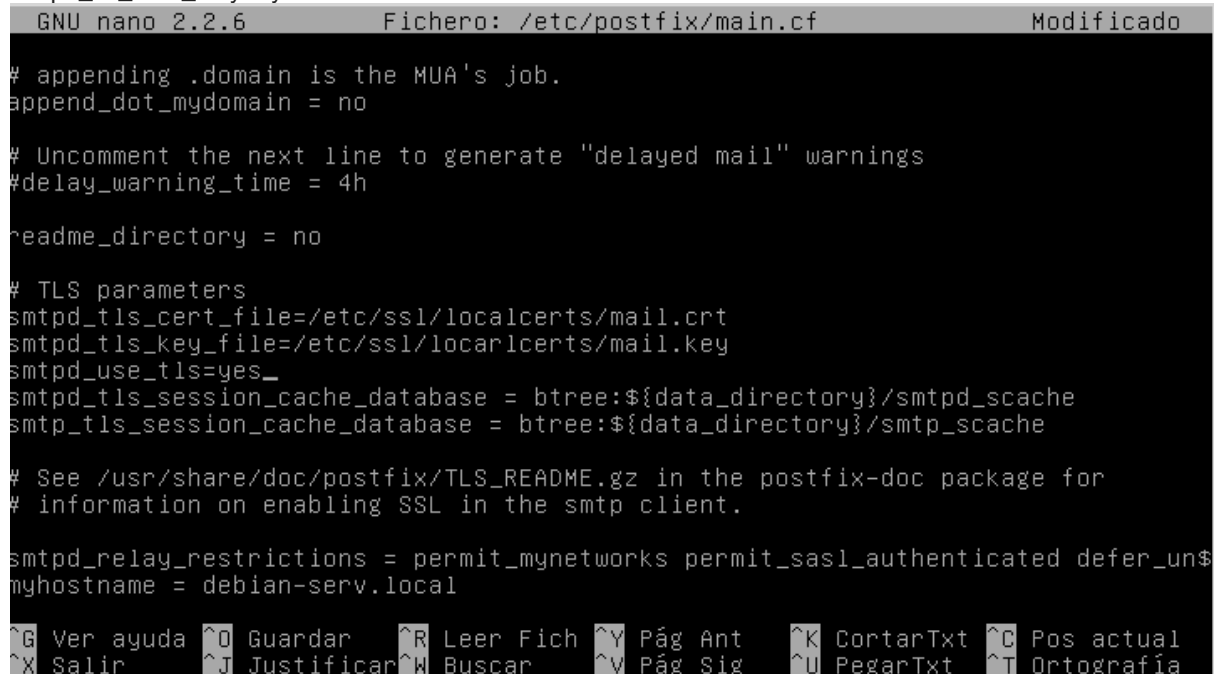
# -o smtpd_helo_restrictions=$mua_helo_restrictions
# -o smtpd_sender_restrictions=$mua_sender_restrictions
# -o smtpd_recipient_restrictions=
# -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
# -o milter_macro_daemon_name=ORIGINATING
smtps      inet  n       -       -       -       -       smtpd
  -o syslog_name=postfix/smtps
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
# -o smtpd_reject_unlisted_recipient=no
# -o smtpd_client_restrictions=permit_sasl_authenticated, reject
# -o smtpd_helo_restrictions=$mua_helo_restrictions
# -o smtpd_sender_restrictions=$mua_sender_restrictions
# -o smtpd_recipient_restrictions=
# -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
# -o milter_macro_daemon_name=ORIGINATING
#628      inet  n       -       -       -       -       qmqpd
pickup     unix  n       -       -       60      1       pickup
cleanup    unix  n       -       -       -       0       cleanup
qmgr        unix  n       -       n       300     1       qmgr

[ 127 líneas escritas ]
^G Ver ayuda ^O Guardar ^R Leer Fich ^Y Pág Ant ^K CortarTxt ^C Pos actual
^X Salir ^J Justificar ^W Buscar ^V Pág Sig ^U PegarTxt ^T Ortografía
```

CONFIGURACION DE SERVIDOR DE CORREO SEGURO BAJO SSL

Modificamos en el fichero `/etc/postfix/main.cf` la ruta del certificado y las siguientes líneas

```
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_auth_enable = yes
smtpd_tls_auth_only = yes
```



```
GNU nano 2.2.6          Fichero: /etc/postfix/main.cf          Modificado

# 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/localcerts/mail.crt
smtpd_tls_key_file=/etc/ssl/localcerts/mail.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

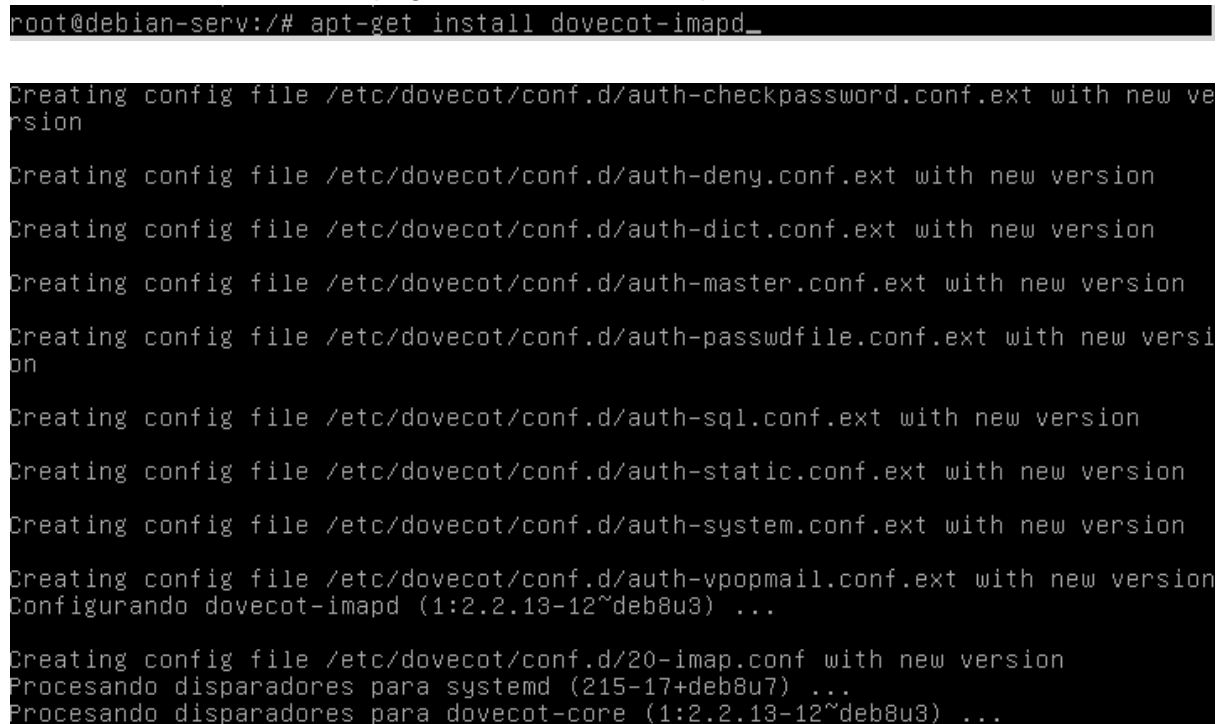
# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
# information on enabling SSL in the smtp client.

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_un$
myhostname = debian-serv.local

^G Ver ayuda  ^O Guardar   ^R Leer Fich ^Y Pág Ant   ^K CortarTxt ^C Pos actual
^X Salir      ^J Justificar^W Buscar    ^V Pág Sig   ^U PegarTxt  ^T Ortografía
```

Instalamos el dovecot con `apt-get install dovecot-imapd`

```
root@debian-serv:/# apt-get install dovecot-imapd_
```



```
Creating config file /etc/dovecot/conf.d/auth-checkpassword.conf.ext with new ve
rsion
Creating config file /etc/dovecot/conf.d/auth-deny.conf.ext with new version
Creating config file /etc/dovecot/conf.d/auth-dict.conf.ext with new version
Creating config file /etc/dovecot/conf.d/auth-master.conf.ext with new version
Creating config file /etc/dovecot/conf.d/auth-passwdfile.conf.ext with new versi
on
Creating config file /etc/dovecot/conf.d/auth-sql.conf.ext with new version
Creating config file /etc/dovecot/conf.d/auth-static.conf.ext with new version
Creating config file /etc/dovecot/conf.d/auth-system.conf.ext with new version
Creating config file /etc/dovecot/conf.d/auth-vpopmail.conf.ext with new version
Configurando dovecot-imapd (1:2.2.13-12~deb8u3) ...
Creating config file /etc/dovecot/conf.d/20-imap.conf with new version
Procesando disparadores para systemd (2:15-17+deb8u7) ...
Procesando disparadores para dovecot-core (1:2.2.13-12~deb8u3) ...
```

CONFIGURACION DE SERVIDOR DE CORREO SEGURO BAJO SSL

Modificamos el fichero 10-ssl.conf con el ssl=yes y la ruta de los certificados creados anteriormente

```
root@debian-serv:/etc/dovecot/conf.d# pwd
/etc/dovecot/conf.d

GNU nano 2.2.6 Fichero: 10-ssl.conf Modificado
##
## SSL settings
##
# SSL/TLS support: yes, no, required. <doc/wiki/SSL.txt>
ssl = yes

# PEM encoded X.509 SSL/TLS certificate and private key. They're opened before
# dropping root privileges, so keep the key file unreadable by anyone but
# root. Included doc/mkcert.sh can be used to easily generate self-signed
# certificate, just make sure to update the domains in dovecot-openssl.cnf
ssl_cert = </etc/ssl/localcerts/mail.crl
ssl_key = </etc/ssl/localcerts/mail.key

# If key file is password protected, give the password here. Alternatively
# give it when starting dovecot with -p parameter. Since this file is often
# world-readable, you may want to place this setting instead to a different
# root owned 0600 file by using ssl_key_password = <path>.
#ssl_key_password =

^G Ver ayuda ^O Guardar ^R Leer Fich ^Y Pág Ant ^K CortarTxt ^C Pos actual
^X Salir ^J Justificar ^W Buscar ^V Pág Sig ^U PegarTxt ^T Ortografía
```

En este paso modificamos el master y descomentamos el inet_listener

```
GNU nano 2.2.6 Fichero: 10-master.conf Modificado

# Internal user is used by unprivileged processes. It should be separate from
# login user, so that login processes can't disturb other processes.
#default_internal_user = dovecot

service imap-login {
  inet_listener imap {
    #port = 143
  }
  inet_listener imaps {
    port = 993
    ssl = yes
  }

  # Number of connections to handle before starting a new process. Typically
  # the only useful values are 0 (unlimited) or 1. 1 is more secure, but 0
  # is faster. <doc/wiki/LoginProcess.txt>
  #service_count = 1

  # Number of processes to always keep waiting for more connections.

^G Ver ayuda ^O Guardar ^R Leer Fich ^Y Pág Ant ^K CortarTxt ^C Pos actual
^X Salir ^J Justificar ^W Buscar ^V Pág Sig ^U PegarTxt ^T Ortografía
```

CONFIGURACION DE SERVIDOR DE CORREO SEGURO BAJO SSL

En el mismo fichero añadimos en el apartado `unix_listener` `user=postfix` y `group=postfix`

```
GNU nano 2.2.6          Fichero: 10-master.conf          Modificado

unix_listener auth-userdb {
    #mode = 0666
    #user =
    #group =
}

# Postfix smtp-auth
unix_listener /var/spool/postfix/private/auth {
    mode = 0666
    user = postfix
    group = postfix_
}

# Auth process is run as this user.
#user = $default_internal_user
}

service auth-worker {
    # Auth worker process is run as root by default, so that it can access
    # /etc/shadow. If this isn't necessary, the user should be changed to
    user = postfix
}
```

Editamos otro fichero distinto, el `10-auth.conf` y añadimos la línea `disable_plaintext_auth = yes`

```
GNU nano 2.2.6          Fichero: 10-auth.conf          Modificado

##_
## Authentication processes
##

# Disable LOGIN command and all other plaintext authentications unless
# SSL/TLS is used (LOGINDISABLED capability). Note that if the remote IP
# matches the local IP (ie. you're connecting from the same computer), the
# connection is considered secure and plaintext authentication is allowed.
# See also ssl=required setting.
disable_plaintext_auth = yes

# Authentication cache size (e.g. 10M). 0 means it's disabled. Note that
# bsdauth, PAM and vpopmail require cache_key to be set for caching to be used.
#auth_cache_size = 0
# Time to live for cached data. After TTL expires the cached record is no
# longer used, *except* if the main database lookup returns internal failure.
# We also try to handle password changes automatically: If user's previous
# authentication was successful, but this one wasn't, the cache isn't used.
# For now this works only with plaintext authentication.
#auth_cache_ttl = 1 hour
```

CONFIGURACION DE SERVIDOR DE CORREO SEGURO BAJO SSL

También modificamos el `auth_mechanisms = plain login`

```
GNU nano 2.2.6          Fichero: 10-auth.conf          Modificado
#auth_ssl_require_client_cert = no

# Take the username from client's SSL certificate, using
# X509_NAME_get_text_by_NID() which returns the subject's DN's
# CommonName.
#auth_ssl_username_from_cert = no

# Space separated list of wanted authentication mechanisms:
#   plain login digest-md5 cram-md5 ntlm rpa apop anonymous gssapi otp skey
#   gss-spnego
# NOTE: See also disable_plaintext_auth setting.
auth_mechanisms = plain login _

##
## Password and user databases
##

#
# Password database is used to verify user's password (and nothing more).
# You can have multiple passdbs and userdbs. This is useful if you want to

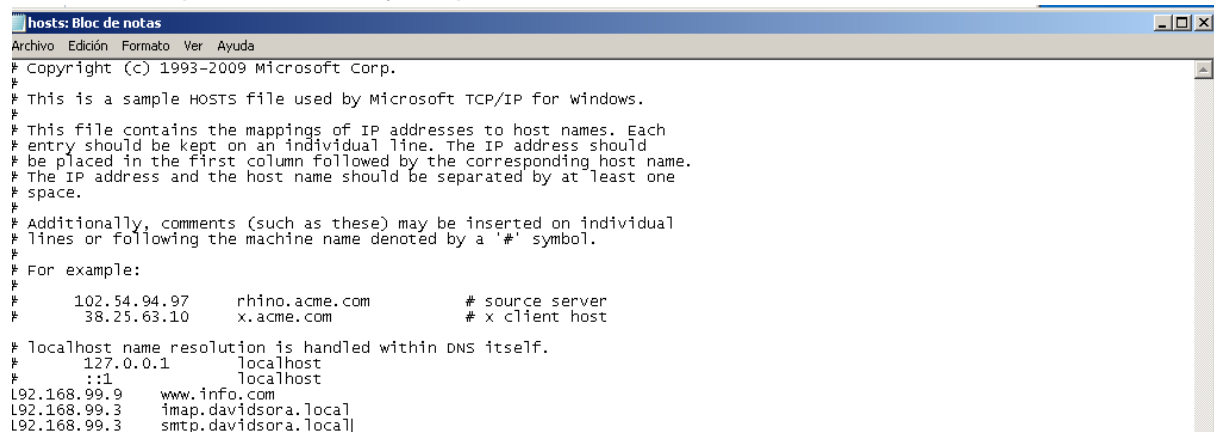
^G Ver ayuda ^O Guardar ^R Leer Fich ^Y Pág Ant ^K CortarTxt ^C Pos actual
^X Salir ^J Justificar ^W Buscar ^V Pág Sig ^U PegarTxt ^T Ortografía
```

Reiniciamos los servicios.

```
root@debian-serv:/etc/dovecot/conf.d# service postfix restart
^C
root@debian-serv:/etc/dovecot/conf.d# /etc/init.d/postfix restart
[ ok ] Restarting postfix (via systemctl): postfix.service.
root@debian-serv:/etc/dovecot/conf.d# /etc/init.d/dovecot restart
[ ok ] Restarting dovecot (via systemctl): dovecot.service.
root@debian-serv:/etc/dovecot/conf.d# tail /var/log/syslog
Oct 24 22:18:47 debian-serv systemd[1]: Started LSB: Postfix Mail Transport Agent.
Oct 24 22:18:47 debian-serv systemd[1]: Starting Mail Transport Agent.
Oct 24 22:18:47 debian-serv systemd[1]: Reached target Mail Transport Agent.
Oct 24 22:18:56 debian-serv systemd[1]: Stopping Dovecot IMAP/POP3 email server.
..
Oct 24 22:18:56 debian-serv dovecot: master: Warning: Killed with signal 15 (by pid=1 uid=0 code=kill)
Oct 24 22:18:56 debian-serv dovecot: anvil: Warning: Killed with signal 15 (by pid=1 uid=0 code=kill)
Oct 24 22:18:56 debian-serv dovecot: log: Warning: Killed with signal 15 (by pid=1 uid=0 code=kill)
Oct 24 22:18:56 debian-serv systemd[1]: Starting Dovecot IMAP/POP3 email server.
..
Oct 24 22:18:56 debian-serv systemd[1]: Started Dovecot IMAP/POP3 email server.
Oct 24 22:18:56 debian-serv dovecot: master: Dovecot v2.2.13 starting up for imap (core dumps disabled)
root@debian-serv:/etc/dovecot/conf.d# tail /var/log/syslog _
```

CONFIGURACION DE SERVIDOR DE CORREO SEGURO BAJO SSL

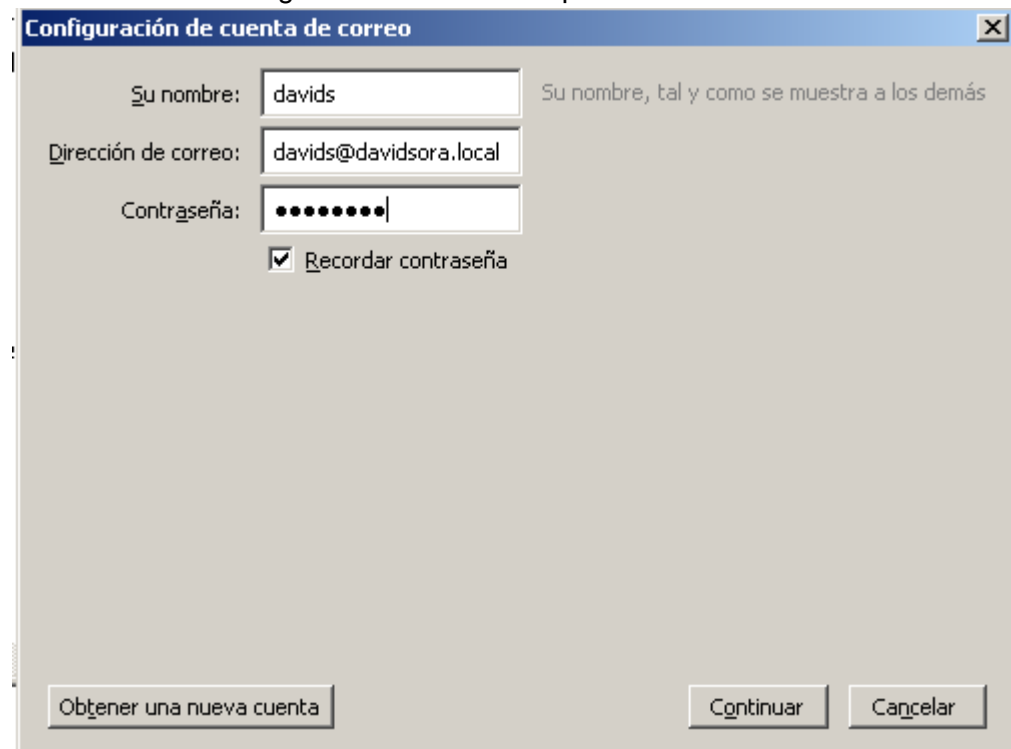
Ahora en el cliente modificamos el fichero hosts ambos con la IP del servidor y distintos nombres imap.dominio.local y smtp.dominio.local



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com   # source server
#       38.25.63.10       x.acme.com      # x client host

# localhost name resolution is handled within DNS itself.
#
#       127.0.0.1         localhost
#       ::1              localhost
192.168.99.9       www.info.com
192.168.99.3       imap.davidsora.local
192.168.99.3       smtp.davidsora.local
```

Por ultimo falta configurar el Thunderbird que será nuestro cliente de correo electronico.



Configuración de cuenta de correo

Su nombre: Su nombre, tal y como se muestra a los demás

Dirección de correo:

Contraseña:

☒ Recordar contraseña

CONFIGURACION DE SERVIDOR DE CORREO SEGURO BAJO SSL

Configuramos en modo avanzado asignando los puertos que vamos a utilizar y la configuración como en la captura.

Configuración de cuenta de correo

Su nombre: Su nombre, tal y como se muestra a los demás

Dirección de correo:

Contraseña:

☒ Recordar contraseña

	Nombre del servidor	Puerto	SSL	Identificación	
Entrante:	IMAP	imap.davidsora.local	993	SSL/TLS	Contraseña normal
Saliente:	SMTP	smtp.davidsora.local	25	STARTTLS	Sin identificación

Nombre de usuario: Entrante:

Obtener una nueva cuenta Config. avanzada Volver a probar Hecho Cancelar

Y finalizamos la configuración del cliente de correo aceptando el certificado auto-firmado por el servidor.

Thunderbird Correo - Carpetas locales

Añadir excepción de seguridad

Está a punto de alterar cómo identifica Thunderbird este sitio. Los bancos, tiendas y otros sitios públicos legítimos no le pedirán hacer esto.

Servidor:

Estado del certificado

Este sitio intenta identificarse a sí mismo con información no válida.

Sitio erróneo

El certificado pertenece a un sitio diferente, lo que podría significar que alguien está intentando hacer pasar por este sitio.

Identidad desconocida

No se confía en el certificado porque no ha sido verificado como emitido por una autoridad confiable usando una firma segura.

☒ Guardar esta excepción de manera permanente