

## Tema3\_P11\_https

### Enunciado:

Vamos a crear un sitio seguro https llamada *wp11.2asir.net* a la que vamos a acceder mediante <https://wp11.2asir.net>.

### Teoría:

https usa el puerto 443 por defecto

### Proceso:

1. Vemos si tenemos instalado el paquete openssl :

```
root@profesor:/home/usuario# dpkg -l | grep openssl
ii  openssl                    1.0.1e-2                i386
    Secure Socket Layer (SSL) binary and related cryptographic tools
root@profesor:/home/usuario#
```

Como vemos, lo tenemos instalado

2. Añadimos el módulo en apache

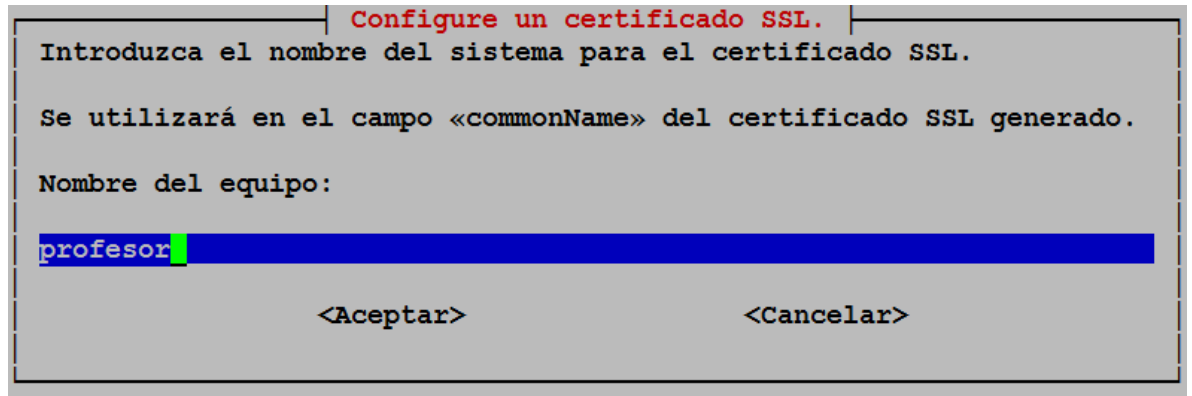
```
authn_anon.load      dav_lock.load      mem_cache.conf      spelling.load
authn_dbd.load       dbd.load           mem_cache.load      ssl.conf
authn_dbm.load       deflate.conf       mime.conf           ssl.load
authn_default.load   deflate.load       mime.load           status.conf
authn_file.load      dir.conf           mime_magic.conf     status.load
authnz_ldap.load     dir.load           mime_magic.load     substitute.load
authnz_dbm.load      disk_cache.conf   negotiation.conf    suexec.load
authnz_default.load  disk_cache.load   negotiation.load    unique_id.load
authnz_groupfile.load dump_io.load       proxy_ajp.load      userdir.conf
authnz_host.load     env.load          proxy_balancer.conf userdir.load
authnz_owner.load    expires.load      proxy_balancer.load usertrack.load
authnz_user.load     ext_filter.load   proxy.conf          vhost_alias.load
autoindex.conf       file_cache.load   proxy_connect.load
autoindex.load       filter.load       proxy_ftp.load
cache.load           headers.load      proxy_ftp.load
root@profesor:/etc/apache2/mods-available# a2enmod ssl
Enabling module ssl.
See /usr/share/doc/apache2.2-common/README.Debian.gz on how to configure SSL and
```

```
root@profesor:/etc/apache2/mods-available# ls ../mods-enabled/
alias.conf      autoindex.conf  env.load        setenvif.load
alias.load      autoindex.load  mime.conf       ssl.conf
auth_basic.load cgid.conf       mime.load       ssl.load
authn_file.load cgid.load       negotiation.conf status.conf
authnz_default.load deflate.conf     negotiation.load status.load
authnz_groupfile.load deflate.load     reqtimeout.conf userdir.conf
authnz_host.load dir.conf        reqtimeout.load userdir.load
authnz_user.load dir.load        setenvif.conf
```

## 3. Crear el certificado:

```
root@profesor:/etc/apache2# make-ssl-cert /usr/share/ssl-cert/ssleay.cnf /etc/ap
ache2/ssl/certificado.pem
```

Me sale un cuadro de diálogo para configurar el certificado:



El nombre alternativo lo dejamos en blanco

Listamos los ficheros:

```
root@profesor:/etc/apache2/ssl# ls -la
total 12
drwxr-xr-x 2 root root 4096 dic  4 13:35 .
drwxr-xr-x 8 root root 4096 dic  4 13:30 ..
-rw----- 1 root root 2705 dic  4 13:35 certificado.pem
lrwxrwxrwx 1 root root  15 dic  4 13:35 cfd3c4c2 -> certificado.pem
```

## 4. Vemos el fichero ports.conf para ver si tiene activo el puerto 443

```
GNU nano 2.2.6 Fichero: ports.conf

NameVirtualHost *:8080
Listen 8080

<IfModule mod_ssl.c>
    # If you add NameVirtualHost *:443 here, you will also have to change
    # the VirtualHost statement in /etc/apache2/sites-available/default-ssl
    # to <VirtualHost *:443>
    # Server Name Indication for SSL named virtual hosts is currently not
    # supported by MSIE on Windows XP.
    Listen 443
</IfModule>

<IfModule mod_gnutls.c>
    Listen 443
</IfModule>

#NameVirtualHost *
```

## 5. Reiniciamos apache

```

root@profesor:/etc/apache2# service apache2 restart
[....] Restarting web server: apache2[Thu Dec 04 13:42:44 2014] [warn] NameVirtualHost *:8080 has no VirtualHosts
... waiting [Thu Dec 04 13:42:45 2014] [warn] NameVirtualHost *:8080 has no VirtualHosts
. ok

```

## 6. Vemos los puertos abiertos

```

root@profesor:/etc/apache2# netstat -atunp |grep apache
tcp6      0      0 :::8080          :::*             LISTEN
3423/apache2
tcp6      0      0 :::80           :::*             LISTEN
3423/apache2
tcp6      0      0 :::443          :::*             LISTEN
3423/apache2

```

Observamos que tiene abierto el 443

## 7. Probamos conectarnos por https



Nos da un error en el certificado

Si nos intentamos conectar a un apache sin el modulo ssl



Si vemos error.log

```

[Thu Dec 04 13:42:44 2014] [notice] caught SIGTERM, shutting down
[Thu Dec 04 13:42:45 2014] [notice] Apache/2.2.22 (Debian) mod_ssl/2.2.22 OpenSSL/1.0.1e configured -- resuming normal operations
[Thu Dec 04 13:44:41 2014] [error] [client 192.168.4.16] Invalid method in request \x16\x03\x01

```

8. Creamos un sitio virtual wp11.2asir.net al cual vamos a acceder mediante la IP, por lo que comentamos el nombre del servidor.

```

GNU nano 2.2.6          Fichero: wp11.2asir.net          Mo
<VirtualHost *:443>      Dirigido al puerto 443 (https por defecto)
#       ServerName wp11.2asir.net
       ServerAdmin usuario@profesor.2asir.net
       DocumentRoot /var/www/wp11.2asir.net

       #Activo la transmisión SSL
       SSLEngine on      Activo la transmisión SSL
       SSLCertificateFile /etc/apache2/ssl/certificado.pem Ruta del certificado

```

Comentamos todo lo demás salvo los logs:

```

GNU nano 2.2.6          Fichero: wp11.2asir.net          Modificado
#       <Directory /var/www/wp11.2asir.net>
#           Options Indexes FollowSymLinks MultiViews
#           AllowOverride None
#           Order allow,deny
#           allow from all
#           AuthType Basic
#           AuthName "Zona Privada"
#           AuthUserFile /usr/local/apache2/etc/passwords
#           Require valid-user
#       </Directory>

       ErrorLog ${APACHE_LOG_DIR}/wp11.2asir.net_error.log
       LogLevel warn
       CustomLog ${APACHE_LOG_DIR}/wp11.2asir.net_access.log combined
</VirtualHost>

```

9. Creamos la carpeta con el index.html

```

root@profesor:/etc/apache2/sites-available# cp -r /var/www/wp7.2asir.net/ /var/www/wp11.2asir.net
root@profesor:/etc/apache2/sites-available# nano /var/www/wp11.2asir.net/index.html

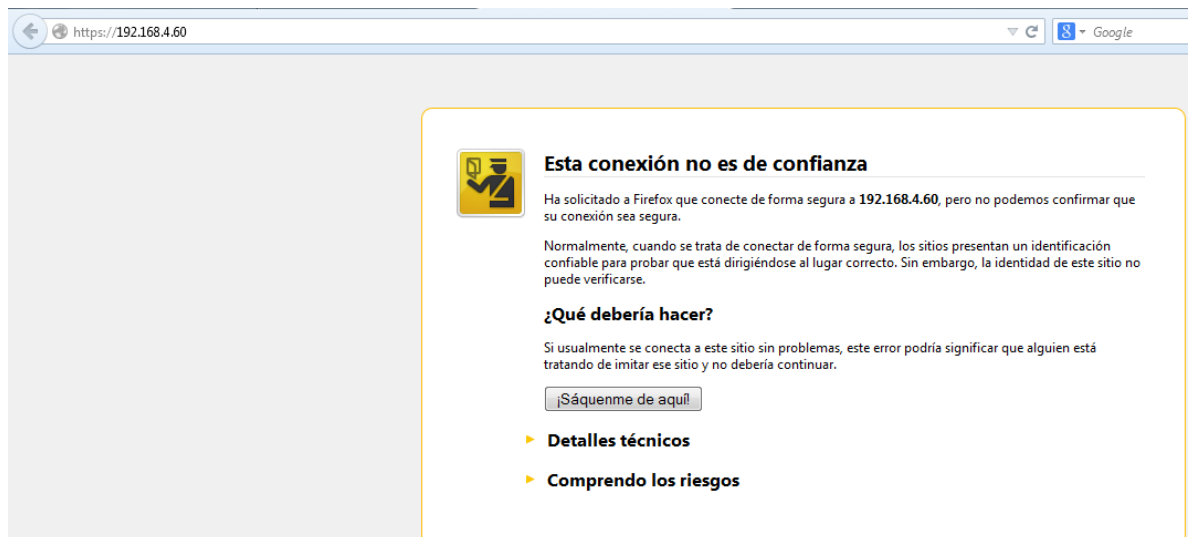
```

```
GNU nano 2.2.6 Fichero: /var/www/wp11.2asir.net/index.html
<html><body><h1>Sitio wp11.2asir.net(192.168.4.60) https </h1>
<p>Tema3. Práctica 11.Sitio https://192.168.4.60 </p>
<p>Autor: Eugenio</p>
</body></html>
```

10. Activamos el sitio wp11.2asir.net y reiniciamos apache

```
root@profesor:/etc/apache2/sites-available# a2ensite wp11.2asir.net
Enabling site wp11.2asir.net.
To activate the new configuration, you need to run:
    service apache2 reload
root@profesor:/etc/apache2/sites-available# service apache2 reload
[...] Reloading web server config: apache2[Wed Dec 10 13:22:52 2014] [warn] NameVirtualHost *:8080 has no VirtualHosts
. ok
root@profesor:/etc/apache2/sites-available#
```

11. Probamos la configuración poniendo <https://192.168.4.60>



Me sale que la conexión no es de confianza.

a. Si vemos los detalles técnicos

#### ▼ Detalles técnicos

Un error ocurrió durante una conexión a 192.168.4.60 porque usa un certificado de seguridad no válido.

El certificado no es confiable porque es auto firmado.  
El certificado solamente es válido para profesor.

(Código de error: sec\_error\_unknown\_issuer)

Ocorre un error de seguridad en firefox.

b. Si comprendemos los riesgos

### ▼ Comprendo los riesgos

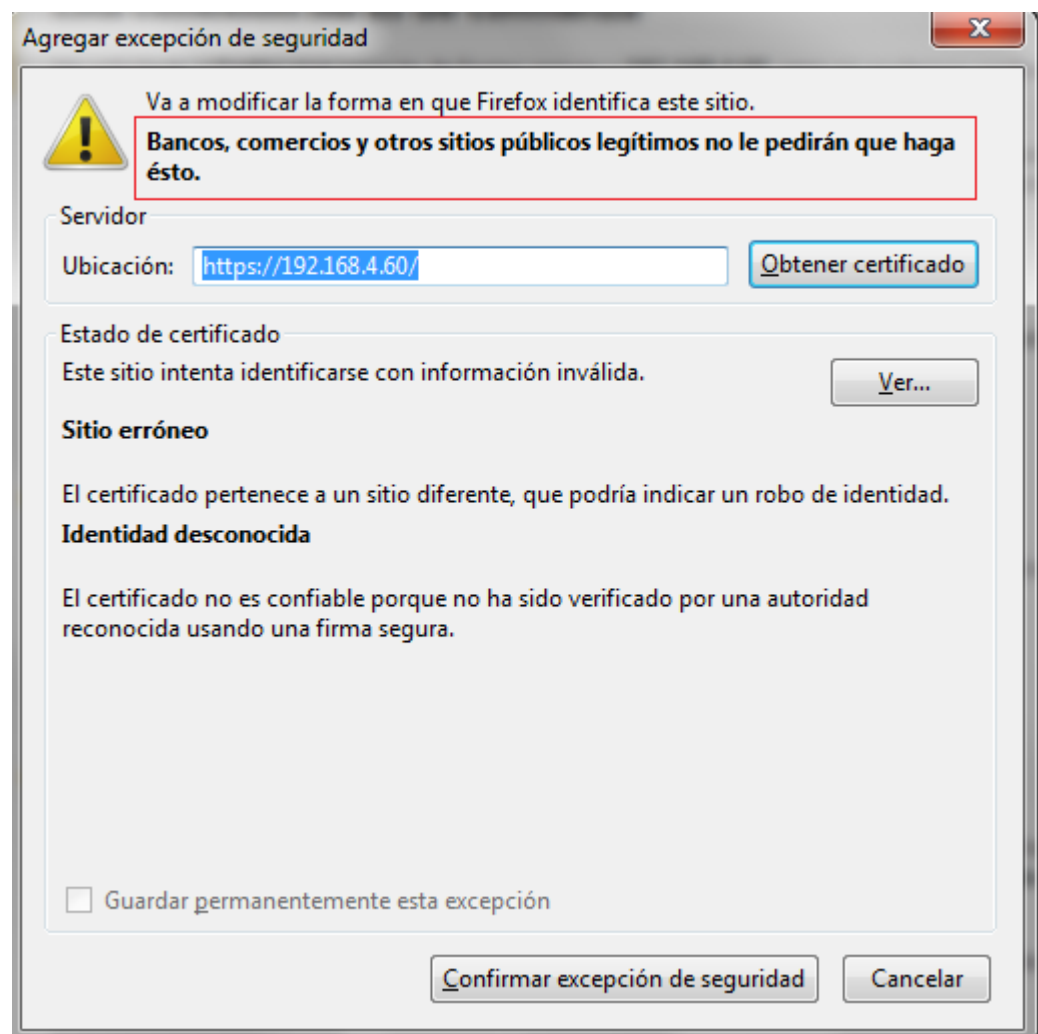
Si entiende lo que está pasando, puede decirle a Firefox que comience a confiar en la identificación de este sitio. **Aunque confíe en el sitio, este error podría significar que alguien está alterando su conexión.**

No agregue una excepción a menos que conozca que hay una buena razón para que este sitio no use una identificación confiable.

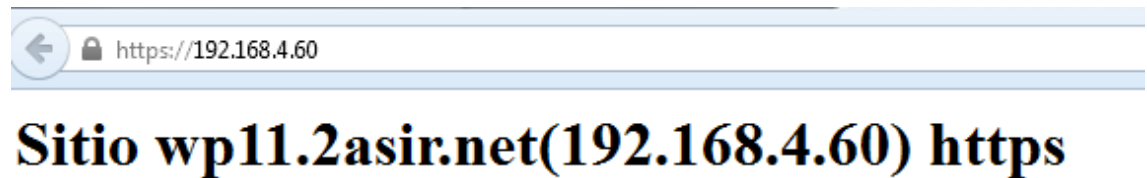
Agregar excepción...

Confiamos plenamente en la identidad del emisor por lo que agregamos una excepción a nuestro navegador.

c. Nos sale otra advertencia:



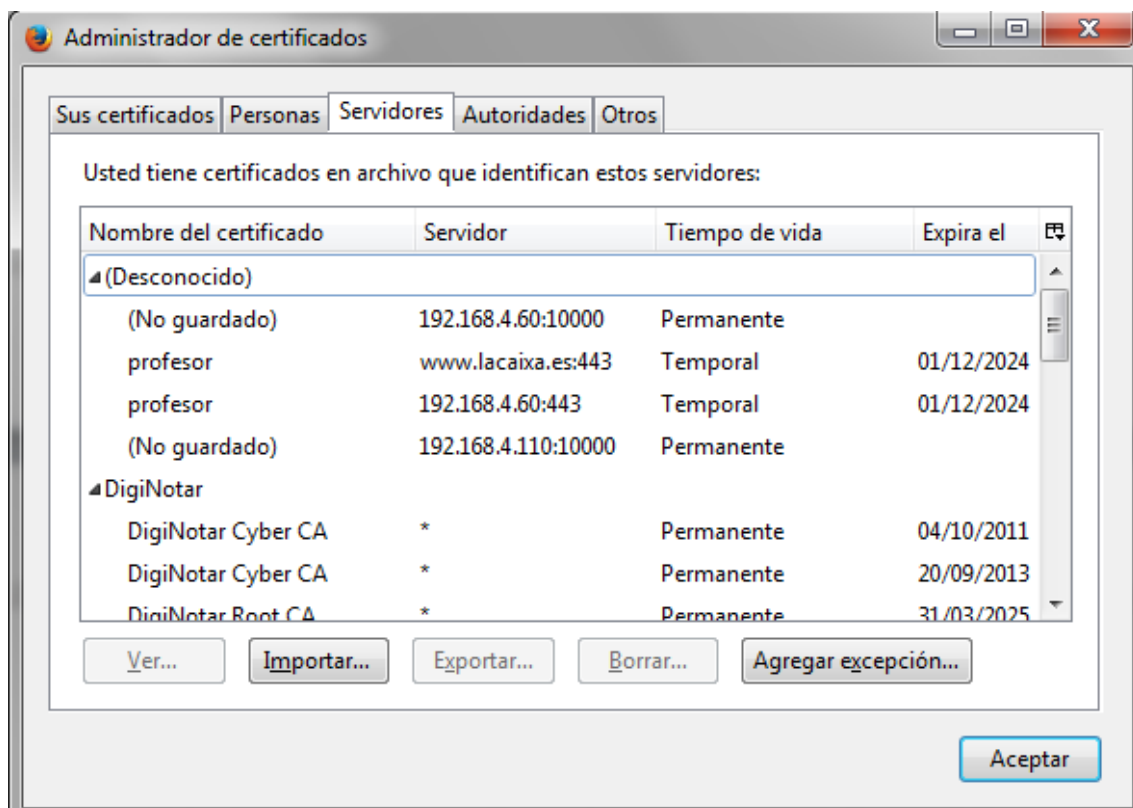
d. Si aún confirmamos la excepción nos abre el sitio web:



Tema3. Práctica 11. Sitio <https://192.168.4.60>

Autor: Eugenio

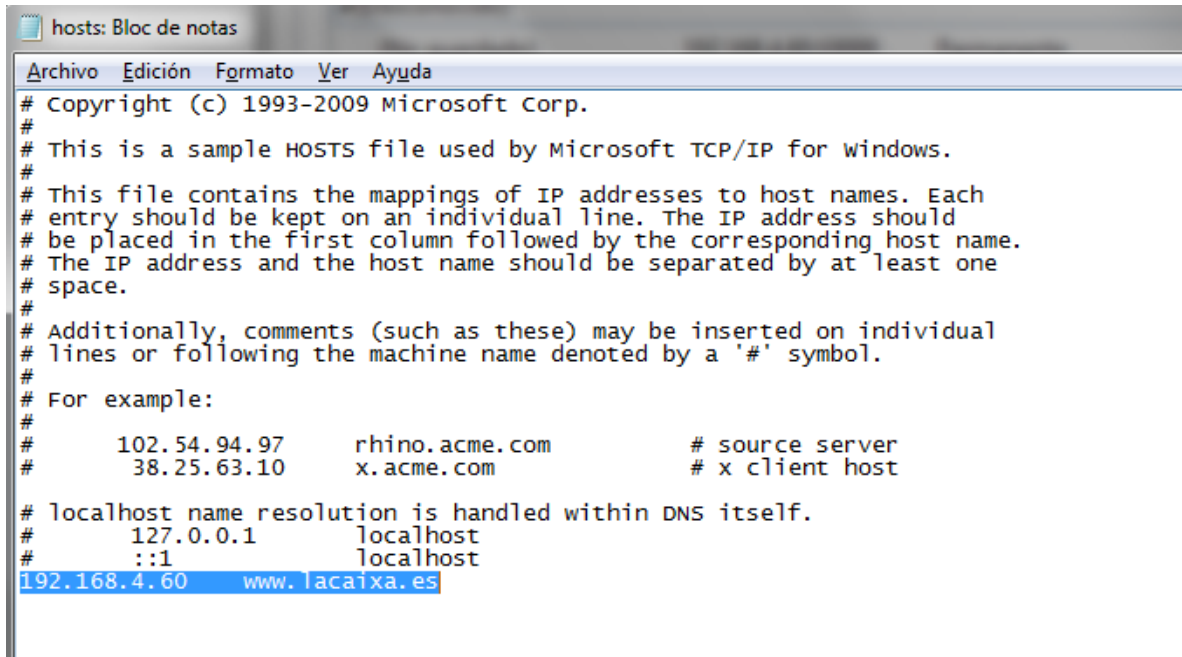
Vemos los certificados:



### **CASO: URSURPACIÓN DE IDENTIDAD**

12. Vamos modificar el fichero C:\Windows\System32\drivers\etc\hosts añadiéndole la siguiente línea:

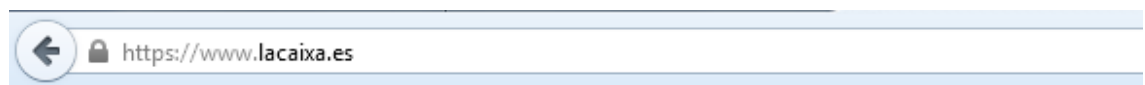
192.168.4.60 [www.lacaixa.es](http://www.lacaixa.es)



```
# 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
192.168.4.60 www.lacaixa.es
```

Asociamos de forma local la dirección 192.168.4.60 con el DNS www.lacaixa.es

13. Ahora <https://www.lacaixa.es>



## Sitio wp11.2asir.net(192.168.4.60) https

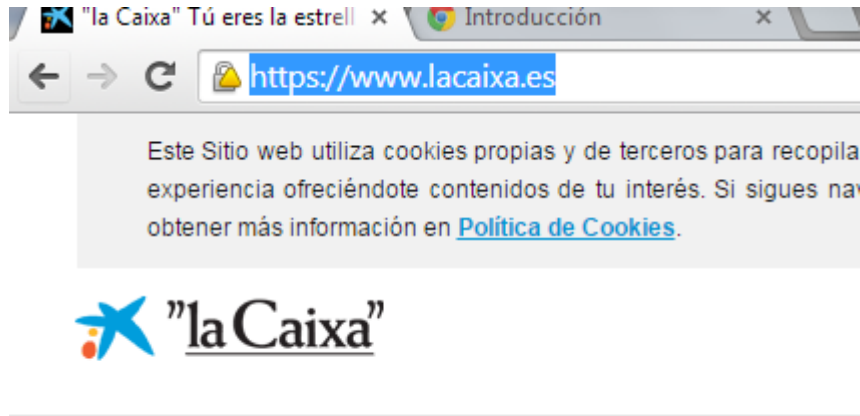
Tema3. Práctica 11. Sitio <https://192.168.4.60>

Autor: Eugenio

Vemos que tras pedirnos que aceptemos una excepción nos muestra la web de 192.168.4.60 cosa que no es correcta.

14. Si entramos en la página verdadera de la caixa





No nos pide que aceptemos ninguna excepción de certificado

Por lo que es mas de confianza.