

## 5.18. HTTPS y certificados digitales

### 1 Certificado digital verificado

1. 1. Inicia sesión en DesarrolloW7XX.
- 1.2. Inicia Firefox.
- 1.3. Conéctate a https://www.bbva.es.
- 1.4. Observa en la URL que el protocolo usado es https.
- 1.5. Pincha en la parte izquierda de la URL.



- 1.6. Pincha sobre "Mostrar detalles de conexión" -> "Más información" para consultar el certificado digital que ha enviado el servidor web y responde de a las siguientes preguntas, Figura 5.106.

- a) ¿Qué algoritmo de clave simétrica se ha utilizado para cifrar la información que viaja por la red? *AES* ¿Cuál es la longitud de la clave utilizada? *128 bits*.
- b) ¿Cuál es el periodo de validez del certificado? *Del 18/08/2014 al 14/08/2015*.

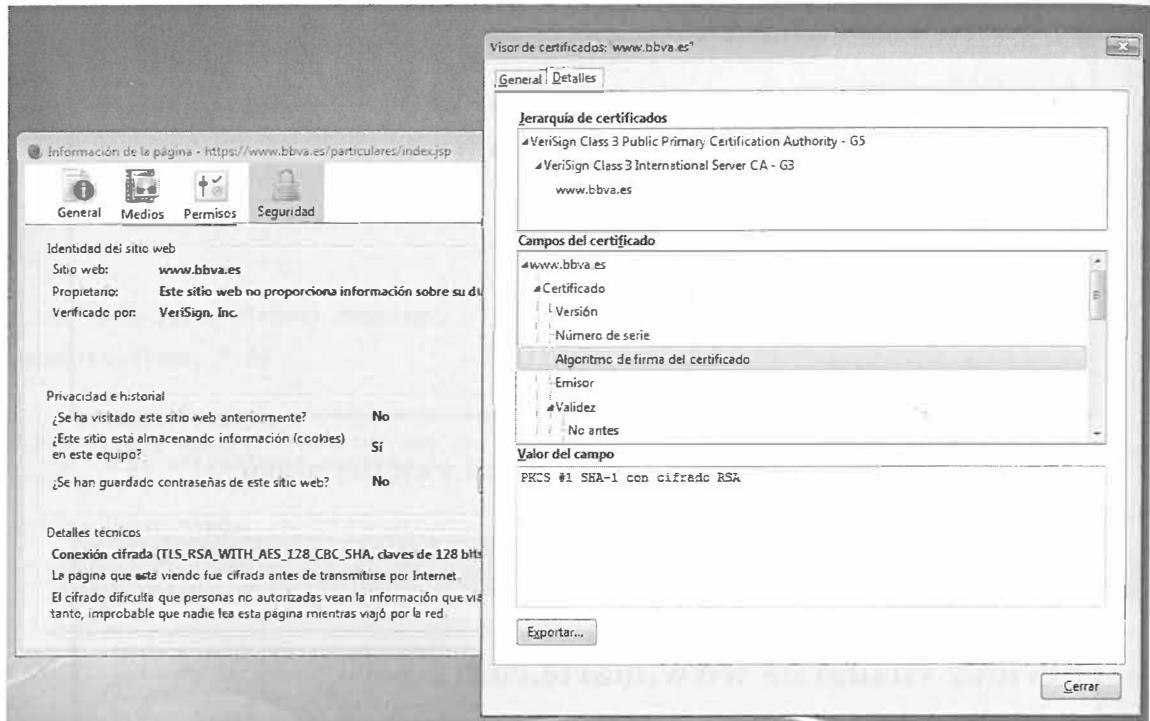


Figura 5.106: Certificado digital

- c) ¿Qué función resumen (hash) ha utilizado la autoridad de certificación para firmar el certificado? *SHA1*.
  - d) ¿Qué algoritmo de clave asimétrica ha utilizado la autoridad de certificación para firmar el certificado? *RSA*.
  - e) ¿De qué tamaño es la clave pública del certificado? *2048 bits*.
  - f) ¿Qué autoridad de certificación ha firmado el certificado? *VeriSign Class 3 International Server CA - G3* ¿De quién depende? *VeriSign Class 3 Public Primary Certification Authority - G5*.
- 1.7. En el menú de *Firefox* accede a **Opciones, Opciones, Pestaña Avanzado, Pestaña Cifrado, Ver certificados** y busca el certificado de la autoridad certificadora que ha firmado el certificado, Figura 5.107.

## 2. Certificado no verificado

- 2.1. Inicia *Firefox*.
- 2.2. Conéctate a la url <https://www.congreso.es>
- 2.3. El navegador muestra un mensaje de error indicando que no ha podido verificar el certificado que le ha enviado el servidor web, Figura 5.108.
- 2.4. Pincha en **Entiendo los riesgos**.
- 2.5. Pincha en **Añadir Excepción**, Figura 5.109. Observa que está marcada la opción **Guardar excepción de forma permanente**.

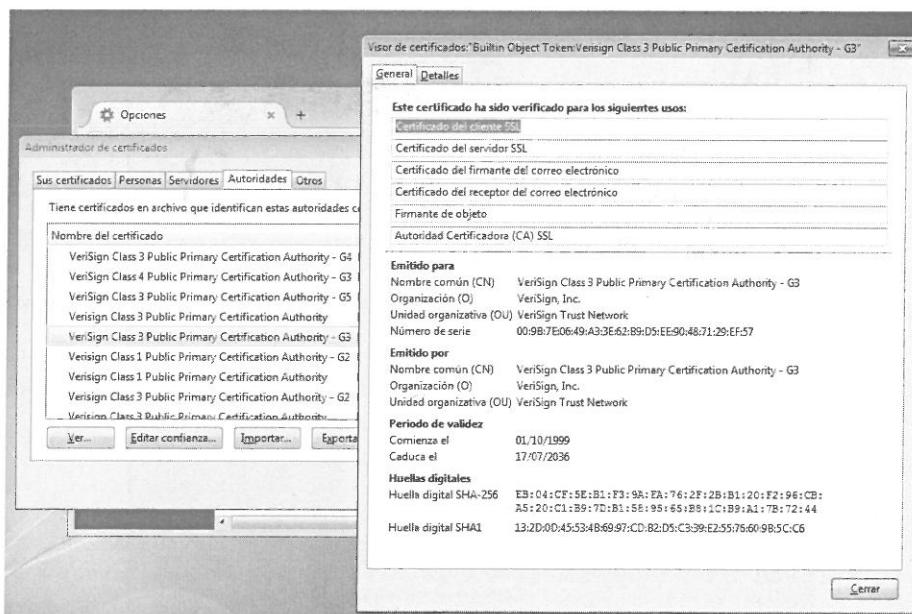


Figura 5.107: Certificado digital de la autoridad de certificación



Figura 5.108: Aviso de certificado digital no verificado

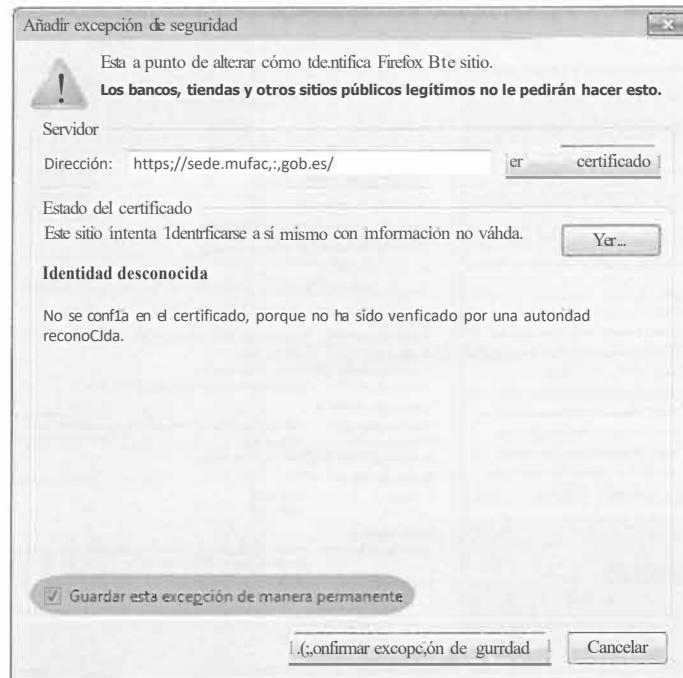


Figura 5.109: Ver el certificado digital no verificado

- 2.6. Pincha en Obtener certificado y en Ver para mostrar los datos del certificado digital que ha enviado el navegador.
- 2.7. Pincha en confirmar excepción de seguridad.
- 2.8. En el menú de Firefox accede a Opciones, Opciones, pestaña Avanzado, Pestaña Cifrado, Ver certificados busca el certificado del servidor que has aceptado y elimínalo, Figura 5.110.

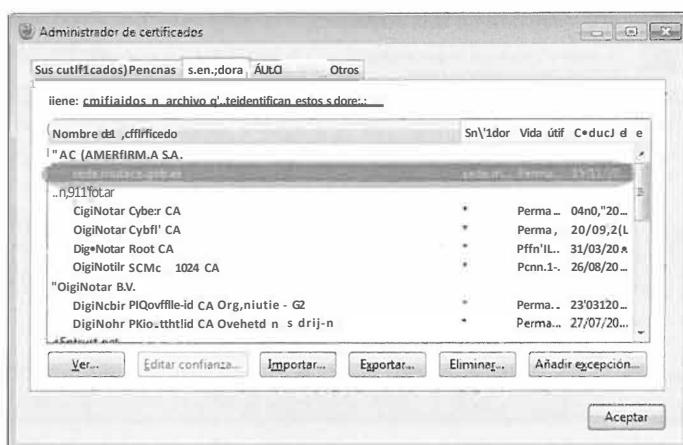


Figura 5.110: Eliminar certificado del servidor

## 5.19. Servidor virtual HTTPS por defecto en Linux

Realiza la siguiente configuración en el servidor *Apache* instalado en **ServidorLinuxXX**.

- Habilita el servidor virtual por defecto.
- Deshabilita los servidores virtuales creados en las prácticas anteriores.
- Habilita el modulo *mod\_ssl*.
- Habilita el servidor virtual *ssl* por defecto.

Prueba la configuración.

1. Inicia una sesión en **ServidorLinuxXX** con un usuario con privilegios de administración.
2. Habilita el servidor virtual por defecto de *Apache*.

```
sudo a2ensite 000-default
```

3. Verifica que dentro del directorio **/etc/apache2/sites-enabled** se ha creado el enlace **000-default.conf**.
4. Deshabilita los servidores virtuales creados en prácticas anteriores.

```
sudo a2dissite software
sudo a2dissite hardware
```

5. Reinicia el servidor para que los cambios tengan efecto.
6. Habilita el módulo *modssl* que permite usar *https*, Figura 5.111.

```
sudo a2enmod ssl
```

```
alumno@ServidorLinux01:/etc/apache2$ sudo a2enmod ssl
[sudo] password for alumno:
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  service apache2 restart
alumno@ServidorLinux01:/etc/apache2$
```

Figura 5.111: Habilitar el modulo modssl

7. Reinicia el servidor para que los cambios tengan efecto.

```
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 80

<IfModule ssl_module>
    Listen 443
</IfModule>

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

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Figura 5.112: Fichero /etc/apache2/port.conf

8. Consulta el fichero /etc/apache2/ports.conf y observa que si habilita el modulo *ssl* el servidor escuchará en el puerto 443, Figura 5.112.
9. Verifica que el servidor escucha en los puertos 80/TCP y 443/TCP.

```
netstat -ltn
```

10. Accede al directorio /etc/apache2/sites-availables y observa que existe un fichero denominado **default-ssl.conf** que contiene la configuración por defecto de un servidor HTTPS.
  11. Habilita el servidor virtual *ssl* defecto (default-ssl.conf) de *Apache*.
- ```
sudo a2ensite default-ssl
```
12. Reinicia el servidor para que los cambios tengan efecto.
  13. Consulta el fichero /etc/apache2/sites-availables/default-ssl.conf y observa su configuración. Fíjate en las directivas que habilitan SSL y que definen la ruta del certificado digital que usurará el servidor, Figuras 5.113 y 5.114.  
El servidor utiliza por defecto un certificado digital autofirmado que se ha creado al instalar Apache. Un certificado autofirmado no está firmado por una autoridad de certificación (tercera parte de confianza) y por tanto, no existen mecanismos automáticos que garanticen su autenticidad. Por eso los navegadores nos pedirán confirmación cuando el servidor se lo envíe.
  14. Desde Desarrollo W7XX abre el navegador y establece una conexión a http://192.168.1.X7, Figura 5.115.
  15. Desde DesarrolloW7XX abre el navegador y establece una conexión a https://192.168.1.X7, Figuras 5.116 y 5.117.

```
<IfModule mod_ssl.c>
  <VirtualHost _default_:443>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

    # Available loglevels: trace8, ..., trace1, debug, info, notices,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf
```

Figura 5.113: Fichero /etc/apache2/sites-available/default-ssl.conf

```
# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on

# A self-signed (snakeoil) certificate can be created by installing
# the ssl-cert package. See
# /usr/share/doc/apache2/README.Debian.gz for more info.
# If both key and certificate are stored in the same file, on
# SSLCertificateFile directive is needed.
SSLCertificateFile      /etc/ssl/certs/ssl-cert-snakeoil.pem
SSLCertificateKeyFile  /etc/ssl/private/ssl-cert-snakeoil.key

# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
# certificate chain for the server certificate. Alternatively
```

Figura 5.114: Fichero /etc/apache2/sites-available/default-ssl.conf

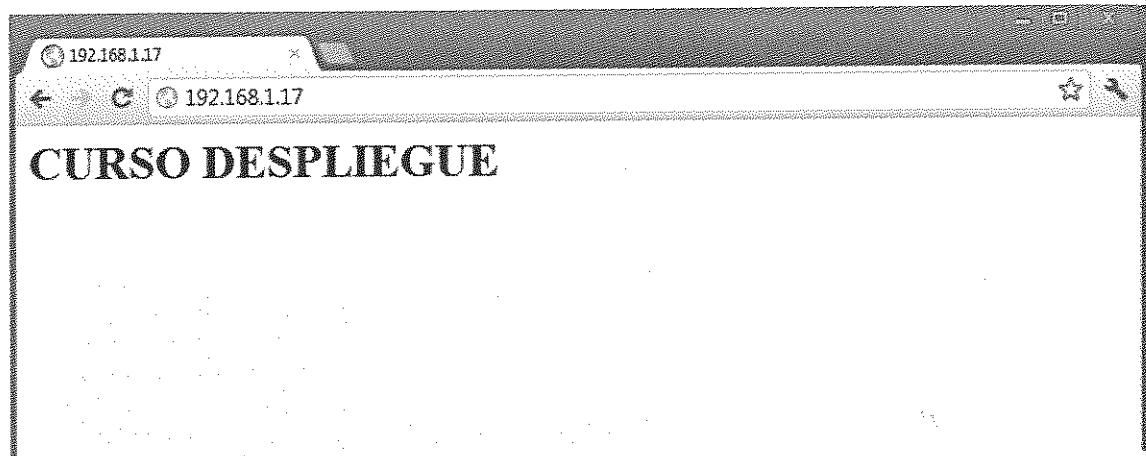


Figura 5.115: Conexión http

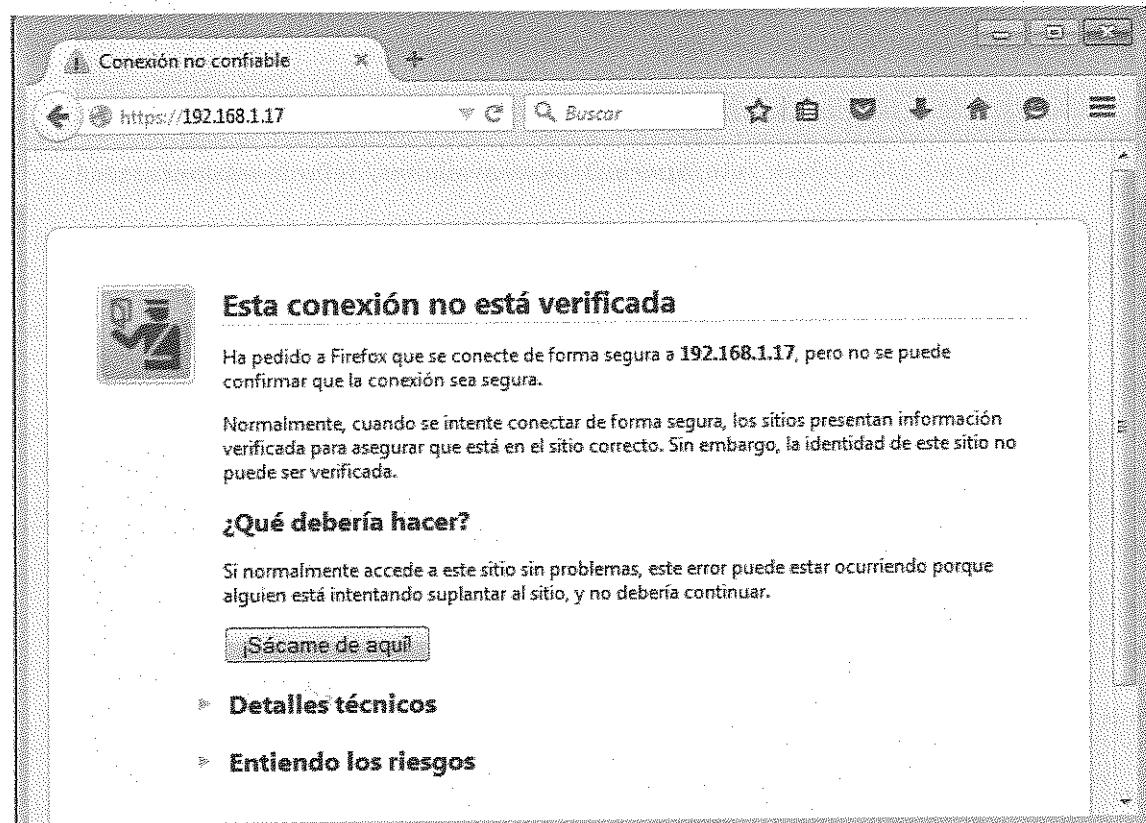


Figura 5.116: Conexión https

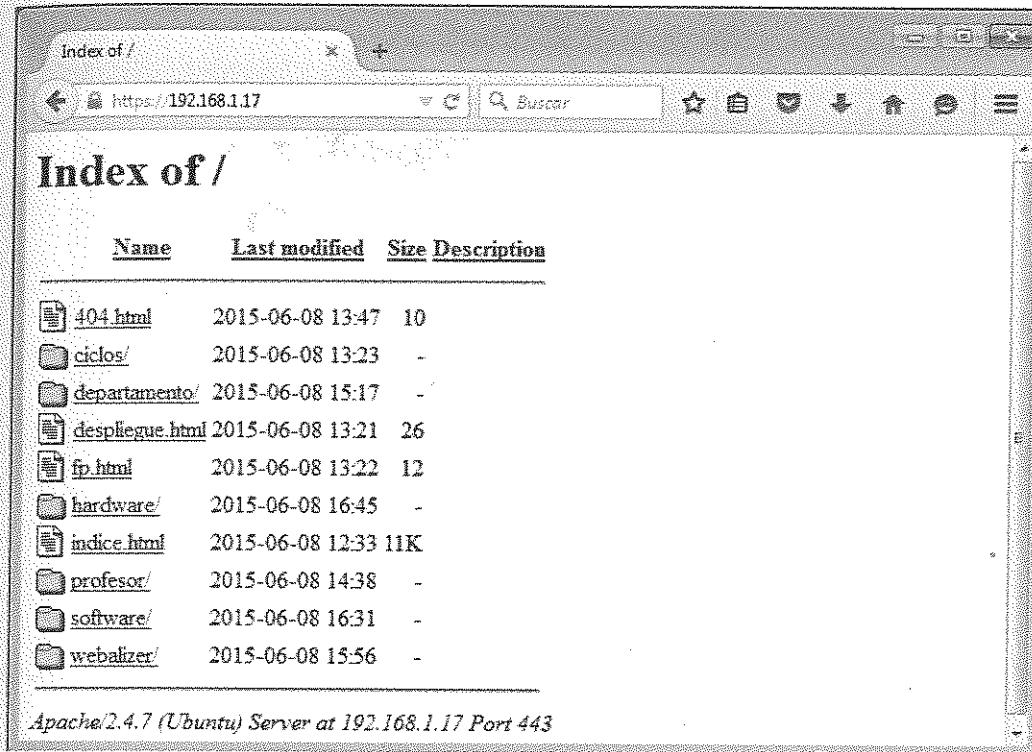


Figura 5.117: Conexión https

## 5.20. Servidor virtual HTTPS en Linux

Realiza la siguiente configuración en el servidor *Apache* instalado en **ServidorLinuxXX**.

- Deshabilita el servidor virtual *ssl* por defecto (*default-ssl*).
- Crea un certificado digital autofirmado con *openssl* para el dominio **seguro.dawXX.net**.
- Crea y habilita un servidor virtual *https* para el dominio **seguro.dawXX.net**
  - Directorio raíz `/var/www/html/seguro/`.
    - Se servirá el fichero `index.html` si no se indica ningún fichero en la URL.
    - Se mostrará un listado del directorio raíz si no se solicita ningún fichero.
    - Podrán acceder todos los usuarios.
  - El *log* de errores será `/var/log/apache2/seguro.error.log`.
  - El *log* de accesos será `/var/log/apache2/seguro.access.log`, con formato *combined*.

Prueba la configuración.

1. Configura el servidor DNS de **ServidorW2008XX** o **ServidorW2012XX** para que resuelva el nombre **seguro.dawXX.net**. La dirección IP asociada al nombre será la IP de **ServidorLinuxXX** es decir, `192.168.1.X7`, Figura 5.118.

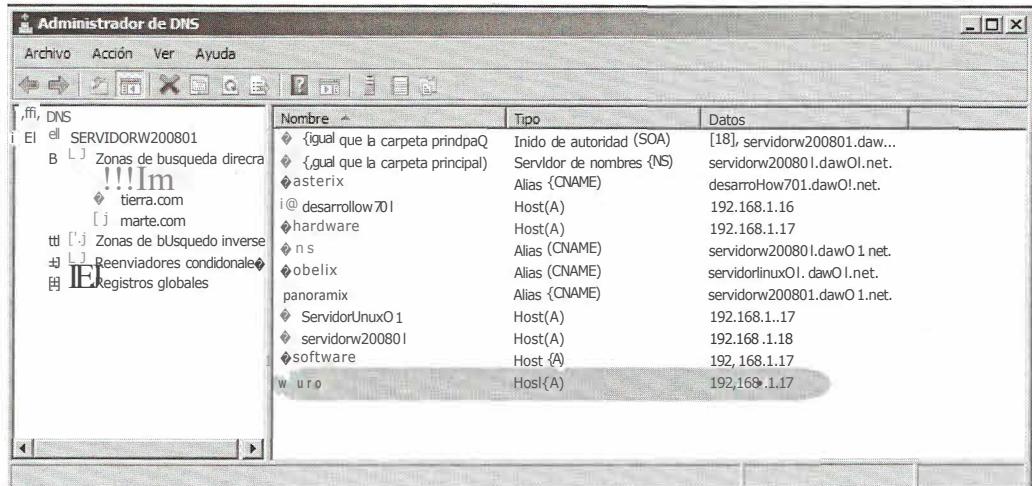


Figura 5.118: Configuraci6n del servidor DNS en ServidorWindowsXX

- 2 Asegurate que DesarrolloW7XX utiliza el servidor DNS que has configurado.
- 3 Inicia una sesi6n en ServidorLinuxXX con un usuario con privilegios de administraci6n.
- 4 Crea el directorio /var/www/html/seguro.
- 5 Crea el fichero de texto /var/www/html/seguro/index.html con el contenido que quieras.
- 6 Crea un certificado digital autofirmado usando openssl.
  - 6.1. Situate en el directorio home del usuario con el que has iniciado sesi6n.
  - 6.2. Crea una clave privada RSA de 2048 bit, Figura 5.119.

```
openssl genrsa -out seguro.key 2048
```

```
alumno@ServidorLinux01:~$ openssl genrsa -out seguro.key 2048
Generating RSA private key, 2048 bit long modulus
.....+
.....+
e is 65537 (0x10001)
alumno@ServidorLinux01:~$
```

Figura 5.119: Creaci6n de una clave privada

- 6.3. Genera una solicitud de certificado (CSR, *Certificate Signing Request*).

```
openssl req -new -key seguro.key -out seguro.csr
```

Introduce los datos del certificado, Figura 5.120

```
alumno@ServidorLinux01:~$ openssl req -new -key seguro.key -out seguro.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Madrid
Locality Name (eg, city) []:Madrid
Organization Name (eg, company) [Internet Widgits Pty Ltd]:daw01
Organizational Unit Name (eg, section) []:daw01
Common Name (e.g. server FQDN or YOUR name) []:seguro.daw01.net
Email Address []:admin@daw01.net

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
alumno@ServidorLinux01:~$ _
```

Figura 5.120: Creación de la solicitud del certificado

Esta solicitud de certificado se la podrías enviar a una autoridad de certificación para que generase el certificado (CRT). En este caso lo vamos a firmar nosotros, vamos a crear un certificado autofirmado.

#### 6.4. Crea el certificado digital autofirmado usando la clave privada, Figura 5.121.

```
openssl x509 -req -days 365 -in seguro.csr -signkey seguro.key -out seguro.crt
```

```
alumno@ServidorLinux01:~$ openssl x509 -req -days 365 -in seguro.csr -signkey se
guro.key -out seguro.crt
Signature ok
subject=/C=ES/ST=Madrid/L=Madrid/O=daw01/OU=daw01/CN=seguro.daw01.net/emailAddre
ss=admin@daw01.net
Getting Private key
alumno@ServidorLinux01:~$ _
```

Figura 5.121: Creación del certificado digital autofirmado

#### 7. Copia la clave y el certificado en los directorios que utiliza por defecto *Apache* y configura los permisos adecuados.

```
sudo mv seguro.key /etc/ssl/private/
sudo mv seguro.crt /etc/ssl/certs/
sudo chown root:ssl-cert /etc/ssl/private/seguro.key
sudo chmod 640 /etc/ssl/private/seguro.key
sudo chown root:root /etc/ssl/certs/seguro.crt
```

#### 8. Crea el fichero */etc/apache/site-available/seguro.conf* con las siguientes directivas, Figura 5.122.

```
<IfModule mod_ssl.c>
  <VirtualHost _default_:443>
    ServerName seguro.daw01.net
    DocumentRoot /var/www/html/seguro
    ErrorLog ${APACHE_LOG_DIR}/seguro.error.log
    CustomLog ${APACHE_LOG_DIR}/seguro.access.log combined

    <Directory /var/www/html/seguro>
      Options Indexes FollowSymLinks
      AllowOverride None
      Require all granted
    </Directory>

    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/seguro.crt
    SSLCertificateKeyFile /etc/ssl/private/seguro.key
  </VirtualHost>
</IfModule>
```

Figura 5.122: Fichero de configuración del servidor seguro

9. Deshabilita el servidor ssl por defecto.

```
sudo a2dissite default-ssl
```

10. Habilita el servidor virtual seguro.

```
sudo a2ensite seguro
```

11. Verifica que dentro del directorio `/etc/apache2/sites-enabled` se ha creado el enlace `seguro.conf`.
12. Reinicia el servidor para que los cambios tengan efecto.
13. Desde **DesarrolloW7XX** abre el navegador y establece una conexión a `https://seguro.dawXX.net`, Figuras 5.123, 5.124, 5.125 y 5.126.

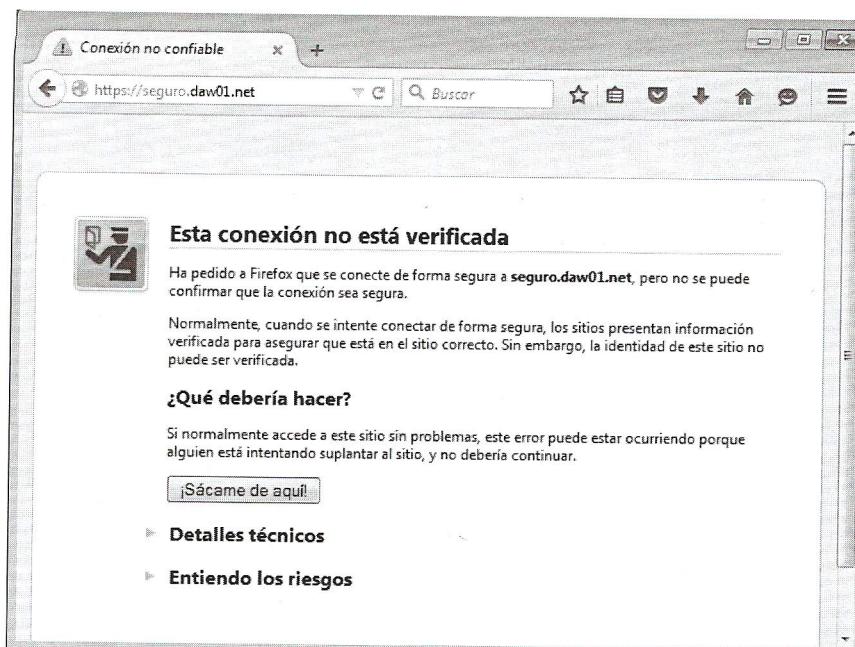


Figura 5.123: Conexión https

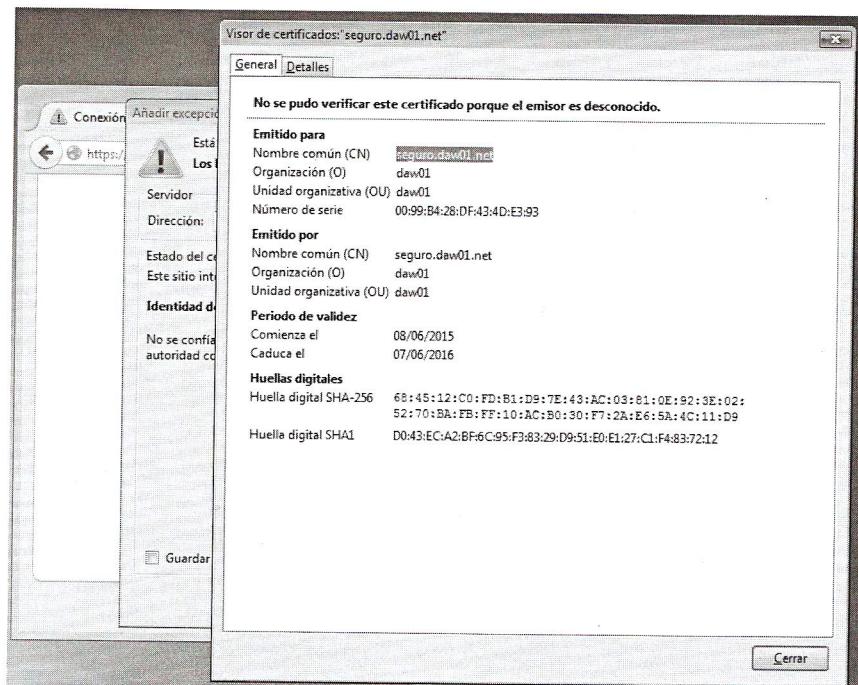


Figura 5.124: Conexión https

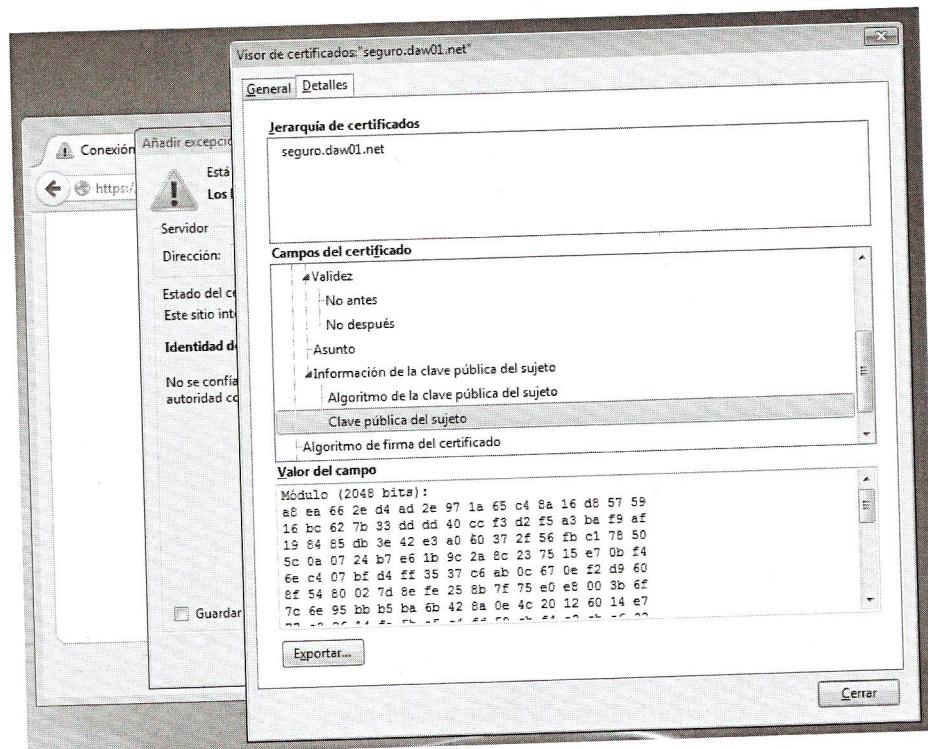


Figura 5.125: Conexión https



Figura 5.126: Conexión https

## 5.21. Servidor virtual HTTPS por defecto en Windows

Realiza la siguiente configuración en el servidor *Apache* instalado en **ServidorW2008XX**.

- Deshabilita los **servidores virtuales** creados en las prácticas anteriores.
- Habilita el modulo *mod\_ssl*.
- Habilita el servidor virtual *ssl* por defecto

Prueba la configuración.

1. Inicia una sesión en **ServidorW2008XX** con un usuario con privilegios de administración.
2. Deshabilita los servidores virtuales creados en prácticas anteriores.
  - 2.1. Edita el fichero **C:\Program Files\Apache Software Foundation\Apache2.2\conf\httpd.conf** y comenta la directiva **Include** del fichero **conf\extra\httpd-vhost.conf**.
  - 2.2. Reinicia el servidor para que los cambios tengan efecto.
3. Edita el fichero **C:\Program Files\Apache Software Foundation\Apache2.2\conf\httpd.conf** y habilita el módulo **mod\_ssl** eliminando el comentario de la directivas **LoadModule**, Figura 5.127.

```
#LoadModule mime_magic_module modules/mod_mime_magic.so
LoadModule negotiation_module modules/mod_negotiation.so
#LoadModule proxy_module modules/mod_proxy.so
#LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
#LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
#LoadModule proxy_connect_module modules/mod_proxy_connect.so
#LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
#LoadModule proxy_http_module modules/mod_proxy_http.so
#LoadModule proxy_scgi_module modules/mod_proxy_scgi.so
#LoadModule reqtimeout_module modules/mod_reqtimeout.so
#LoadModule rewrite_module modules/mod_rewrite.so
LoadModule setenvif_module modules/mod_setenvif.so
#LoadModule spelling_module modules/mod_speling.so
LoadModule ssl_module modules/mod_ssl.so
#LoadModule status_module modules/mod_status.so
#LoadModule substitute_module modules/mod_substitute.so
#LoadModule unique_id_module modules/mod_unique_id.so
LoadModule userdir_module modules/mod_userdir.so
#LoadModule usertrack_module modules/mod_usertrack.so
#LoadModule version_module modules/mod_version.so
```

Figura 5.127: Habilitar el módulo *mod\_ssl*

4. Habilita el servidor virtual *ssl* defecto (*default-ssl*) de *Apache*. Edita el fichero **C:\Program Files\Apache Software Foundation\Apache2.2\conf\httpd.conf** y eliminana el comentario de la directiva **Include** del fichero **conf\extra\httpd-ssl.conf**, Figura 5.128.
5. Si observas en el fichero **C:\Program Files\Apache Software Foundation\Apache2.2\conf\extra\httpd-ssl.conf** existen dos directivas para definir el certificado digital y la clave privada del servidor (que debemos crear), Figura 5.129.
6. Crea un certificado digital autofirmado usando *openssl*.
  - 6.1. Abre un terminal.
  - 6.2. Accede al directorio **C:\Program Files\Apache Software Foundation\Apache2.2\conf**.
  - 6.3. Ejecuta el comando **C:\Program Files\Apache Software Foundation\Apache2.2\bin\openssl**.

```
#include conf/extra/httpd-vhosts.conf  
# Local access to the Apache HTTP Server Manual  
#Include conf/extra/httpd-manual.conf  
# Distributed authoring and versioning (WebDAV)  
#Include conf/extra/httpd-dav.conf  
# Various default settings  
#Include conf/extra/httpd-default.conf  
# Secure (SSL/TLS) connections  
#Include conf/extra/httpd-ssl.conf  
# Note: The following must be present to support  
# starting without SSL on platforms with no /dev/random equivalent  
# but a statically compiled-in mod_ssl.  
#  
<IfModule ssl_module>  
SSLRandomSeed startup builtin
```

Figura 5.128: Habilitar el servidor virtual https

```
#SSLCipherSuite RC4-SHA:AES128-SHA:HIGH:MEDIUM::!aNULL:!MD5  
#SSLHonorCipherOrder on  
#  
# Server Certificate:  
# Point SSLCertificateFile at a PEM encoded certificate. If  
# the certificate is encrypted, then you will be prompted for a  
# pass phrase. Note that a kill -HUP will prompt again. Keep  
# in mind that if you have both an RSA and a DSA certificate you  
# can configure both in parallel (to also allow the use of DSA  
# ciphers, etc.)  
#SSLCertificateFile "C:/Program Files/Apache Software Foundation/Apache2.2/conf/server.crt"  
#SSLCertificateFile "C:/Program Files/Apache Software Foundation/Apache2.2/conf/server-dsa.crt"  
#  
# Server Private Key:  
# If the key is not combined with the certificate, use this  
# directive to point at the key file. Keep in mind that if  
# you've both a RSA and a DSA private key you can configure  
# both in parallel (to also allow the use of DSA ciphers, etc.)  
#SSLCertificateKeyFile "C:/Program Files/Apache Software Foundation/Apache2.2/conf/server.key"  
#SSLCertificateKeyFile "C:/Program Files/Apache Software Foundation/Apache2.2/conf/server-dsa.key"
```

Figura 5.129: Fichero httpd-ssl.conf

```
C:\Program Files\Apache Software Foundation\Apache2.2\conf>"c:\Program Files\Apache Software Foundation\Apache2.2\bin\openssl.exe"
OpenSSL> genrsa -out server.key 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....+++
e is 65537 <0x10001>
OpenSSL>
```

Figura 5.130: Creación de una clave privada

6.4. Crea una clave privada RSA de 2048 bit, Figura 5.130.

```
Openssl> genrsa -out server.key 2048
```

6.5. Genera una solicitud de certificado (CSR, *Certificate Signing Request*).

```
Openssl> req -config openssl.cnf -new -key server.key -out server.csr
```

Introduce los datos del certificado, Figura 5.131

```
OpenSSL> req -new -key server.key -out server.csr
Unable to load config info from /usr/local/ssl/openssl.cnf
error in req
OpenSSL> req -config openssl.cnf -new -key server.key -out server.csr
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value.
If you enter '.', the field will be left blank.

Country Name <2 letter code> [AU]:ES
State or Province Name <full name> [Some-State]:Madrid
Locality Name <eg, city> []:Madrid
Organization Name <eg, company> [Internet Widgits Pty Ltd]:daw01.net
Organizational Unit Name <eg, section> []:daw01.net
Common Name <e.g. server FQDN or YOUR name> []:servidorwindows01.daw01.net
Email Address []:admin@daw01.net

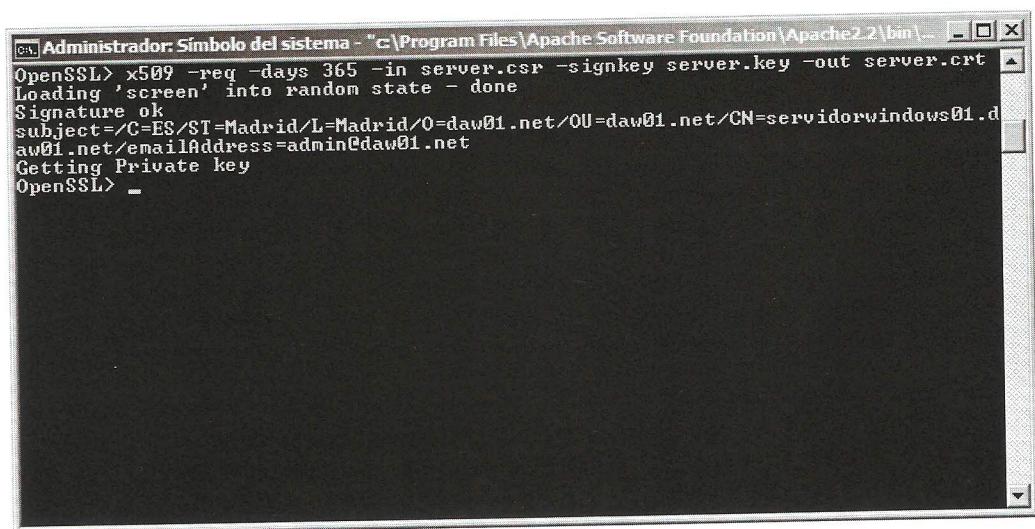
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
OpenSSL>
```

Figura 5.131: Creación de la solicitud del certificado

Esta solicitud de certificado se la podrías enviar a una autoridad de certificación para que generase el certificado (CRT). En este caso lo vamos a firmar nosotros, vamos a crear un certificado autofirmado.

- 6.6. Crea el certificado digital autofirmado usando la clave privada, Figura 5.132.

```
OpenSSL> x509 -req -days 365 -in server.csr -signkey server.key -out server...
```



```
Administrator: Símbolo del sistema - "c:\Program Files\Apache Software Foundation\Apache2.2\bin"... [ ] □ X
OpenSSL> x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
Loading 'screen' into random state - done
Signature ok
subject=/C=ES/ST=Madrid/L=Madrid/O=daw01.net/OU=daw01.net/CN=servidorwindows01.d
aw01.net/emailAddress=admin@daw01.net
Getting Private key
OpenSSL> _
```

Figura 5.132: Creación del certificado digital autofirmado

7. Reinicia el servidor para que los cambios tengan efecto.
8. Verifica que el servidor escucha en los puertos 80/TCP y 443/TCP.
- netstat -a -p TCP -n
9. Desde DesarrolloW7XX abre el navegador y establece una conexión a <http://192.168.1.18>, Figura 5.133.

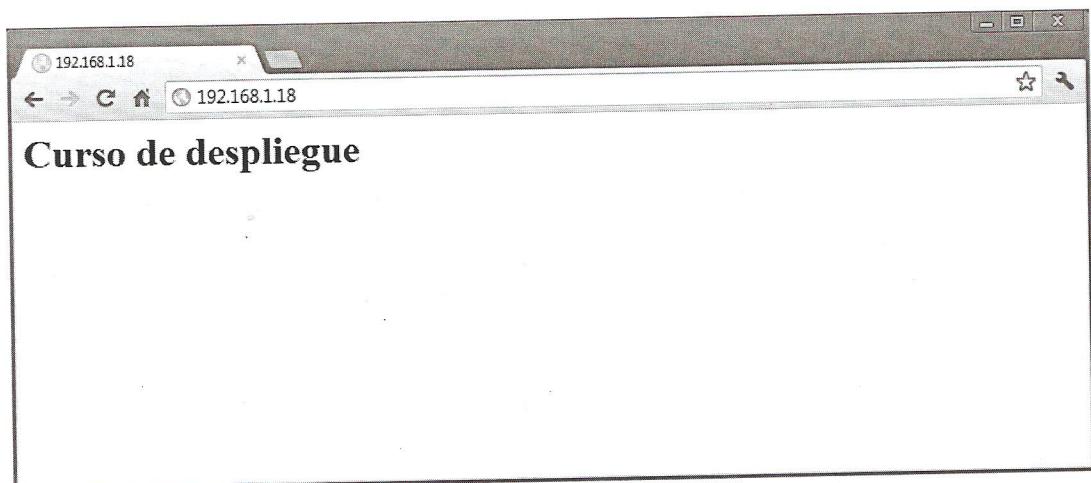


Figura 5.133: Conexión http

10. Desde DesarrolloW7XX abre el navegador y establece una conexión a `https://192.168.1.X8`, Figuras 5.134 y 5.135.

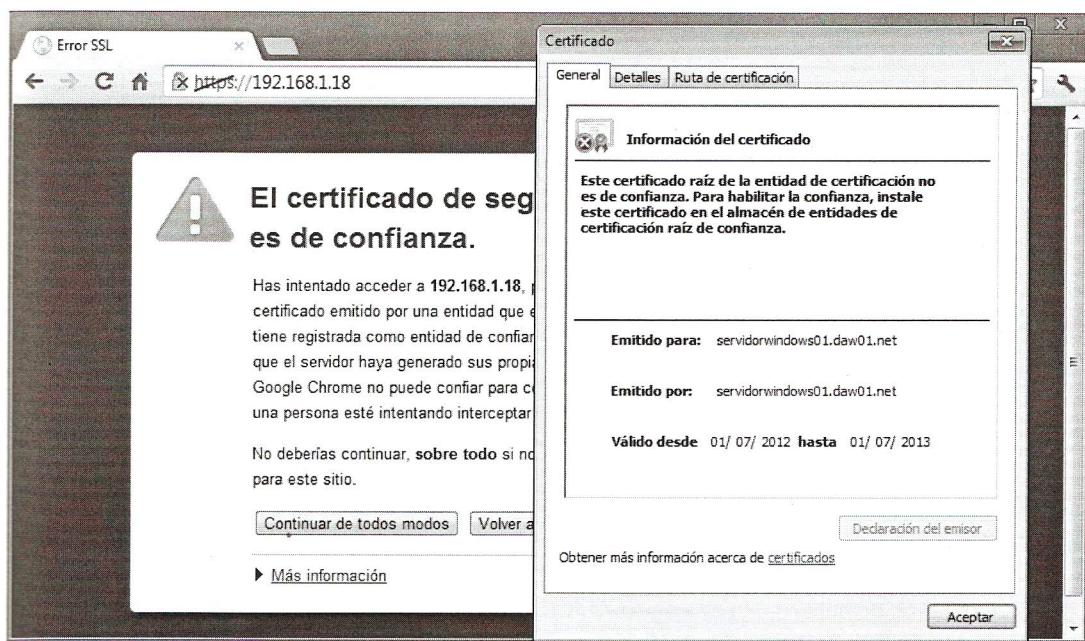


Figura 5.134: Conexión https

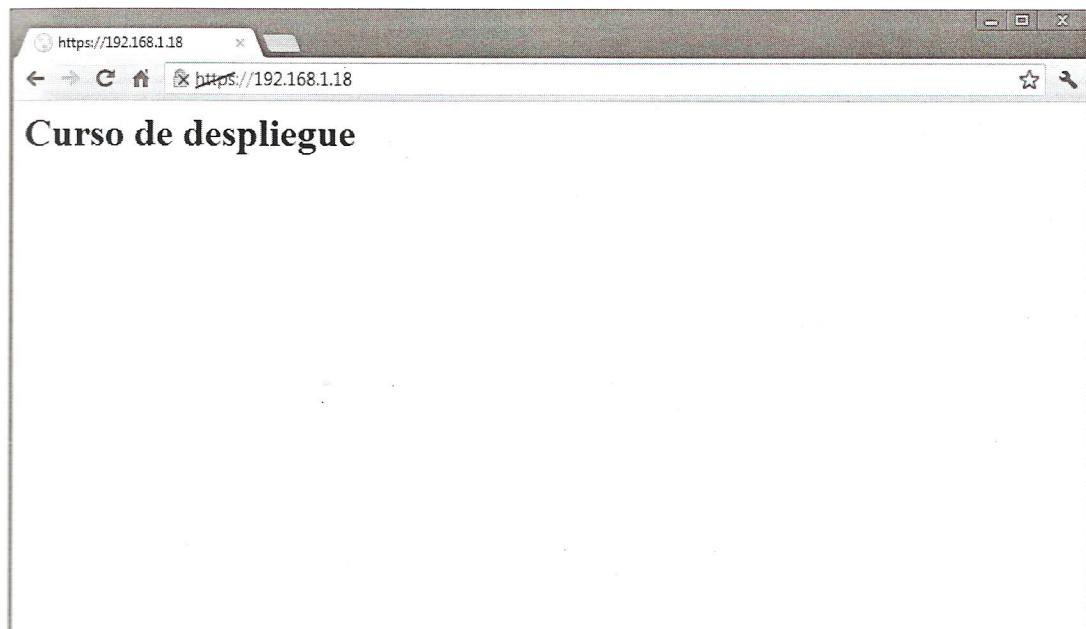


Figura 5.135: Conexión https