Unidad de Trabajo nº2 – Actividad de desarrollo – Servidor Web Seguro
Despliegue de Aplicaciones Web - 2º DPL (Mañana) - I.E.S. El Rincón
Curso 2012-2013 (Doc. nº10 - 10/10/2012)

- ***Objetivo general:***
  Configuración de servidor web seguro.
- ***Duración prevista:*** 2 horas aproximadamente.
- ***Software:*** Distribución Ubuntu.
- ***Mínimos que se persiguen en la actividad:***
  - Diferenciación entre claves simétricas y asimétricas.
  - Comprensión de un esquema de claves asimétricas.
  - Comprensión de los cuatro conceptos básicos en seguridad
  - Comprensión de qué es una entidad certificadora.
  - Buscar en un navegador web los certificados y las entidades certificadoras que han emitido dichos certificados.
  - Instalación de un servidor web seguro
- ***Documentación:***
  - http://www.tc.umn.edu/~brams006/selfsign.html

- ***Pasos de la Actividad:***

Introducción teórica:

Conceptos básicos en seguridad:

- Control de integridad: ausencia de modificación o destrucción no autorizados de la información.
- Disponibilidad/no repudio: consiste en impedir la denegación no autorizada de acceso a la información.
- Secreto/confidencialidad: supone evitar la divulgación no autorizada la información.
- Validación de identificación/autenticación: busca la seguridad en el proceso de dar y reconocer la autenticidad de la información y/o la identidad de los actores y/o el permiso por parte de los autorizadores.

Cifrado con esquema de clave simétrica:

Se trata de realizar una comunicación de información en la que:

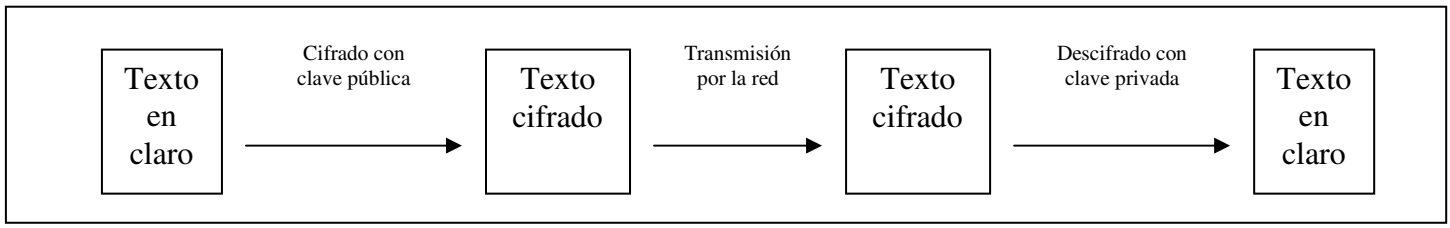
- Se cifra la información en el emisor con la clave k
- Se transmite la información cifrada
- Se descifra la información en el receptor con la misma clave k

En este esquema el problema está en la distribución de las claves, de manera que emisor y receptor tienen la misma clave y ambos deben conocer dicha clave que nadie más debe conocer. Y el problema está en la distribución de las claves porque se debe buscar un mecanismo seguro para la distribución de estas: Valija diplomática, comunicarse las claves por teléfono (que no esté pinchado), etc.

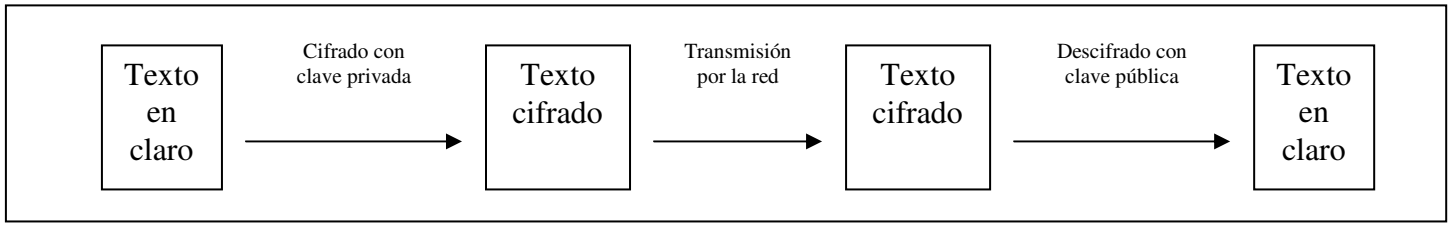
Cifrado con esquema de claves asimétrica:

Con este sistema se crean mediante un algoritmo matemático dos claves llamadas pública y privada, de tal manera que si se cifra con una de ellas sólo se puede descifrar con la otra.

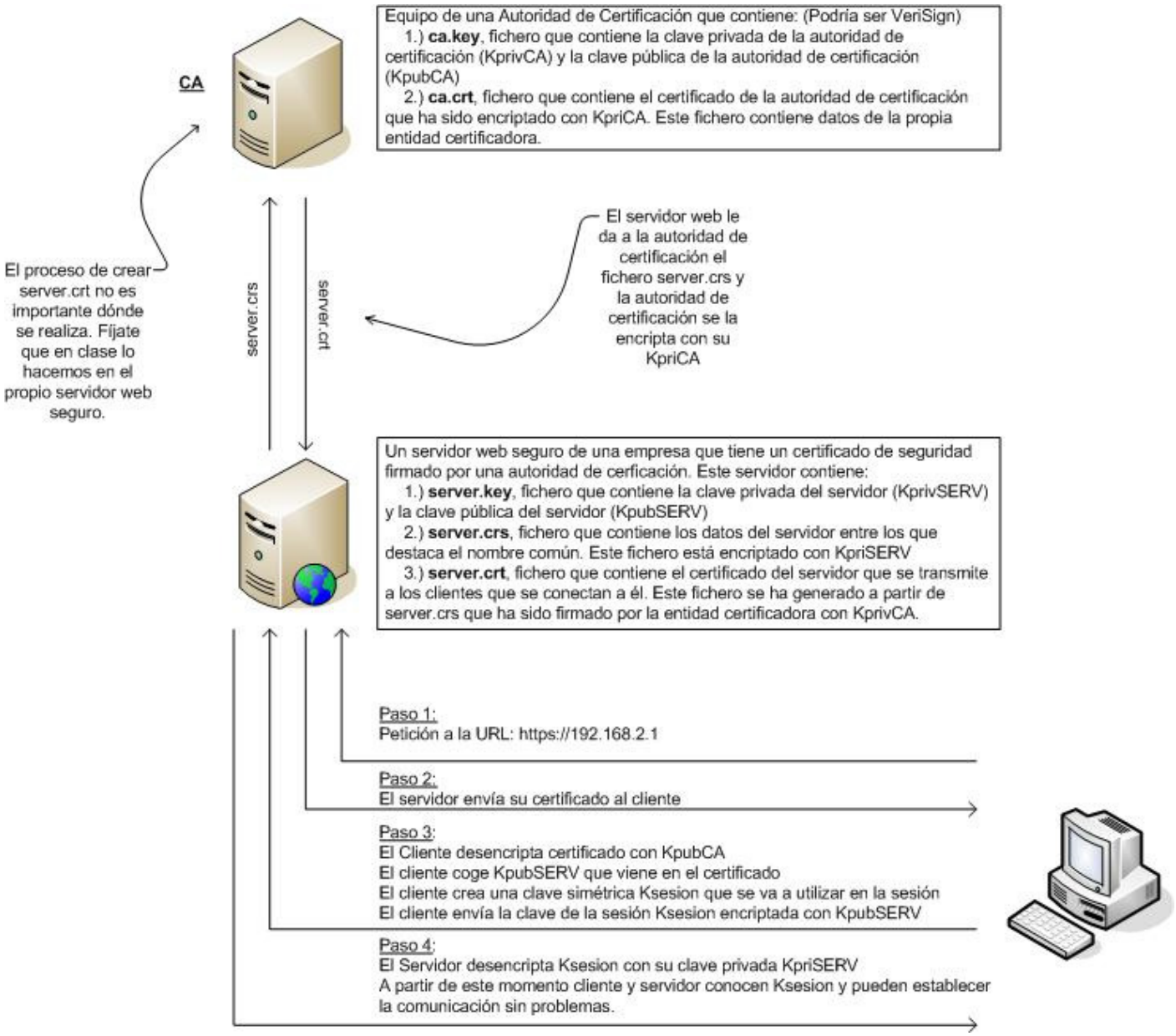
Esquema en el que se consigue confidencialidad:



Esquema en el que se consigue autenticación:



Esquema de una conexión a un servidor web seguro:



Enunciado del supuesto que queremos realizar:

En el siguiente supuesto haremos en clase un servidor web seguro con Apache en Linux y accederemos a él a través del navegador web Internet Explorer desde Windows.

Configuración de un servidor web seguro (https):

- *Paso 1*: Instala los paquetes necesarios:
  apt-get install openssl
  apt-get install apache2

  Nota: Evidentemente comprueba antes si ya están instalados. Para ello, tienes el comando siguiente, que te mostrará *todos los paquetes que contienen el string ssl y si el paquete está instalado.*
  *dpkg -l *ssl**

- *Paso 2*: Crea el par de claves privada y pública para tu entidad certificadora.
  openssl genrsa -des3 -out ca.key 4096

- *Paso 3*: Crea el certificado de la entidad certificadora.
  openssl req –new -x509 –days 365 -key ca.key -out ca.crt

  Nota: Ten en cuenta que estos son los datos que aparecerán en el certificado de la entidad certificadora. De esta manera los certificados firmados por esta entidad emisora de certificados tendrán en los datos de emisor estos datos.

- *Paso 4*: Crea el par de claves privada y pública para tu servidor web seguro.
  openssl genrsa -des3 -out server.key 4096

- *Paso 5:* Crea una petición de creación de certificado para tu servidor web seguro.
  openssl req -new -key server.key -out server.csr

  Nota: Ten en cuenta que los datos introducidos son los datos de tu servidor web y por tanto debes tener especialmente cuidado en indicar el common name que es el nombre DNS o la IP de tu servidor web y es uno de los parámetros que va a comprobar un cliente web cuando reciba un certificado de este servidor web seguro, y de esta manera determinar que viene de quién dice venir.

- *Paso 6*: Firma el CSR creado anteriormente con la clave pública de la entidad certificadora que avala la autenticidad del certificado que se va a crear con este paso.
  openssl x509 -req -days 365 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out server.crt

- *Paso 7*: Ahora ya sólo tienes que colocar el fichero de claves con el par de claves privada y pública del servidor server.key y el certificado de tu servidor web seguro server.cert en el lugar adecuado para que tu servidor web los pueda encontrar. Un buen lugar es:
  mv server.key /etc/ssl/private/server.key
  mv server.crt /etc/ssl/certs/server.crt

- *Paso 8*: El siguiente paso consiste en acceder al fichero generado por la instalación del Apache y colocar los valores adecuados de las directivas SSLCertificateFile y SSLCertificateKeyFile para que contengan los ficheros del paso anterior.
  vi /etc/apache2/sites-available/default-ssl

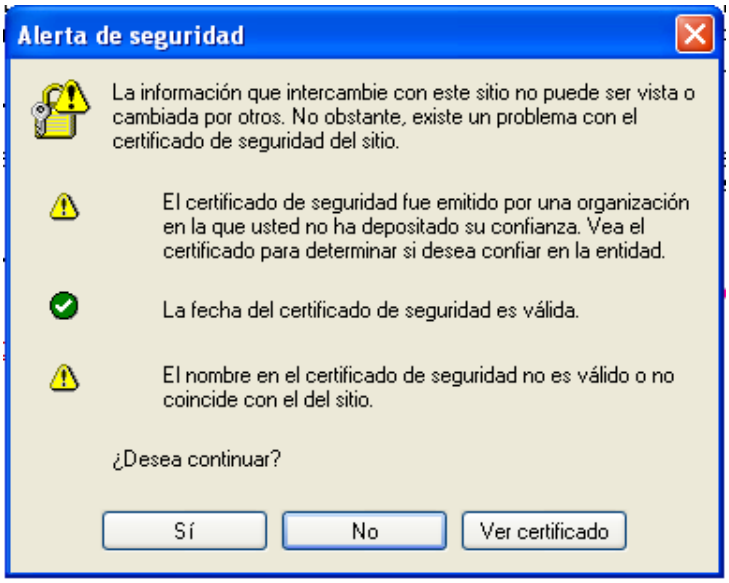
  Nota: Observa que el fichero /etc/apache2/sites-available/default-ssl realmente contiene un host virtual que escucha por el puerto 443 y que constituye tu servidor web seguro.

- *Paso 9*: A continuación debes habilitar el mod_ssl de Apache. Para ello ejecuta el siguiente comando:
  a2enmod ssl

- *Paso 10*: Crea el enlace simbólico para el nuevo host virtual y rearranca apache.
  ln -s /etc/apache2/sites-available/default-ssl /etc/apache2/sites-enable/001-default-ssl
  /etc/init.d/apache2 restart

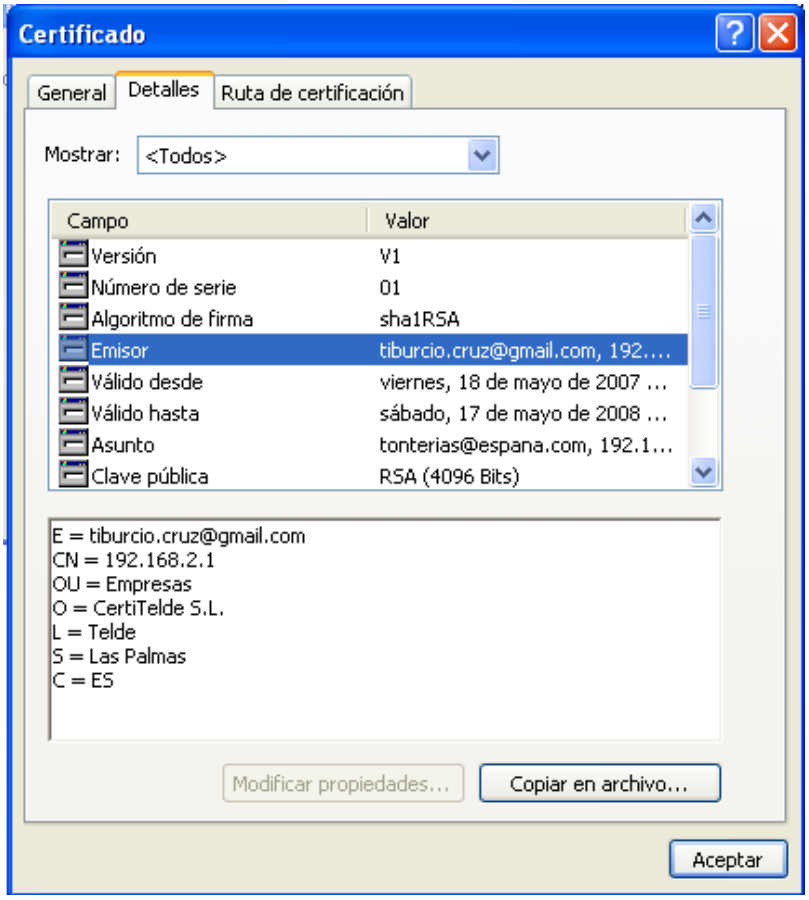
Acceso al servidor https desde Internet Explorer:

- *Paso 11*: Accede a la URL de tu servidor web seguro. (https://192.168.2.1) En este ejemplo utilizaremos Internet Explorer desde Windows para acceder a nuestro servidor web seguro. El proceso es similar con cualquier otro cliente web en cualquier otro sistema operativo. Cuando accedes aparecerá la siguiente ventana:



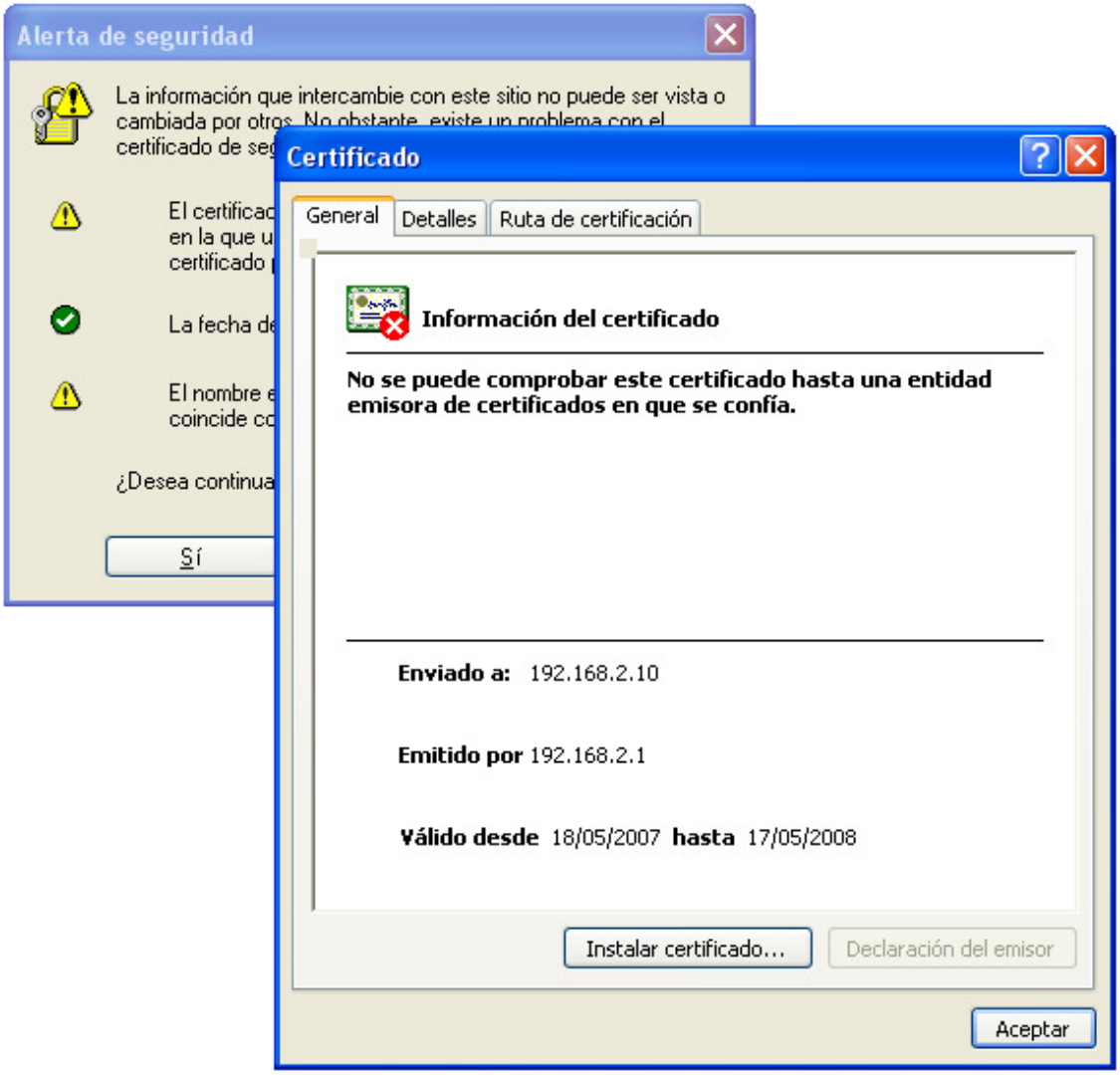
En esta ventana no está diciendo que el certificado ha sido emitido por una entidad certificadora que no tenemos como una organización de confianza aún. Nos pide si aceptamos el certificado o no, o si queremos ver el certificado.

- *Paso12*: Para ver el certificado hacemos clic en ver certificado. Y en la ventana de detalles podremos ver quién es la entidad emisora y si nos fiamos de ella.

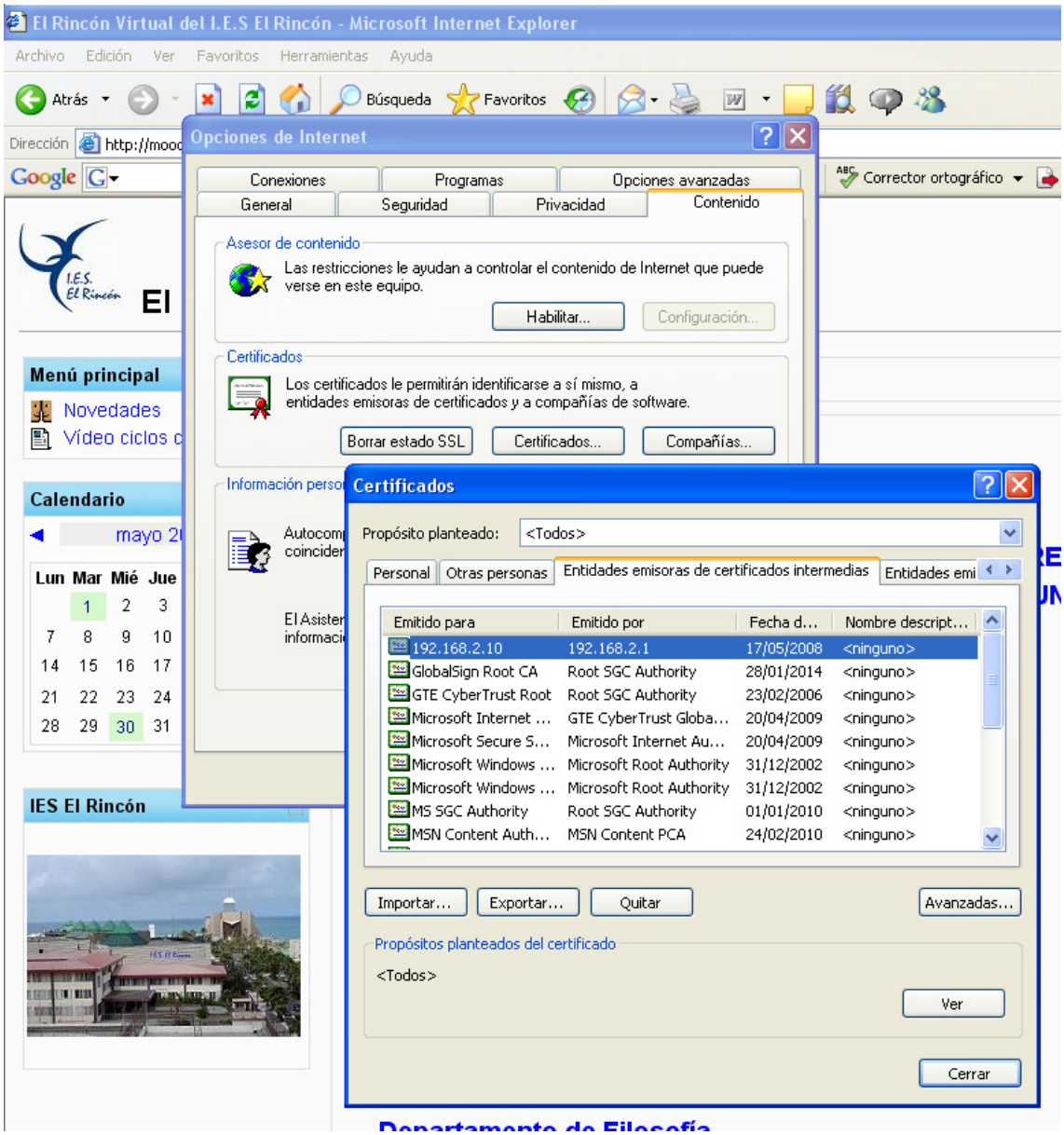


- *Paso13*: Al darle a aceptar volveremos a la ventana anterior y diremos que sí queremos confiar en la entidad emisora con lo cual accederemos al sitio web.

- *Paso 14*: Cierra el navegador y vuelve a entrar a la misma página web. Observarás que te vuelve a salir otra vez la página para preguntarte si confías en la entidad certificadora. Para evitar este proceso puedes instalar el certificado en tu navegador. Para ello, haz clic en ver certificado y posteriormente en la ficha general haz clic en instalar certificado. A partir de ahora ya no te aparecerá la ventana para ver si confías en el emisor del certificado.



- *Paso15*: En cualquier momento puedes ver los certificados instalados en tu navegador y eventualmente borrarlos. Para ello accede desde la barra de menú Herramientas del Internet Explorer a Opciones de Internet, ficha Contenido:



Observarás además que en esta ventana se encuentran los certificados de entidades emisoras que te vienen con el navegador web además de las que has aceptado con el proceso descrito anteriormente.