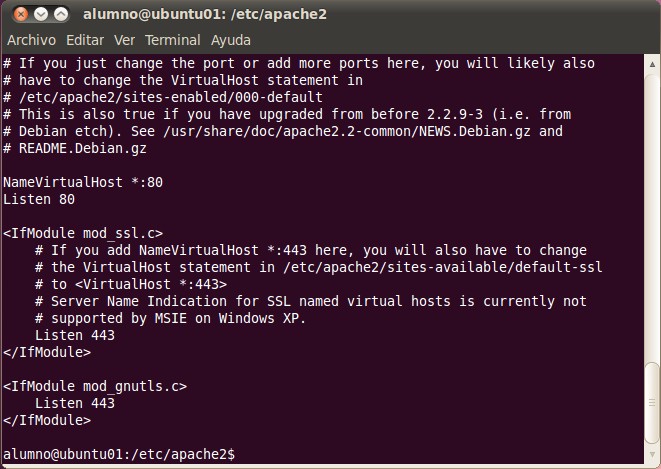
ServidorHTTPSen*Apache*2.2sobre*Linux*

1. Habilita el m´odulo *ssl* que permite usar *https:*

*#****a2enmod ssl***

1. En el archivo que almacena los puertos de escuha /etc/apache2/ports.conf, comprueba la existencia de una directiva <**IfModule**> que incluye la escucha en el Puerto 443 si el modulo SSL está activado .La directiva *<IfModule****nombremodulo****> </IfModule>* permite especificar directivas que se tendr´an en cuenta si el m´odulo indicado est´a cargado.



1. Verificaqueelservidorescuchaenlospuertos80/TCPy443/TCP.

***# netstat -ltn***

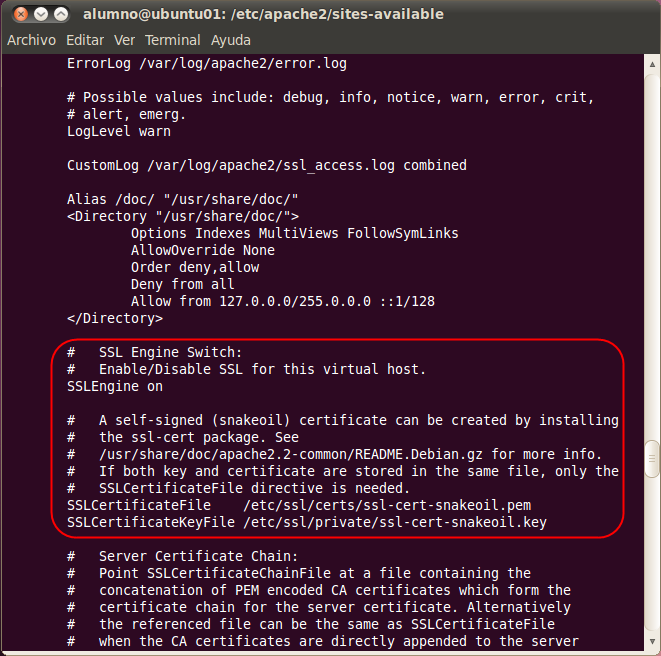
1. Accede al directorio **/etc/apache2/sites-availables** y observa que existe un fichero denominado **default-ssl** que contiene la configuraci´on por defecto de un servidor HTTPS.
2. Habilita el servidor virtual ssl defecto (default-ssl) de *Apache:*

*#* ***a2ensitedefault-ssl***

1. Deshabilita los servidores virtuales si los has creados en prácticas anteriores.
2. Reinicia el servidor para que los cambios tengan efecto.

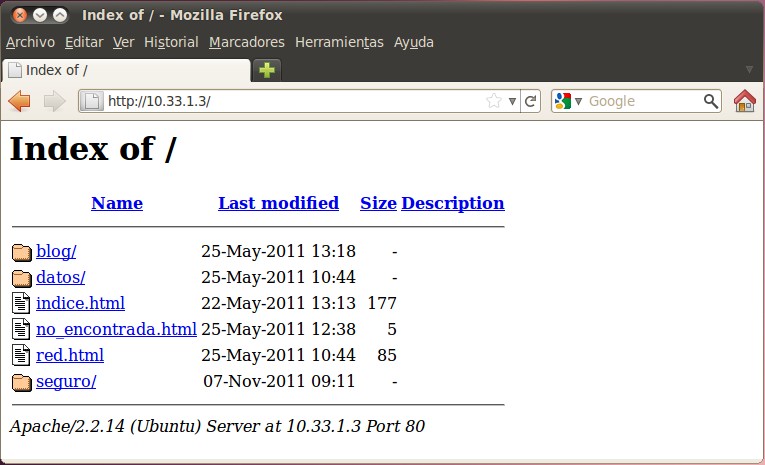
**#service apache2 restart**

1. Consulta el fichero **/etc/apache2/sietes-availabes/default-ssl.conf** y observa su configuraci´on. F´ıjate en las directivas que habilitan SSL y que definen la ruta del certificado digital que usurar´a el servidor, v´easeFigura.



El servidor utilize por defecto un certificado digital autofirmado que se ha creado al instalar *Apache*. Un certificado autofirmado no est´a firmado por una autoridad de certificaci´on (tercera parte de confianza) y por tanto no existen mecanismos autom´aticos que garanticen su autenticidad. Por eso los navegadores nos pedir´an confirmaci´on cuando el servidor se lo env´ıe.

1. Abre el navegador y establece una conexi´on a <http://10.33.X.3>, v´eanse Figuras:

.

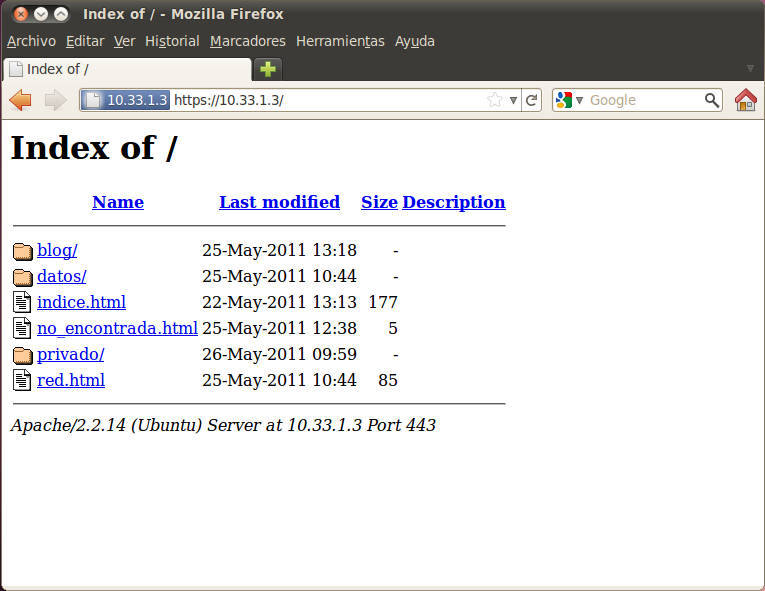
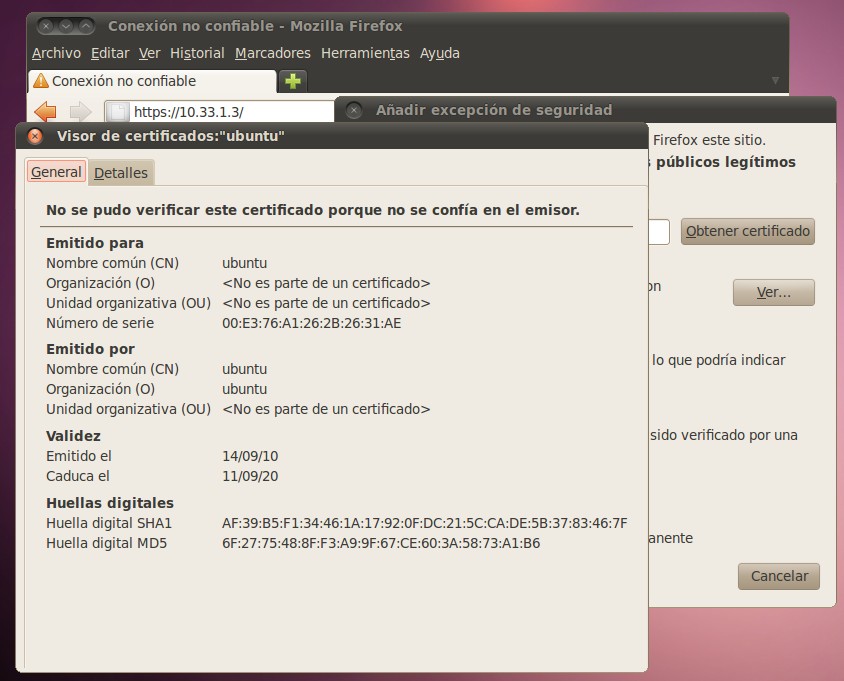


Figura7:Prueba2

2. **Servidor virtual para el dominio** seguro.asirXX.net

2.1. Configura alguno de los servidores DNS instalados en pr´acticas anteriores para que resuelva el nombres **seguro.asirXX.net**. La direcci´on IP asociada ser´a la IP de **ubuntux** es decir 10.33.XX.3.

2.2. Asegu´rate de que **ubuntuXX** utilize el servidor DNS que has configurado.

2.3.Crea eldirectorio**/var/www/seguro**

2.4.Crea el fichero de texto **/var/www/seguro/index.html** con el siguiente c´odigo HTML.

*<html><body>*

*<h1>ESTE ES EL SERVIDOR WEB SEGURO DE AULA DAWXX.NET</h1>*

*</body></html>*

2.5.Crea un certificado digital autofirmado usando openssla. Crea una clave privada RSA de 2048bit.

***# openssl genrsa –out /etc/ssl/private/seguro.key 2048***

Crea el certificado digital autofirmado usando la clave privada.

***# openssl req –new -key /etc/ssl/private/seguro.key –x 509 -days 365 –out /etc/ssl/certs/seguro.pem***

Introducelosdatosdelcertificado,v´easeFigura8.

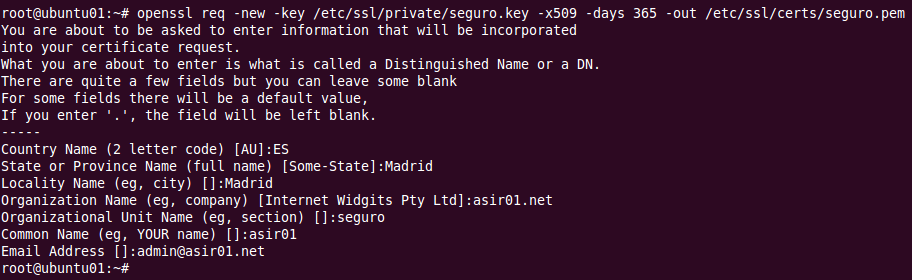


Figura8:Creaci´ondelcertificadoautofirmado

2.6.Creaelfichero**/etc/apache2/site-available/seguro.conf**conlassiguientesdirectivas,v´ease

Figura9.

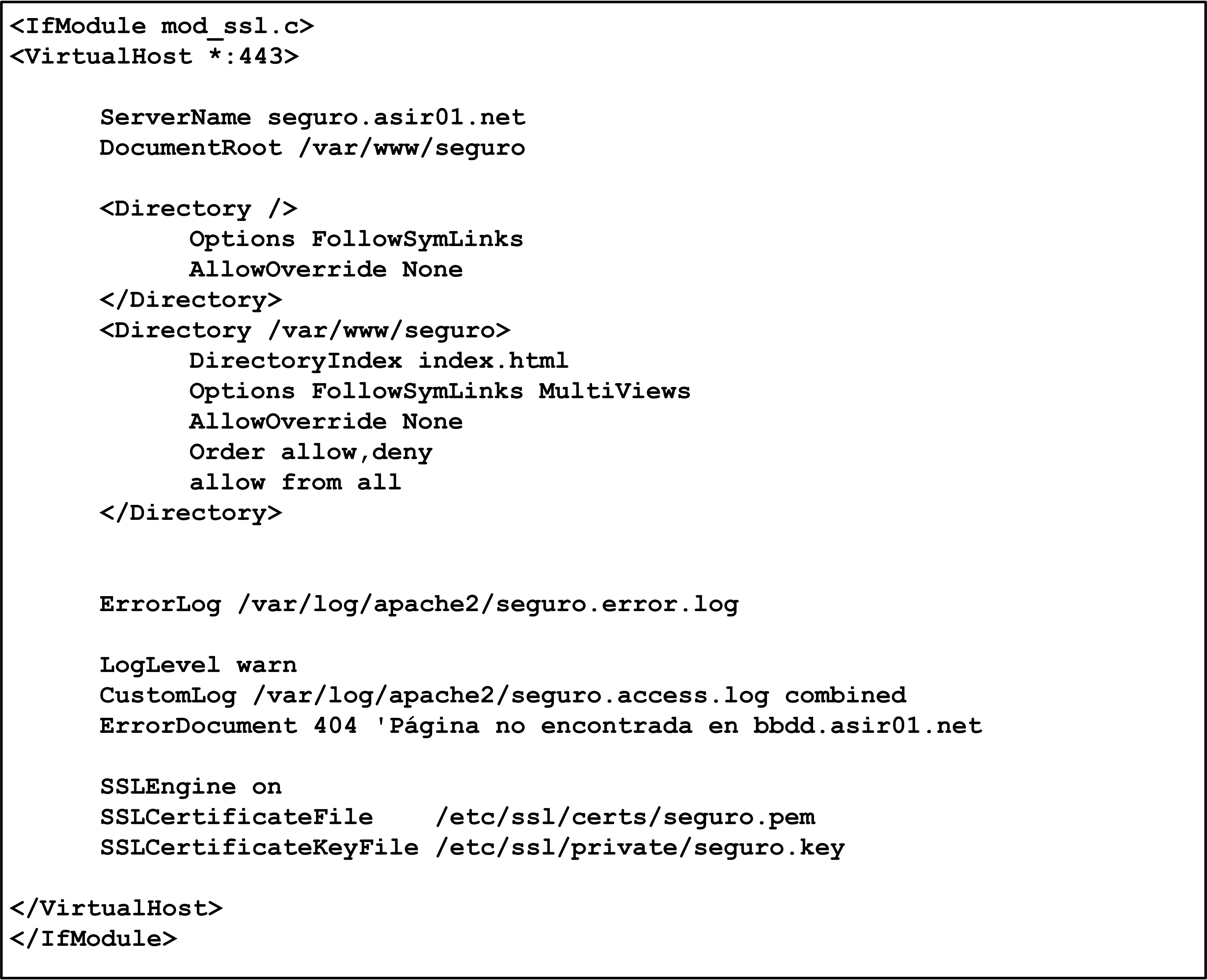


Figura:Ficherodeconfiguraci´ondelservidorseguro

2.7.Deshabilita elservidorsslpordefecto.

***# a2dissitedefault-ssl***

2.8.Habilita el servidor virtual seguro ejecutando el siguiente comando:

***# a2ensite seguro***

2.9.Verifica que dentro del directorio **/etc/apache2/sites-enabled** se ha creado el enlace

**seguro**.

2.10.Reinicia elservidor para que los cambios tengan efecto.

2.11.Abre el navegador y accede a la siguiente URLs para probar el funcionamiento del servidor, <https://seguro.asirXX.net>, v´eanselas Figuras10,11y12.



Figura10:Prueba3

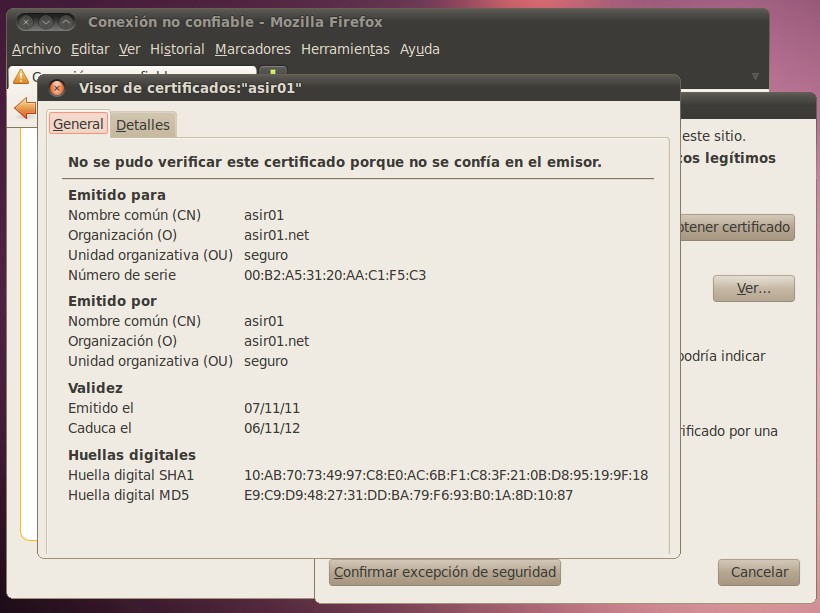


Figura11:Prueba3

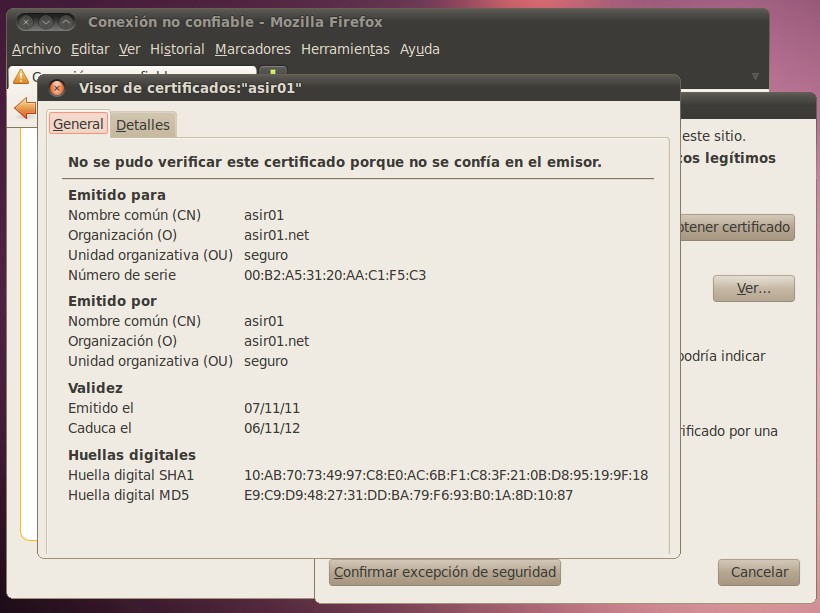


Figura12:Prueba3

*()*