**Práctica Servidor virtual HTTPS en Linux**

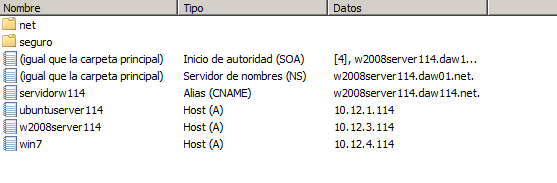
Realiza la siguiente configuración en el servidor Apache instalado en UbuntuServerXX.

* 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 raíız /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.

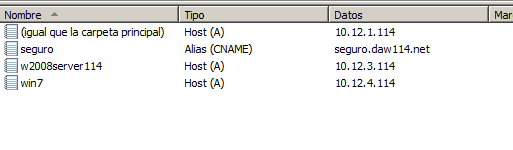
**CONFIGURACIÓN 1: Servidor seguro.daw01.net**

1. Configura el servidor DNS de Windows2008ServerXX para que resuelva el nombre **seguro**. **dawXX.net.** La dirección IP asociada al nombre será la IP de UbuntuServerXX, es decir, 10.12.1.xx



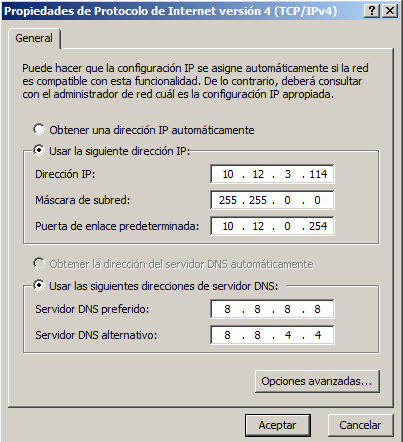
Creamos el nuevo dominio seguro dentro del servidor daw114.net

Figura 1: Configuración del servidor DNS en Windows2008ServerXX



Agregamos Host A para win7 y w2008server dentro del nuevo dominio seguro.daw114.net.

Figura 2: Configuración de red del servidor windows2008



2. Asegúrate que Windows7 utiliza el servidor DNS que has configurado.

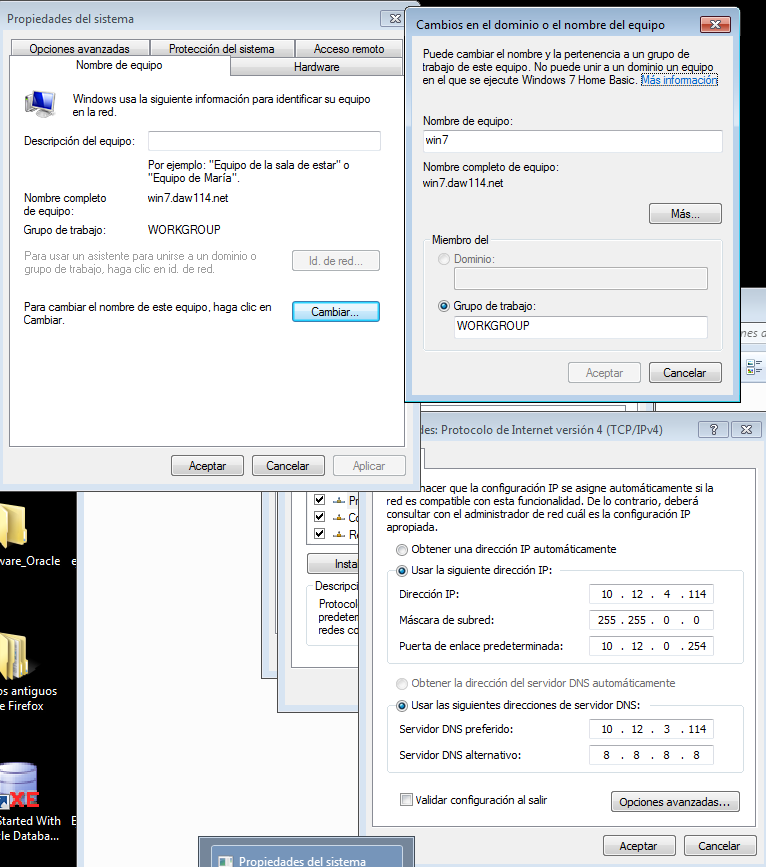


Figura 3: Configuración de red del cliente windows2007

3. Iniciar una sesión en UbuntuServerXX.

4. Crear el directorio /var/www/html/seguro

Sudo mkdir /var/www/html/seguro

5. Crea el fichero de texto /var/www/html/seguro/index.html con el contenido que quieras.

Sudo nano /var/www/html/seguro/index.html

<h1>Este es un sitio seguro </h1>

6. Crea un certificado digital autofirmado usando openssl

6.1. Sitúate en el directorio home del usuario con el que has iniciado sesión.

6.2. Crea una clave privada RSA de 2048 bit

openssl genrsa -out seguro.key 2048

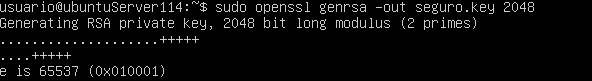




Figura 4: Creación de una clave privada

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:

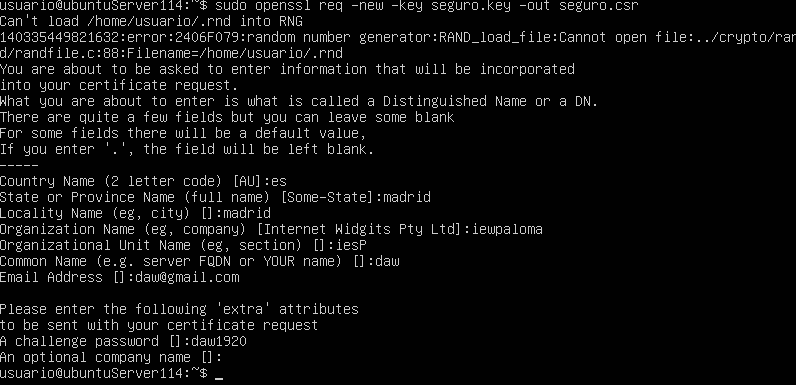




Figura 5: Creación de la solicitud del certificado

Esta solicitud de certificado se podrá 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

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

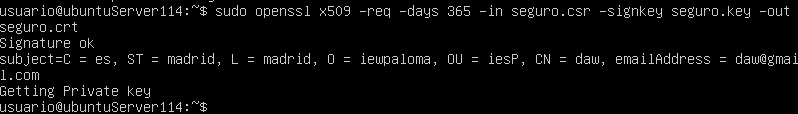


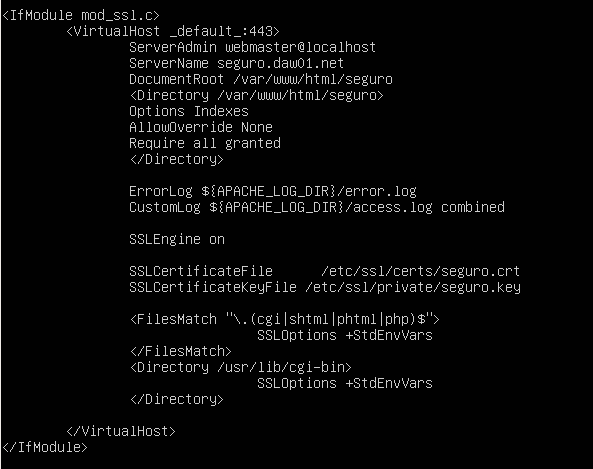


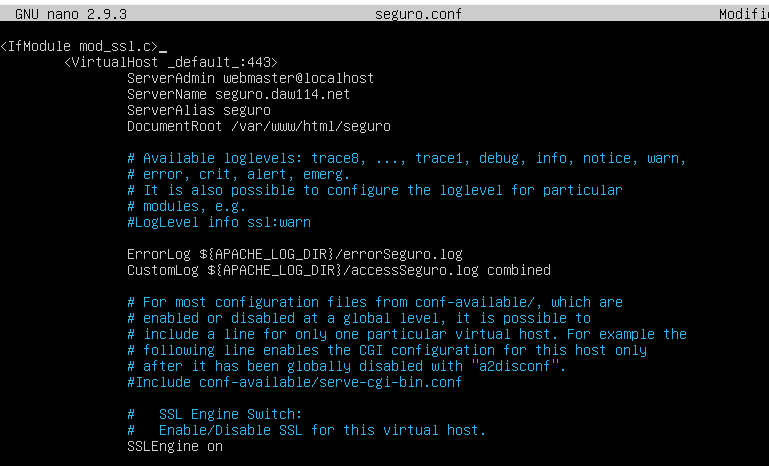
Figura 6: Creación del certificado digital autofirmado

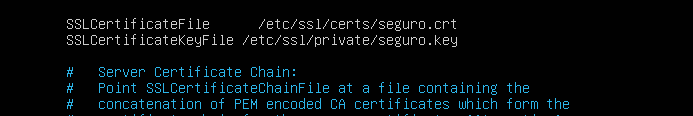
7. Copia la clave y el certificado en los directorios que utiliza por defecto Apache y configura el propietario y el grupo del fichero .key y dale los permisos de lectura y escritura para el usuario y de sólo lectura para el grupo. El fichero tendrá como usuario root y como grupo a ssl-cert. Y para el certificado cambia la propiedad a root:root

|  |
| --- |
|  |

8. Crea el fichero /etc/apache/site-available/seguro con las siguientes directivas:







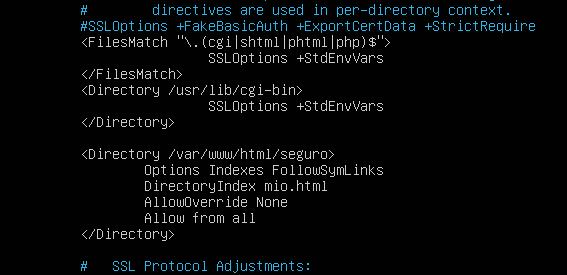
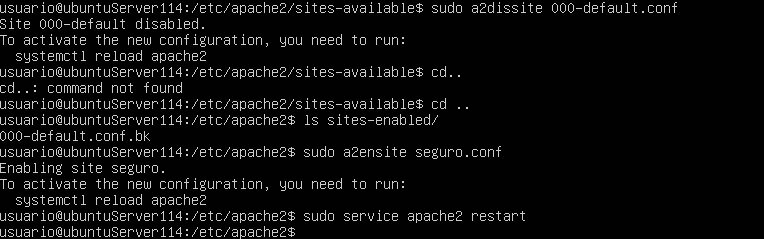
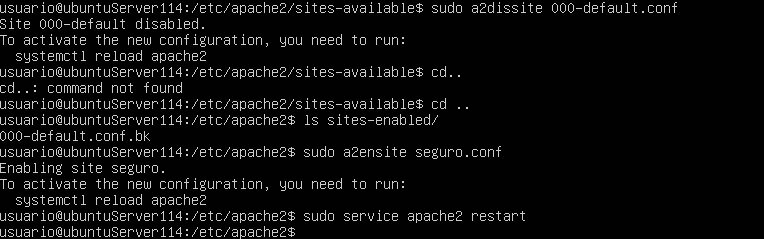


Figura 7: Fichero de configuración del servidor seguro

9. Deshabilita el servidor ssl por defecto.



10. Habilita el servidor virtual seguro.



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



Figura 8: Servidor seguro activo

12. Reinicia el servidor para que los cambios tengan efecto, de todos las formas posibles:

**Sudo service apache2 restart**

Figura 9: reinicio de apache

13. Desde Windows7XX abre el navegador y establece una conexión a https:\\seguro. dawXX.net.



Figura 10: Conexión https desde Windows2007

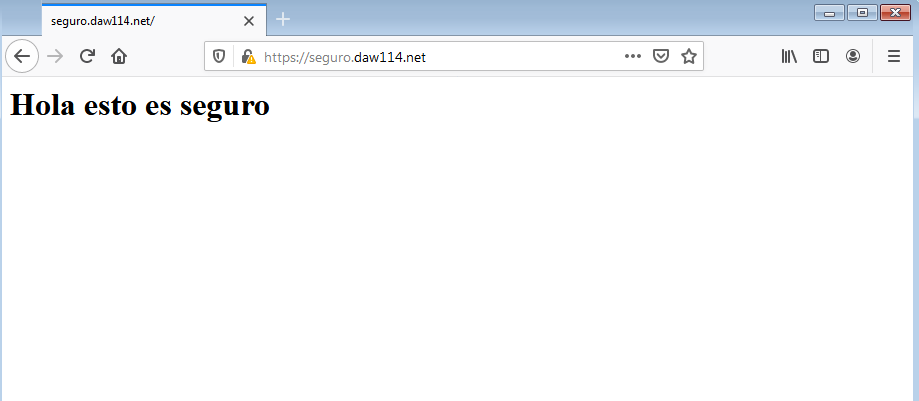


Figura 11: Certificado autofirmado

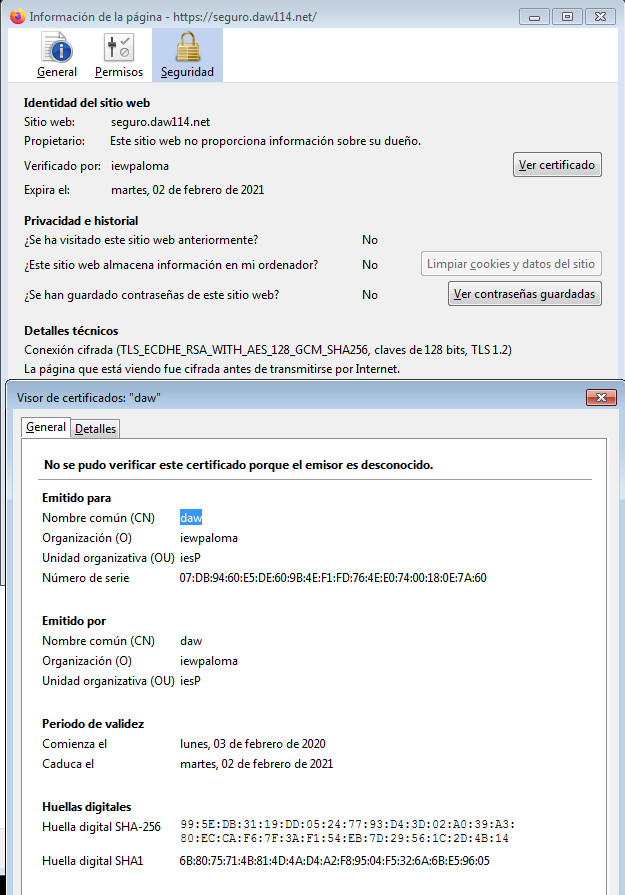


Figura 12: Aceptando los riesgos ...

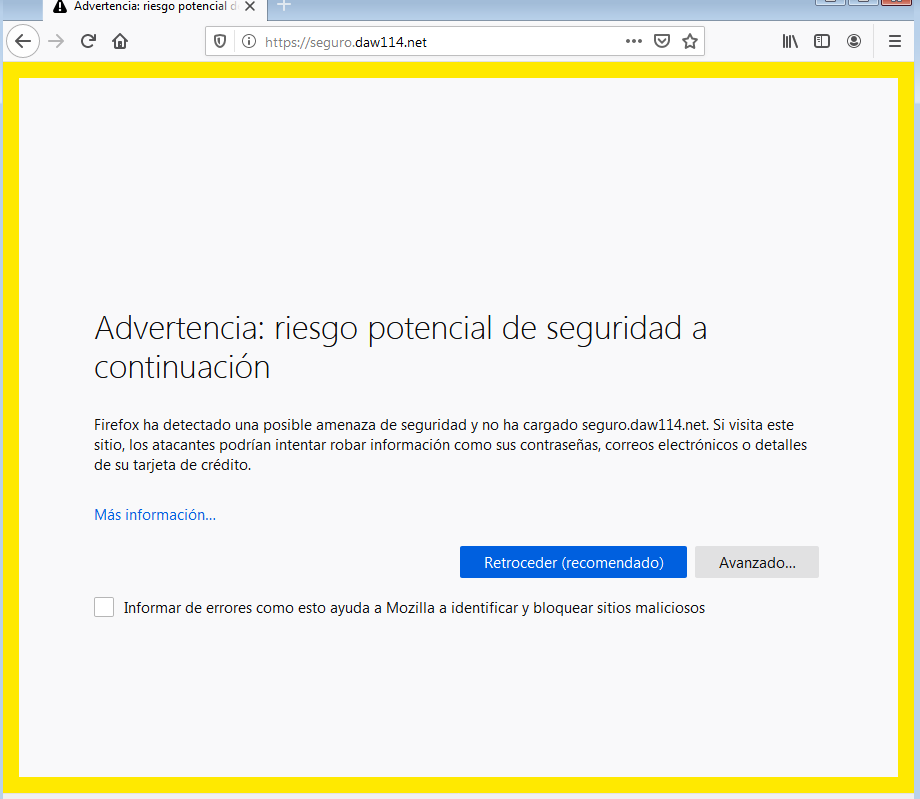


Figura 13: Conexión https desde Windows2007

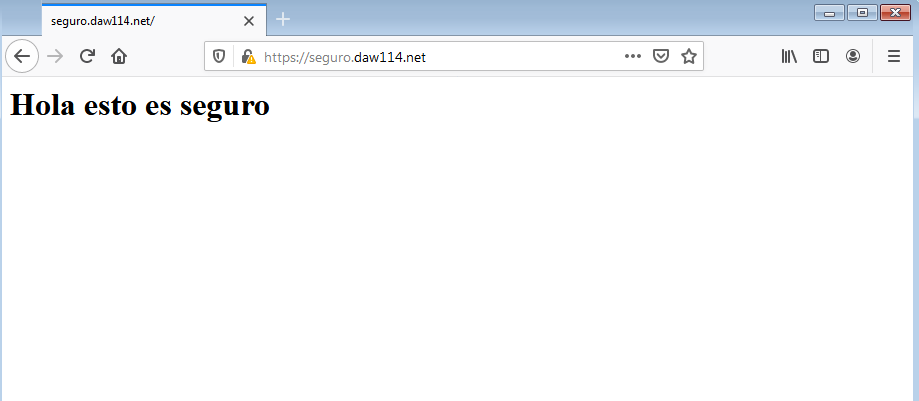
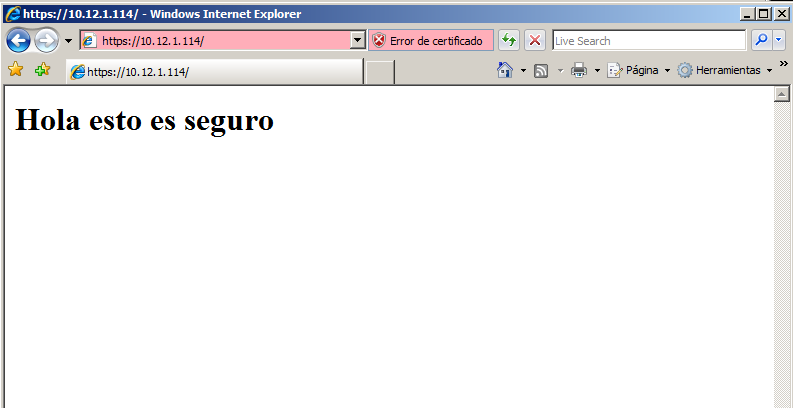


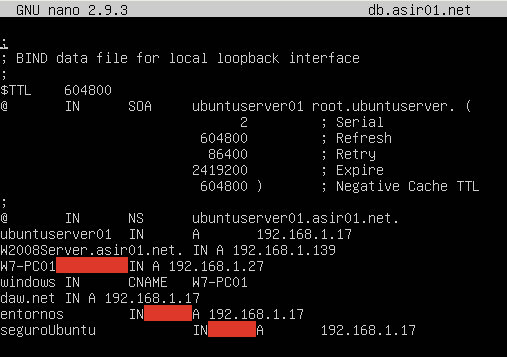
Figura 14: Conexión https desde Windows2008





**CONFIGURACIÓN 2: Servidor seguroUbuntu.asir01.net**

1. Configura el servidor DNS de UbunruServerXX para que resuelva el nombre **seguroUbuntu**. **asirXX.net.** La dirección IP asociada al nombre será la IP de UbuntuServerXX, es decir, 10.12.1.xx



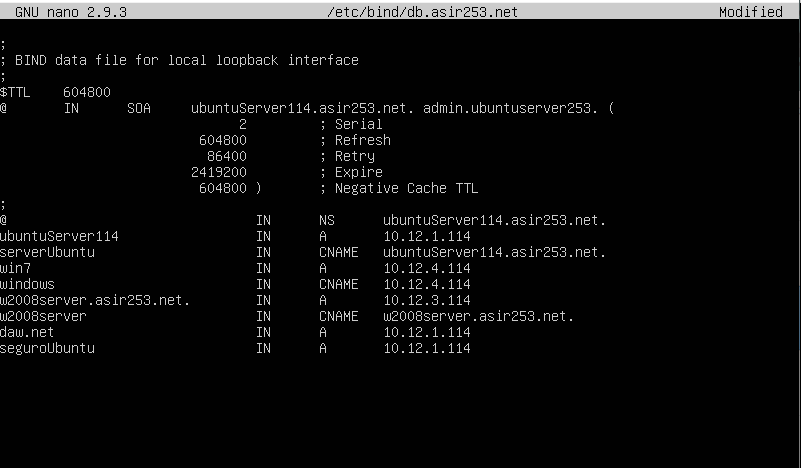
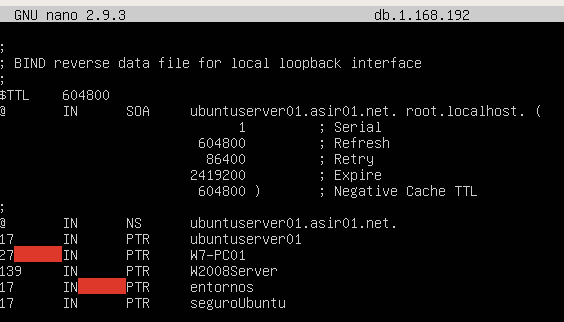


Figura 2.1: Fichero de zona directa para el dominio asir01.net



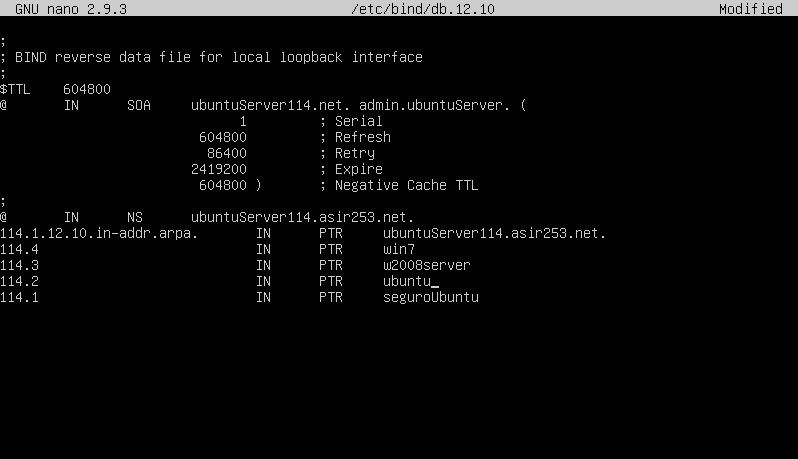


Figura 2.2: Fichero de zona inversa para el dominio 1.168.192.in-addr.arpa.



Figura 2.3: Reinicio servidor DNS (bind9)

2. Configurar el cliente DNS de Windows7 para que utilice el servidor DNS que has configurado (modificar IP del DNS y sufijo de red).

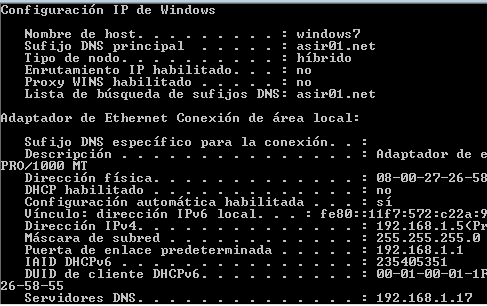


Figura 2.4: Configuración cliente Windows2007

3.- Crear la carpeta seguroUbuntu dentro del DocumentRoot y un fichero a servir por defecto:

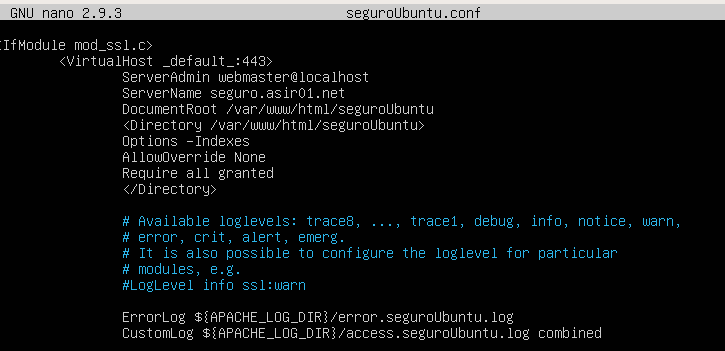
Sudo mkdir /var/www/html/ubuntuSeguro

Sudo nano /var/www/html/ubuntuSeguro/index.html

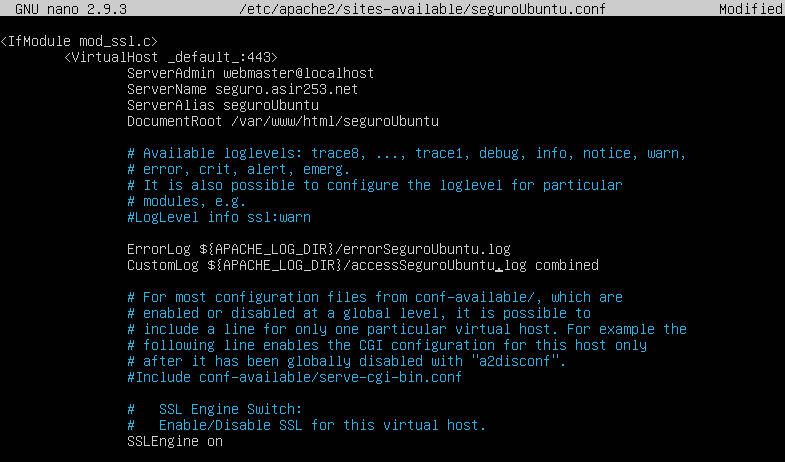
Figura 2.5: Configuración del DocumentRoot del nuevo sitio a servir.

4.- Crear el sitio seguroUbuntu.





Sugerencia: se puede copiar el fichero seguro.conf y modificar el nombre del sitio, el DocumentRoot, fichero de errores y accesos, etc.





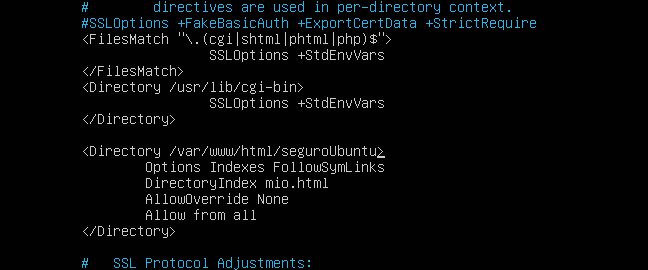


Figura 2.6: Configuración del sitio seguroUbuntu

5.- Deshabilitar el sitio seguro, habilitar seguroUbuntu y recargar apache.

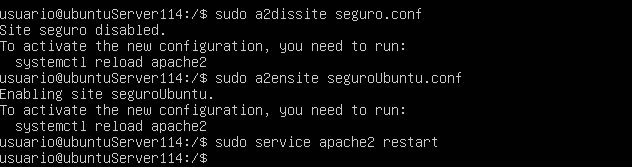


Figura 2.7: Activación del sitio seguroUbuntu y de apache.

6.- Comprobación desde el cliente Windows 2007

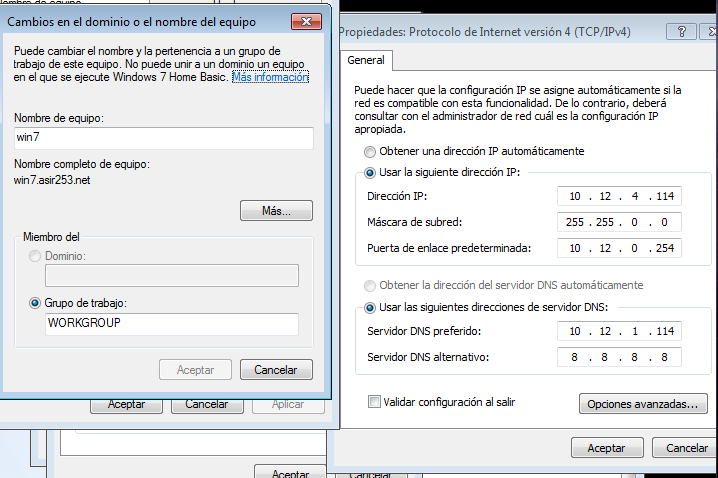
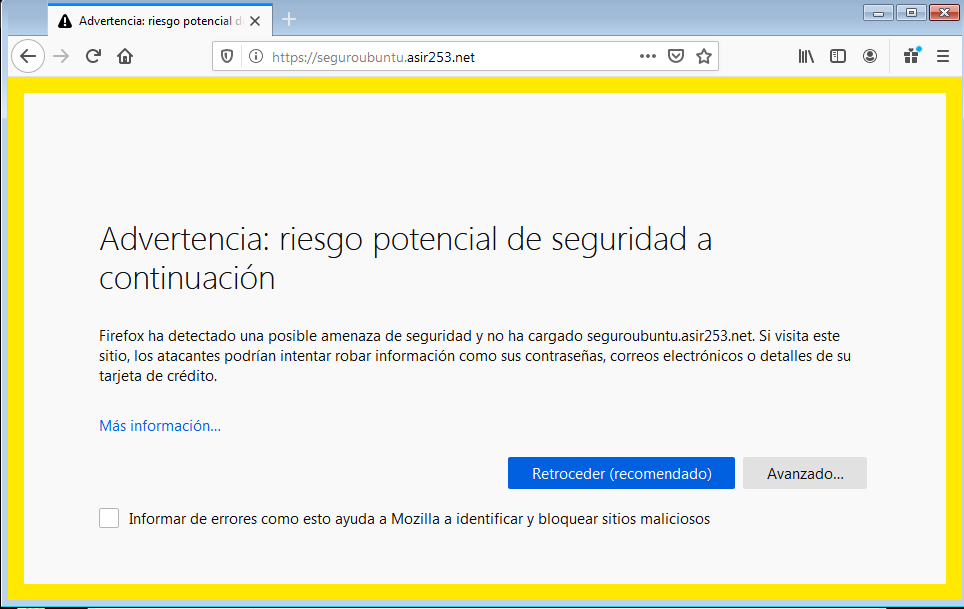


Figura 2.8: Petición desde la máquina de Windows2007



Figura 2.9: Petición desde la máquina de Windows2007



¿Qué operación se ha hecho en el servidor de ubuntu, para que muestre esta página?

Desde cualquier máquina que no sea la de Windows2007, ¿podremos acceder al servidor seguro que acabamos de configurar?. Indicar cómo.

**Deberíamos cambiar el servidor DNS y tanto el dominio como la IP del servidor y en ciertos casos abrir los puertos del firewall para que permita la conexión.**