

**Alumno/a: José Manuel González Peña**

## **PRÁCTICA 6: Crear un servidor Web virtual seguro.**

- Objetivo: Crear servidores web seguros.

- Procedimiento:

Será necesario que los servicios DHCP y DNS configurados en las prácticas anteriores están levantados.

Nota: si aún no tienes configurado el servicio DNS, usa el ficheros de hosts

[http://es.wikipedia.org/wiki/Archivo\\_hosts](http://es.wikipedia.org/wiki/Archivo_hosts)

Webgrafía: Configuración Apache seguro

- [Tutorial de configuración de Certificados SSL de Cliente](#)

- Curso [Servicios Linux](#): Instalación y configuración de OpenSSL (página 50) , 57-62

- [Editorial ENI: Configuración Apache SSL](#)

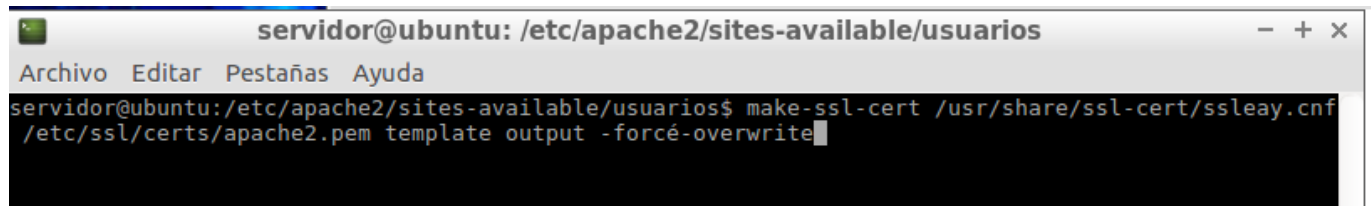
Entidades Certificadoras. Web Seguras:

- SSL y Certificados: <http://tldp.org/HOWTO/SSL-Certificates-HOWTO/x64.html>

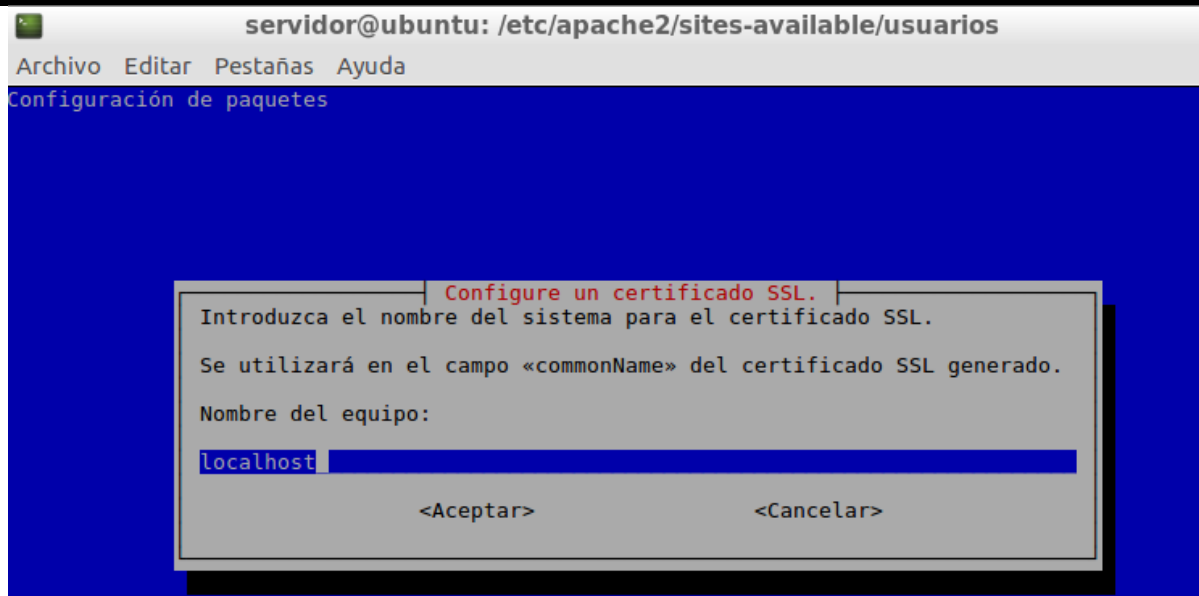
- Ceres, entidad pública de certificación española: <http://www.cert.fnmt.es/certificados>

En esta bibliografía encontrareis al menos dos modos de generar el certificado autofirmado: con make-ssl-cert (solo genera fichero con certificado) y con openssl (genera certificado y clave pública)

# make-ssl-cert /usr/share/ssl-cert/ssleay.cnf /etc/ssl/certs/apache2.pem template output -force-overwrite



```
servidor@ubuntu: /etc/apache2/sites-available/usuarios
Archivo Editar Pestañas Ayuda
servidor@ubuntu:/etc/apache2/sites-available/usuarios$ make-ssl-cert /usr/share/ssl-cert/ssleay.cnf /etc/ssl/certs/apache2.pem template output -force-overwrite
```



servidor@ubuntu: /etc/apache2/sites-available/usuarios

Archivo Editar Pestañas Ayuda

Configuración de paquetes

**Configure un certificado SSL.**

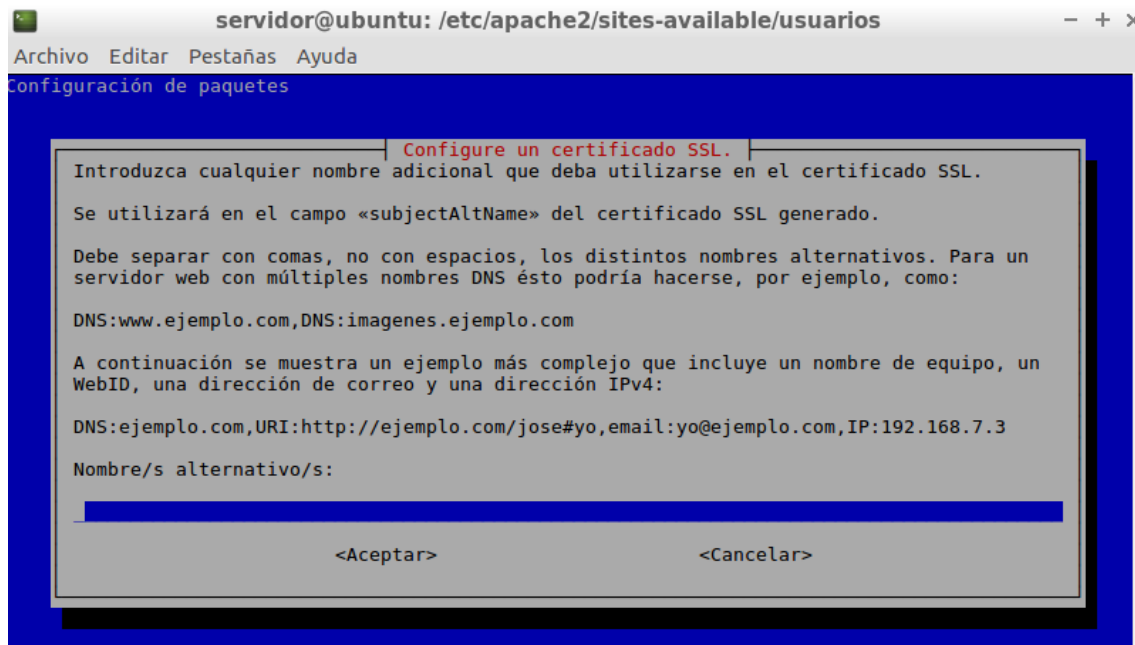
Introduzca el nombre del sistema para el certificado SSL.

Se utilizará en el campo «commonName» del certificado SSL generado.

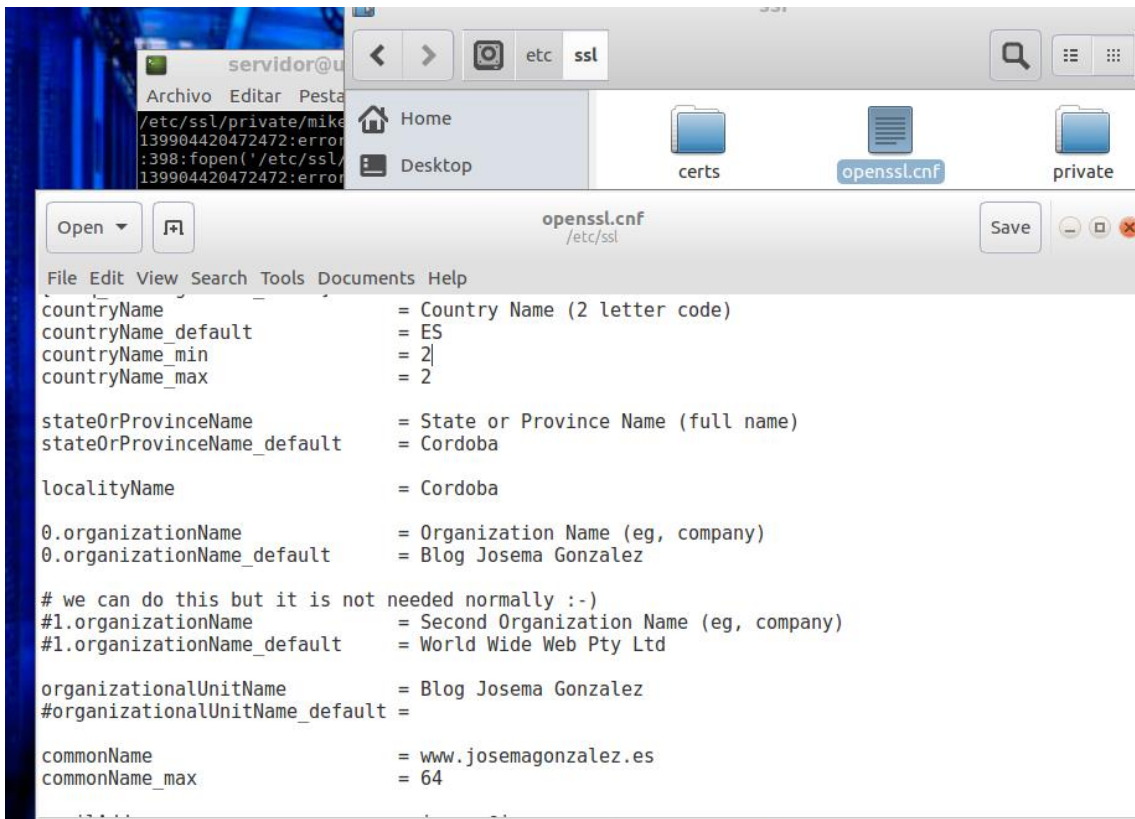
Nombre del equipo:

localhost

<Aceptar> <Cancelar>

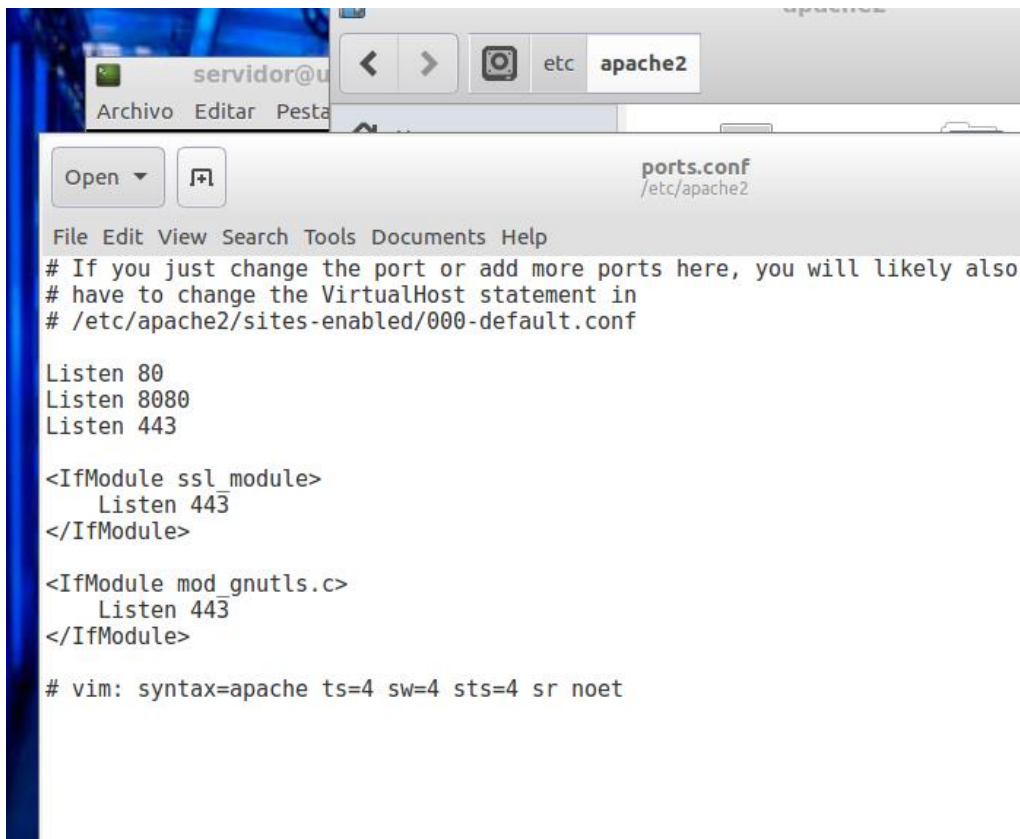


```
# openssl req -new -x509 -nodes -out /etc/ssl/certs/despliegue/micertificado.crt -keyout /etc/ssl/private/despliegue/mikey.key
```



```
servidor@ubuntu:/etc/apache2/sites-available/usuarios$ sudo openssl req -new -x509 -nodes -out /etc/ssl/certs/micertificado.crt -keyout /etc/ssl/private/mikey.key
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to '/etc/ssl/private/mikey.key'
-----
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) [ES]:ES
State or Province Name (full name) [Cordoba]:Cordoba
Cordoba []:Cordoba
Organization Name (eg, company) [Blog Josema Gonzalez]:Blog de Josema
Blog Josema Gonzalez []:Blog de Josema Gonzalez
www.josemagonzalez.es []:www.josemagonzalez.es
josema@josema.com []:josema@josema.es
servidor@ubuntu:/etc/apache2/sites-available/usuarios$ sudo service apache2 restart
```

Ponemos en el archivo de ports.conf que escuche por el puerto seguro



```
servidor@u
Archivo  Editar  Pesta
ports.conf
/etc/apache2
File Edit View Search Tools Documents Help
# 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
Listen 8080
Listen 443

<IfModule ssl_module>
    Listen 443
</IfModule>

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

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

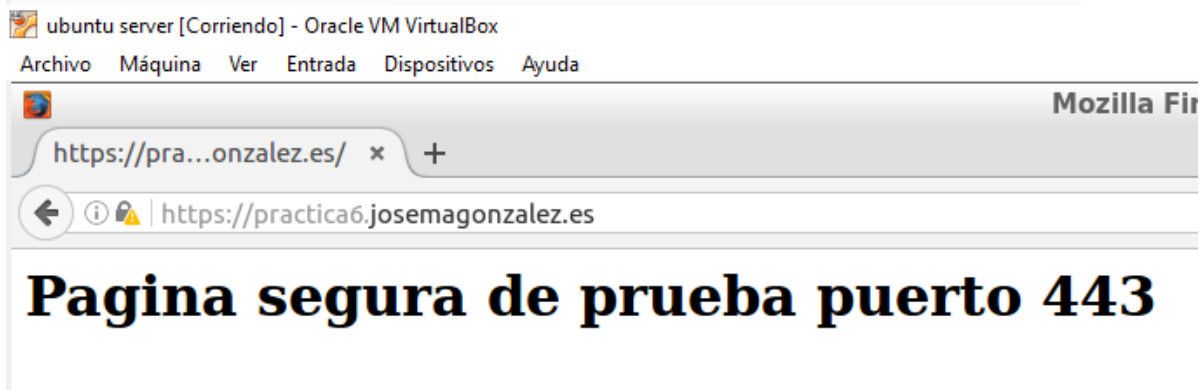
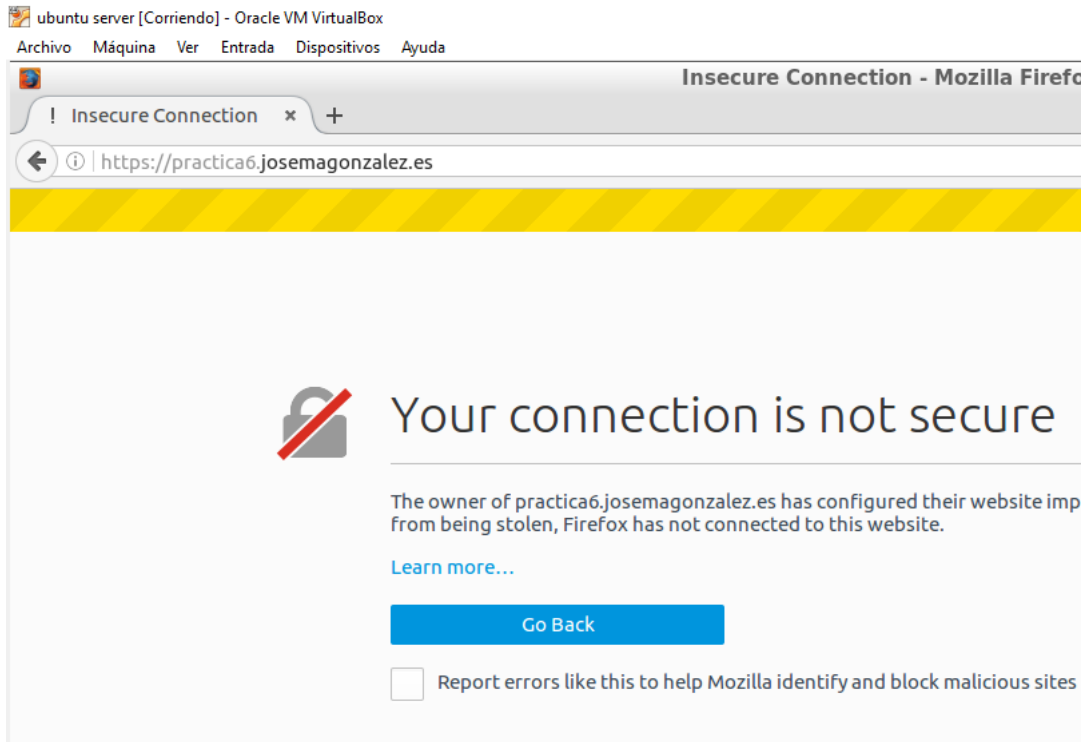
1. Describe con tus palabras:

- ¿Qué es un servidor web seguro?

Es un servidor de páginas web que asegura que el tráfico de datos está encriptado entre el cliente y el servidor.

Con esto nos aseguramos que en caso de interceptar el tráfico otra persona no pueda acceder a nuestros datos.

## 2.1. Haz una captura de pantalla, tanto de forma segura (https): https://IPdelservidorwebvirtual



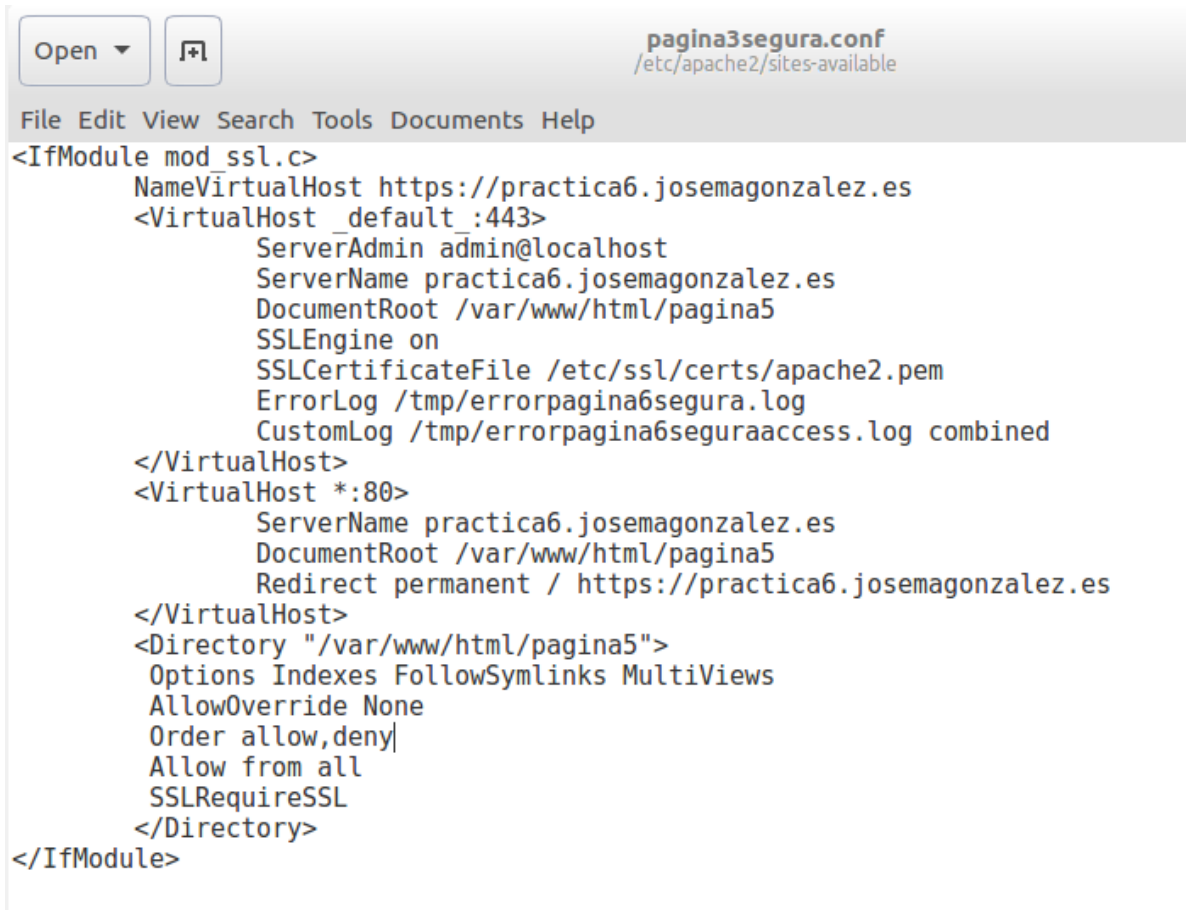
## como de forma 'insegura' (http): http://IPdelservidorwebvirtual



¿Qué ocurre? ¿Cuál está funcionando correctamente y cuál no?  
Me manda a la página por defecto de mi servidor

2.2. Forzar ahora que lo anterior funcione, es decir, aunque se acceda de modo no seguro (http) hacer que se pase a modo seguro (https). Usar para ello Redirect de modo que al acceder por http automáticamente te redirija a https

<http://www.jdbaldoma.net/2012/05/redirigir-una-conexion-segura-https-en.html>



```
<IfModule mod_ssl.c>
    NameVirtualHost https://practica6.josemagonzalez.es
    <VirtualHost _default_:443>
        ServerAdmin admin@localhost
        ServerName practica6.josemagonzalez.es
        DocumentRoot /var/www/html/pagina5
        SSLEngine on
        SSLCertificateFile /etc/ssl/certs/apache2.pem
        ErrorLog /tmp/errorpagina6segura.log
        CustomLog /tmp/errorpagina6seguraaccess.log combined
    </VirtualHost>
    <VirtualHost *:80>
        ServerName practica6.josemagonzalez.es
        DocumentRoot /var/www/html/pagina5
        Redirect permanent / https://practica6.josemagonzalez.es
    </VirtualHost>
    <Directory "/var/www/html/pagina5">
        Options Indexes FollowSymlinks MultiViews
        AllowOverride None
        Order allow,deny
        Allow from all
        SSLRequireSSL
    </Directory>
</IfModule>
```

Como intento entrar a <http://practica6.josemagonzalez.es> me redirige a la página segura directamente.

