

## CONFIGURACION DEL SERVIDOR APACHE2 EN LINUX MINT

**Requisitos previos:** Tener instalado un sistema de virtualización en este caso VirtualBox y tener a disposición los siguientes sistemas Windows 7, Linux Mint y pfSense

**Descripción de la práctica:** Instalar Apache2 en Linux Mint, crear páginas, establecer accesos seguros y hacer que las paginas sean seguras bajo SSL.

**Descripción de Hardware:** Equipo real, Intel Core i7 con 16GB de RAM y 199GB de disco duro

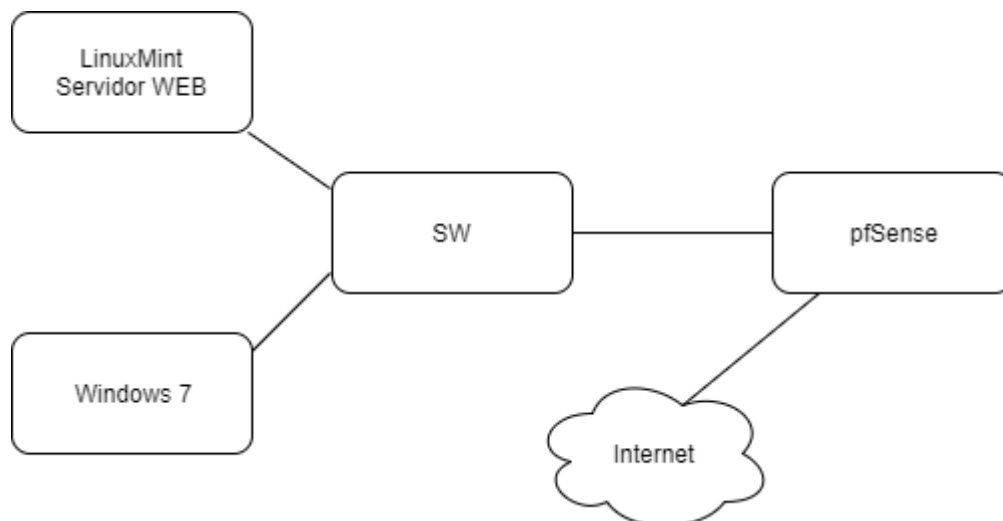
### *Esquema de la Red*

#### **Rangos de direcciones:**

192.168.99.9 –Linux Mint

192.168.99.1 – pfSense

192.168.99.12 – Windows 7

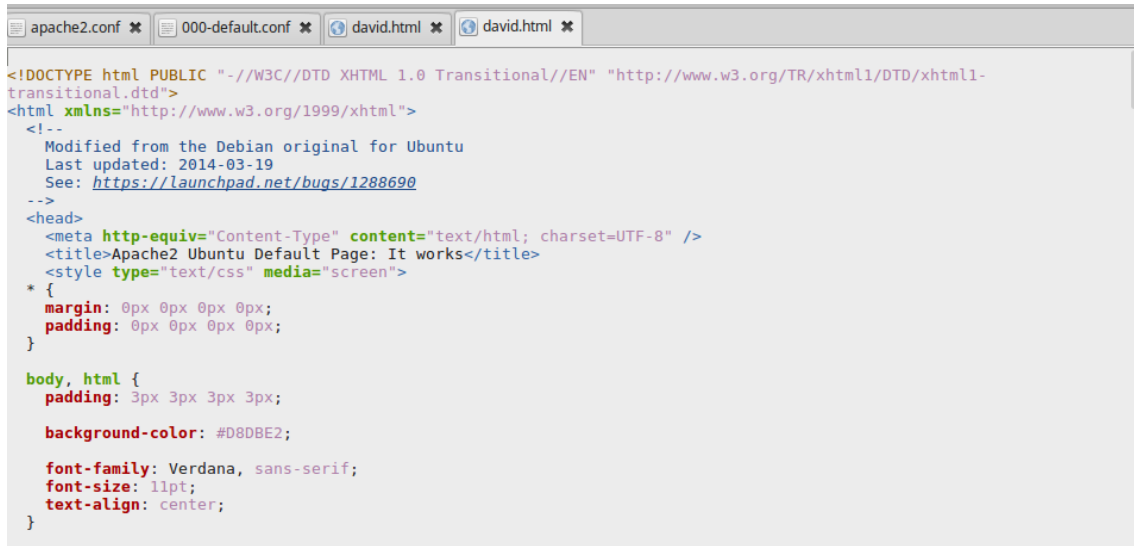


## CONFIGURACION DEL SERVIDOR APACHE2 EN LINUX MINT

Lo primero que debemos hacer es ejecutar apt-get update y acto seguido instalar el servidor apache2 con apt-get install apache2.

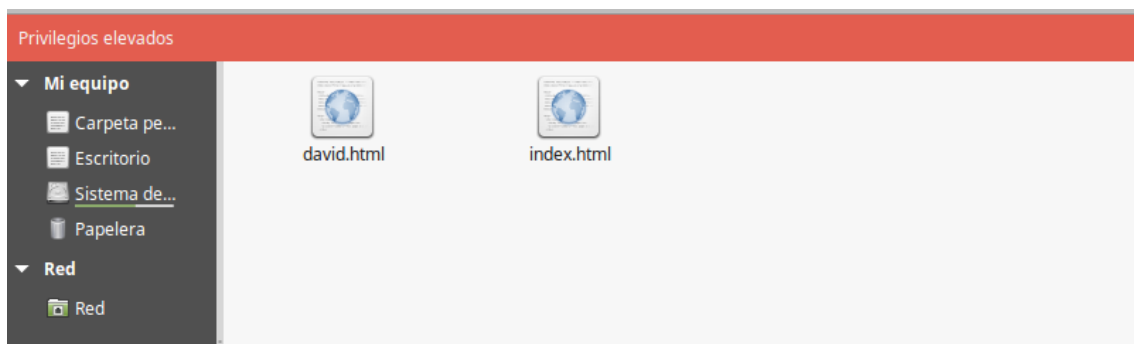
El servidor quedará instalado y por defecto nos mostrará la página de inicio de apache alojada en /etc/var/www/html

Ahora alojaremos una segunda pagina en el directorio que será nuestra nueva pagina de inicio.



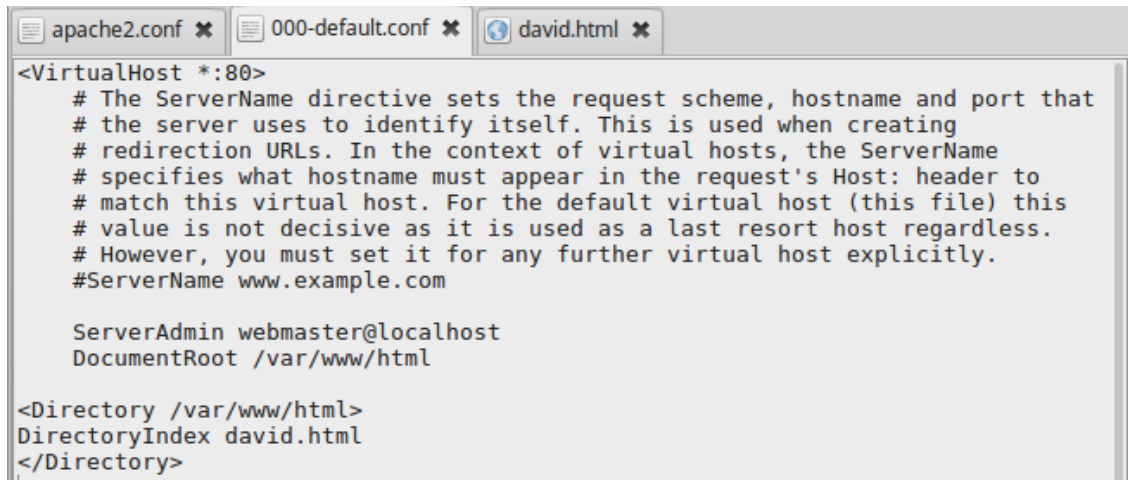
```
apache2.conf 000-default.conf david.html david.html
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<!--
  Modified from the Debian original for Ubuntu
  Last updated: 2014-03-19
  See: https://launchpad.net/bugs/1288690
-->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Apache2 Ubuntu Default Page: It works</title>
<style type="text/css" media="screen">
* {
  margin: 0px 0px 0px 0px;
  padding: 0px 0px 0px 0px;
}
body, html {
  padding: 3px 3px 3px 3px;
  background-color: #D8DBE2;
  font-family: Verdana, sans-serif;
  font-size: 11pt;
  text-align: center;
}
```

Y la guardamos en /www/html



## CONFIGURACION DEL SERVIDOR APACHE2 EN LINUX MINT

Por ultimo modificaremos el fichero `/etc/apache2/sites-enabled` y cambiaremos el index por defecto del servidor actual.



```
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

<Directory /var/www/html>
    DirectoryIndex david.html
</Directory>
```

Con esta ultima configuracion, el servidor por defecto mostrará la pagina david.html alojada en `/var/www/html`, solo quedaría reiniciar el servicio `service apache2 restart`

Ahora vamos a hacer visible la pagina desde la red WAN, añadiremos una regla NAT en pfSense

### Firewall: NAT: Port Forward: Edit



Edit Redirect entry	
Disabled	<input type="checkbox"/> <b>Disable this rule</b> Set this option to disable this rule without removing it from the list.
No RDR (NOT)	<input type="checkbox"/> <b>Enabling this option will disable redirection for traffic matching this rule.</b> Hint: this option is rarely needed, don't use this unless you know what you're doing.
Interface	WAN ▾ Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.
Protocol	TCP ▾ Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.
Source	Advanced - Show source address and port range
Destination	<input type="checkbox"/> <b>not</b> Use this option to invert the sense of the match. Type: WAN address ▾ Address: <input type="text"/> / <input type="text"/> ▾
Destination port range	from: HTTP ▾ <input type="text"/> to: HTTP ▾ <input type="text"/> Specify the port or port range for the destination of the packet for this mapping. Hint: you can leave the 'to' field empty if you only want to map a single port
Redirect target IP	192.168.99.9 Enter the internal IP address of the server on which you want to map the ports. e.g. 192.168.1.12
Redirect target port	HTTP ▾ <input type="text"/> Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). Hint: this is usually identical to the 'from' port above
Description	<input type="text"/> You may enter a description here for your reference (not parsed).
No XMLRPC Sync	<input type="checkbox"/> Hint: This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.
NAT reflection	Use system default ▾

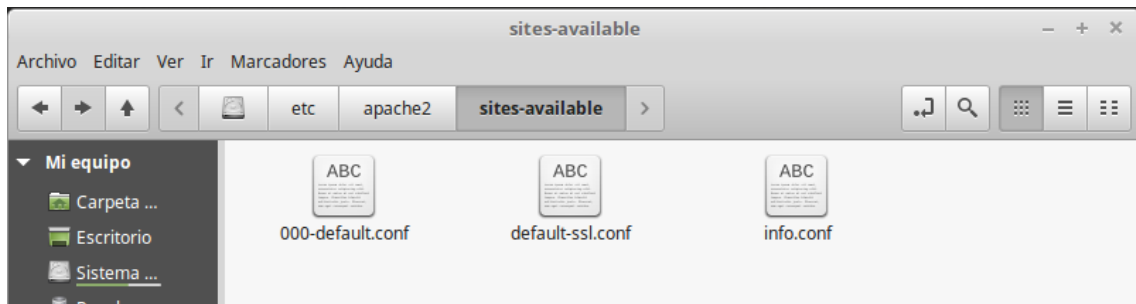
## CONFIGURACION DEL SERVIDOR APACHE2 EN LINUX MINT

Continuamos con la configuración de Apache2 en Linux Mint

Creamos el siguiente árbol de carpetas y ficheros, dentro de /var/www crearemos la carpeta INFO donde estara la pagina inicio.html, tambien crearemos la carpeta privado donde estara privado.html.

```
servicios-VirtualBox www # tree
.
├── html
│   ├── david.html
│   └── index.html
├── info
│   ├── inicio.html
│   └── privado
│       └── privado.html
└── 3 directories, 4 files
```

Ahora haremos una copia del fichero 000-default.conf y lo renombramos como info.conf, este fichero contendrá la configuración del sitio info.



Editamos la configuración de info.conf, establecemos inicio.html como página principal, y el ServerName www.info.com

```
info.conf (/etc/apache2/sites-enabled)
Archivo Editar Ver Buscar Herramientas Documentos Ayuda
Privilegios Elevados
<VirtualHost *:80>
    ServerName www.info.com
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/info

    <Directory /var/www/info>
        DirectoryIndex inicio.html
    </Directory>

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

</VirtualHost>
```

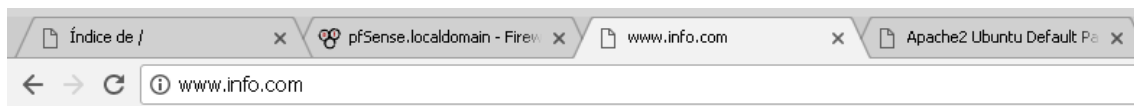
## CONFIGURACION DEL SERVIDOR APACHE2 EN LINUX MINT

Ahora ejecutaremos el comando “a2ensite info” para habilitar el nuevo sitio y reiniciamos el servicio.

Añadimos [www.info.com](http://www.info.com) al fichero hosts y reiniciamos el servicio apache2

```
servicios@servicios-VirtualBox ~ $ cat /etc/hosts
127.0.0.1    localhost
127.0.1.1    servicios-VirtualBox
#127.0.1.1    www.info.com
# The following lines are desirable for IPv6 capable hosts
::1         ip6-localhost ip6-loopback
fe00::0     ip6-localnet
ff00::0     ip6-mcastprefix
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
192.168.99.2 www.info.com
```

ahora la página web será accesible desde el navegador colocando [www.info.com](http://www.info.com)



### Pagina inicio.html alojada en la carpeta INFO

Ahora modificamos el info.conf añadiendo el directorio privado. e introducimos las restricciones, solo se podrá acceder desde el W7 y localhost.

```
<VirtualHost *:80>
    ServerName www.info.com
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/info

    <Directory /var/www/info>
        DirectoryIndex inicio.html
    </Directory>

    #Establecer directorio privado y restringir el acceso IP
    <Directory /var/www/info/privado>
        DirectoryIndex privado.html
        <RequireAny>
            Require local
            Require ip 192.168.99.12
        </RequireAny>
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

## CONFIGURACION DEL SERVIDOR APACHE2 EN LINUX MINT

Reiniciamos el servicio y entrarán en funcionamiento las restricciones añadidas, continuamos añadiendo restricciones esta vez, serán de usuario y contraseña.

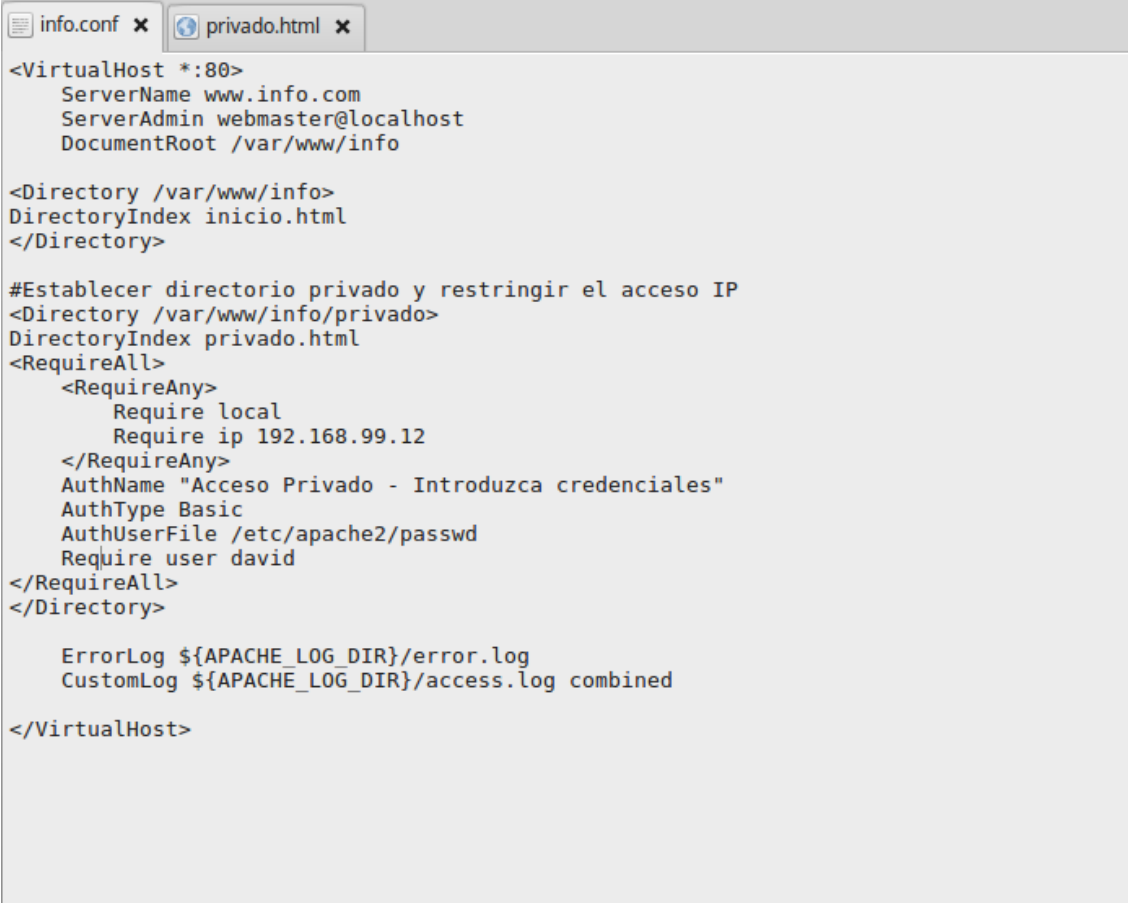
El primer paso para restringir el acceso a usuarios es añadir los usuarios del servidor.

```
servicios-VirtualBox servicios # htpasswd -c /etc/apache2/passwd david
New password:
Re-type new password:
Adding password for user david
```

Utilizaremos el atributo -c solo para el primer usuario.

```
servicios-VirtualBox servicios # htpasswd /etc/apache2/passwd pepe
New password:
Re-type new password:
Adding password for user pepe
```

Volvemos a editar el fichero de info.conf y añadimos los AuthName,AuthType y AutUserFile también el require user david



```
info.conf x privado.html x
<VirtualHost *:80>
    ServerName www.info.com
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/info

    <Directory /var/www/info>
        DirectoryIndex inicio.html
    </Directory>

    #Establecer directorio privado y restringir el acceso IP
    <Directory /var/www/info/privado>
        DirectoryIndex privado.html
        <RequireAll>
            <RequireAny>
                Require local
                Require ip 192.168.99.12
            </RequireAny>
            AuthName "Acceso Privado - Introduzca credenciales"
            AuthType Basic
            AuthUserFile /etc/apache2/passwd
            Require user david
        </RequireAll>
    </Directory>

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

</VirtualHost>
```

Ejecutamos a2ensite y service apache2 reload para poner en funcionamiento esta configuración, ahora la pagina solo será accesible desde localhost,W7 y usuario autenticado.

## CONFIGURACION DEL SERVIDOR APACHE2 EN LINUX MINT

Por último vamos a añadirle SSL al sitio info.com, lo primero que tenemos que hacer es descargar el paquete OpenSSL con *apt-get install openssl*, después crearemos la carpeta */etc/ssl/localcerts* y generamos la clave

```
servicios@servicios-VirtualBox /etc/ssl $ sudo mkdir localcerts
servicios@servicios-VirtualBox /etc/ssl $ sudo openssl req -new -x509 -days 365 -nodes -out /etc/ssl/localcerts/apache.crt -keyout /etc/ssl/localcerts/apache.key
Generating a 2048 bit RSA private key
.....+++++
writing new private key to '/etc/ssl/localcerts/apache.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) [AU]:34
State or Province Name (full name) [Some-State]:Vizcaya
Locality Name (eg, city) []:Bilbao
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Elorrieta
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
servicios@servicios-VirtualBox /etc/ssl $ sudo chmod 600 /etc/ssl/localcerts/apache*
servicios@servicios-VirtualBox /etc/ssl $
```

Ahora habilitaremos el módulo SSL con *a2enmod ssl*

```
servicios@servicios-VirtualBox /etc/ssl $ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
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
servicios@servicios-VirtualBox /etc/ssl $ service apache2 restart
```

Ahora editamos la configuración de *default-ssl.conf* en *sites-available* escogiendo la ruta de nuestro certificado en el apartado *SSLCertificateFile* y *SSLCertificateKeyFile*

```
default-ssl.conf [Sólo lectura] (/etc/apache2/sites-available)
Archivo Editar Ver Buscar Herramientas Documentos Ayuda
<IfModule mod_ssl.c>
<VirtualHost default *:443>
    ServerAdmin webmaster@localhost

    DocumentRoot /var/www/html

    # Available loglevels: trace8, ..., tracel, debug, info, notice, warn,
    # 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 the
    # 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

    #
    # 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, only the
    # SSLCertificateFile directive is needed.
    SSLCertificateFile /etc/ssl/localcerts/apache.crt
    SSLCertificateKeyFile /etc/ssl/localcerts/apache.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
    # the referenced file can be the same as SSLCertificateFile
    # when the CA certificates are directly appended to the server
    # certificate for convinience.
    #SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt

    #
    # Certificate Authority (CA):
    # Set the CA certificate verification path where to find CA
    # certificates for client authentication or alternatively one
    # huge file containing all of them (file must be PEM encoded)
    # Note: Inside SSLCACertificatePath you need hash symlinks
    # to point to the certificate files. Use the provided
    # Makefile to update the hash symlinks after changes.
```

## CONFIGURACION DEL SERVIDOR APACHE2 EN LINUX MINT

Por último, habilitamos el sitio y recargamos la configuración de apache

```
servicios@servicios-VirtualBox /etc/ssl $ sudo a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
  service apache2 reload
servicios@servicios-VirtualBox /etc/ssl $ service apache2 reload
```

El servidor tendría que tener disponible la página con seguridad, vamos a probar, aceptamos la confirmación de seguridad ya que es un certificado autofirmado.

