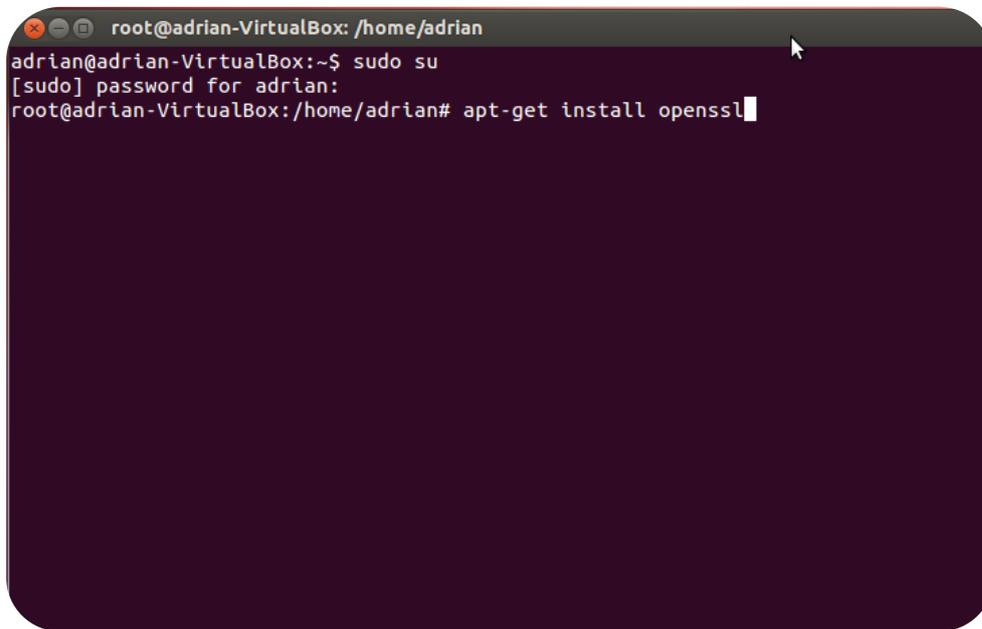


SERVICIOS Y APLICACIONES WEB

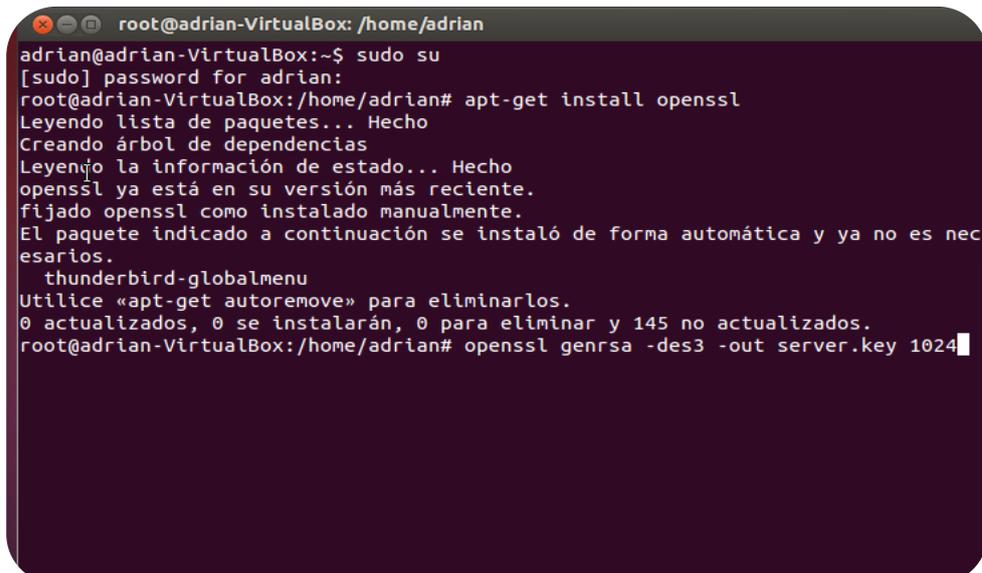
5. Crea un sitio Web seguro usando tu propio certificado digital (Windows y Linux).

Tenemos que instalar openssl para crear el certificado digital en apache2



```
root@adrian-VirtualBox: /home/adrian
adrian@adrian-VirtualBox:~$ sudo su
[sudo] password for adrian:
root@adrian-VirtualBox:/home/adrian# apt-get install openssl
```

Una vez instalado, ejecutamos la siguiente orden. `sudo openssl genrsa -des3 -out server.key 1024`, para generar nuestra llave.



```
root@adrian-VirtualBox: /home/adrian
adrian@adrian-VirtualBox:~$ sudo su
[sudo] password for adrian:
root@adrian-VirtualBox:/home/adrian# apt-get install openssl
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
openssl ya está en su versión más reciente.
fijado openssl como instalado manualmente.
El paquete indicado a continuación se instaló de forma automática y ya no es necesario.
  thunderbird-globalmenu
Utilice «apt-get autoremove» para eliminarlos.
0 actualizados, 0 se instalarán, 0 para eliminar y 145 no actualizados.
root@adrian-VirtualBox:/home/adrian# openssl genrsa -des3 -out server.key 1024
```

SERVICIOS Y APLICACIONES WEB

Nos pedirá que introduzcamos una contraseña de 4 caracteres como mínimo.

```
root@adrian-VirtualBox: /home/adrian
adrian@adrian-VirtualBox:~$ sudo su
[sudo] password for adrian:
rpot@adrian-VirtualBox:/home/adrian# apt-get install openssl
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
openssl ya está en su versión más reciente.
fijado openssl como instalado manualmente.
El paquete indicado a continuación se instaló de forma automática y ya no es necesario.
  thunderbird-globalmenu
Utilice «apt-get autoremove» para eliminarlos.
0 actualizados, 0 se instalarán, 0 para eliminar y 145 no actualizados.
root@adrian-VirtualBox:/home/adrian# openssl genrsa -des3 -out server.key 1024
Generating RSA private key, 1024 bit long modulus
.....+++++
.....+++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
root@adrian-VirtualBox:/home/adrian#
```



Ejecutamos el siguiente comando para crear el certificado

```
root@adrian-VirtualBox: /home/adrian
root@adrian-VirtualBox:/home/adrian# openssl req -new -key server.key -out server.csr
```



SERVICIOS Y APLICACIONES WEB

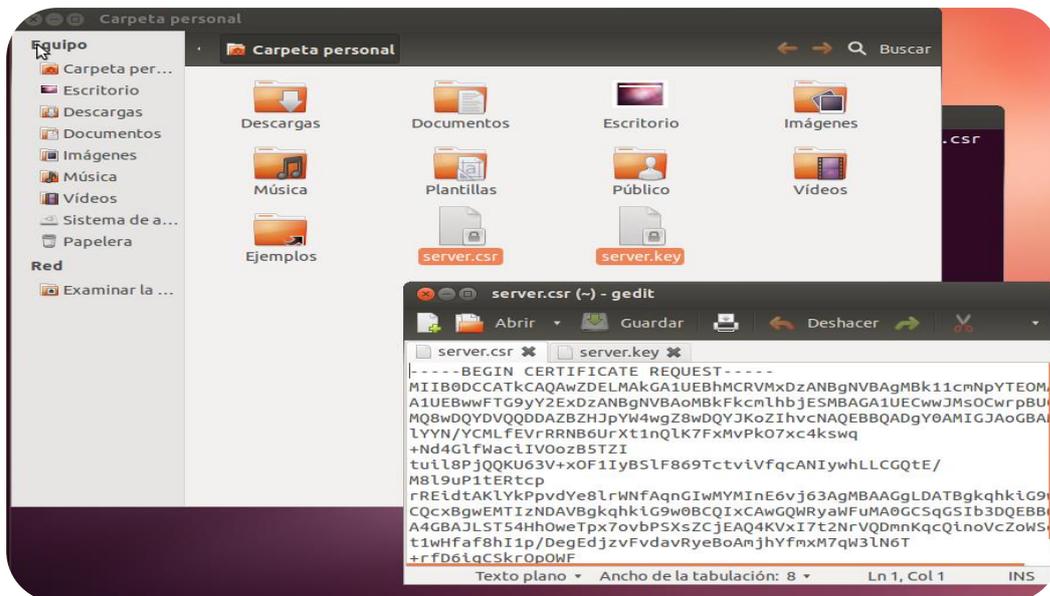
Ponemos la contraseña y después rellenamos los datos que nos pregunten como País, Provincia, localidad, nombre.....

```
root@adrian-VirtualBox: /home/adrian
root@adrian-VirtualBox:/home/adrian# openssl req -new -key server.key -out server.csr
Enter pass phrase for server.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]:ES
State or Province Name (full name) [Some-State]:Murcia
Locality Name (eg, city) []:Lorca
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Adrian
Organizational Unit Name (eg, section) []:2ºASIR
Common Name (e.g. server FQDN or YOUR name) []:Adrian
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234
An optional company name []:Adrian
root@adrian-VirtualBox:/home/adrian#
```



Vemos que los archivos del certificado están creados



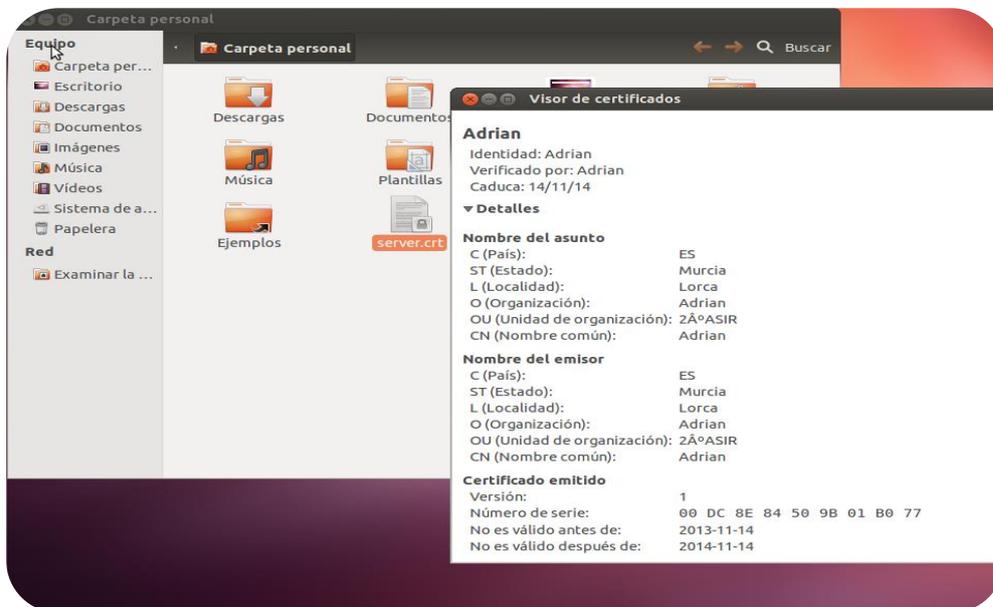
SERVICIOS Y APLICACIONES WEB

Ejecutamos el siguiente comando que nos genera el archivo .crt que es el certificado.

```
root@adrian-VirtualBox: /home/adrian
root@adrian-VirtualBox:/home/adrian# openssl x509 -req -days 365 -in server.csr -signkey
server.key -out server.crt

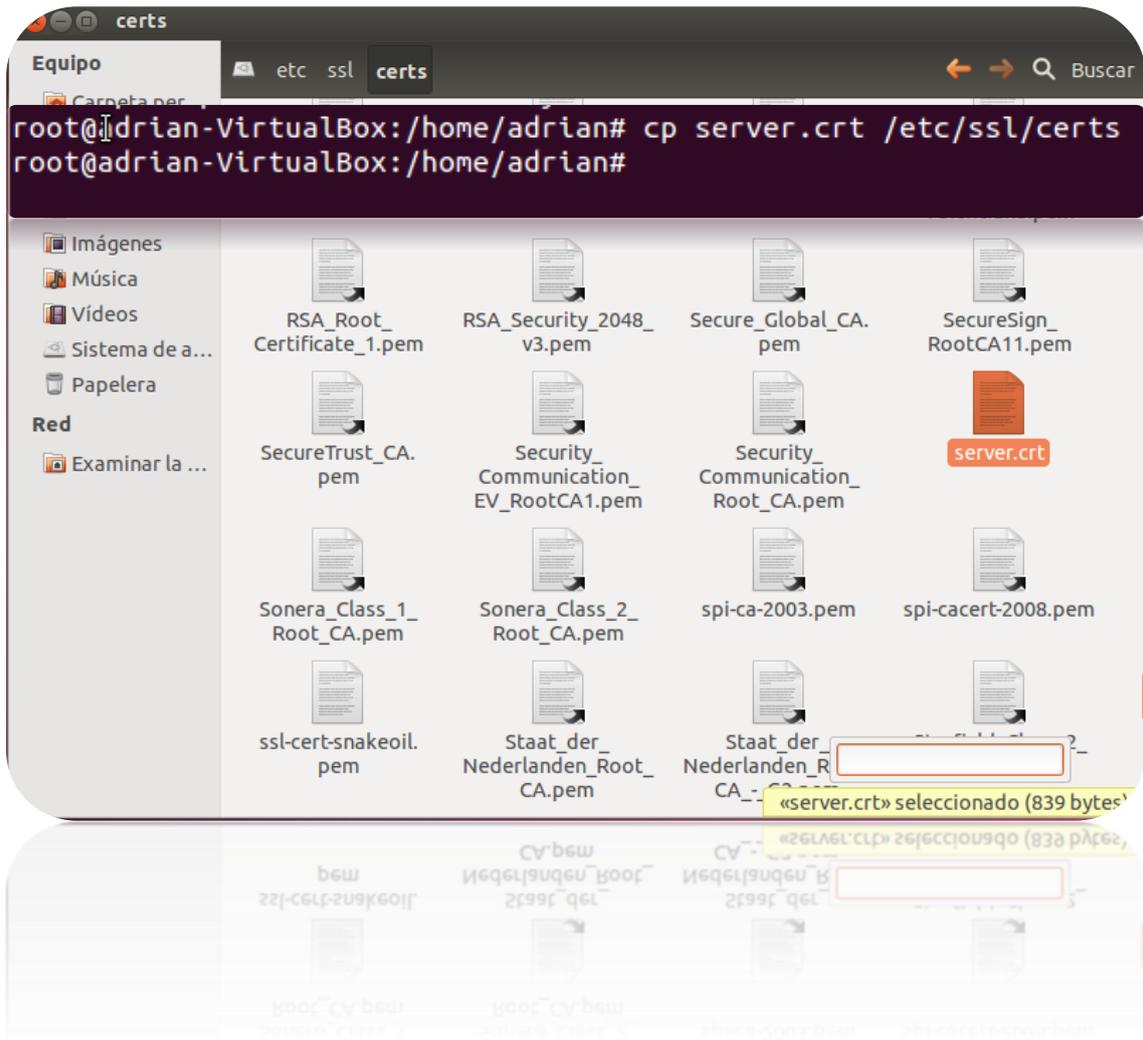
root@adrian-VirtualBox:/home/adrian
root@adrian-VirtualBox:/home/adrian# openssl x509 -req -days 365 -in server.csr -signkey
server.key -out server.crt
Signature ok
subject=/C=ES/ST=Murcia/L=Lorca/O=Adrian/OU=2\xC3\x82\xC2\xBAASIR/CN=Adrian
Getting Private key
Enter pass phrase for server.key:
root@adrian-VirtualBox:/home/adrian#
```

Vemos que el certificado esta creado correctamente

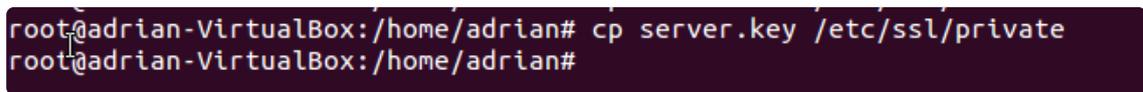


SERVICIOS Y APLICACIONES WEB

Copiamos el certificado server.crt a la carpeta /etc/ssl/certs



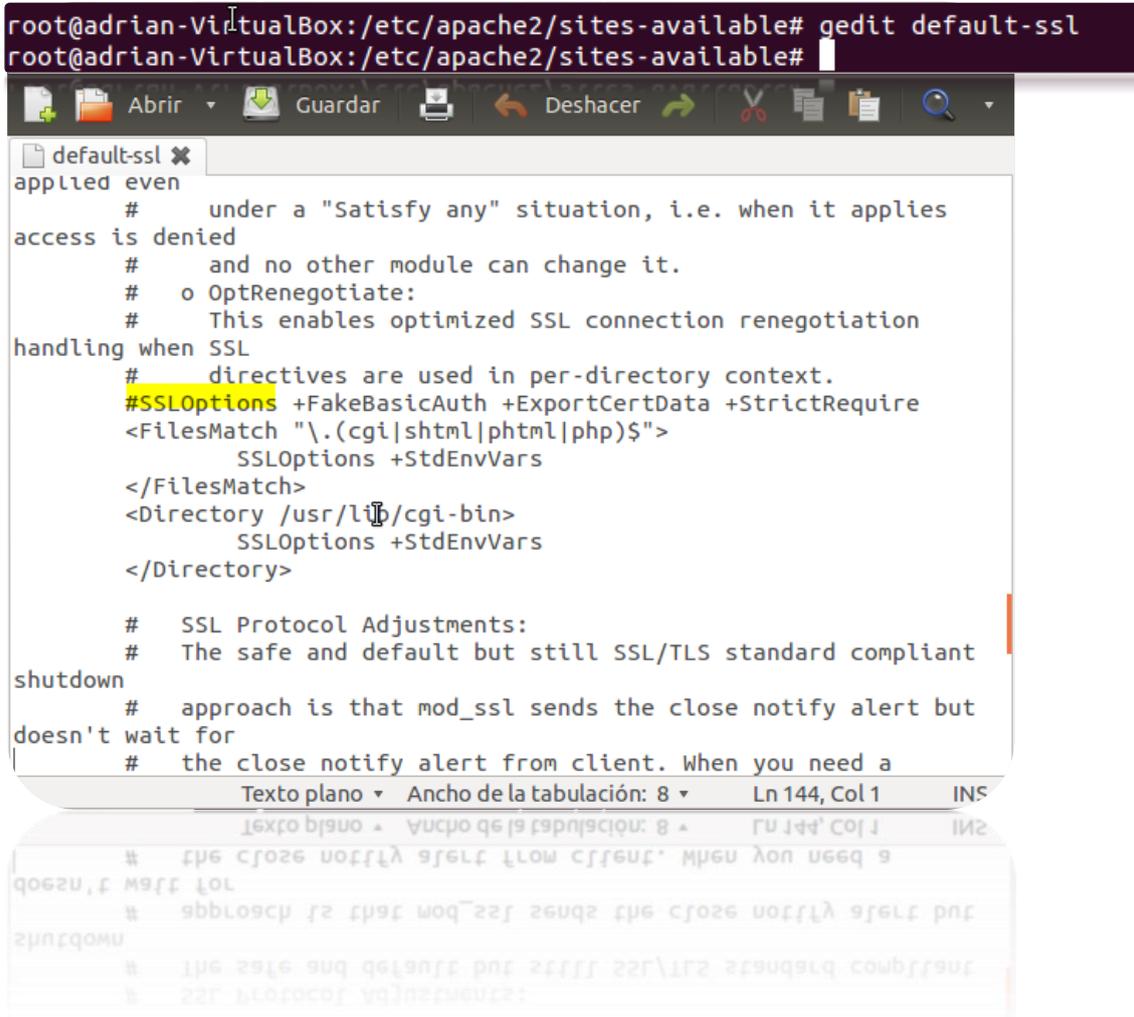
Y también copiamos server.key a la carpeta /etc/ssl/private



SERVICIOS Y APLICACIONES WEB

Nos vamos a `/etc/apache2/sites-available` y modificamos `default-ssl` quitando las almohadillas al `SSLOptions`

```
root@adrian-VirtualBox:/etc/apache2/sites-available# gedit default-ssl
root@adrian-VirtualBox:/etc/apache2/sites-available#
```

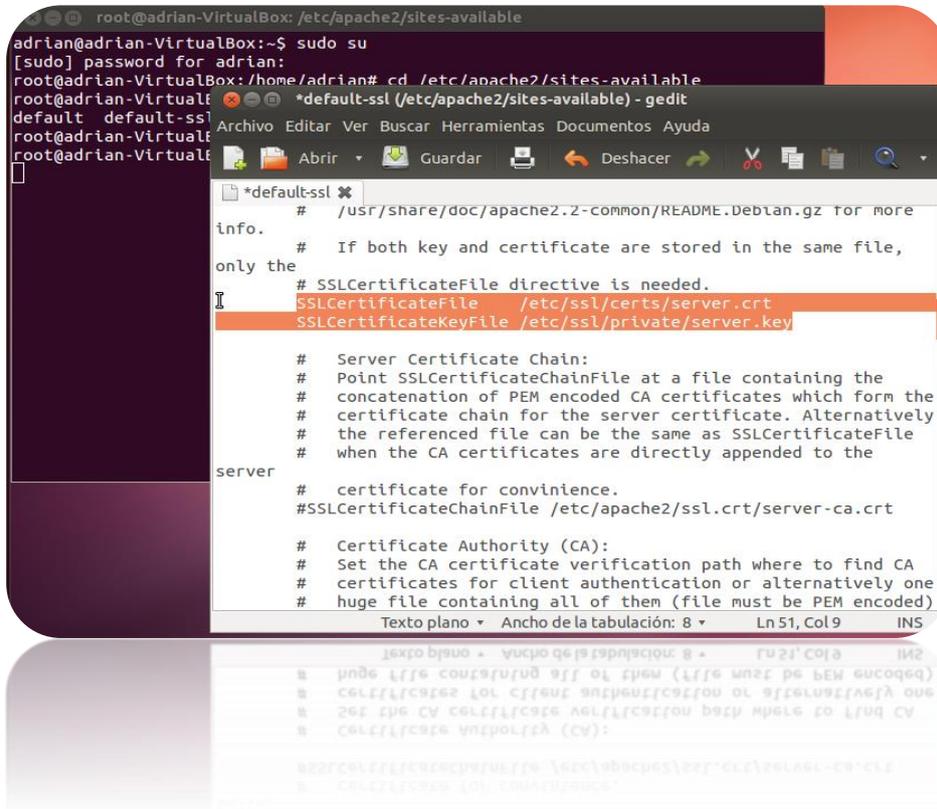


```
default-ssl
applied even
#       under a "Satisfy any" situation, i.e. when it applies
access is denied
#       and no other module can change it.
#       o OptRenegotiate:
#       This enables optimized SSL connection renegotiation
handling when SSL
#       directives are used in per-directory context.
#SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire
<FilesMatch "\.(cgi|shtml|phtml|php)$">
    SSLOptions +StdEnvVars
</FilesMatch>
<Directory /usr/lib/cgi-bin>
    SSLOptions +StdEnvVars
</Directory>

#       SSL Protocol Adjustments:
#       The safe and default but still SSL/TLS standard compliant
shutdown
#       approach is that mod_ssl sends the close notify alert but
doesn't wait for
#       the close notify alert from client. When you need a
```

SERVICIOS Y APLICACIONES WEB

También modificamos el SSLcertificatefile y el Key file por las rutas donde hemos copiado el certificado y la llave



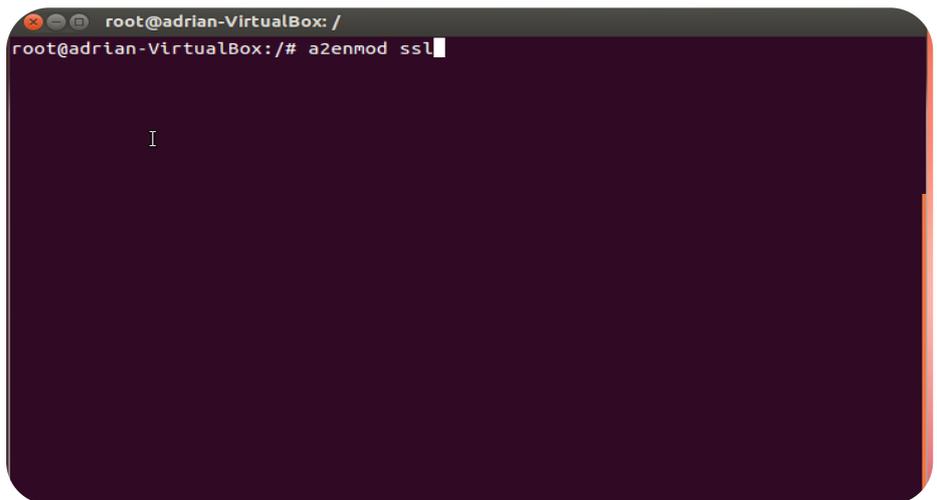
```
root@adrian-VirtualBox: /etc/apache2/sites-available
adrian@adrian-VirtualBox:~$ sudo su
[sudo] password for adrian:
root@adrian-VirtualBox: /home/adrian# cd /etc/apache2/sites-available
root@adrian-VirtualBox:~$ *default-ssl (/etc/apache2/sites-available) - gedit
default default-ssl
root@adrian-VirtualBox:~$
root@adrian-VirtualBox:~$
```

```
*default-ssl
# /usr/share/doc/apache2.2-common/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/certs/server.crt
SSLCertificateKeyFile /etc/ssl/private/server.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)
# SSLCertificateChainFile /etc/ssl/certs/ca-bundle.crt
```

Habilitamos el SSL con el siguiente comando



```
root@adrian-VirtualBox: /
root@adrian-VirtualBox:~# a2enmod ssl
```

SERVICIOS Y APLICACIONES WEB

Habilitamos default-ssl con la orden "a2ensite default-ssl"

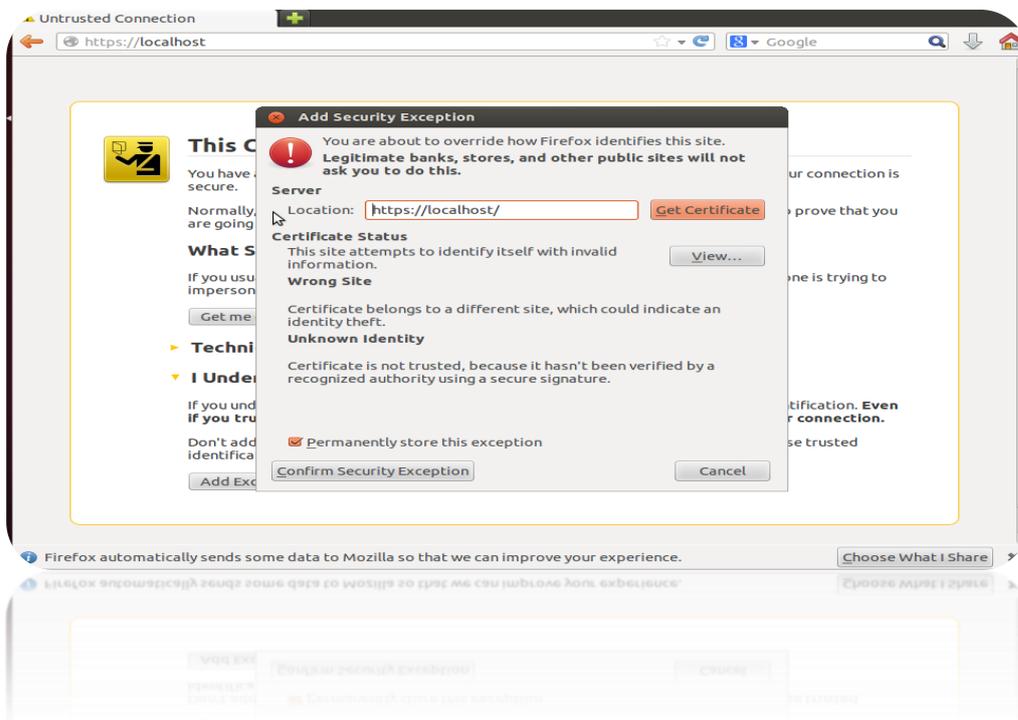
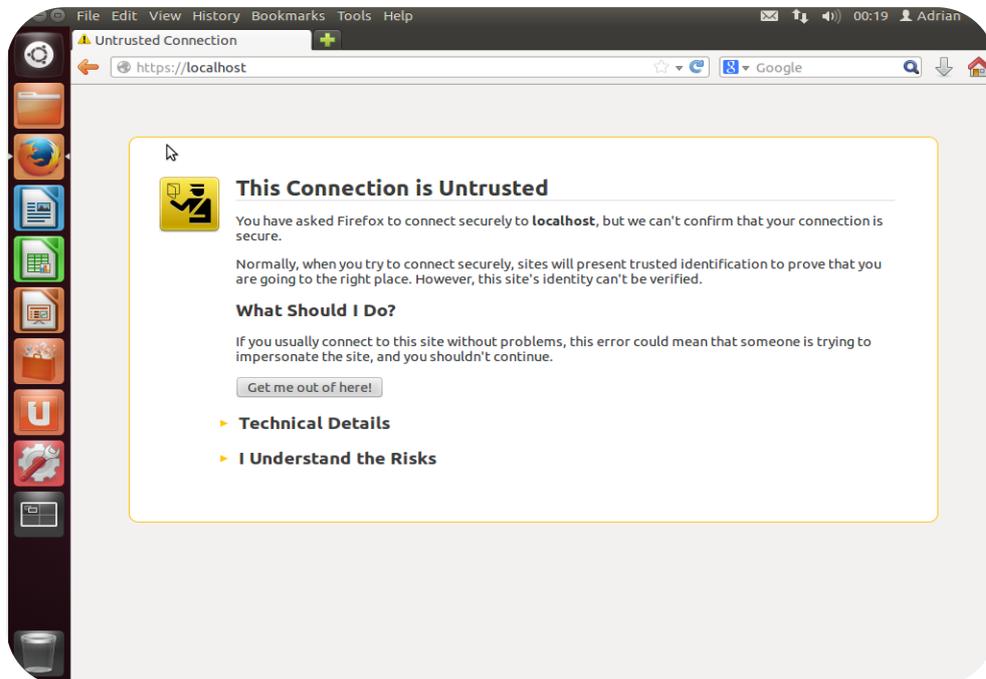
```
root@adrian-VirtualBox: /etc/apache2/sites-available
root@adrian-VirtualBox:/# a2enmod ssl
Enabling module ssl.
See /usr/share/doc/apache2.2-common/README.Debian.gz on how to configure SSL and
create self-signed certificates.
To activate the new configuration, you need to run:
  service apache2 restart
root@adrian-VirtualBox:/# cd /etc/apache2/sites-available
root@adrian-VirtualBox:/etc/apache2/sites-available# a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
  service apache2 reload
root@adrian-VirtualBox:/etc/apache2/sites-available#
```

Reiniciamos el servicio apache con la siguiente orden y nos pedirá la clave del certificado

```
root@adrian-VirtualBox: /
root@adrian-VirtualBox:/etc/apache2/sites-available# cd ..
root@adrian-VirtualBox:/etc/apache2# cd ..
root@adrian-VirtualBox:/etc# cd ..
root@adrian-VirtualBox:/# /etc/init.d/apache2 restart
* Restarting web server apache2
apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
... waiting apache2: Could not reliably determine the server's fully qualified
domain name, using 127.0.1.1 for ServerName
Apache needs to decrypt your SSL Keys for 127.0.1.1:443 (RSA)
Please enter passphrase: [ OK ]
root@adrian-VirtualBox:/#
```

SERVICIOS Y APLICACIONES WEB

Ahora si entramos en el navegador y ponemos el protocolo https nos saldrá el aviso para aceptar nuestro certificado, le damos a entiendo los riesgos y añadimos excepción para entrar a la página.



SERVICIOS Y APLICACIONES WEB

Y ya podemos entrar a la página con el protocolo https.

