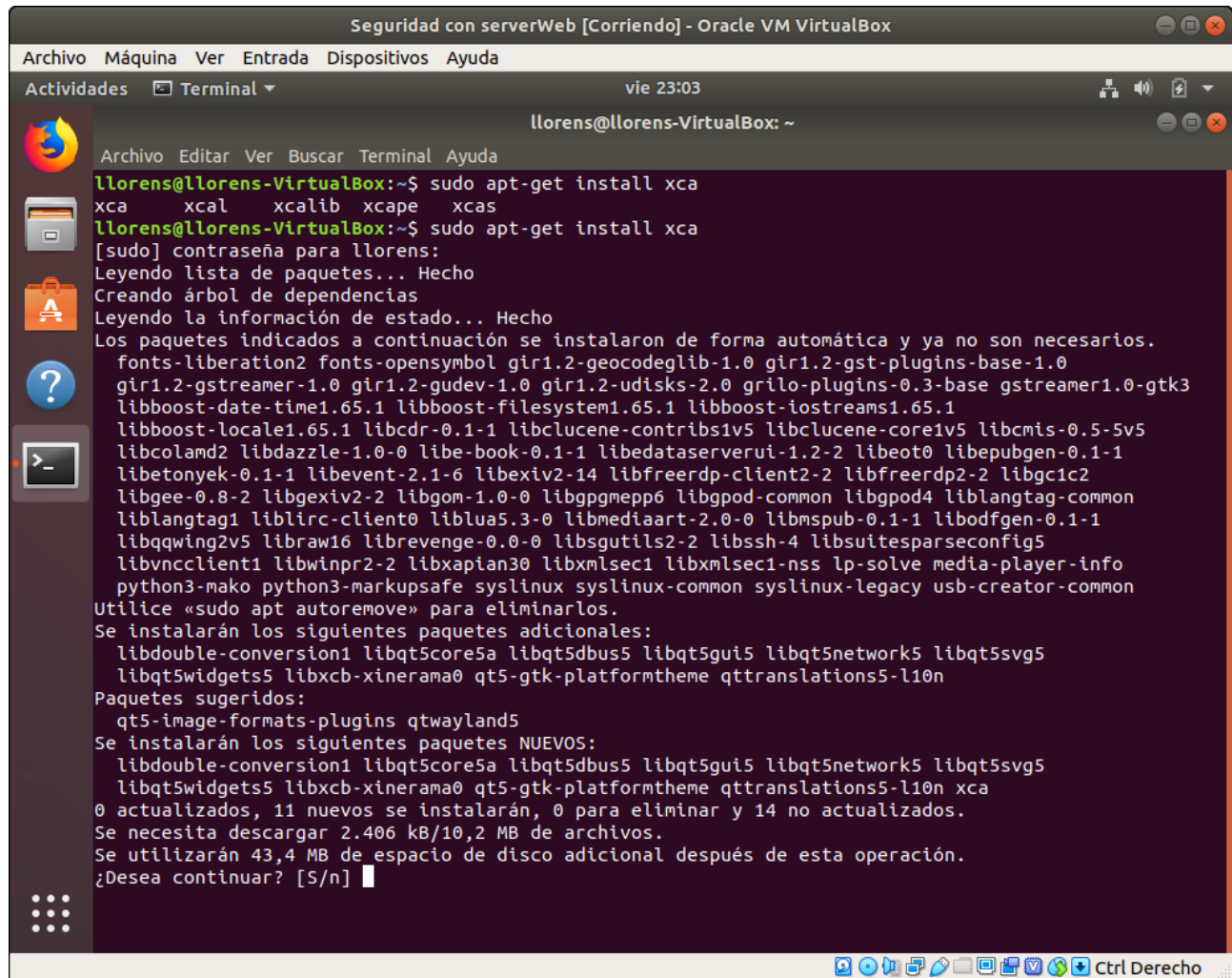


## Práctica 3: Creación de un certificado SSL/TLS multisite

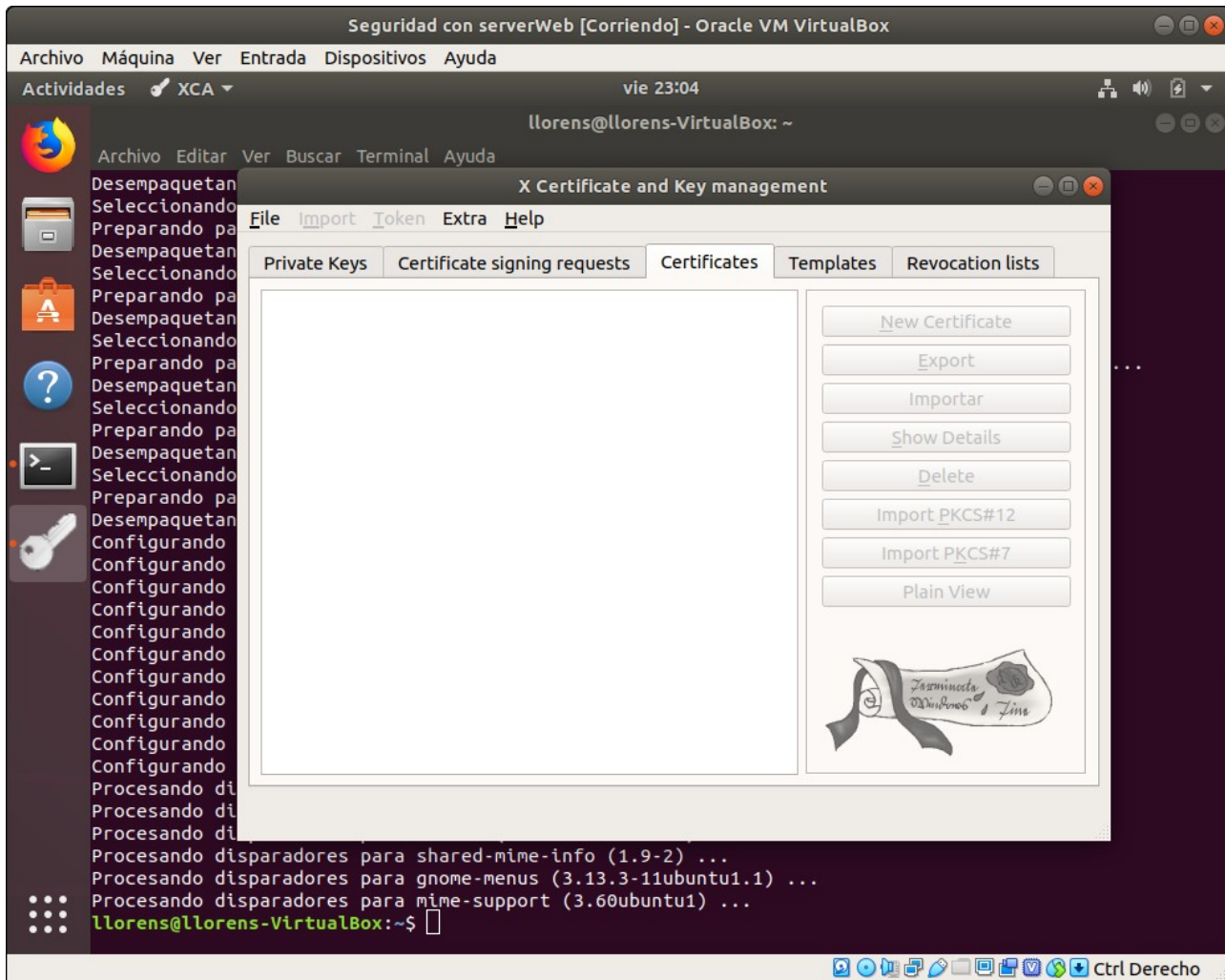
Para esta practica he clonado una maquina virtual de IAW que justamente tiene instalado el servidor Web.

Instalación de XCA



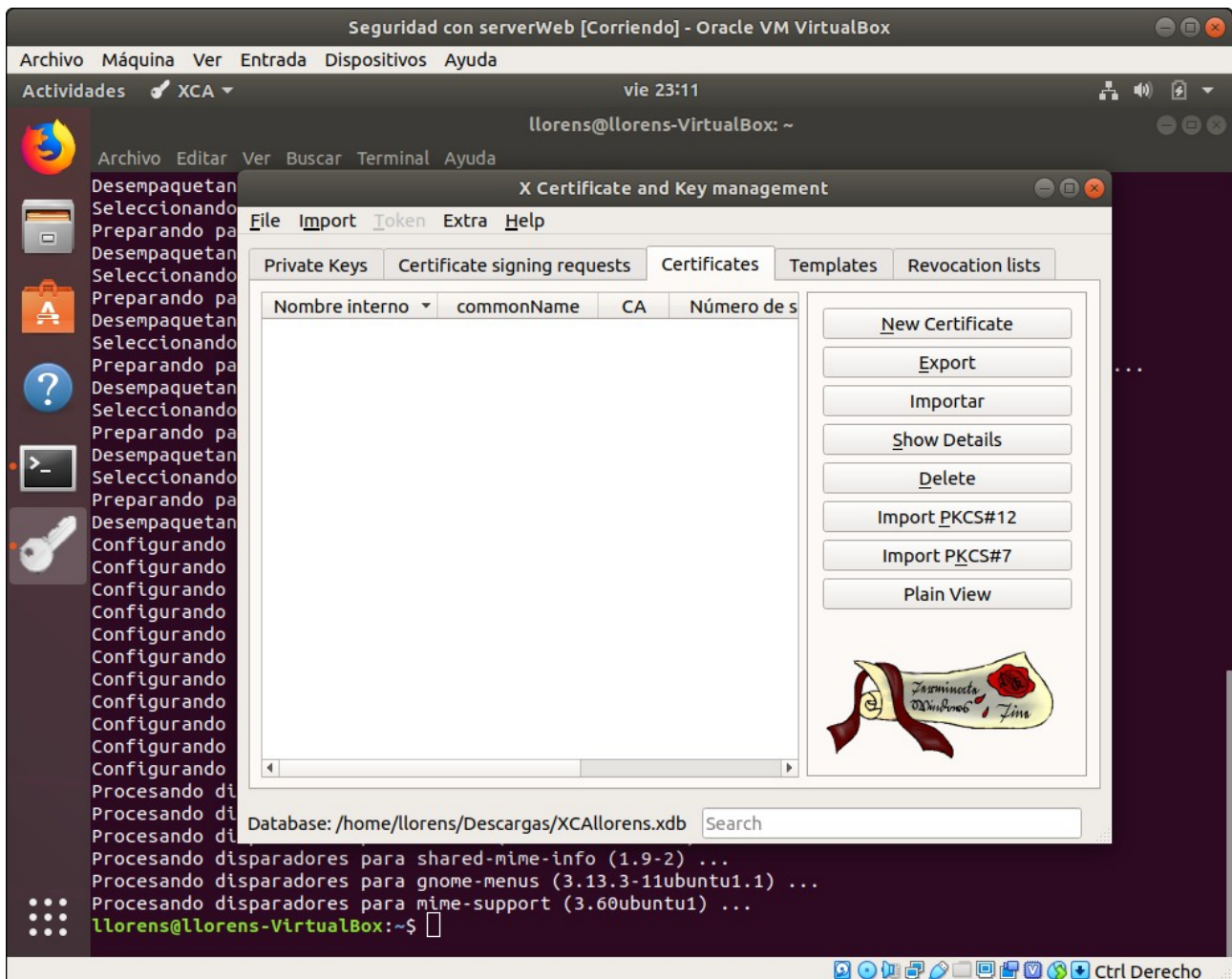
```
Seguridad con serverWeb [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal vie 23:03
llorens@llorens-VirtualBox: ~
llorens@llorens-VirtualBox:~$ sudo apt-get install xca
xca xcal xcalib xcape xcas
llorens@llorens-VirtualBox:~$ sudo apt-get install xca
[sudo] contraseña para llorens:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
 fonts-liberation2 fonts-opensymbol gir1.2-geocodeglib-1.0 gir1.2-gst-plugins-base-1.0
 gir1.2-gstreamer-1.0 gir1.2-gudev-1.0 gir1.2-udisks-2.0 grilo-plugins-0.3-base gstreamer1.0-gtk3
 libboost-date-time1.65.1 libboost-filesystem1.65.1 libboost-iostreams1.65.1
 libboost-locale1.65.1 libcdr-0.1-1 libclucene-contribs1v5 libclucene-core1v5 libcmis-0.5-5v5
 libcolamd2 libdazzle-1.0-0 libe-book-0.1-1 libedataserverui-1.2-2 libeot0 libepubgen-0.1-1
 libetonyek-0.1-1 libevent-2.1-6 libexiv2-14 libfreerdp-client2-2 libfreerdp2-2 libgc1c2
 libgee-0.8-2 libgexiv2-2 libgom-1.0-0 libgpgmepp6 libgpod-common libgpod4 liblangtag-common
 liblangtag1 liblirc-client0 liblua5.3-0 libmediaart-2.0-0 libmspub-0.1-1 libodfgen-0.1-1
 libqqwing2v5 libraw16 librevenge-0.0-0 libsgutils2-2 libssh-4 libsuitesparseconfig5
 libvncclient1 libwinpr2-2 libxapian30 libxmlsec1 libxmlsec1-nss lp-solve media-player-info
 python3-mako python3-markupsafe syslinux syslinux-common syslinux-legacy usb-creator-common
 Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
 libdouble-conversion1 libqt5core5a libqt5dbus5 libqt5gui5 libqt5network5 libqt5svg5
 libqt5widgets5 libxcb-xinerama0 qt5-gtk-platformtheme qttranslations5-l10n
 Paquetes sugeridos:
 qt5-image-formats-plugins qtwayland5
Se instalarán los siguientes paquetes NUEVOS:
 libdouble-conversion1 libqt5core5a libqt5dbus5 libqt5gui5 libqt5network5 libqt5svg5
 libqt5widgets5 libxcb-xinerama0 qt5-gtk-platformtheme qttranslations5-l10n xca
0 actualizados, 11 nuevos se instalarán, 0 para eliminar y 14 no actualizados.
Se necesita descargar 2.406 kB/10,2 MB de archivos.
Se utilizarán 43,4 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

### Práctica 3: Creación de un certificado SSL/TLS multisite



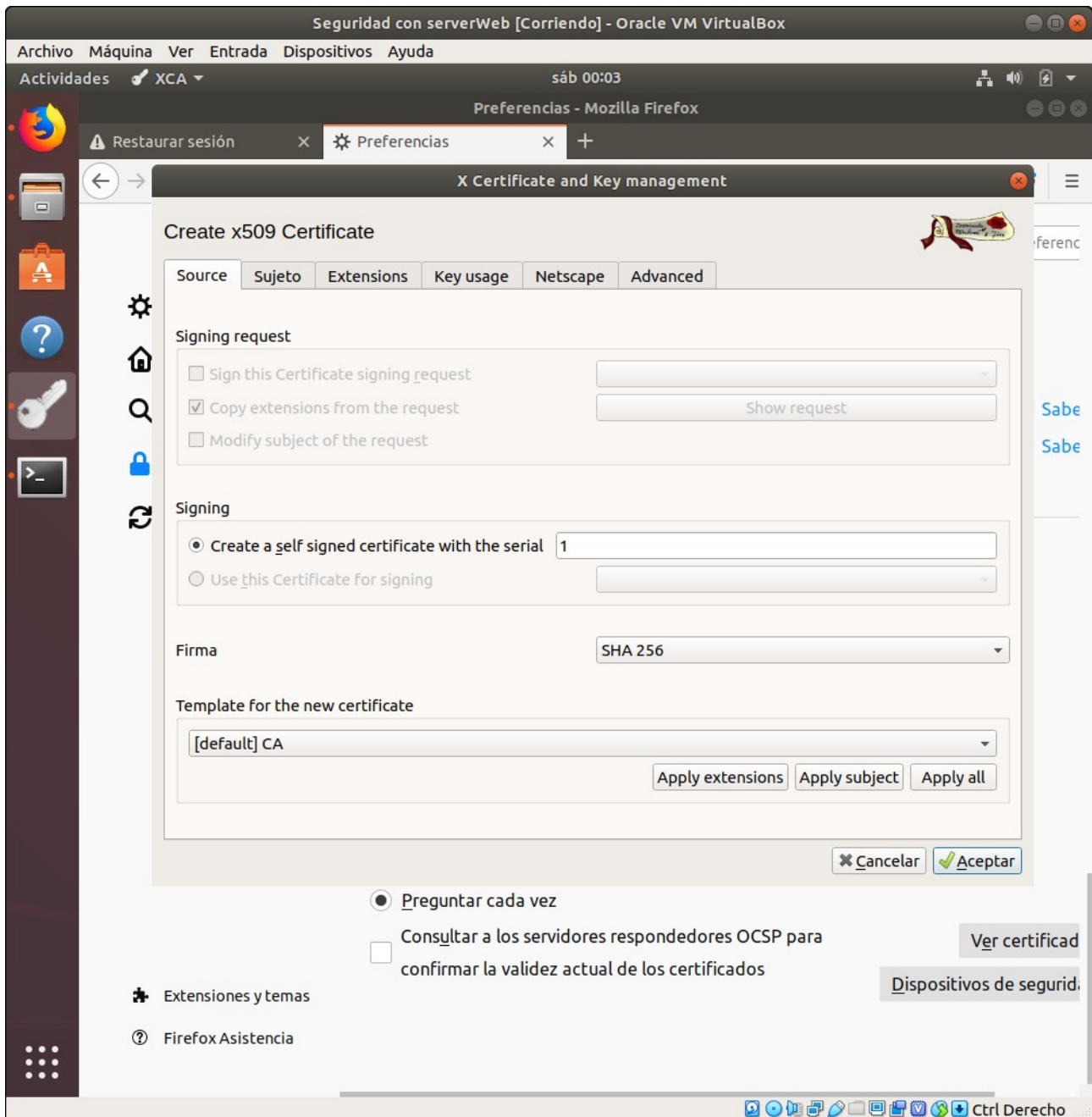
### Práctica 3: Creación de un certificado SSL/TLS multisite

Una vez instalados crearemos la base de datos lo he nombrado XCAллоrens.xdb como se aprecia abajo se ve la ubicación de la base de datos y los botones de la derecha se han habilitado

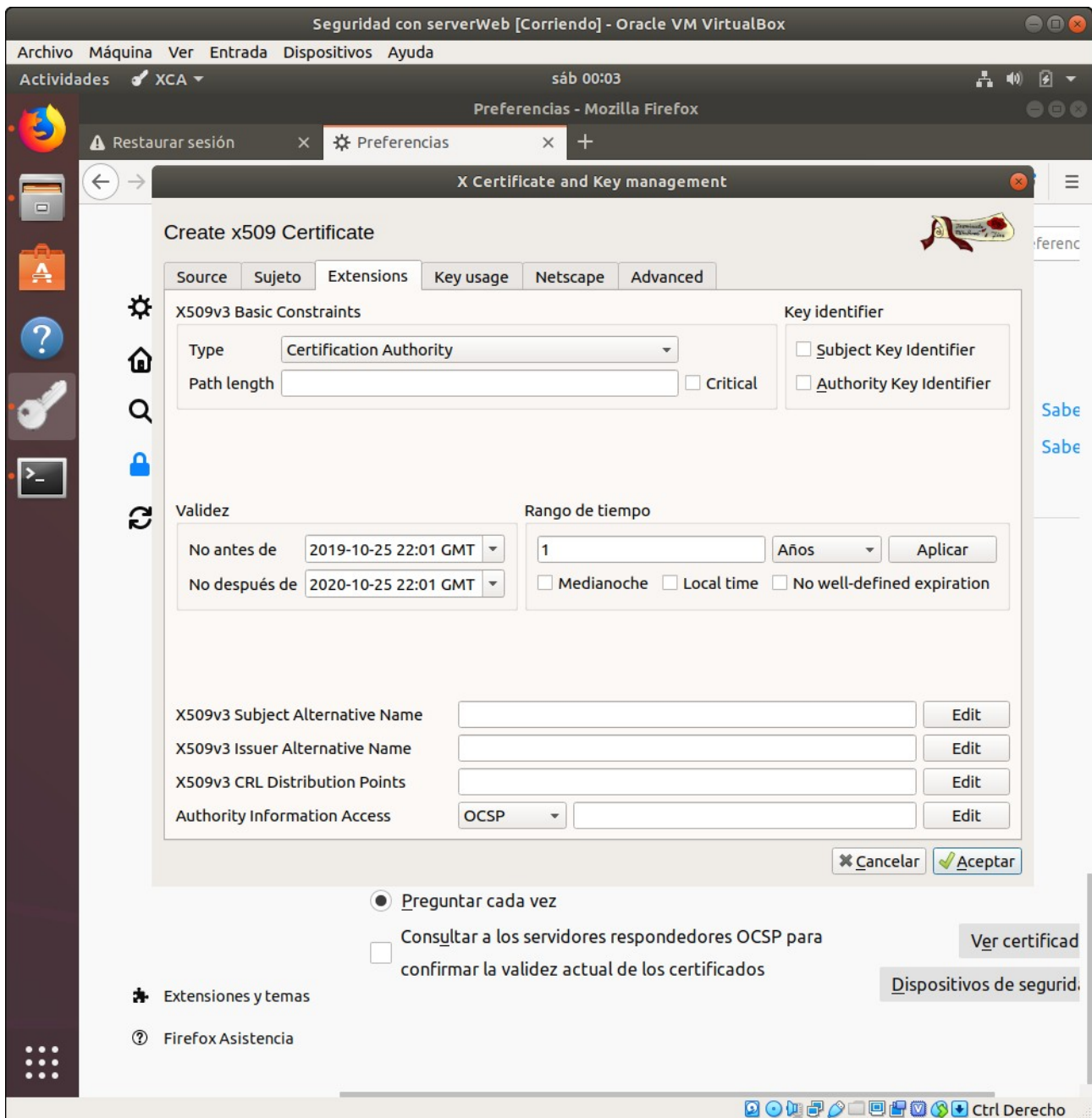


## Práctica 3: Creación de un certificado SSL/TLS multisite

Seguimos la practica y constituimos la nueva AC



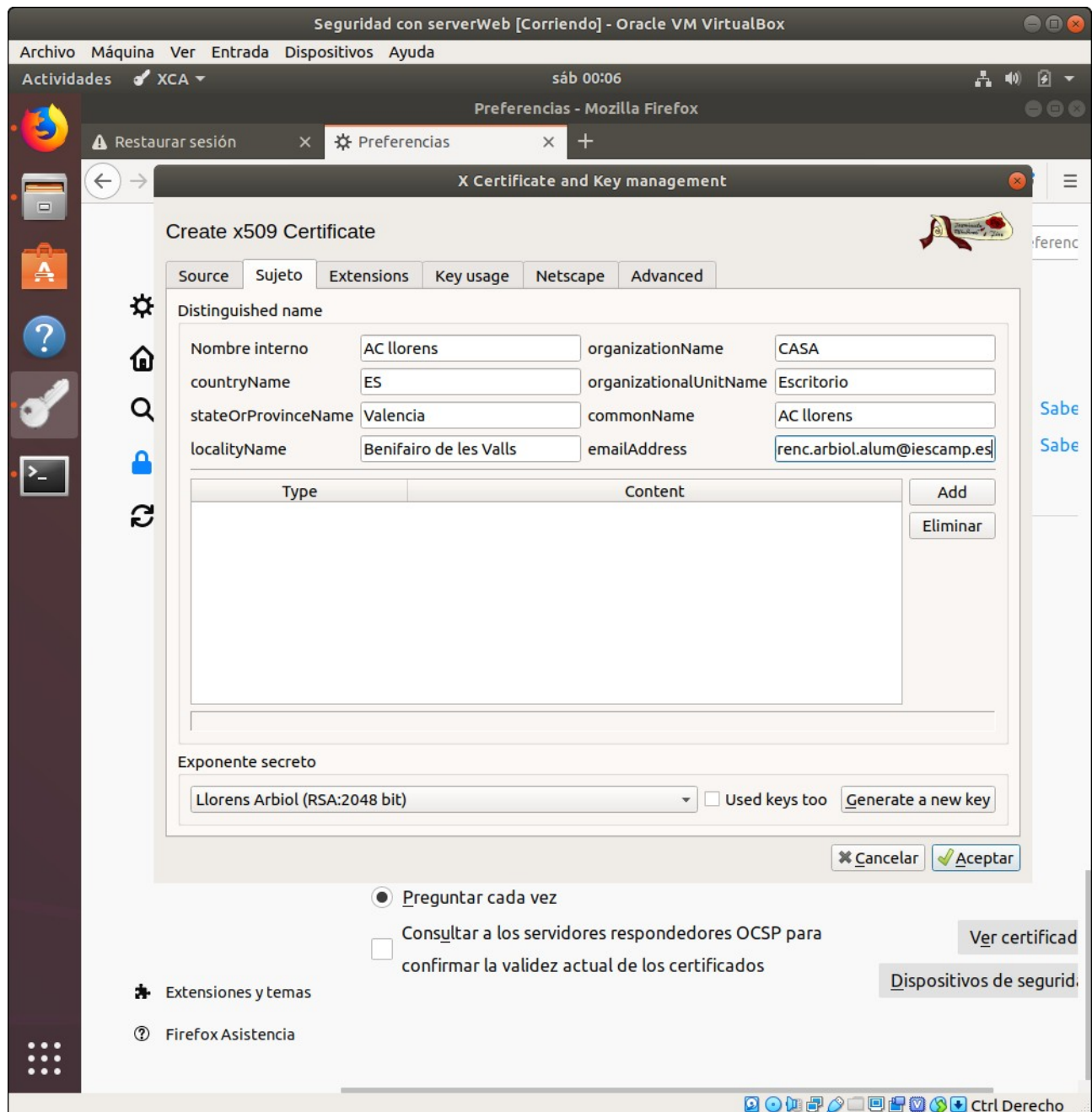
## Práctica 3: Creación de un certificado SSL/TLS multisite





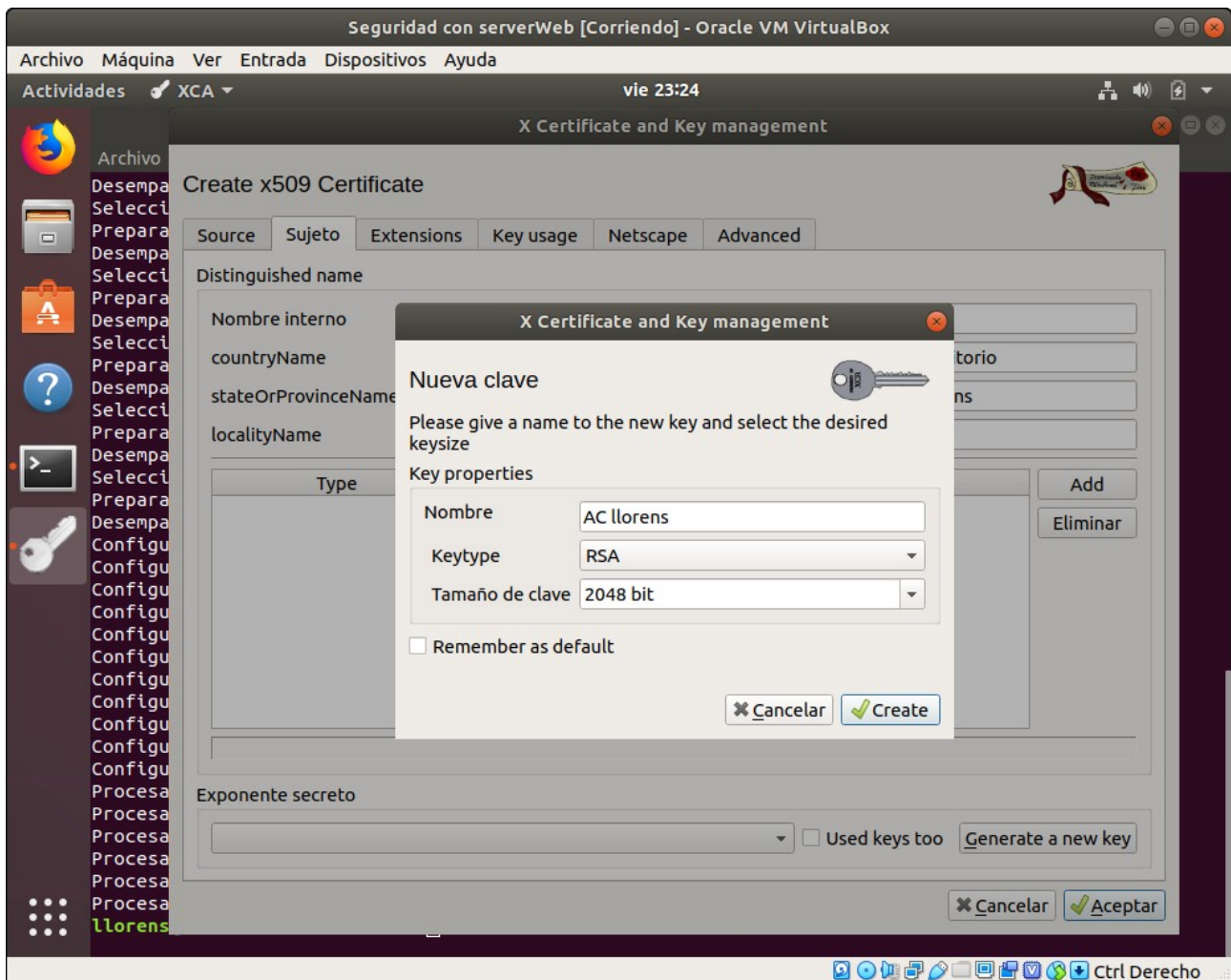
## Práctica 3: Creación de un certificado SSL/TLS multisite

Una vez todo verificado, vamos a rellenar la pestaña Sujeto

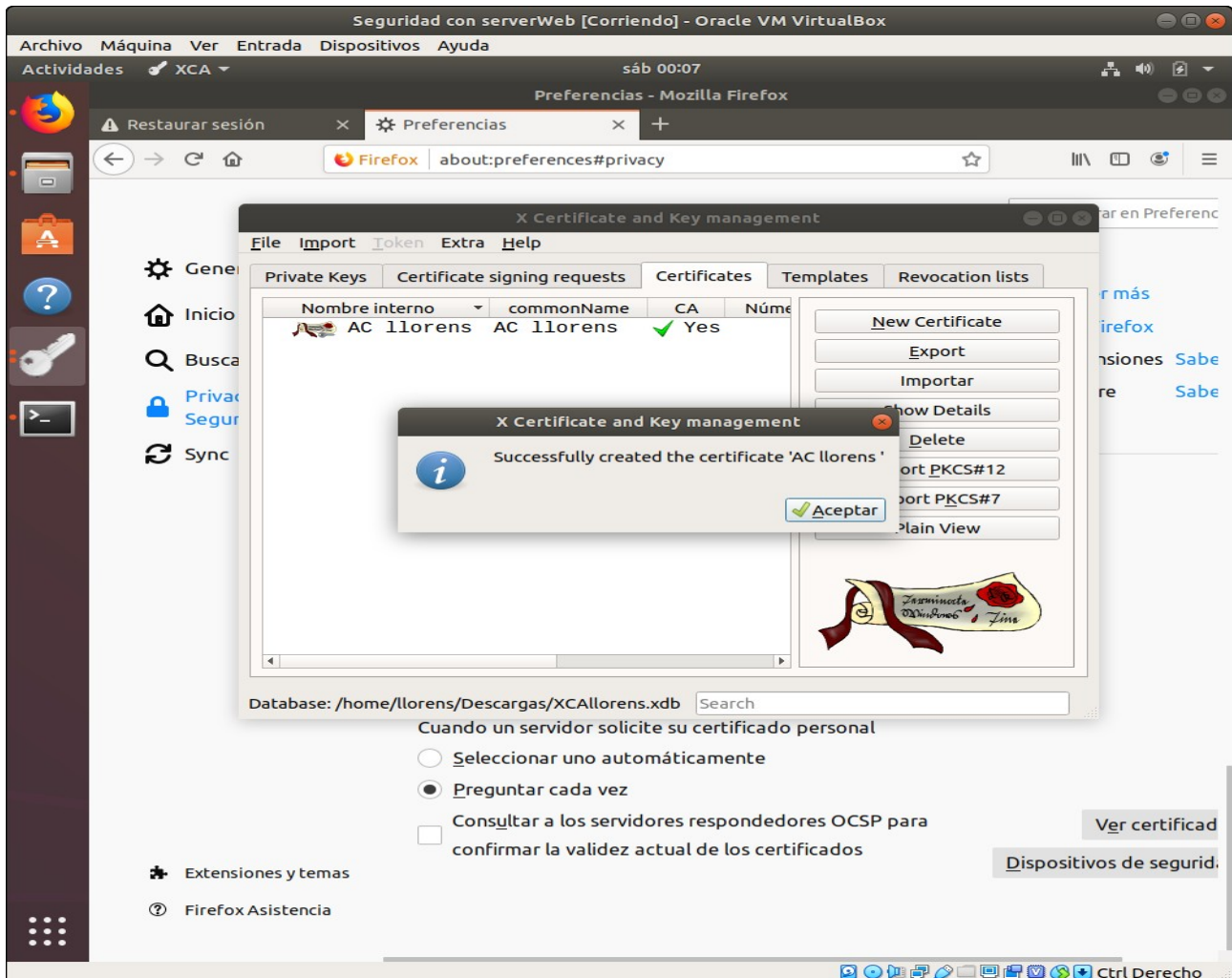


## Práctica 3: Creación de un certificado SSL/TLS multisite

Una vez rellenado pulsamos Generate a new key y seleccionamos 2048 bits



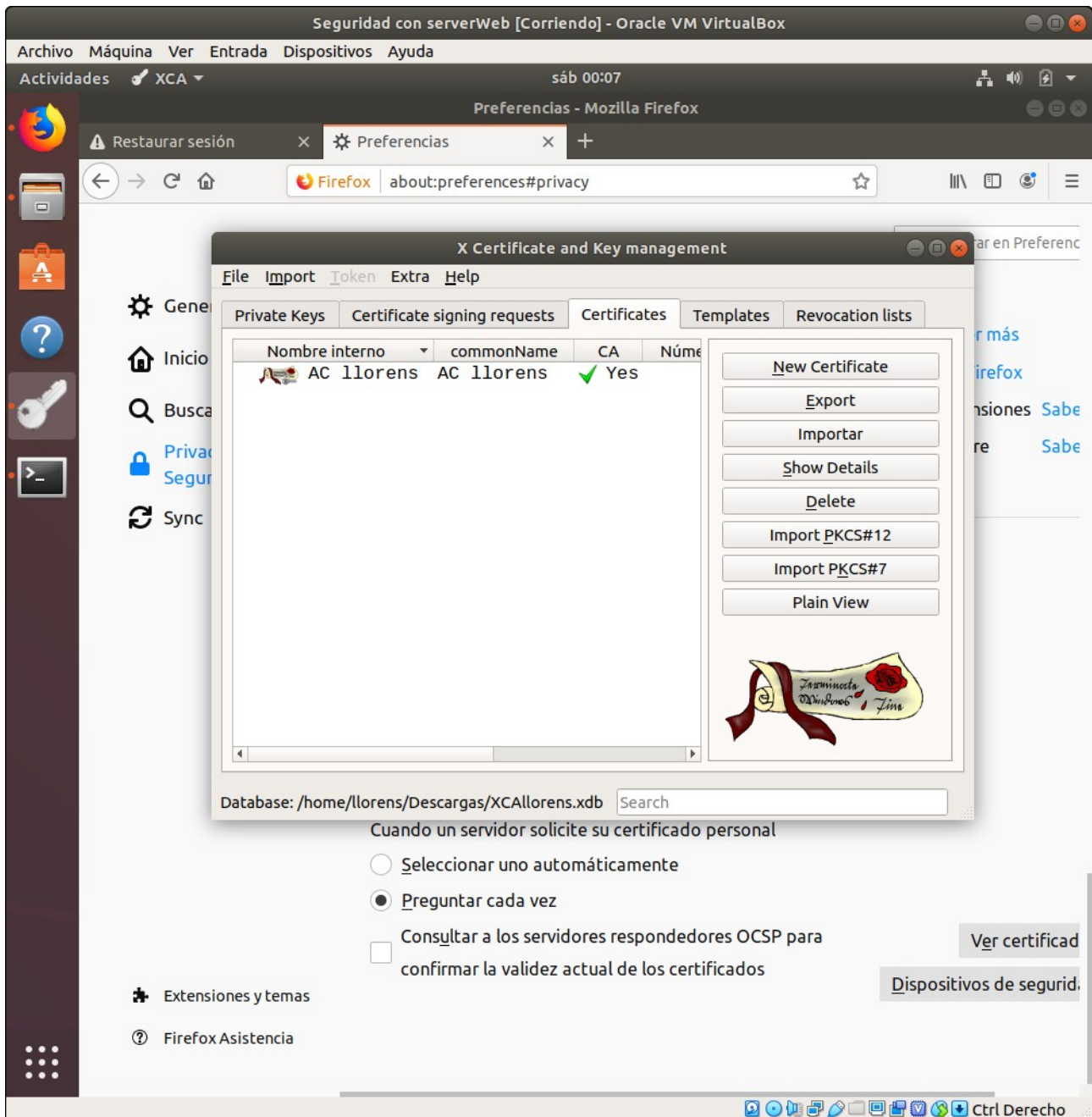
### Práctica 3: Creación de un certificado SSL/TLS multisite



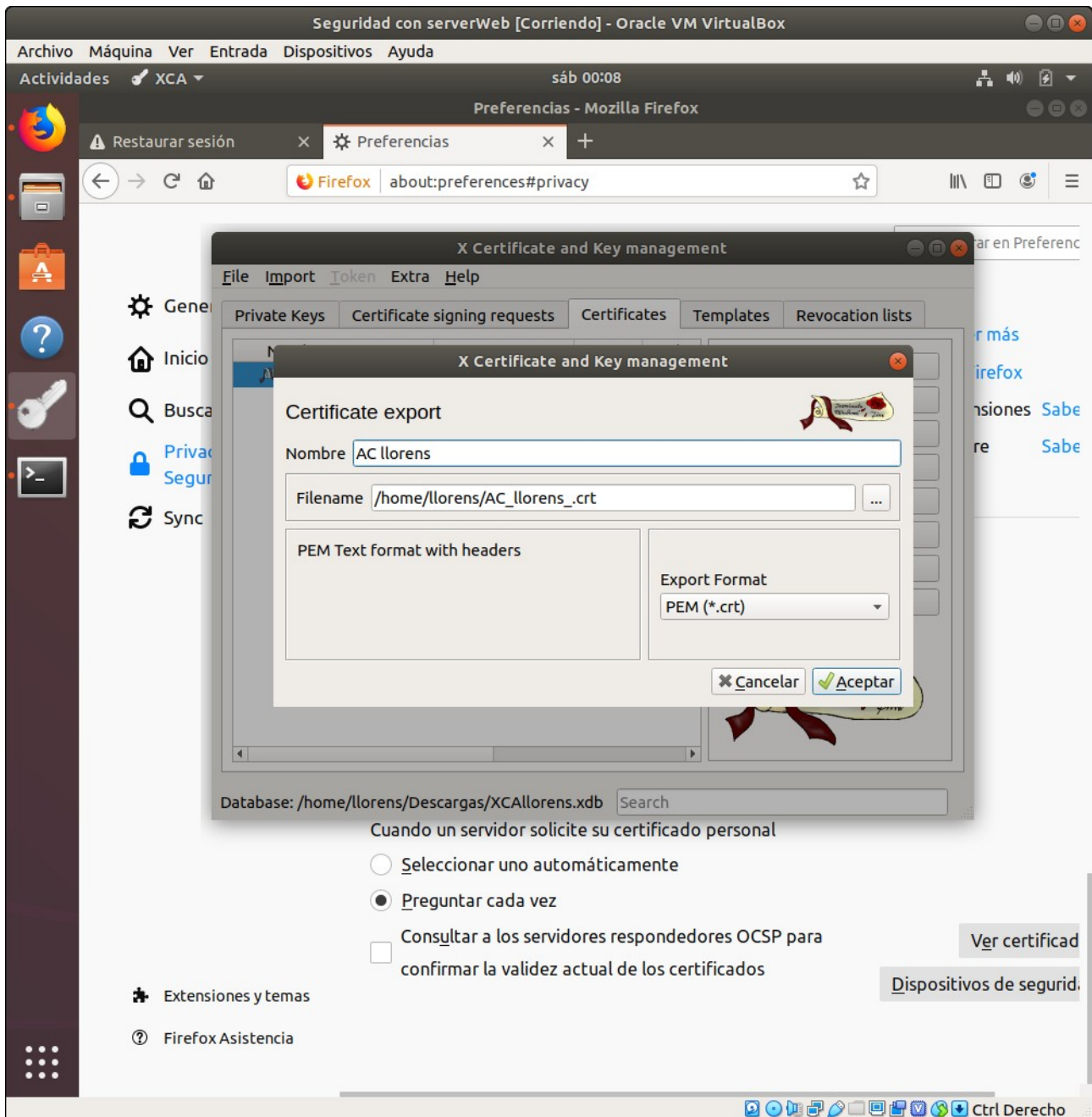
Ya tenemos la AC constituida, ahora procederemos a exportar el certificado y instalarlo en el navegador.



## Práctica 3: Creación de un certificado SSL/TLS multisite

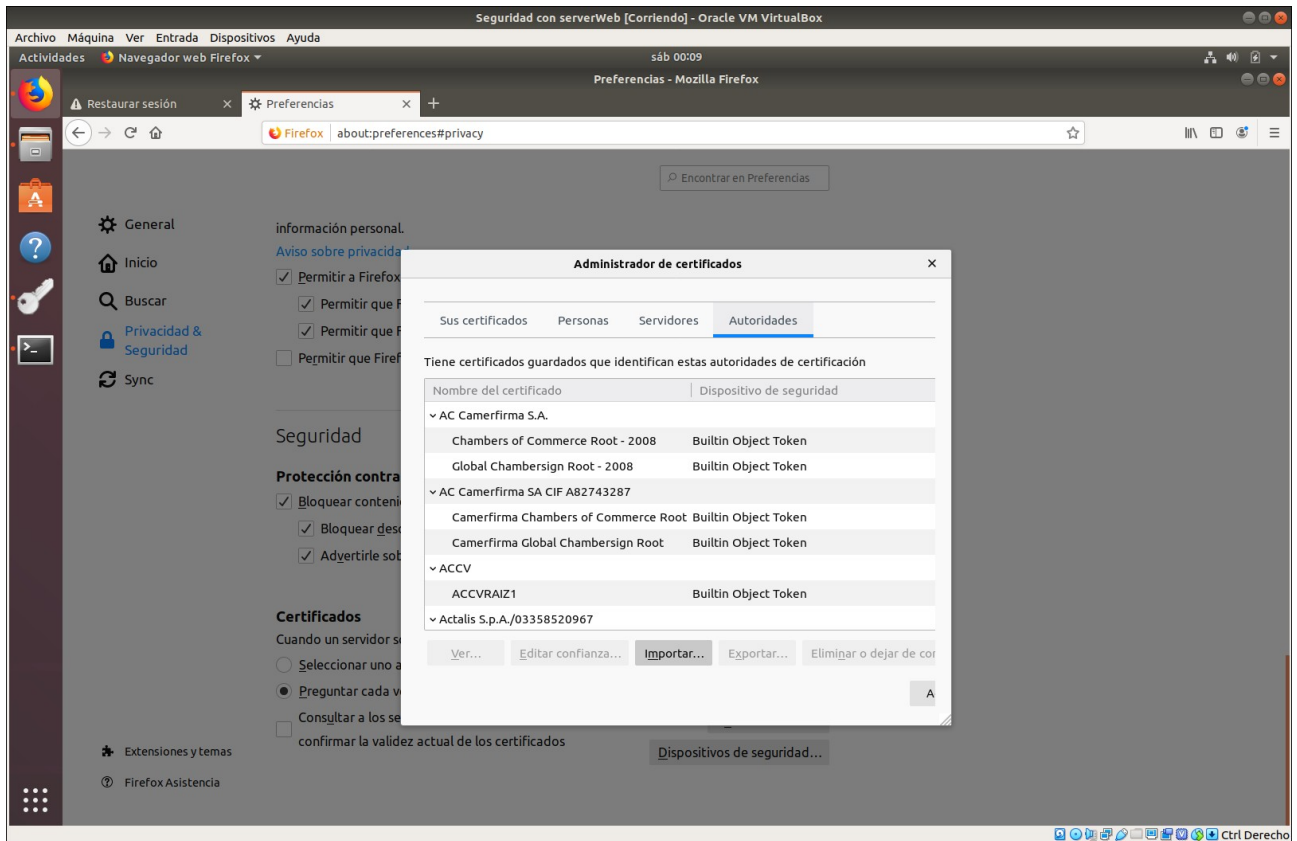


## Práctica 3: Creación de un certificado SSL/TLS multisite

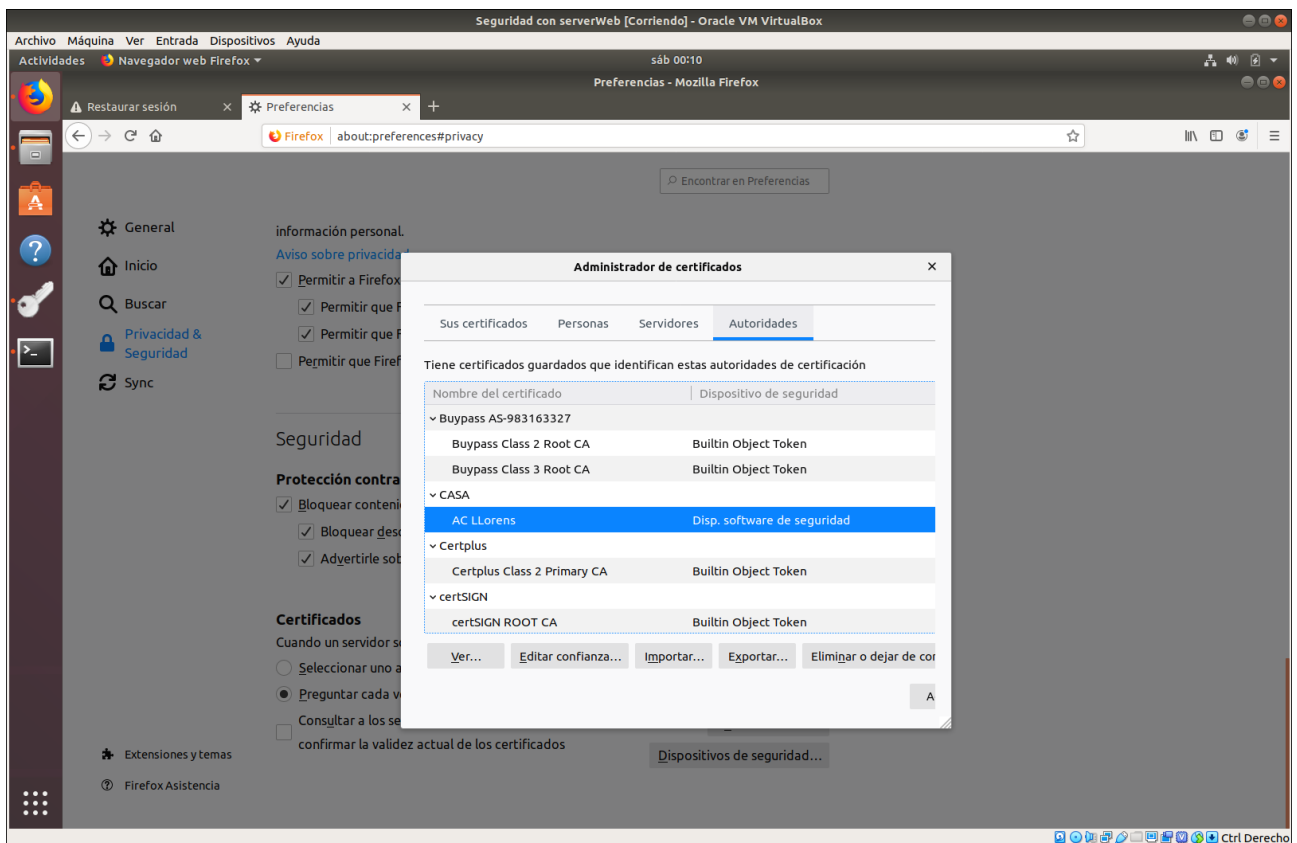
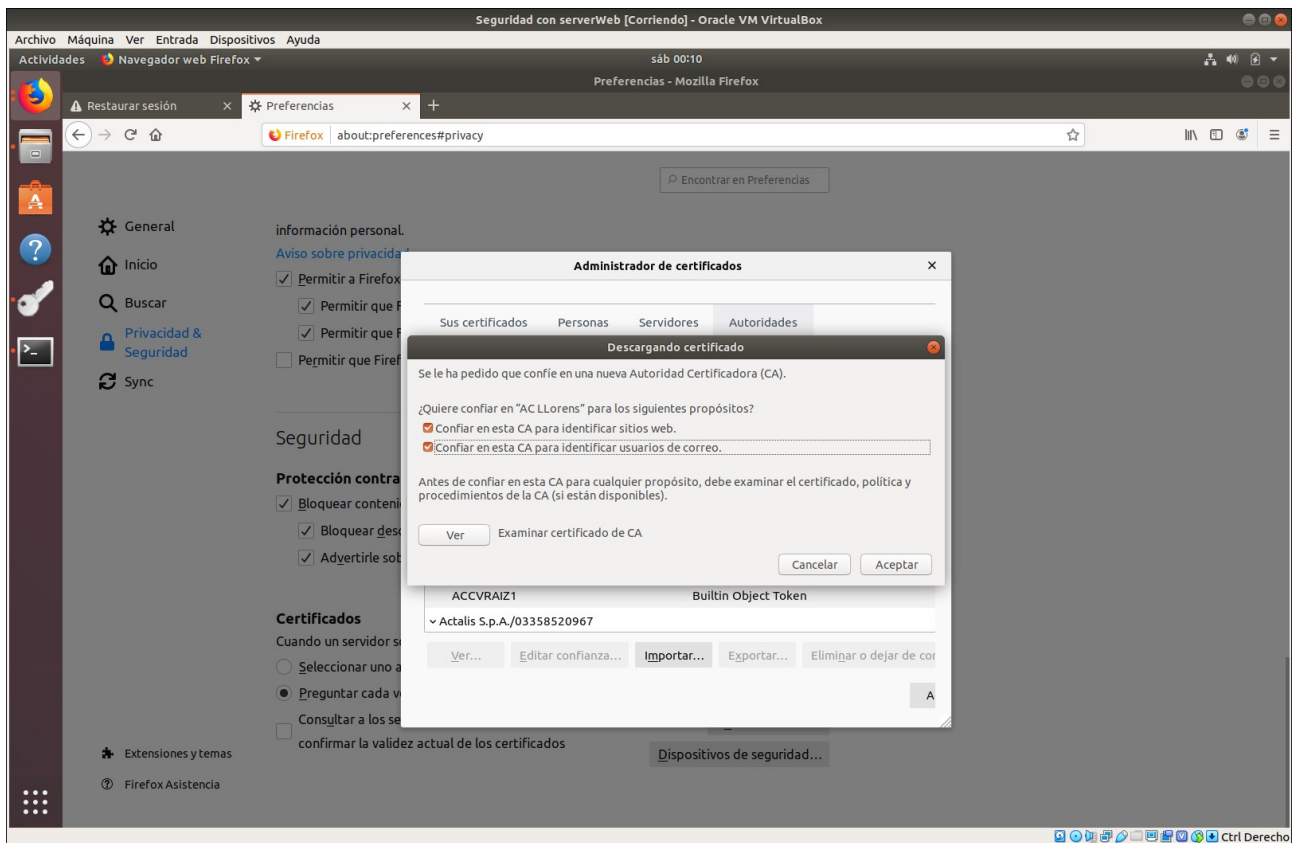


## Práctica 3: Creación de un certificado SSL/TLS multisite

Ya esta creado ahora lo instalamos en Firefox

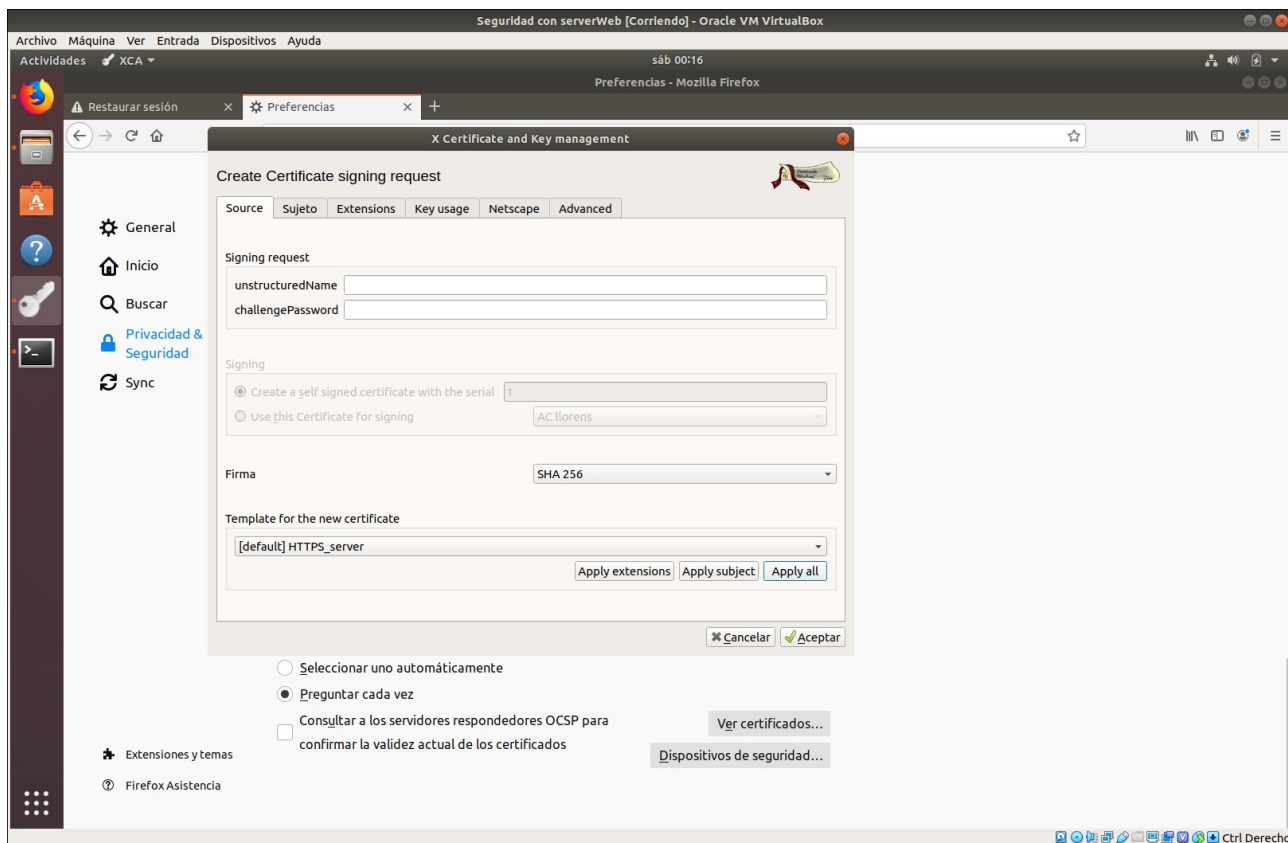


## Práctica 3: Creación de un certificado SSL/TLS multisite



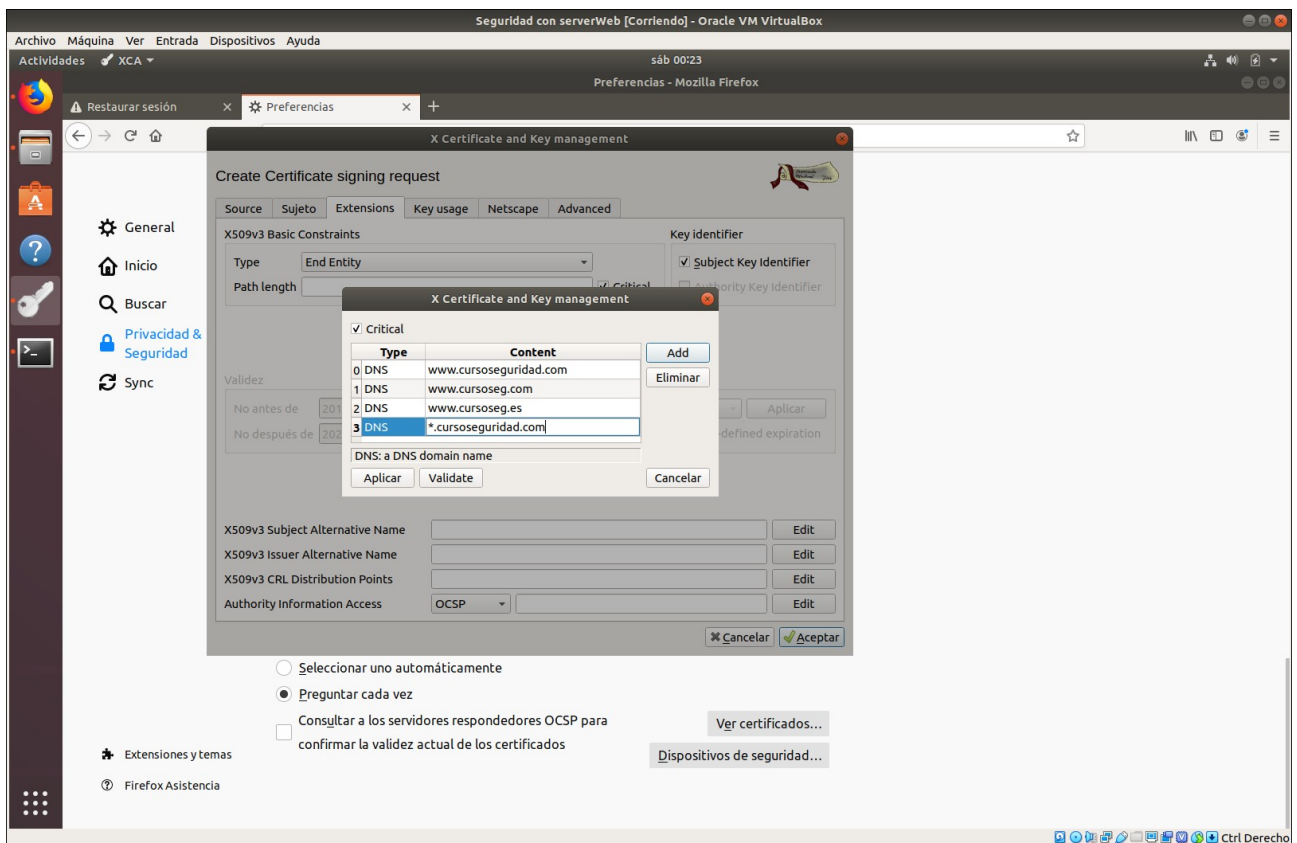
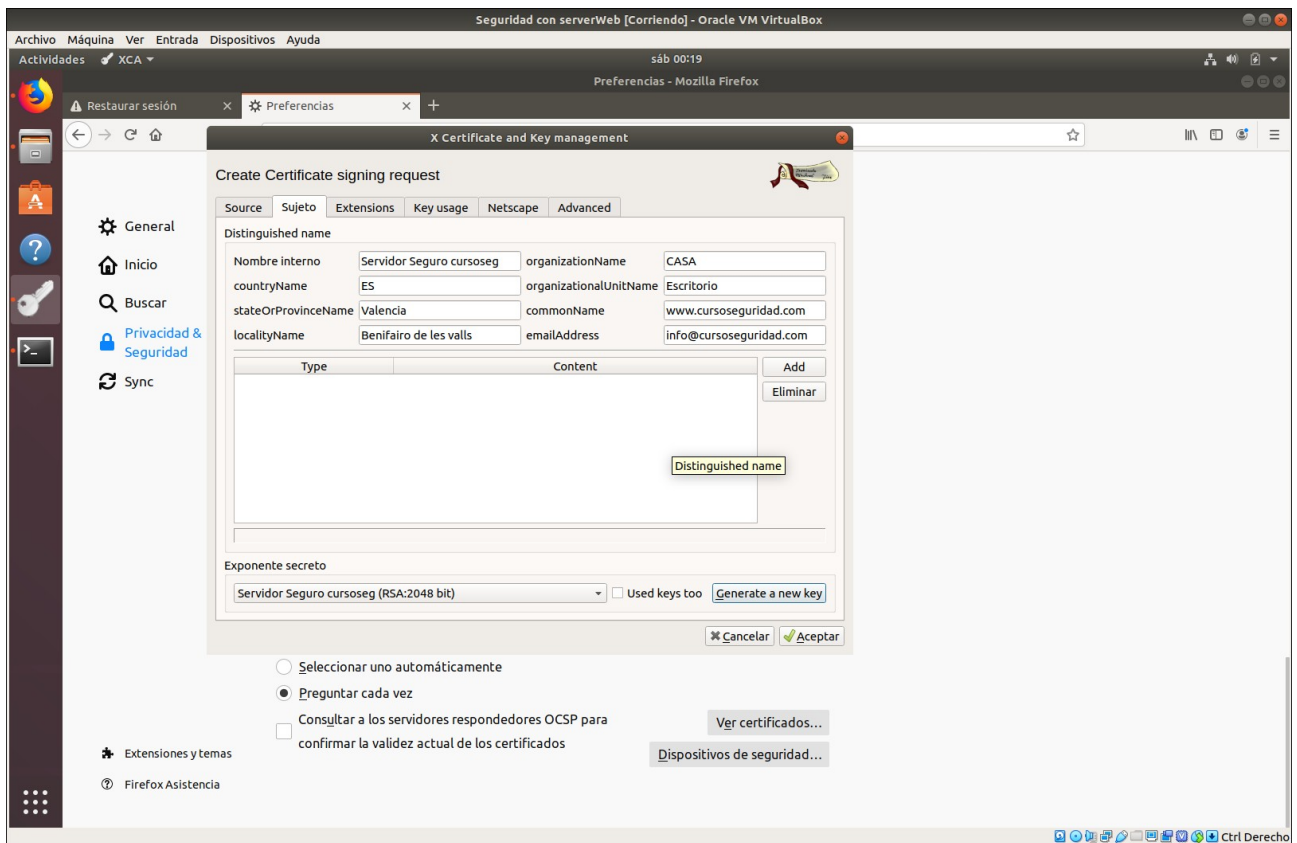
## Práctica 3: Creación de un certificado SSL/TLS multisite

Ahora procedemos a crear un certificado digital para el servidor web de la organización con dominios [www.cursoseguridad.com](http://www.cursoseguridad.com), [www.cursoseg.com](http://www.cursoseg.com), [www.cursoseguridad.es](http://www.cursoseguridad.es) y [www.cursoseg.es](http://www.cursoseg.es)





## Práctica 3: Creación de un certificado SSL/TLS multisite



## Práctica 3: Creación de un certificado SSL/TLS multisite

Una vez creado lo firmamos con todos los pasos de la tarea:

“Asegúrate que está marcado **Copy extensions from the request** para que se copien las extensiones adicionales como Subject Alternate Names del CSR original al certificado que se va a crear. Para evitar

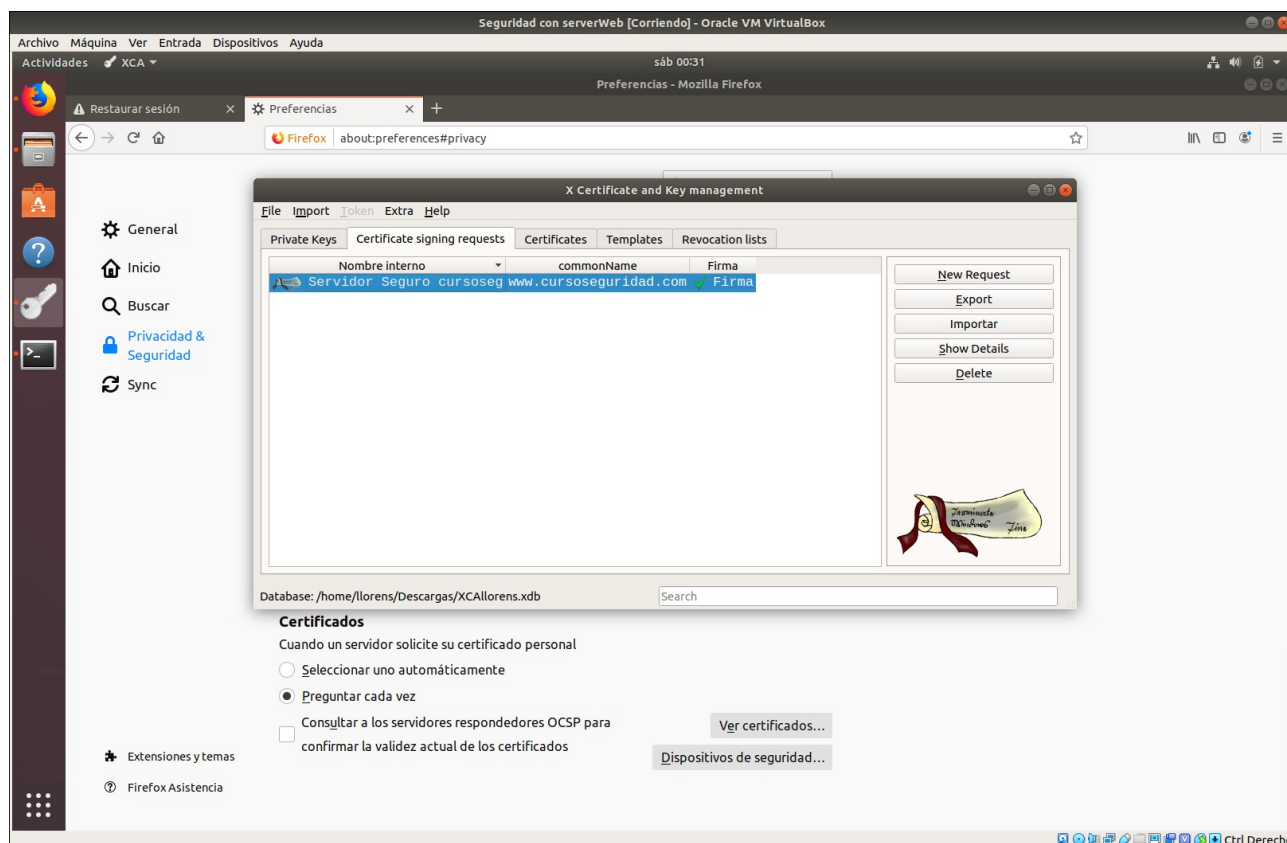
que haya extensiones duplicadas al copiarlas desde la CSR y se produzca un error, en la pestaña **Extensions** selecciona como tipo **Not defined**. Después en la pestaña **Key Usage**, desmarca las tres

opciones marcadas bajo **Key Usage**. En la pestaña **Netscape**, elimina la opción **SSL Server** y el comentario. “

Asegúrate que está marcado **Copy extensions from the request** para que se copien las extensiones adicionales como Subject Alternate Names del CSR original al certificado que se va a crear. Para evitar

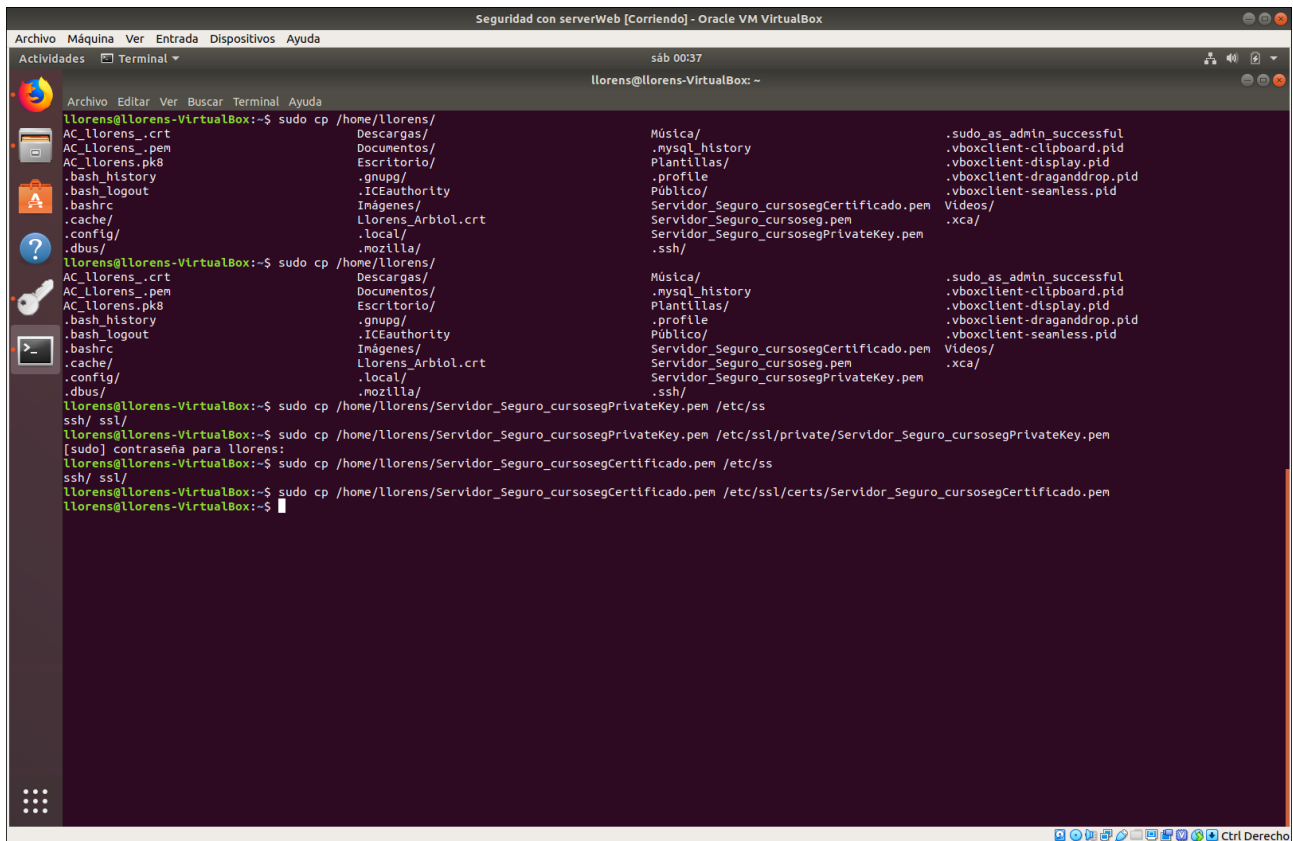
que haya extensiones duplicadas al copiarlas desde la CSR y se produzca un error, en la pestaña **Extensions** selecciona como tipo **Not defined**. Después en la pestaña **Key Usage**, desmarca las tres

opciones marcadas bajo **Key Usage**. En la pestaña **Netscape**, elimina la opción **SSL Server** y el comentario. Finalmente pulsa **Aceptar** y el certificado aparecerá “



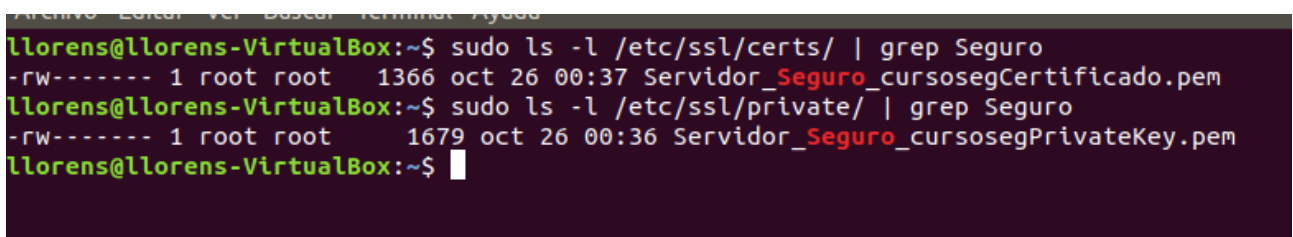
## Práctica 3: Creación de un certificado SSL/TLS multisite

Ahora vamos a exportar la key y el certificado y los copiaremos en el directorio correspondiente /etc/ssl/certs para certificados /etc/ssl/private para claves privadas



```
llorens@llorens-VirtualBox:~$ sudo cp /home/llorens/
AC_llorens.crt      Música/      .sudo_as_admin_successful
AC_llorens.pem      .mysql_history .vboxclient-clipboard.pid
AC_llorens.pk8      Plantillas/ .vboxclient-display.pid
.bash_history       .gnupg/     .vboxclient-draganddrop.pid
.bash_logout        .ICEauthority .vboxclient-seamless.pid
.bashrc             Imágenes/   Videos/
.cache/             Llorens_Arbiol.crt .xca/
.config/            .local/
.dbus/              .mozilla/
llorens@llorens-VirtualBox:~$ sudo cp /home/llorens/
AC_llorens.crt      Música/      .sudo_as_admin_successful
AC_llorens.pem      .mysql_history .vboxclient-clipboard.pid
AC_llorens.pk8      Plantillas/ .vboxclient-display.pid
.bash_history       .gnupg/     .vboxclient-draganddrop.pid
.bash_logout        .ICEauthority .vboxclient-seamless.pid
.bashrc             Imágenes/   Videos/
.cache/             Llorens_Arbiol.crt .xca/
.config/            .local/
.dbus/              .mozilla/
llorens@llorens-VirtualBox:~$ sudo cp /home/llorens/Servidor_Seguro_cursosegPrivateKey.pem /etc/ssl/
ssh/ ssl/
llorens@llorens-VirtualBox:~$ sudo cp /home/llorens/Servidor_Seguro_cursosegPrivateKey.pem /etc/ssl/private/Servidor_Seguro_cursosegPrivateKey.pem
[sudo] contraseña para llorens:
llorens@llorens-VirtualBox:~$ sudo cp /home/llorens/Servidor_Seguro_cursosegCertificado.pem /etc/ssl/
ssh/ ssl/
llorens@llorens-VirtualBox:~$ sudo cp /home/llorens/Servidor_Seguro_cursosegCertificado.pem /etc/ssl/certs/Servidor_Seguro_cursosegCertificado.pem
llorens@llorens-VirtualBox:~$
```

Para ahorrar capturas añadido esta se ve como tiene permisos 600 y es del user root



```
llorens@llorens-VirtualBox:~$ sudo ls -l /etc/ssl/certs/ | grep Seguro
-rw----- 1 root root 1366 oct 26 00:37 Servidor_Seguro_cursosegCertificado.pem
llorens@llorens-VirtualBox:~$ sudo ls -l /etc/ssl/private/ | grep Seguro
-rw----- 1 root root 1679 oct 26 00:36 Servidor_Seguro_cursosegPrivateKey.pem
llorens@llorens-VirtualBox:~$
```

## Práctica 3: Creación de un certificado SSL/TLS multisite

Configuramos el servidor Apache para que funcione con SSL/TTS

Sacado de aquí

<https://www.ochobitshacenunbyte.com/2015/10/14/habilitar-https-servidor-web/>

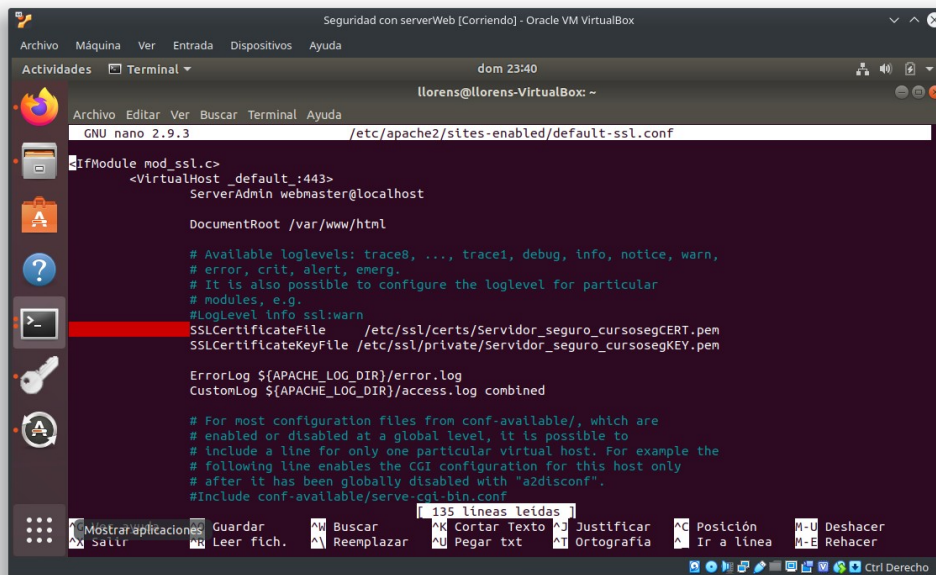
```
llorens@llorens-VirtualBox:~$ a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Could not create /etc/apache2/mods-enabled/socache_shmcb.load: Permission denied
llorens@llorens-VirtualBox:~$ 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:
    systemctl restart apache2
llorens@llorens-VirtualBox:~$ sudo a2ensite default-ssl
ERROR: Site default-ssl does not exist!
llorens@llorens-VirtualBox:~$ sudo a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
    systemctl reload apache2
llorens@llorens-VirtualBox:~$ service apache2 restart
llorens@llorens-VirtualBox:~$
```

## Práctica 3: Creación de un certificado SSL/TLS multisite

Activamos los modulos y editaremos el archivo “/etc/apache2/sites-enabled/default-ssl.conf” para añadir

### NOTA IMPORTANTE

El nombre de los archivos del certificado y la key sufre un cambio de nombre por que no me arrancaba el servidor y volví a repetir la practica unos pasos anteriores.



```
GNU nano 2.9.3 /etc/apache2/sites-enabled/default-ssl.conf

<IfModule mod_ssl.c>
<VirtualHost _default_:443>
    ServerAdmin webmaster@localhost

    DocumentRoot /var/www/html

    # Available loglevels: trace8, ..., trace1, 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
    LogLevel info ssl:warn
    SSLCertificateFile /etc/ssl/certs/Servidor_seguro_cursosegCERT.pem
    SSLCertificateKeyFile /etc/ssl/private/Servidor_seguro_cursosegKEY.pem

    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

135 líneas leídas
```



## Práctica 3: Creación de un certificado SSL/TLS multisite

El servidor Apache me da el siguiente error

```
llorens@llorens-VirtualBox:~$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Drop-In: /lib/systemd/system/apache2.service.d
            └─apache2-systemd.conf
   Active: failed (Result: exit-code) since Wed 2019-10-30 21:48:38 CET; 7s ago
     Process: 2217 ExecStop=/usr/sbin/apachectl stop (code=exited, status=0/SUCCESS)
    Process: 3027 ExecStart=/usr/sbin/apachectl start (code=exited, status=1/FAILURE)
   Main PID: 2076 (code=exited, status=0/SUCCESS)

oct 30 21:48:38 www.cursoseguridad.com systemd[1]: Starting The Apache HTTP Server...
oct 30 21:48:38 www.cursoseguridad.com apachectl[3027]: Action 'start' failed.
oct 30 21:48:38 www.cursoseguridad.com apachectl[3027]: The Apache error log may have more information.
oct 30 21:48:38 www.cursoseguridad.com systemd[1]: apache2.service: Control process exited, code=exited status=1
oct 30 21:48:38 www.cursoseguridad.com systemd[1]: apache2.service: Failed with result 'exit-code'.
oct 30 21:48:38 www.cursoseguridad.com systemd[1]: Failed to start The Apache HTTP Server.
llorens@llorens-VirtualBox:~$
```

He estado tratando lo que puede ser pero no doy con la tecla, así que no puedo avanzar con la practica. Y no he podido realizar la ultima comprobación