Paso 1. Instalar Apache

```
# para Fedora y derivados
sudo dnf install httpd
# para Arch Linux y derivados
sudo pacman -S apache
```

Paso 2. Copiar los certificados

```
# crear un directorio para los certificados SSL
sudo mkdir -p /etc/httpd/ssl
# copiar los certificados generados
# $PKI es el directorio generado por el comando 'easyrsa init-pki'
sudo cp $PKI/ca.rt /etc/httpd/ssl   # ca.rt es la autoridad certificadora
sudo cp $PKI/redes.crt /etc/httpd/ssl  # llave del servidor
sudo co $PKI/redes.key /etc/httpd/ssl  # certificado del servidor
```

Paso 3. Usar los certificados en la configuración

```
# editar el certificado con el editor de su elección
sudo nvim /etc/httpd/conf.d/ssl.conf
```

Una vez dentro del archivo de configuración, hay que buscar las líneas de `SSLCertificateFile`, `SSLCertificateKeyFile` y `SSLCACertificateFile`, y asignarle los certificados copiados.

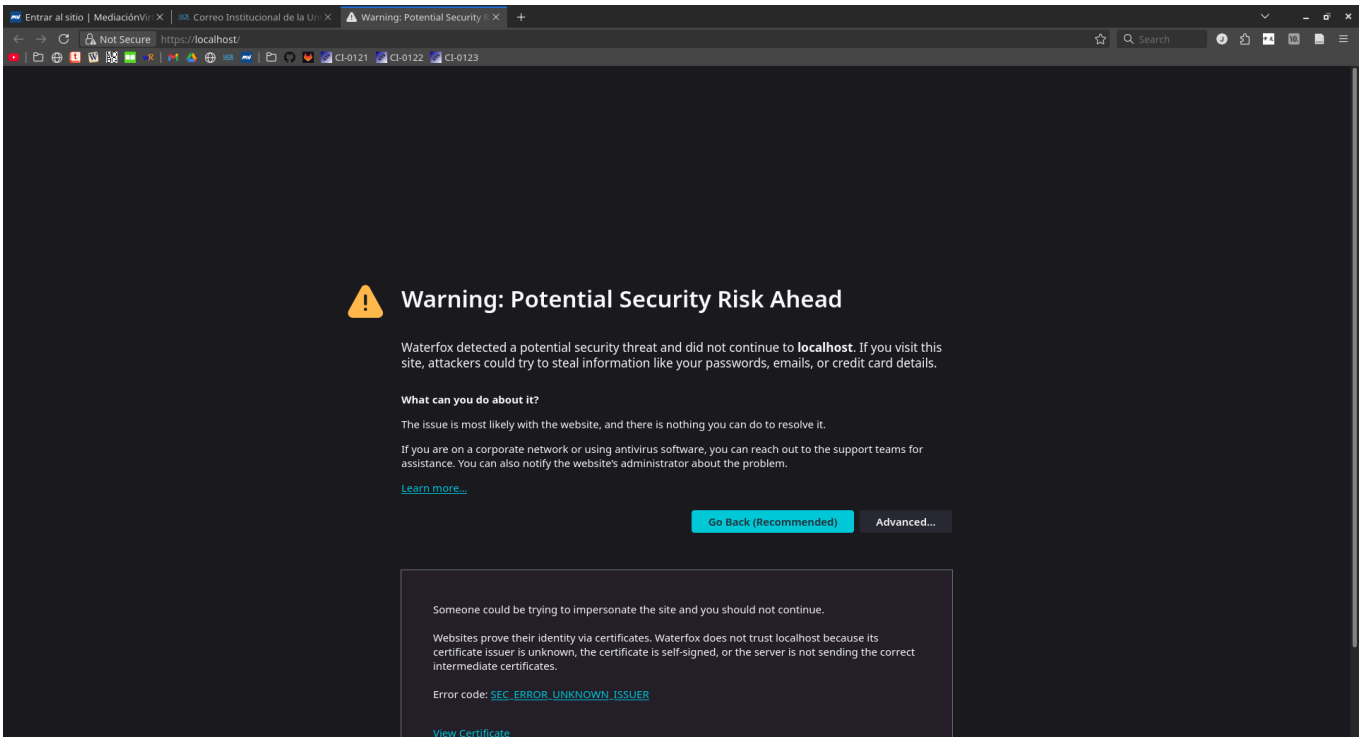
```
SSLCertificateFile /etc/httpd/ssl/redes.crt
SSLCertificateKeyFile /etc/httpd/ssl/redes.key
SSLCACertificateFile /etc/httpd/ssl/ca.crt
```

Paso 4. Habilitar HTTP de Apache

```
sudo systemctl enable httpd --now  # activar el http de Apache
sudo systemctl restart httpd       # reinicar el http para que inicie con el de Apache
```

Paso 5. Probar

Una manera en la que se puede probar que el servicio está funcionando es conectarse al `localhost` desde el navegador. Puesto que las llaves y los certificados están generados automáticamente, los navegadores alzan una alerta de seguridad. Si esta alerta aparece, y, al aceptarla, se accede a la raíz de la máquina local, entonces el servicio está configurado correctamente.



Index of /

Name	Last modified	Size	Description