

PRÁCTICA SERVIDORES WEB


Rodríguez Jácome, David
DESPREGAMENTO DE SITIOS WEB 2º DAW

En esta actividad desplegaremos dos sitios web para acceder a ellos mediante el navegador a través de un dominio. Para ello usaremos dos máquinas virtuales: una con SO Ubuntu que actuará de servidor y otra con SO Windows 10 que actuará de cliente, ambas ejecutadas con VirtualBox.

En la configuración de red pondremos las máquinas en modo puente; respecto a las IPs de las máquinas, a la máquina servidor le asignaremos la dirección 192.168.0.200 y máscara de subred 255.255.255.0, mientras que a la máquina cliente le asignaremos la dirección 192.168.0.201 y máscara de subred 255.255.255.0.

1. Instalación del servidor apache.

Partiremos del punto de que ya tenemos una máquina Ubuntu 20 limpia. Mediante la terminal comprobaremos si hay actualizaciones disponibles con “sudo apt update” y actualizaremos si es necesario.

A screenshot of a terminal window titled 'david@david-VirtualBox: ~'. The terminal shows the command 'sudo apt update' being executed. It prompts for a password, then lists four update objects from Ubuntu repositories. It reports that 3 packages can be updated and suggests running 'apt list --upgradable' for more details. The prompt returns to 'david@david-VirtualBox:~\$'.

```
david@david-VirtualBox:~$ sudo apt update
[sudo] contraseña para david:
Obj:1 http://es.archive.ubuntu.com/ubuntu focal InRelease
Obj:2 http://security.ubuntu.com/ubuntu focal-security InRelease
Obj:3 http://es.archive.ubuntu.com/ubuntu focal-updates InRelease
Obj:4 http://es.archive.ubuntu.com/ubuntu focal-backports InRelease
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se pueden actualizar 3 paquetes. Ejecute «apt list --upgradable»
para verlos.
david@david-VirtualBox:~$
```

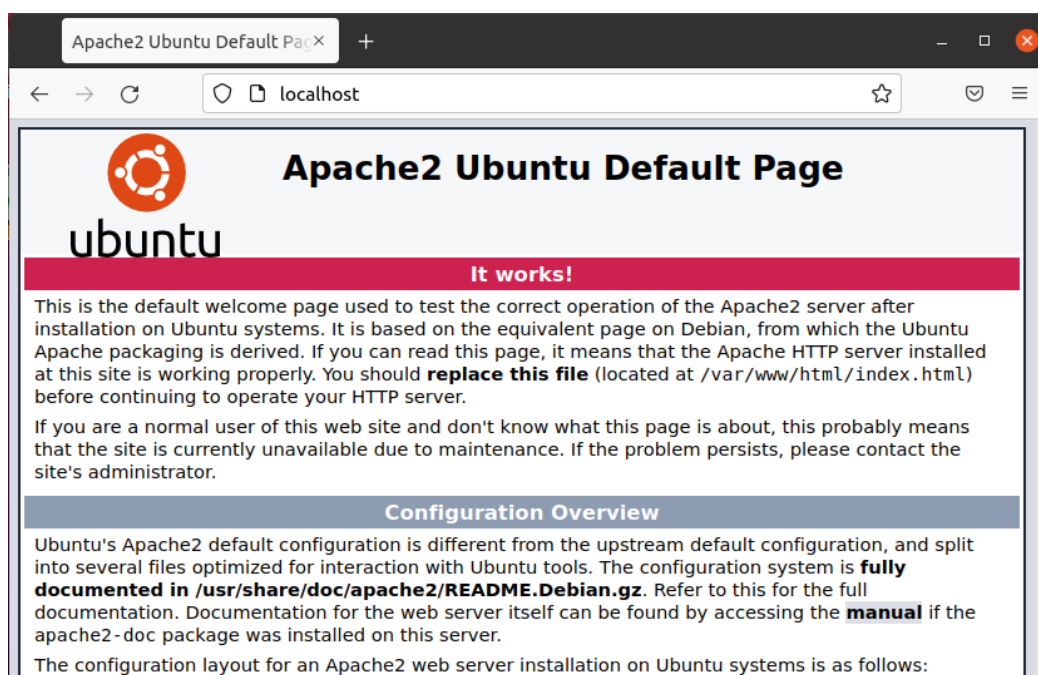
Seguidamente usaremos “sudo apt install -y apache2” para instalar Apache en el sistema.

```
david@david-VirtualBox:~$ sudo apt install -y apache2
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.
 chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi
 libgstreamer-plugins-bad1.0-0 libva-wayland2
 Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
 apache2-bin apache2-data apache2-utils libapr1 libaprutil1
 libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.2-0
 Paquetes sugeridos:
 apache2-doc apache2-suexec-pristine | apache2-suexec-custom
 Se instalarán los siguientes paquetes NUEVOS:
 apache2 apache2-bin apache2-data apache2-utils libapr1
 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
 liblua5.2-0
 0 actualizados, 9 nuevos se instalarán, 0 para eliminar y 3 no actualizados.
Se necesita descargar 1.820 kB de archivos.
Se utilizarán 7.945 kB de espacio de disco adicional después de esta operación.
```

Podemos comprobar que se ha instalado correctamente mediante “sudo service apache2 status” y accediendo mediante el navegador.

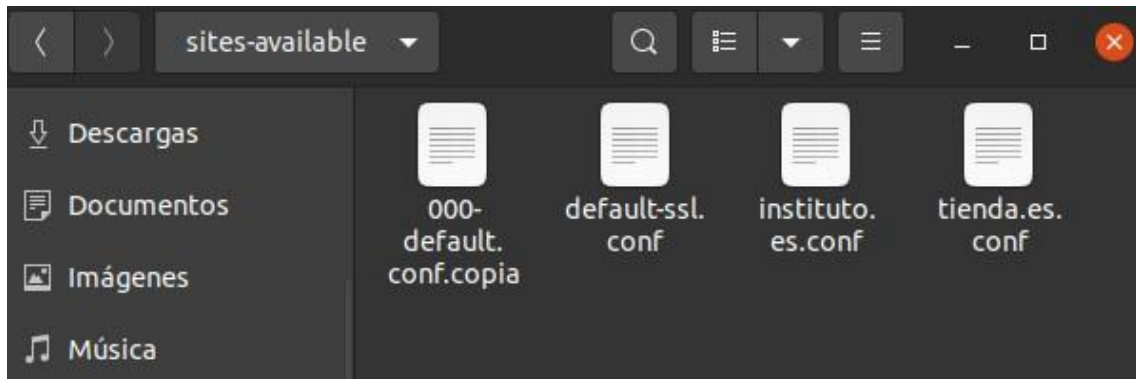
```
david@david-VirtualBox:~$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2021-11-22 19:30:30 CET; 3min 17s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 2644 (apache2)
    Tasks: 55 (limit: 2299)
   Memory: 4.8M
    CGroup: /system.slice/apache2.service
           └─2644 /usr/sbin/apache2 -k start
             └─2645 /usr/sbin/apache2 -k start
               └─2646 /usr/sbin/apache2 -k start

nov 22 19:30:30 david-VirtualBox systemd[1]: Starting The Apache HTTP Server...
nov 22 19:30:30 david-VirtualBox apache2[2643]: AH00558: apache2: Could not reliably determine
nov 22 19:30:30 david-VirtualBox systemd[1]: Started The Apache HTTP Server.
lines 1-15/15 (END)
```

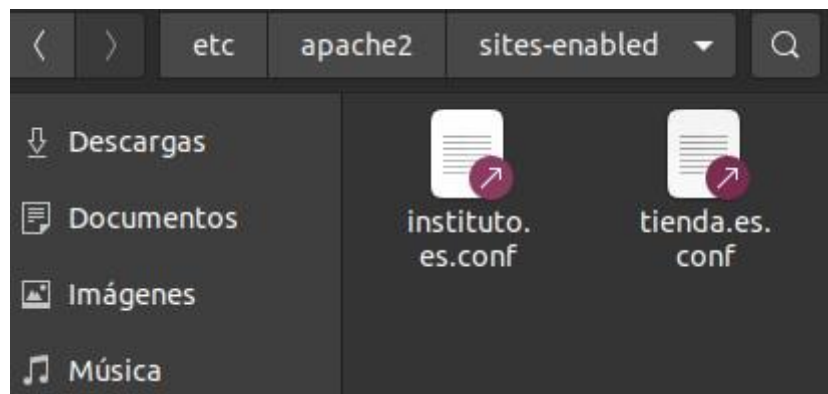


1.2. Desplegar dos sitios virtuales.

Ahora iremos a la carpeta “sites-available” dentro del directorio “apache2” y clonaremos el archivo “000-default.conf” para engendrar otros dos y renombrarlos como “instituto.es.conf” y “tienda.es.conf”.

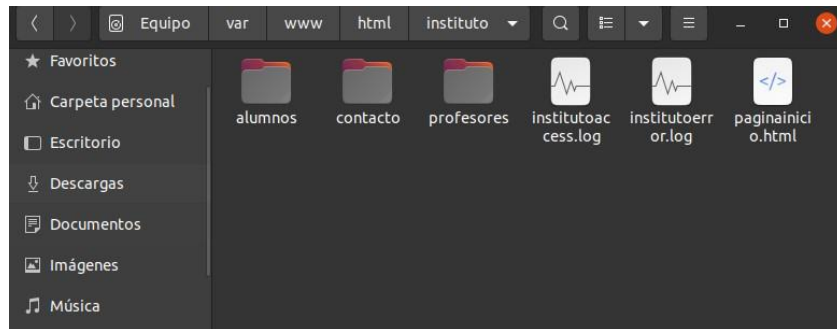


Luego eliminaremos el archivo “000-default.conf” y mediante la terminal ejecutaremos el comando “sudo a2dissite 000-default.conf” para eliminar el sitio por defecto y además ejecutaremos “sudo a2ensite instituto.es.conf” y “sudo a2ensite tienda.es.conf” para habilitar ambos sitios virtuales. Reiniciaremos Apache con “sudo service apache2 restart”.



1.2.1. Primer sitio virtual: instituto.

Para el primer sitio crearemos la siguiente estructura con tres carpetas (alumnos, profesores y contacto) que tendrán sus respectivos archivos HTML, además de un archivo HTML en el directorio raíz llamado “paginainicio.html”.

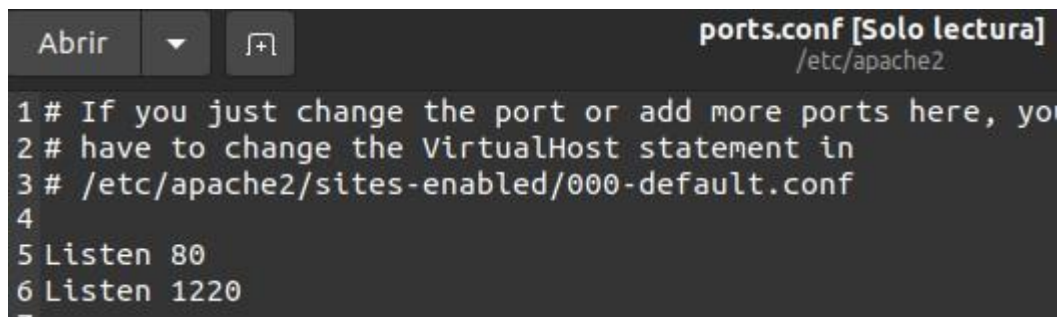


Crearemos un host virtual para el instituto editando el archivo “instituto.es.conf” en el directorio “sites-available” con las siguientes líneas:

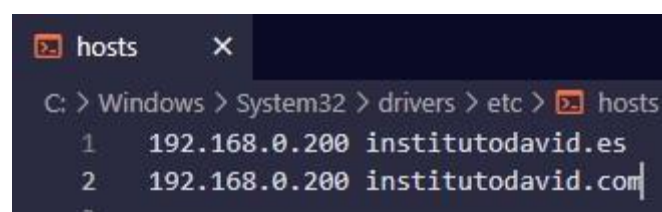
```
<VirtualHost *:1220>

    ServerName institutodavid.es
    ServerAlias instituto.com
    DocumentRoot /var/www/html/instituto
    DirectoryIndex paginainicio.html
```

Para el puerto de escucha iremos al archivo “ports.conf” en el directorio “apache2” y añadimos la línea “Listen 1220”.



En la máquina cliente editaremos el archivo “hosts” para que se pueda conectar al sitio web del instituto:



Estableceremos un alias para el sitio web editando el enlace del archivo HTML “paginainicio” que refiere al apartado “Contacto” añadiendo en dicho enlace “/info/”:

```
<body>
  <h1>Página Inicio instituto; ruta: /var/www/html/instituto/</h1>
  <p><a href="profesores/pagprofesores.html">Profesores</a></p>
  <p><a href="alumnos/pagalumnos.html">Alumnos</a></p>
  <p><a href="alumnos/pagantiguosalumnos.html">Antiguos alumnos</a></p>
  <p><a href="/info/datoscontacto.html">Contacto</a></p>
```

Además, incluiremos la línea “Alias /info /var/www/html/instituto/contacto” en el archivo “instituto.es.conf” junto con el Directory para contacto:

```
Alias /info /var/www/html/instituto/contacto

<Directory /var/www/html/instituto/contacto>
  AllowOverride None
  Require all granted
</Directory>
```

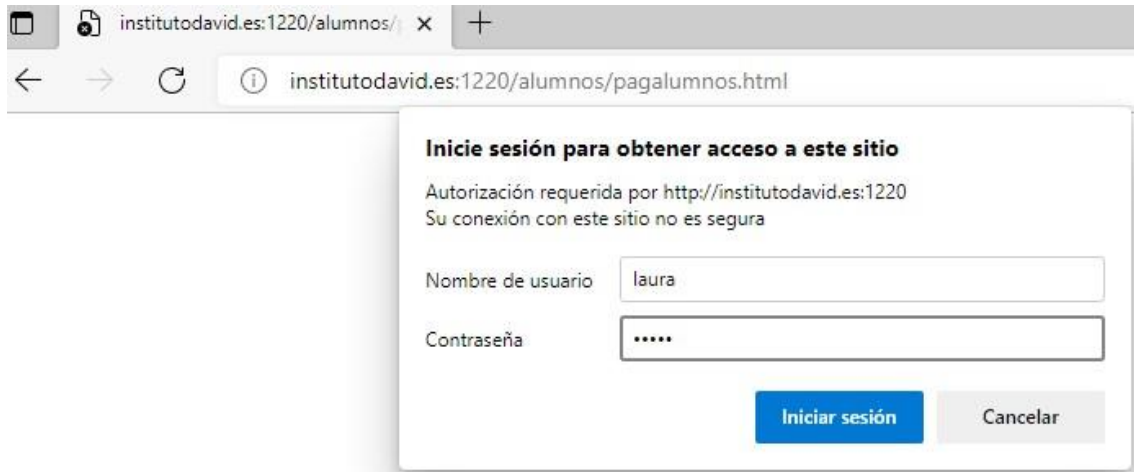
Ahora crearemos los usuarios alumnos Juan, Laura y Sara que podrán acceder con autenticación basic a la carpeta “alumnos” mediante terminal con “sudo htpasswd -c /etc/apache2/contr_basic juan”, “sudo htpasswd /etc/apache2/contr_basic laura” y “sudo htpasswd /etc/apache2/contr_basic sara”. Las contraseñas serán los nombres de los alumnos. Seguidamente añadiremos en el fichero de configuración “instituto.es.conf” la autenticación de los alumnos:

```
<Directory /var/www/html/instituto/alumnos>
  AuthType Basic
  AuthName "Para alumnos"
  AuthBasicProvider file
  AuthUserFile "/etc/apache2/contr_basic"
  AuthGroupFile "/etc/apache2/grupos"
  Require group alumnos
  Require valid-user
</Directory>
```

También crearemos un archivo llamado “grupos” con los alumnos:

```
Abrir grupos [Solo lectura] /etc/apache2
1 alumnos: juan laura sara
```

Habilitamos el grupo de alumnos con “sudo a2enmod authz_groupfile” y reiniciamos Apache. Comprobamos que funciona en la máquina cliente:



Página alumnos; ruta: /var/www/instituto/alumnos/

[Volver a inicio](#)

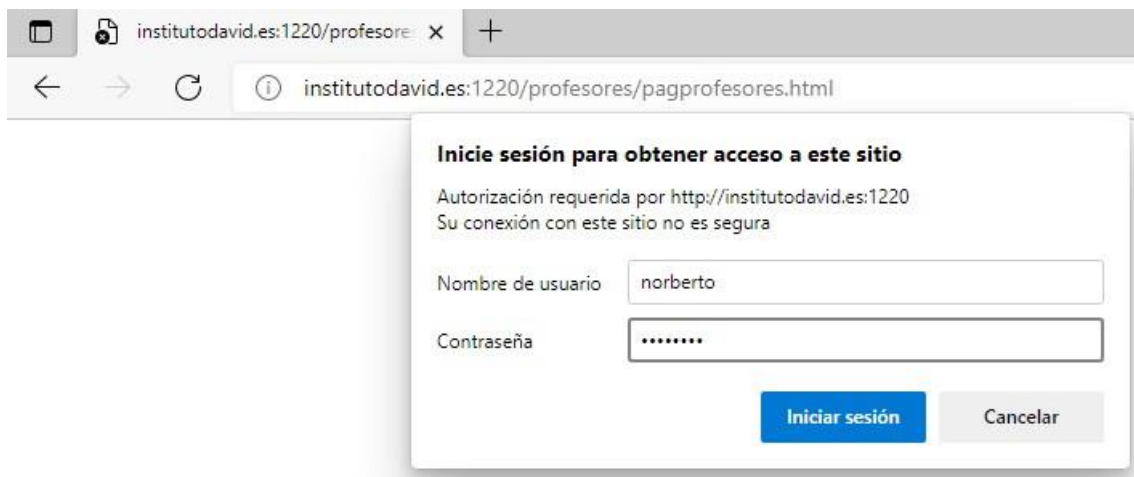
Ahora crearemos a los usuarios profesores Norberto y Andrea para que puedan acceder con autenticación digest a la carpeta “profesores” mediante terminal con “sudo htdigest -c /etc/apache2/contr_digest profesores norberto” y “sudo htdigest /etc/apache2/contr_digest profesores andrea”. Además, incluiremos la Directory correspondiente en el archivo de configuración “instituto.es.conf”. Las contraseñas de los profesores serán los nombres de los mismos:

```
<Directory /var/www/html/instituto/profesores>
    AllowOverride All
    Require all granted
</Directory>
```


En el siguiente paso crearemos un archivo `.htaccess` en la carpeta “profesores” y lo editaremos con el siguiente contenido:

```
.htaccess x
var > www > html > instituto > profesores > .htaccess
1  AuthType Digest
2  AuthName "profesores"
3  AuthBasicProvider file
4  AuthUserFile "/etc/apache2/contr_digest"
5  Require user norberto andrea
```

Reiniciamos Apache y comprobamos que funciona en la máquina cliente:



Finalmente, en el archivo de configuración “instituto.es.conf” añadimos una serie de líneas para los ficheros de log con un mensaje de error 404 personalizado:

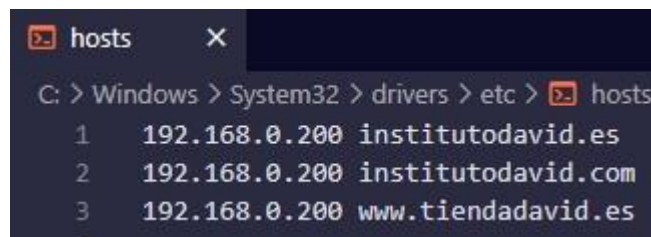
```
LogLevel info
ErrorLog /var/www/html/instituto/institutoerror.log
CustomLog /var/www/html/instituto/institutoaccess.log combined
ErrorDocument 404 "Se ha producido un error 404"
```


Estos ficheros se almacenarán en el directorio raíz del instituto:

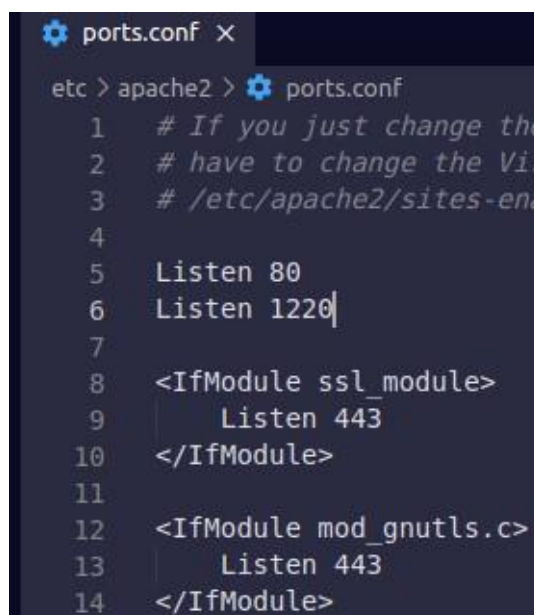


1.3. Segundo sitio virtual.

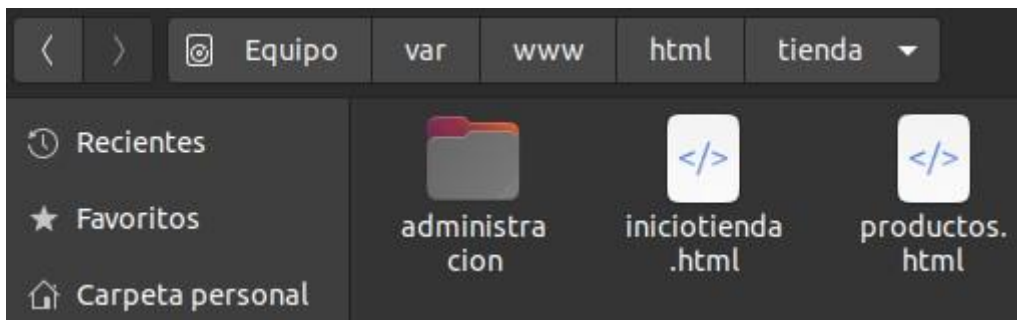
El segundo sitio virtual será una tienda online. Lo primero será añadir una nueva línea en el archivo “hosts” de la máquina cliente:



El siguiente paso será habilitar el puerto de escucha 443, que por defecto ya está habilitado.



Ahora crearemos la estructura de archivos de la tienda online en /var/www/html/:



Seguidamente abrimos una terminal y ejecutamos una serie de comandos.

```
sudo a2enmod ssl

openssl genrsa -out clave-privada.key 2048

openssl req -new -key clave-privada.key -out solicitud-certificado.csr
openssl x509 -req -days 365 -in solicitud-certificado.csr -signkey clave-privada.key -out certificado-autofirmado.crt

sudo mv clave-privada.key /etc/ssl/private/
sudo mv certificado-autofirmado.crt /etc/ssl/certs/
```

Habilitamos el módulo SSL con “sudo a2enmod ssl” y reiniciamos el servidor Apache. Ahora nos situamos dentro del directorio de la tienda web y creamos la clave privada para el sitio web de la tienda con “openssl genrsa -out clave-privada.key 2048”, y creamos el certificado añadiendo los datos que nos pida con “openssl req -new -key clave-privada.key -out solicitud-certificado.csr” y “openssl x509 -req -days 365 -in solicitud-certificado.csr -signkey clave-privada.key -out certificado-autofirmado.crt”.

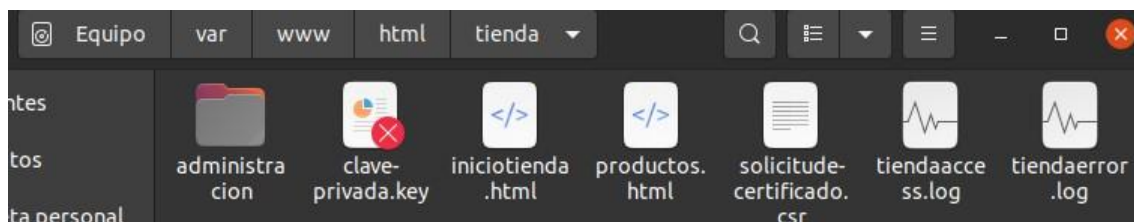
```
david@david-VirtualBox:~/certificados$ openssl x509 -req -days 365 -in solicitud-certificado.csr
-signkey clave-privada.key -out certificado-autofirmado.crt
Signature ok
subject=C = ES, ST = Pontevedra, L = Poio, O = DAW, OU = DAW, CN = David
Getting Private key
```

Con “mv clave-privada.key /etc/ssl/private/” y “mv certificado-autofirmado.crt /etc/ssl/certs/” copiaremos los certificados a los directorios correspondientes, y con “sudo chown root:ssl-cert /etc/ssl/private/clave-privada.key”, “sudo chmod 644 /etc/ssl/private/clave-privada.key” y “sudo chown root:ssl-cert /etc/ssl/certs/certificado-autofirmado.crt” modificaremos los propietarios y los permisos.

A continuación, iremos al archivo de configuración “tienda.es.conf” y lo editaremos así:

```
<IfModule mod_ssl.c>
  <VirtualHost *:443>
    ServerName tiendadavid.es
    DocumentRoot /var/www/html/tienda
    DirectoryIndex iniciotienda.html
    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/certificado-autofirmado.crt
    SSLCertificateKeyFile /etc/ssl/private/clave-privada.key
```

```
LogLevel info
ErrorLog /var/www/html/tienda/tiendaerror.log
CustomLog /var/www/html/tienda/tiendaaccess.log combined
ErrorDocument 404 "Se ha producido un error 404"
```



Ahora crearemos dos usuarios para la carpeta “administración” con autenticación digest:

```
sudo a2enmod auth_digest
sudo a2ensite tienda.es.conf
sudo service apache2 restart

sudo htdigest -c /etc/apache2/contr_digest xestion pepe
sudo htdigest /etc/apache2/contr_digest xestion manolo
```

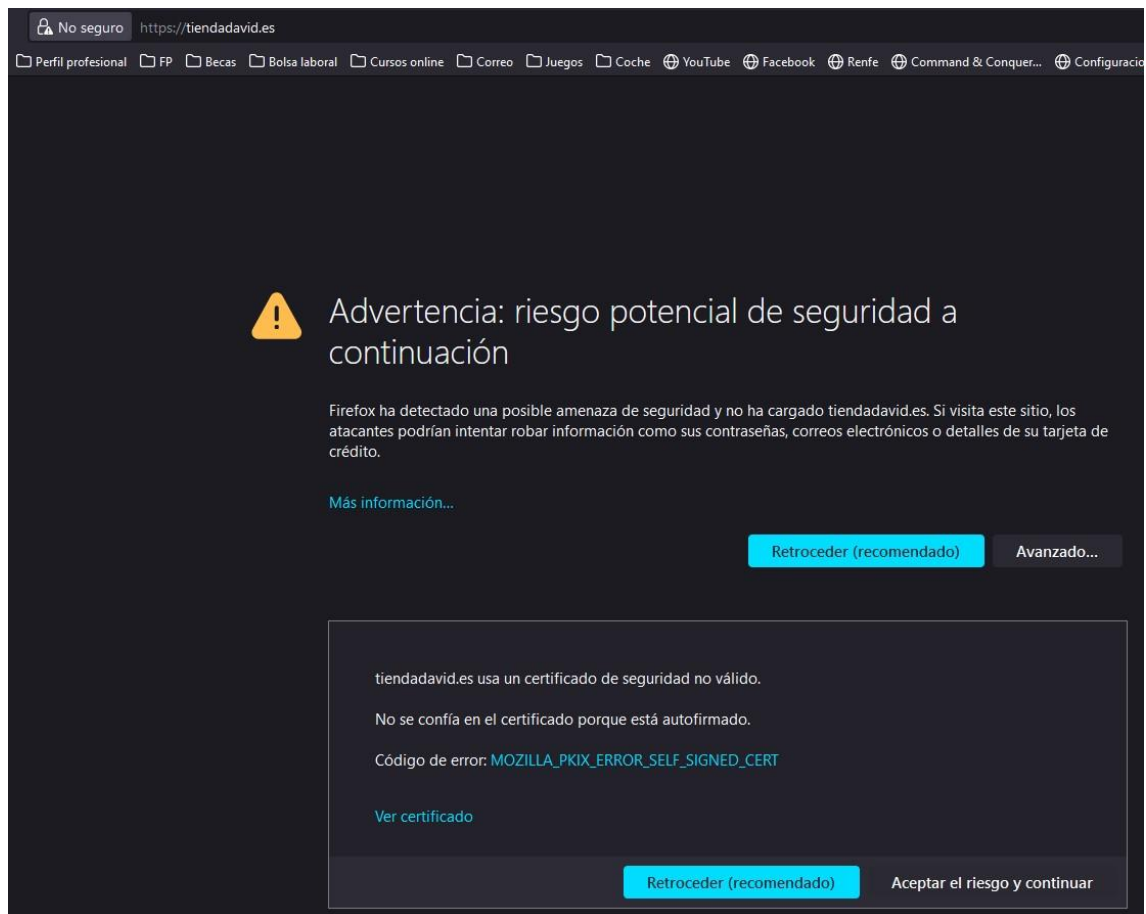
Finalmente, editamos el archivo “tienda.es.conf” añadiendo el siguiente Directory y reiniciamos el servidor Apache:

```
<Directory /var/www/html/tienda/administracion>
  AuthType Digest
  AuthName "xestion"
  AuthBasicProvider file
  AuthUserFile "/etc/apache/contr_digest"
  Require user pepe manolo
</Directory>
```

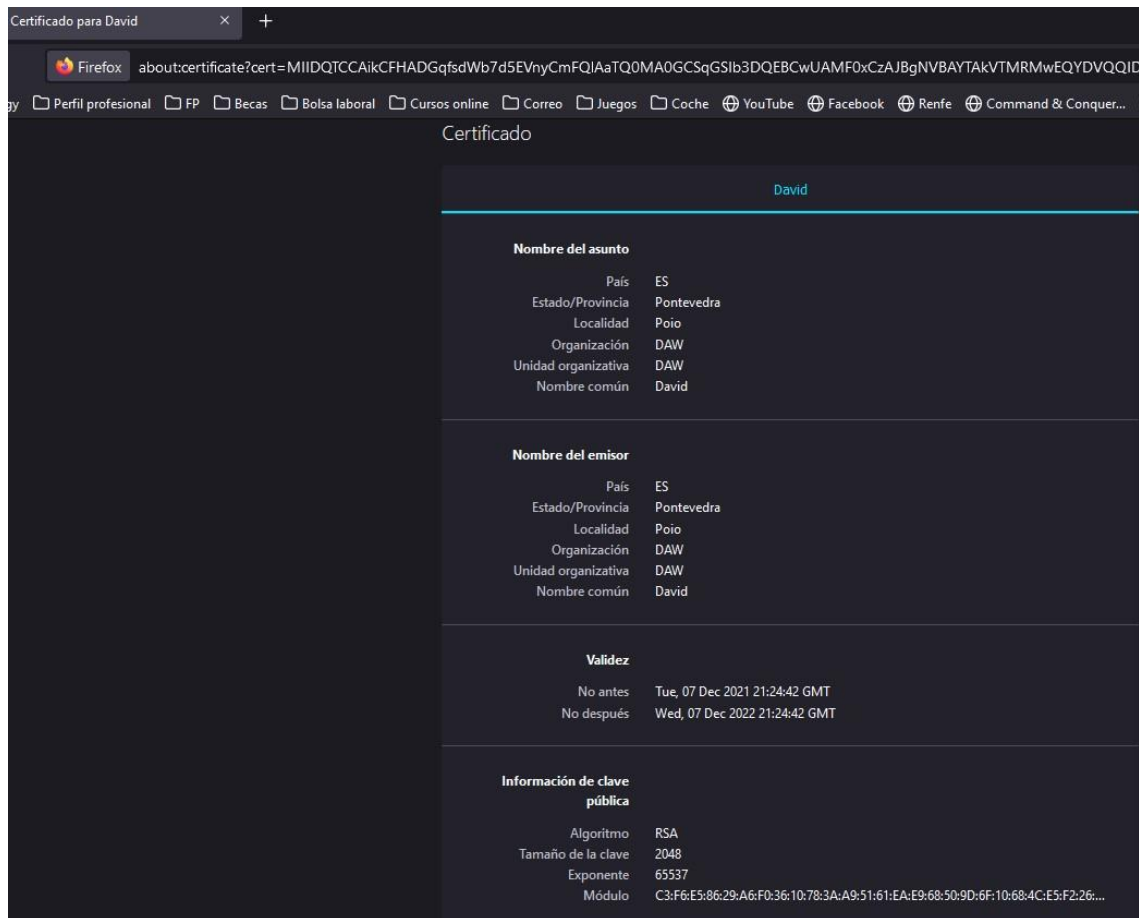
Ahora comprobamos que debemos usar HTTPS para acceder al sitio web de la tienda:



Al acceder mediante HTTPS se nos mostrará un mensaje de advertencia porque no se ha podido verificar el certificado que nosotros mismos hemos creado, pero es un error esperable ya que dicho certificado no ha sido emitido por una autoridad competente.



Sin embargo, dicho certificado sí se tiene en cuenta a la hora de visitar el sitio web, tal y como vemos al clicar sobre el certificado del sitio:



Y finalmente, comprobamos que al tratar de acceder al enlace “administración”, deberá saltar un control de acceso de usuarios:

