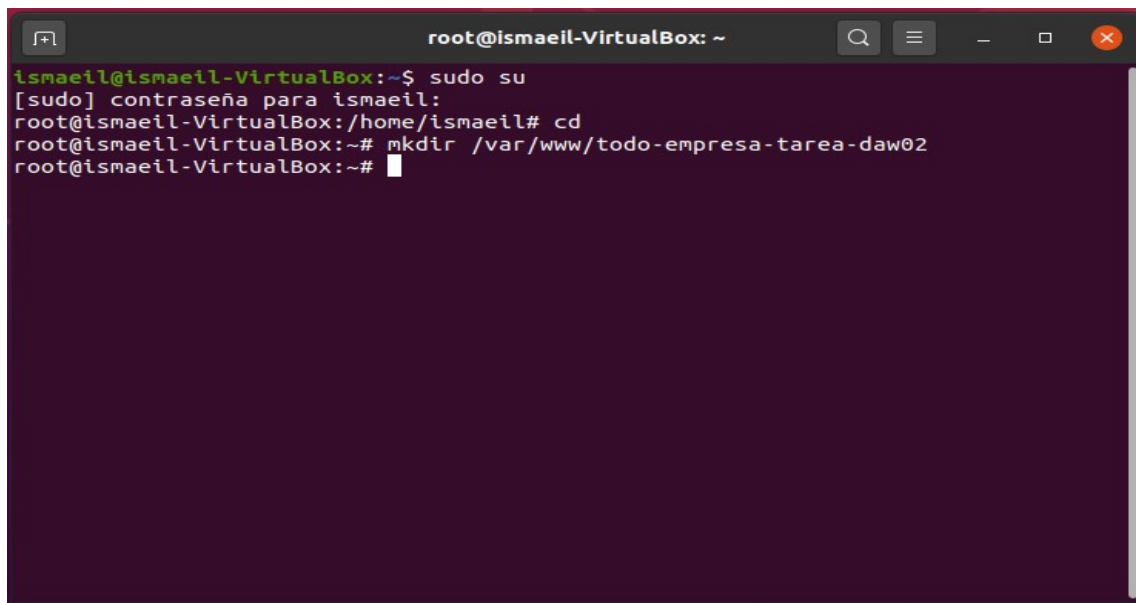


Tarea para DAW02:

- Configurar un **virtualhost basado en nombre** denominado **empresa-tarea-daw02** que permita el acceso de la página web de la empresa en Internet al directorio del servidor web: **todo-empresa-tarea-daw02**.

Para poder realizar esto, Nos dirigimos al terminal y nos identificamos como usuario **root**, mediante el uso del código **sudo su**, y luego escribimos nuestra contraseña y así estaremos identificados como usuario **root**, después nos situamos en la carpeta **/var/www** para crear el directorio “**todo-empresa-tarea-daw02**” ejecutando :

mkdir /var/www/todo-empresa-tarea-daw02



```
root@ismaeil-VirtualBox: ~  
ismaeil@ismaeil-VirtualBox:~$ sudo su  
[sudo] contraseña para ismaeil:  
root@ismaeil-VirtualBox:/home/ismaeil# cd  
root@ismaeil-VirtualBox:~# mkdir /var/www/todo-empresa-tarea-daw02  
root@ismaeil-VirtualBox:~#
```

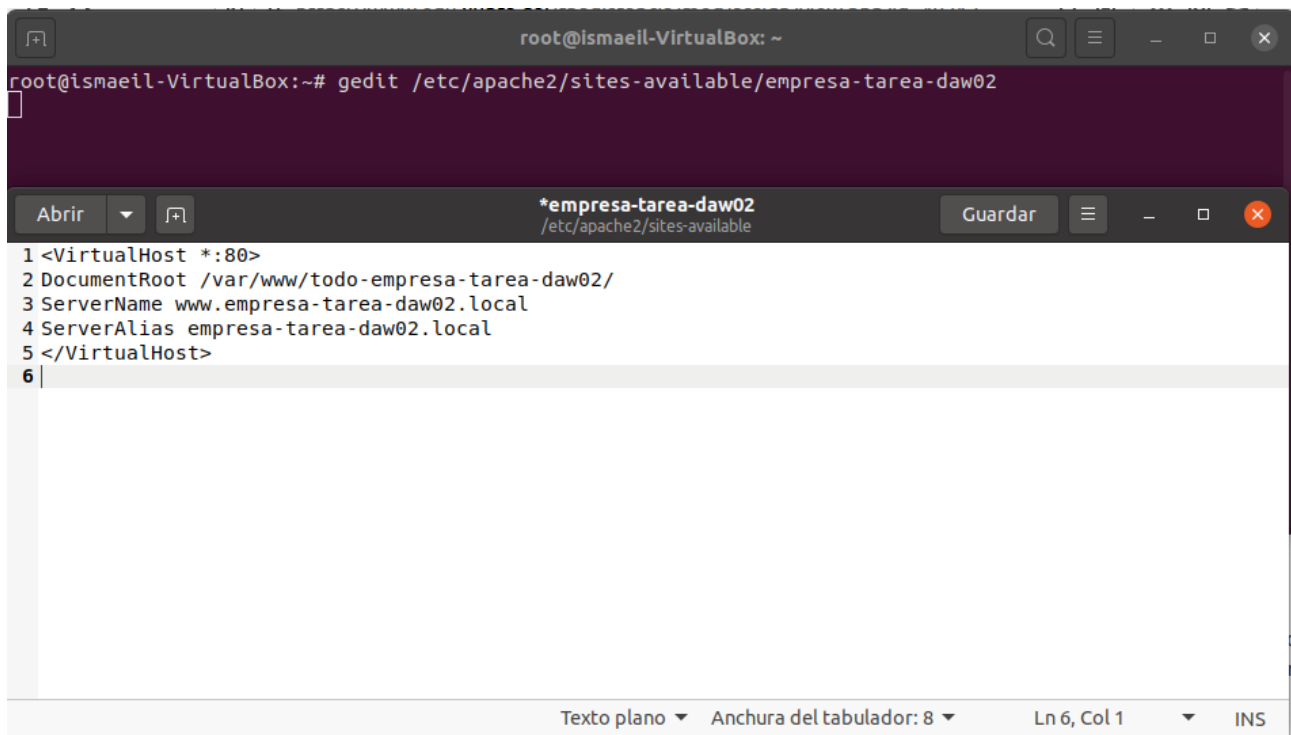
Y Ahora vamos a crear el fichero de configuración para el virtualhost ejecutando el siguiente código:

gedit /etc/apache2/sites-available/empresa-tarea-daw02

y dentro del fichero escribimos el siguiente código:

```
<VirtualHost *:80>  
DocumentRoot /var/www/todo-empresa-tarea-daw02/  
ServerName www.empresa-tarea-daw02.local  
ServerAlias empresa-tarea-daw02.local  
</VirtualHost>
```

y ahora al añadir el **serverName** y el **serverAlias** en nuestra fichero **todo-empresa-tarea-daw02** tendremos el apartado 2 hecho también.



```
root@ismaeil-VirtualBox: ~  
root@ismaeil-VirtualBox:~# gedit /etc/apache2/sites-available/empresa-tarea-daw02  
  
*empresa-tarea-daw02  
/etc/apache2/sites-available  
Guardar  
1 <VirtualHost *:80>  
2 DocumentRoot /var/www/todo-empresa-tarea-daw02/  
3 ServerName www.empresa-tarea-daw02.local  
4 ServerAlias empresa-tarea-daw02.local  
5 </VirtualHost>  
6  
Texto plano Anchura del tabulador: 8 Ln 6, Col 1 INS
```

Después de guardar el fichero, vamos a activar el VirtualHost ejecutando el siguiente código:

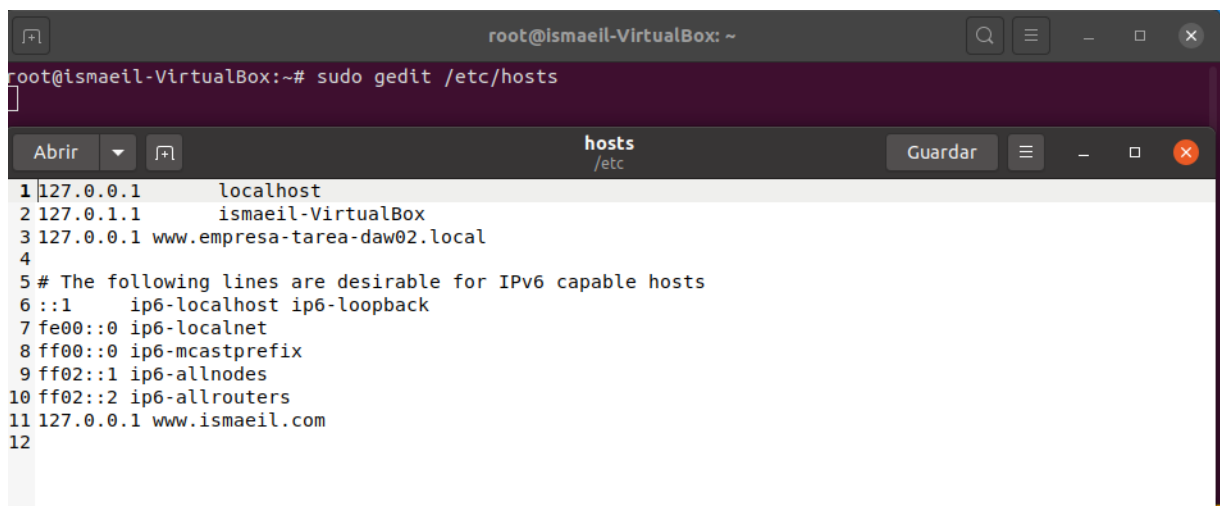
a2ensite empresa-tarea-daw02.local

Ahora vamos a darle de alta a nuestro dominio en el servidor DNS para que nuestro servidor pueda recibir las peticiones, y para hacer eso tenemos que dirigirnos al fichero **etc/hosts** mediante el uso de este código:

sudo gedit etc/hosts

y añadimos esta linea de código:

127.0.0.1 www.empresa-tarea-daw02.local

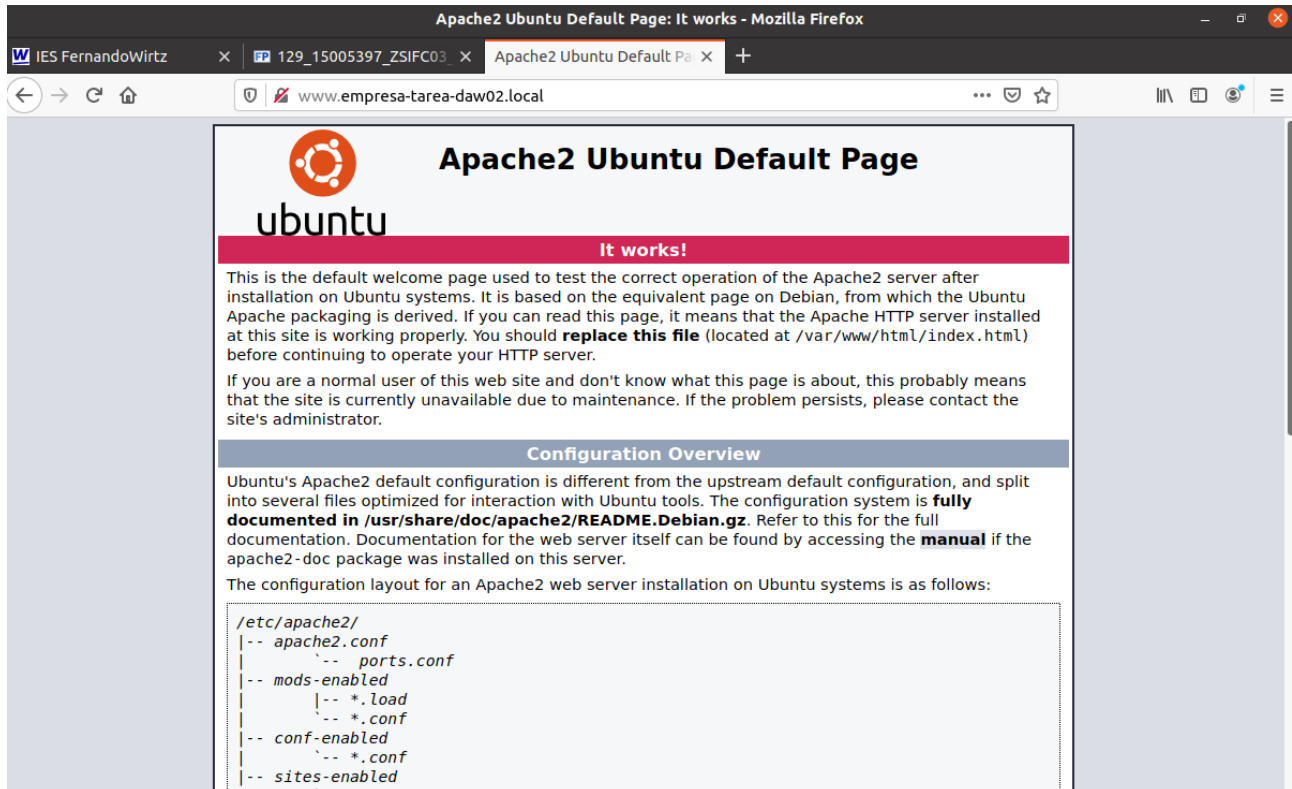


```
root@ismaeil-VirtualBox: ~  
root@ismaeil-VirtualBox:~# sudo gedit /etc/hosts  
  
hosts  
/etc  
Guardar  
1 127.0.0.1 localhost  
2 127.0.1.1 ismaeil-VirtualBox  
3 127.0.0.1 www.empresa-tarea-daw02.local  
4  
5 # The following lines are desirable for IPv6 capable hosts  
6 ::1 ip6-localhost ip6-loopback  
7 fe00::0 ip6-localnet  
8 ff00::0 ip6-mcastprefix  
9 ff02::1 ip6-allnodes  
10 ff02::2 ip6-allrouters  
11 127.0.0.1 www.ismaeil.com  
12
```

y ahora para ver que está funcionando, nos dirigimos al navegador y escribimos el nuestra URL:

www.empresa-tarea-daw02.local

Y así se muestra a continuación:



- Hacer accesible a través de Internet las siguientes URL que identifican a la empresa: **www.empresa-tarea-daw02.local y empresa-tarea-daw02.local**.

Después de configurar el archivo **etc/hosts** y añadir las rutas:

www.empresa-tarea-daw02.local y empresa-tarea-daw02.local

Al **ServerName** y **ServerAlias**, ahora estas rutas son accesibles desde la URL en el navegador.

- Configurar en el servidor el **tipo MIME** posible que permite la identificación correcta del vídeo presentación formato **flv** situado dentro del directorio **videos** y de nombre **entrada.flv**.

Para poder realizarlo tenemos que dirigirnos al fichero **/etc/mime.types** y después añadimos esta línea:

video/x-flv

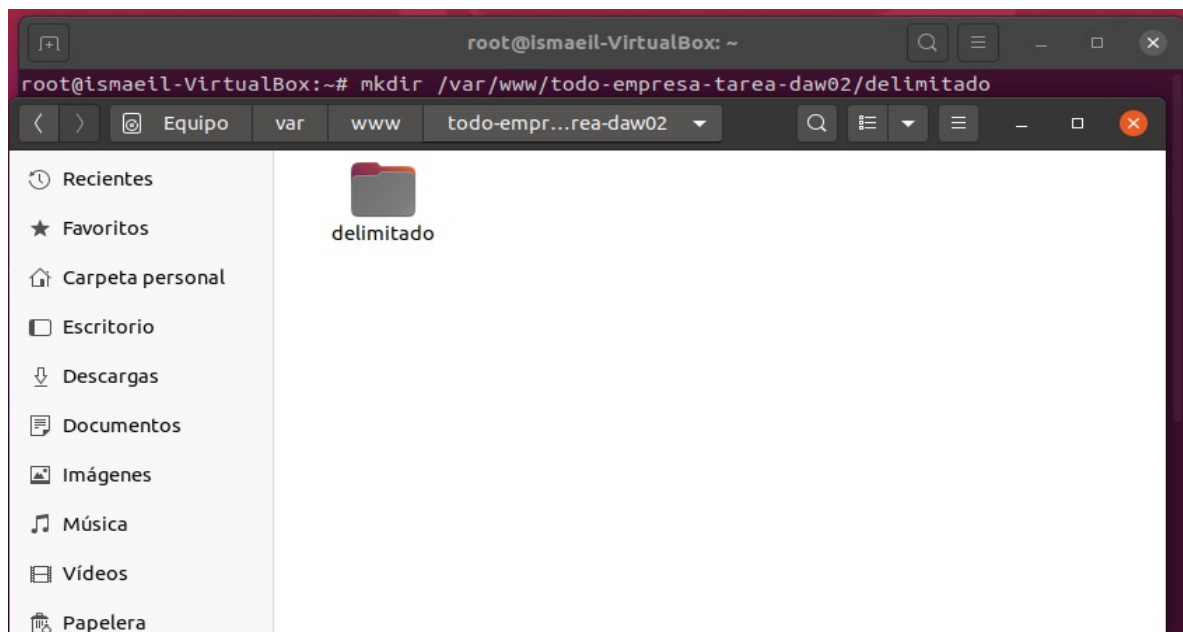
pero en mi caso ya estaba añadida, y eso nos indica que los fichero de video de tipo **flv** son reconocidos por mi servidor.

```
root@ismaeil-VirtualBox: ~  
root@ismaeil-VirtualBox:~# sudo gedit /etc/mime.types  
mime.types  
/etc  
Abrir Guardar  
828 video/vnd.mts  
829 video/vnd.nokia.interleaved-multimedia  
830 video/vnd.vivo  
831 video/x-flv flv  
832 video/x-la-asf lsf lsx  
833 video/x-mng mng  
834 video/x-ms-asf asf asx  
835 video/x-ms-wm wm  
836 video/x-ms-wmv wmv  
837 video/x-ms-wmx wmx  
838 video/x-ms-wvx wvx  
839 video/x-msvideo avi  
840 video/x-sgi-movie movie  
841 video/x-matroska mpv mkv  
842  
843 x-conference/x-cooltalk ice  
844  
845 x-epoc/x-sisx-app sisx  
846 x-world/x-vrml vrm vrml wrl  
Matlab Anchura del tabulador: 8 Ln 831, Col 1 INS
```

- Crear el subdirectorio **todo-empresa-tarea-daw02/delimitado** teniendo en cuenta que:
 - El directorio **todo-empresa-tarea-daw02** permite el acceso a cualquier usuario.
 - El subdirectorio **todo-empresa-tarea-daw02/delimitado** permite el acceso solamente al personal de la empresa que tenga el rol: **admin**.

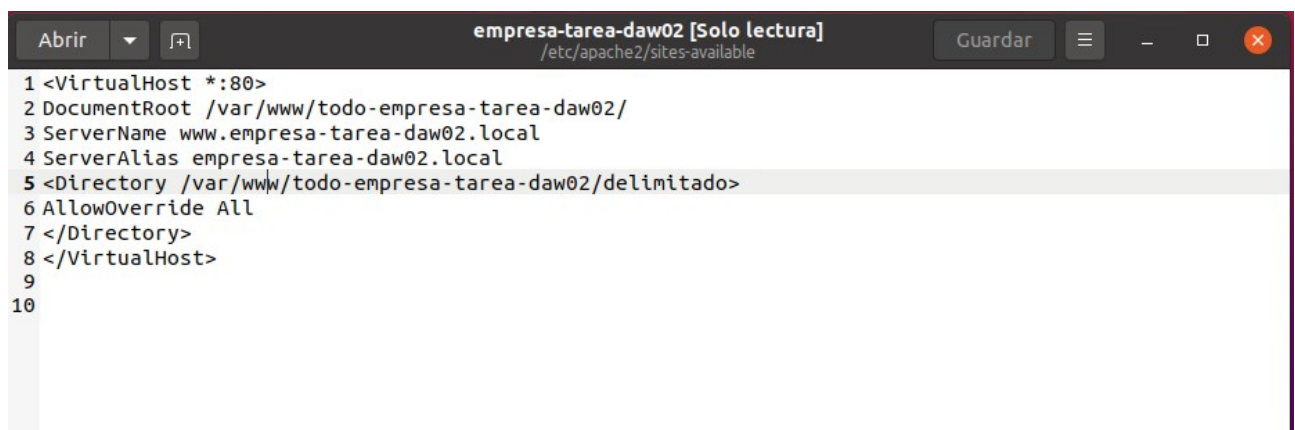
Vamos a crear el directorio **todo-empresa-tarea-daw02/delimitado** para diferenciar el acceso a los usuarios que no tienen el rol **admin**, así para ello desde el terminal nos dirigimos a la carpeta **/var/www** ejecutando el siguiente código:

mkdir var/www/todo-empresa-tarea-daw02/delimitado



Después de crear el subdirectorio, nos dirigimos al fichero de configuración del **virtualhost** que hemos creado antes y le añadimos la siguiente línea para que empiece a restringir el acceso a los usuarios:

```
<Directory var/www/todo-empresa-tarea-daw02/delimitado>
AllowOverride All
</Directory>
```



Y ahora vamos a crear el fichero **.htaccess** dentro del directorio que queremos controlar y en este caso será en **delimitado** y le añadimos el siguiente código :

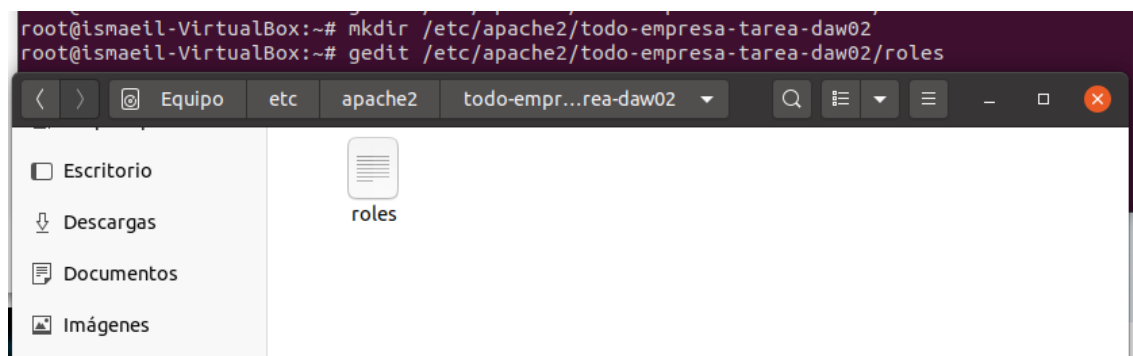


The screenshot shows a terminal window with the command prompt `root@ismaeil-VirtualBox: ~`. The user has executed `gedit /var/www/todo-empresa-tarea-daw02/delimitado/.htaccess`. The gedit editor is open, showing the following content in the `.htaccess` file:

```
1 AuthType Basic
2 AuthName "Area restringida para administradores"
3 AuthUserFile /etc/apache2/todo-empresa-tarea-daw02/passwd
4 AuthGroupFile /etc/apache2/todo-empresa-tarea-daw02/roles
5 Require group admin
```

The status bar at the bottom of the gedit window indicates "Texto plano", "Anchura del tabulador: 8", "Ln 5, Col 20", and "INS".

Y ahora después de indicarle al servidor que nos restrinja el acceso de los usuarios, vamos a crear el fichero **roles** dentro de `etc/apache2/todo-empresa-tarea-daw02/` y dentro del fichero escribimos el siguiente código:



admin: root ismaeil

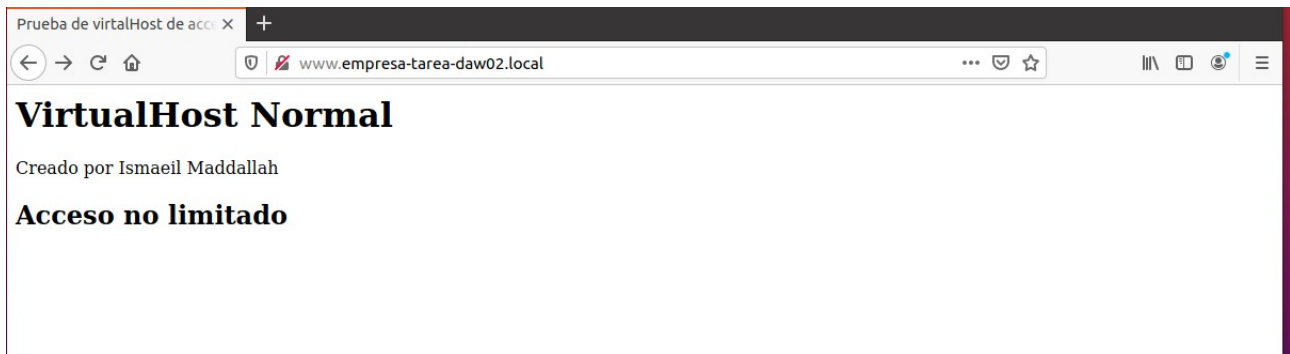
y así ya tenemos 2 usuarios de tipo **admin** que son **root** y **ismaeil**.

y ahora como ya tenemos los usuarios creados, vamos a crear sus contraseñas mediante el uso del comando **htpasswd** y con la ayuda del parámetro **-c**.

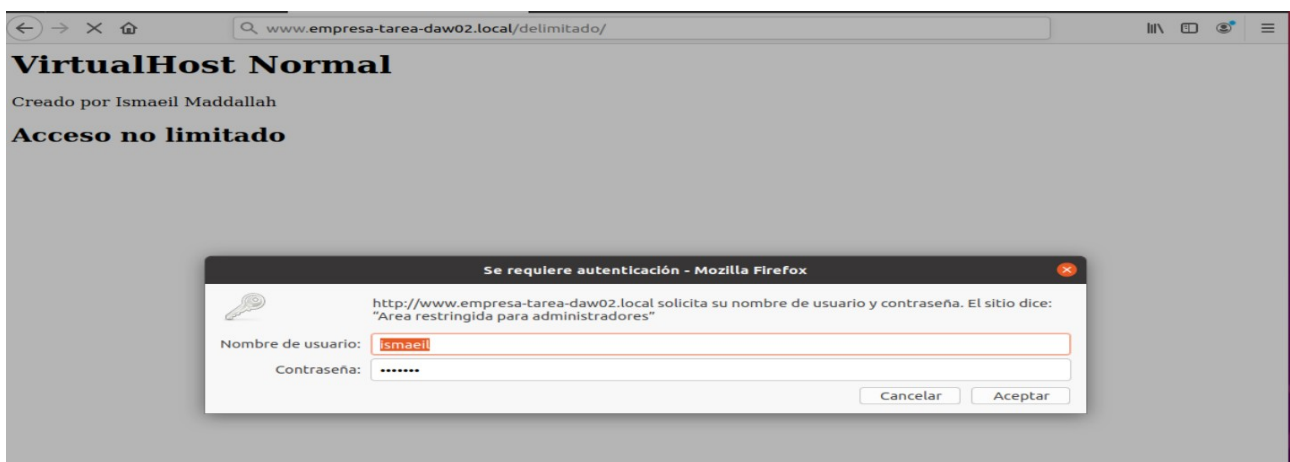
htpasswd -c /etc/apache2/todo-empresa-tarea-daw02/passwd ismaeil

y nos pedirá una contraseña y le indicamos la que queremos, y ahora reiniciamos nuestro servidor y ahora lo tenemos listo.

Y ahora como se muestra a continuación, vemos que el acceso a un ejemplo creado antes en nuestro servidor:



Y ahora para probar el acceso del root o del admin ismaeil, escribimos en la barra de URL lo siguiente:
www.empresa-tarea-daw02.local/delimitado y nos pedirá usuario y contraseña, le metemos lo que nos pide y vemos lo que se muestra a continuación:



Y ahora vemos en la siguiente imagen como se mostrará nuestra página :



- Permitir el protocolo HTTPS en el **virtualhost empresa-tarea-daw02**

Para poder permitir el protocolo HTTPS, tendríamos que instalar el openssl con el siguiente código:

apt-get install openssl

```

root@ismaeil-VirtualBox:~# 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 (1.1.1f-1ubuntu2).
fijado openssl como instalado manualmente.
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
 libfprint-2-tod1 linux-headers-5.4.0-42 linux-headers-5.4.0-42-generic
 linux-image-5.4.0-42-generic linux-modules-5.4.0-42-generic
 linux-modules-extra-5.4.0-42-generic
Utilice «sudo apt autoremove» para eliminarlos.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 59 no actualizados.

```

y después vamos a activarlo con el siguiente código :

a2enmod ssl

y después reiniciamos el servidor con el siguiente código:

service apache2 restart

```

root@ismaeil-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.
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
root@ismaeil-VirtualBox:~# service apache2 restart

```

Ahora vamos a crear un nuevo directorio que contiene los certificados y lo llamamos **ssl** y luego nos situamos dentro de ella y creamos una clave privada a través de la herramienta de generación aleatoria y mediante el siguiente código:

openssl genrsa -des3 -out server.key 1024

Ahora nos pide escribir una palabra que lo va a pedir en caso que reiniciar el servidor.

```

root@ismaeil-VirtualBox:~# mkdir /etc/apache2/ssl
root@ismaeil-VirtualBox:~# cd /etc/apache2/ssl
root@ismaeil-VirtualBox:/etc/apache2/ssl# openssl genrsa -des3 -out server.key 1024
Generating RSA private key, 1024 bit long modulus (2 primes)
....+++++
....+++++
e is 65537 (0x010001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:

```

Ahora vamos a crear un archivo con la extensión csr mediante el siguiente código :

openssl req -new -key server.key -out server.csr

y ahora nos pedirá unos datos y donde nos pide el **Common Name** le ponemos la ruta de nuestro dominio y es: www.empresa-tarea-daw02.local


```

root@ismaeil-VirtualBox:/etc/apache2/ssl# 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]:sp
State or Province Name (full name) [Some-State]:coruña
Locality Name (eg, city) []:a coruña
Organization Name (eg, company) [Internet Widgits Pty Ltd]:iess fernando wirtz
Organizational Unit Name (eg, section) []:fernando wirtz
Common Name (e.g. server FQDN or YOUR name) []:www.empresa-tarea-daw02.local
Email Address []:esmaeelalasmr302@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:.
An optional company name []:.

```

Ahora vamos a generar autofirmado de autoridad certificada mediante el siguiente código y le ponemos que caduque en 500 días por ejemplo:

openssl x509 -req -days 500 -in server.csr -signkey server.key -out server.crt

```

root@ismaeil-VirtualBox:/etc/apache2/ssl# openssl x509 -req -days 500 -in server.csr -signkey server.key -out server.crt

```

Ahora vamos a crear el VirtualHost que contiene los certificados y la carpeta donde se ubica mediante el siguiente código:

mkdir var/www/todo-empresa-tarea-daw02-ssl

y después nos dirigimos al fichero sites-available y lo copiamos y llamamos el nuevo fichero **empresa-tarea-daw02-ssl**

```

root@ismaeil-VirtualBox:~# mkdir /var/www/todo-empresa-tarea-daw02-ssl
root@ismaeil-VirtualBox:~# cd /etc/apache2/sites-available
root@ismaeil-VirtualBox:/etc/apache2/sites-available# cp empresa-tarea-daw02 empresa-tarea-daw02-ssl

```

Ahora vamos a editar su contenido añadiendo el fichero de mi certificado y el fichero clave de mi certificado:

```

root@ismaeil-VirtualBox:/etc/apache2/sites-available# gedit empresa-tarea-daw02-ssl

```



The screenshot shows a gedit editor window titled 'empresa-tarea-daw02-ssl [Solo lectura]' with the file path '/etc/apache2/sites-available'. The content of the file is as follows:

```

1 <VirtualHost *:443>
2
3 ServerAdmin webmaster@empresa-tarea-daw02.local
4 ServerName www.empresa-tarea-daw02.local
5 ServerAlias empresa-tarea-daw02.local
6 DocumentRoot /var/www/todo-empresa-tarea-daw02-ssl/
7 SSLEngine on
8 SSLCertificateFile /etc/apache2/ssl/server.crt
9 SSLCertificateKeyFile /etc/apache2/ssl/server.pem
10
11 </VirtualHost>
12

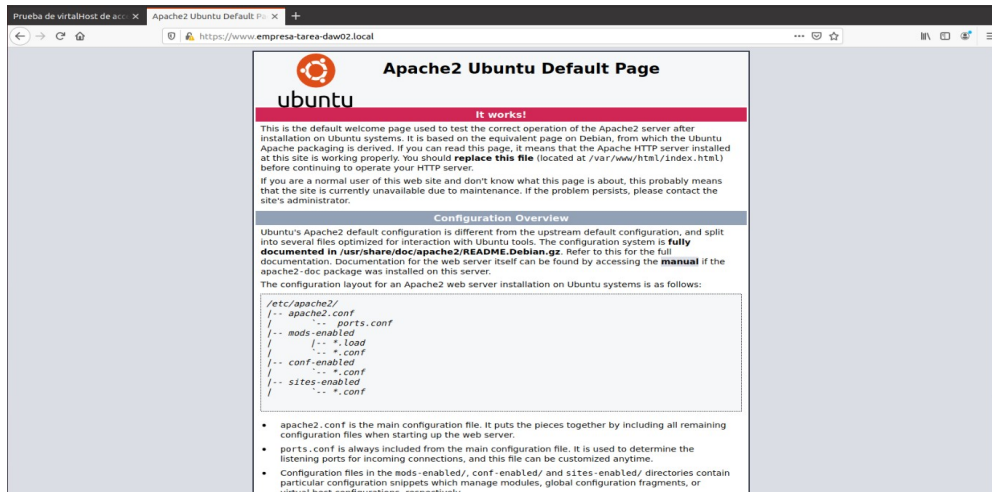
```

Ahora solo tenemos que reiniciar el servidor para que se aplica la nueva configuración.

Y ahora nos dirigimos a la URL y escribimos la siguiente ruta:

<https://empresa-tarea-daw02.local>

y nos mostrará una ventana de advertencia que esta web no es segura y le damos aceptar el riesgo y vemos que efectivamente nuestra web se habilitó en el https como se muestra a continuación:



- Configurar los archivos de registro como sigue:
 - ◆ Identificación log de acceso: **empresa-tarea-daw02-access.log**
 - ◆ Identificación log de error: **empresa-tarea-daw02-error.log**
 - ◆ Alias logformat: **combined**

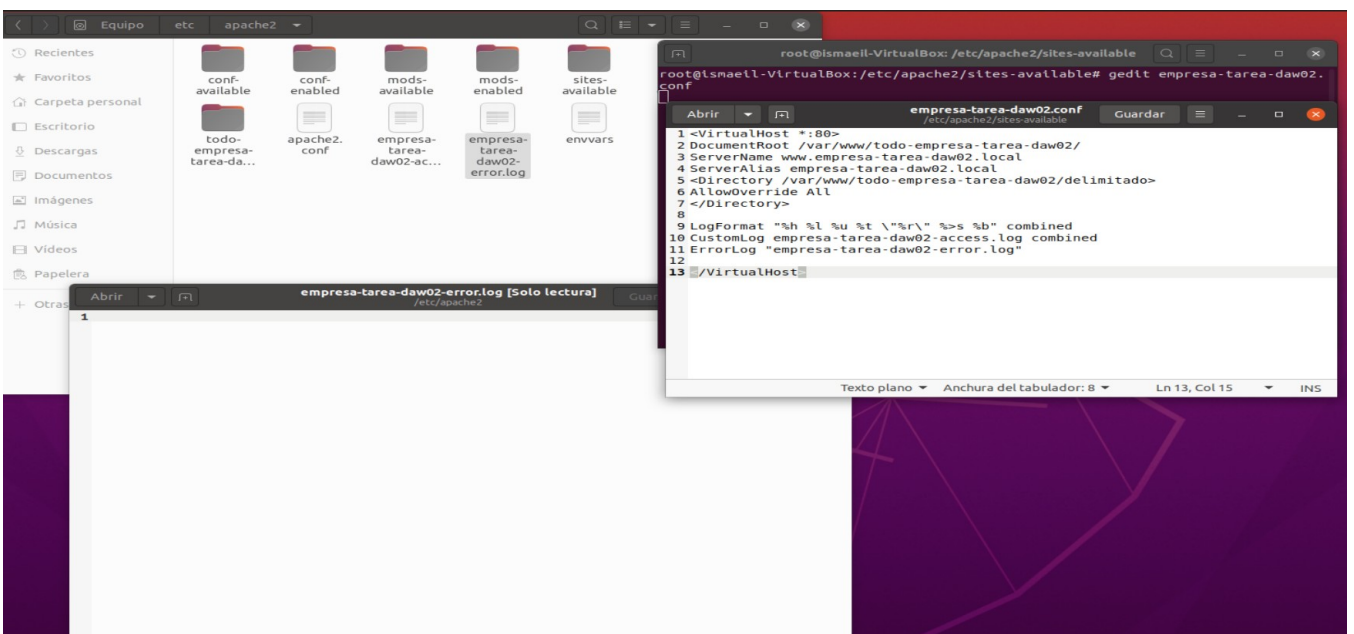
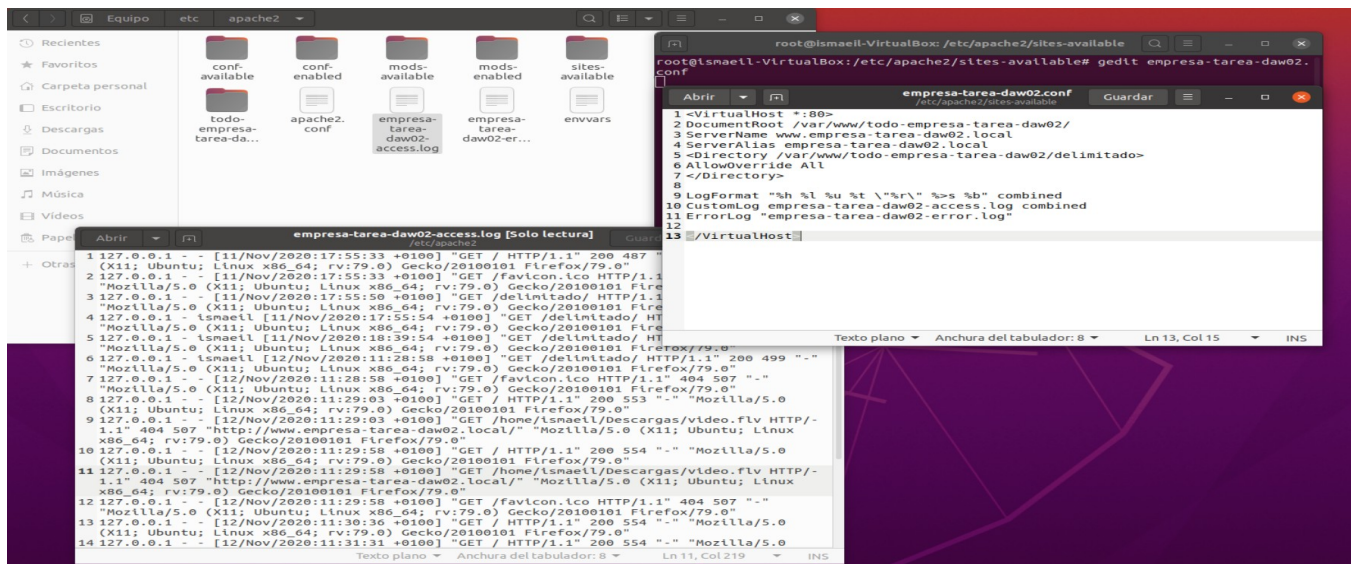
Para poder configurar estos archivos, nos dirigimos al fichero de configuración donde se encuentra en la carpeta del VirtualHost y editamos su contenido mediante el uso del siguiente código:

gedit /etc/apache2/sites-available/empresa-tarea-daw02.conf

añadiendo las siguientes líneas de código para poder generar los archivos de Acceso y de Error:

LogFormat "%h %l %u %t \"%r\" \"%>s %b" combined
CustomLog empresa-tarea-daw02-access.log combined
ErrorLog "empresa-tarea-daw02-error.log"

A continuación se mostrará los archivos generados :



- **Rotar logs por intervalo temporal: cada 24horas.**

Para poder realizar este punto nos dirigimos al fichero de configuración **empresa-tarea-daw02.conf** donde se encuentra en la carpeta: **etc/apache2/sites-available** y le añadimos las siguientes líneas:

CustomLog “|bin/rotatelog var/log/empresa-tarea-daw02-acceso.log 86400” combined
CustomLog “|bin/rotatelog var/log/empresa-tarea-daw02-error.log 86400” combined

y así le indicamos que los ficheros **empresa-tarea-daw02-acceso.log** y **empresa-tarea-daw02-error.log** se almacenarán cada 24 horas en **rotateCostom** y **rotateError** Como se muestra a continuación:

```
root@ismaeil-VirtualBox:~# gedit /etc/apache2/sites-available/empresa-tarea-daw02.conf

empresa-tarea-daw02.conf
/etc/apache2/sites-available

1 VirtualHost *:80
2 DocumentRoot /var/www/todo-empresa-tarea-daw02/
3 ServerName www.empresa-tarea-daw02.local
4 ServerAlias empresa-tarea-daw02.local
5 <Directory /var/www/todo-empresa-tarea-daw02/delimitado>
6 AllowOverride All
7 </Directory>
8
9 LogFormat "%h %l %u %t \"%r\" %>s %b" combined
10 CustomLog empresa-tarea-daw02-access.log combined
11 ErrorLog "empresa-tarea-daw02-error.log"
12
13 CustomLog "|bin/rotatelogs /var/log/empresa-tarea-daw02-acceso.log 86400" combined
14 CustomLog "|bin/rotatelogs /var/log/empresa-tarea-daw02-error.log 86400" combined
15 </VirtualHost>
```

después de añadir esas líneas reiniciamos nuestro servidor y listo.

```
root@ismaeil-VirtualBox:~# gedit /etc/apache2/sites-available/empresa-tarea-daw02.conf
(gedit:7874): Tepl-WARNING **: 11:48:59.031: GVfs metadata is not supported. Fallback to TeplMetadataManager. Either GVfs is not correctly installed or GVfs metadata are not supported on this platform. In the latter case, you should configure Tepl with --disable-gvfs-metadata
root@ismaeil-VirtualBox:~# sudo service apache2 reload
root@ismaeil-VirtualBox:~# sudo service apache2 restart
root@ismaeil-VirtualBox:~#
```