**CICLO : DESARROLLO APLICACIONES WEB-DISTANCIA**
**MÓDULO : DESPLIEGUE DE APLICACIONES WEB**
**ALUMNO : DAVID MEDINA GARCIA**
**TAREA : DAW02**

1. **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**
2. **Hacer accesible a través de Internet las siguientes URL que identifican a la empresa: www.empresa-tarea-daw02.local y empresa-tarea-daw02.local**

Primero de todo creamos el directorio "**todo-empresa-tarea-daw02**" en la ruta **/var/www** con el comando:

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

Ahora creamos el archivo de configuración, "**empresa-tarea-daw02.local.conf**" para el **virtualhost** en la ruta **/etc/apache2/sites-available** con el comando:

**nano /etc/apache2/sites-available/empresa-tarea-daw02.local.conf**

En el archivo creado añadimos:

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

Activamos el fichero de configuración del **virtualhost** con **a2ensite** con este comando:

**a2ensite empresa-tarea-daw02.local.conf**

Recargamos **Apache** para activar esta configuración con el comando:

**systemctl reload apache2**

Editamos el archivo **"/etc/hosts**" para redirigir las peticiones a ese dominio a nuestro servidor, con este comando:

**nano /etc/hosts**

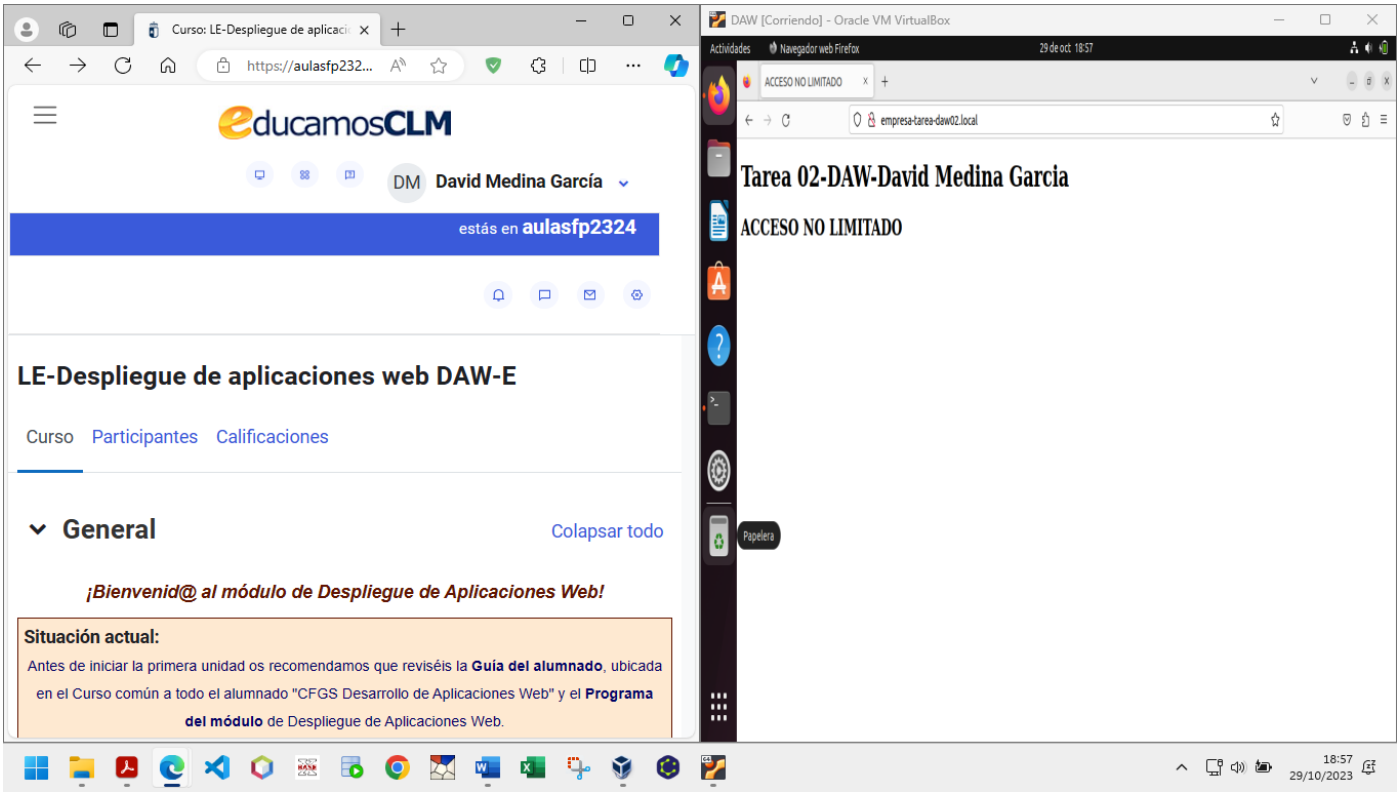
Añadimos la línea **127.0.0.1 empresa-tarea-daw02.local www. empresa-tarea-daw02.local**

Ahora en la ruta **/var/www/todo-empresa-tarea-daw02** creamos el **archivoindex.html** con este comando:

**nano /var/www/todo-empresa-tarea-daw02/index.html**

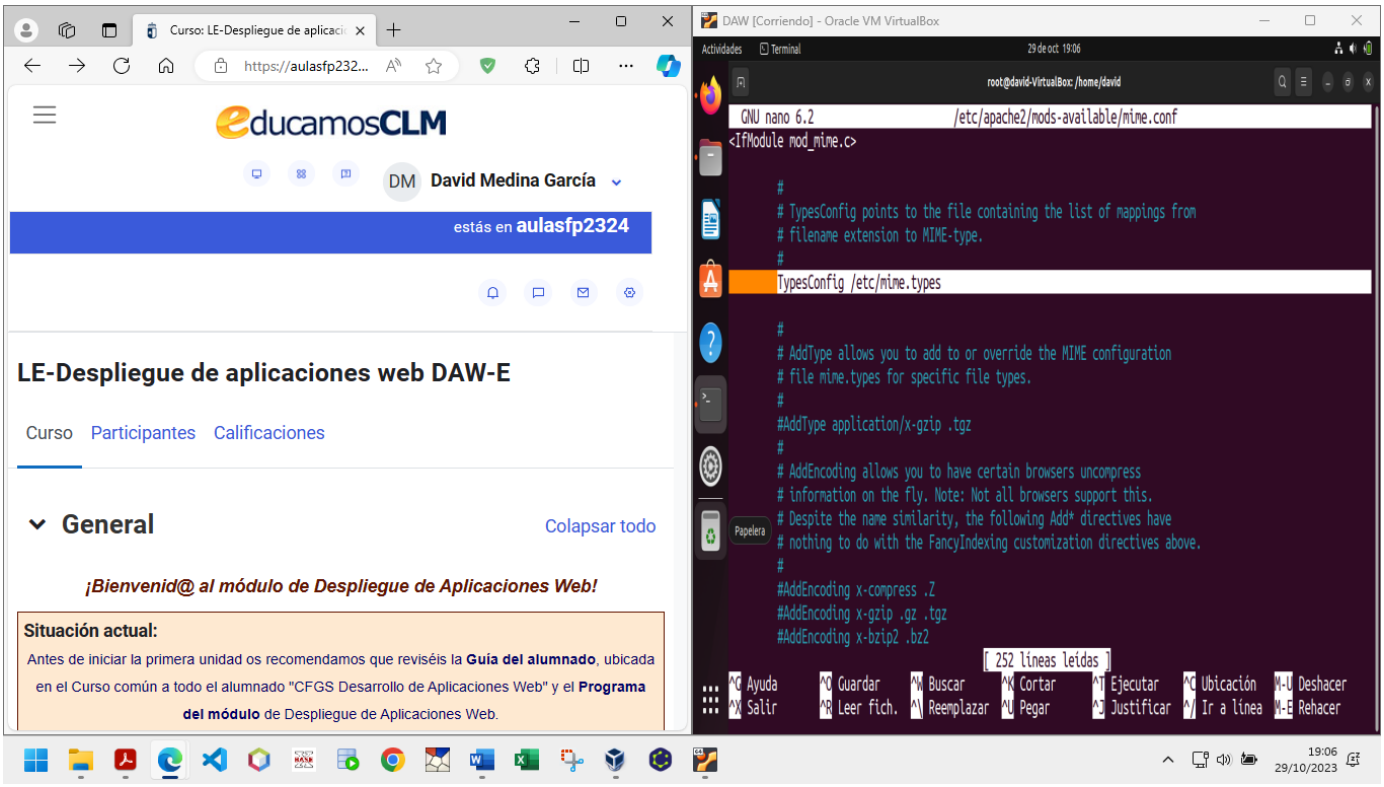
Creamos una página:

```
<!DOCTYPE html>
<html>
        <head>
        <meta http-equiv="Content-Type" content="text/html;charset=utf-8" />
        <title> ACCESO LIMITADO</title>
        </head>
        <body>
            <h1>Tarea 02-DAW-David Medina Garcia</h1>
        <h2>ACCESO NO LIMITADO</h2>
        </body>
</html>
```

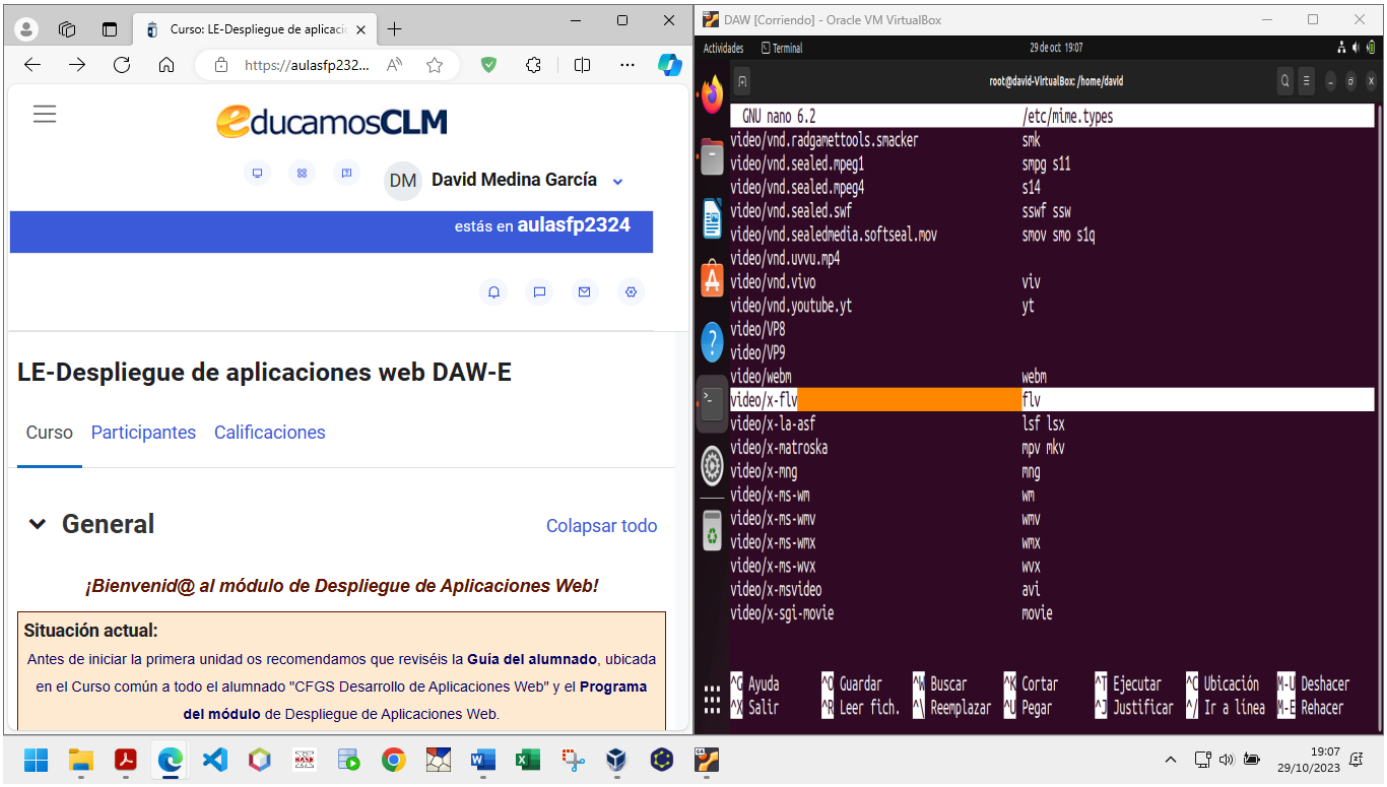



3. **Configurar en el servidor el tipo MIME posible que permite la identificación correcta de la vídeo presentación formato flv situado dentro del directorio videos y de nombre entrada.flv.**

   Abrimos el archivo **mime.conf** de la ruta **/etc/apache2/mods-available/mime.conf** con el comando **nano /etc/apache2/mods-available/mime.conf** y vemos en la línea 7 que ya tiene **TypesConfig /etc/mime.types,** lo cual indica que los tipos de archivos conocidos se encuentran en ese fichero.




Abrimos **/etc/mime.types** con el comando **nano /etc/mime.types** y vemos que tiene una línea con **video/x-flv flv**, es decir ya había una referencia, por tanto los archivos de tipo **flv** ya están reconocidos por el servidor como archivos de video, sino existiera, la crearíamos nosotros.



4. **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.**

Creamos primero el subdirectorio delimitado con el comando:

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

Creamos el archivo "**index.html**" para el subdirectorio "**delimitado**" con el comando:

**nano /var/www/todo-empresa-tarea-daw02/delimitado/index.html**

Estructura de la página:

```
<!DOCTYPE html>
<html>
        <head>
        <meta http-equiv="Content-Type" content="text/html;charset=utf-8" />
        <title>ACCESO LIMITADO</title>
        </head>
        <body>
            <h1>Tarea 02-DAW-David Medina Garcia</h1>
        <h2>ACCESOLIMITADO</h2>
        </body>
</html>
```

Modificamos el fichero de configuración **virtualhost anterior** para que permita el uso del fichero **htaccess** en el directorio que deseamos restringir su acceso:

**nano /etc/apache2/sites-available/empresa-tarea-daw02.local.conf**

Y le añadimos:

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

Creamos la carpeta **todo-empresa-tarea-daw02** en **/etc/apache2/,** es donde alojaremos los roles.
**mkdir /etc/apache2/todo-empresa-tarea-daw02**

Y a continuación creamos un fichero .**htaccess** en el directorio que deseamos controlar:
**nano /var/www/todo-empresa-tarea-daw02/delimitado/.htaccess**

En el añadimos:

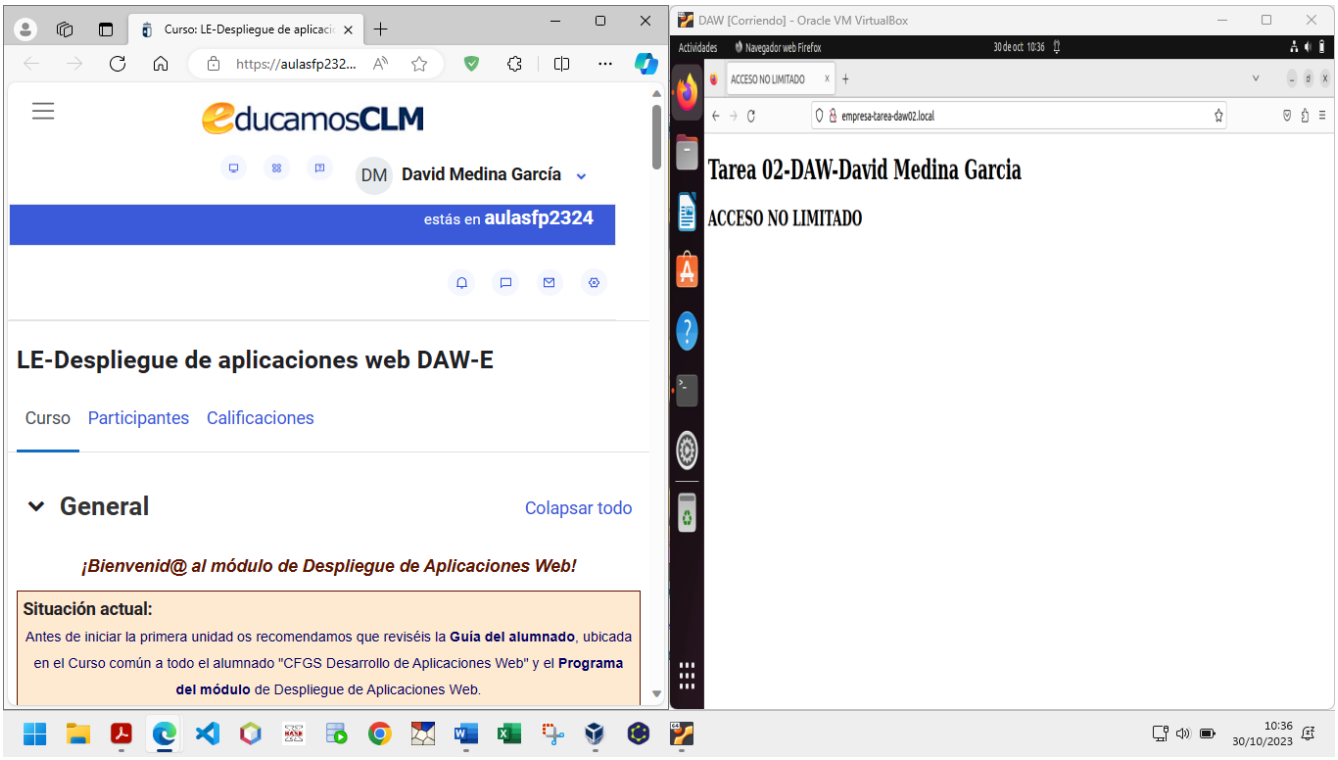
```
AuthType Basic
AuthName "Area restringida para administradores"
AuthUserFile /etc/apache2/todo-empresa-tarea-daw02/passwd
AuthGroupFile /etc/apache2/todo-empresa-tarea-daw02/roles
Require group admin
```

Creamos el archivo roles en **/etc/apache2/todo-empresa-tarea-daw02**
**nano /etc/apache2/todo-Empresa-tarea-daw02/roles**
Dentro del fichero definimos el **rol** y le asignamos los **usuarios admin: root David**

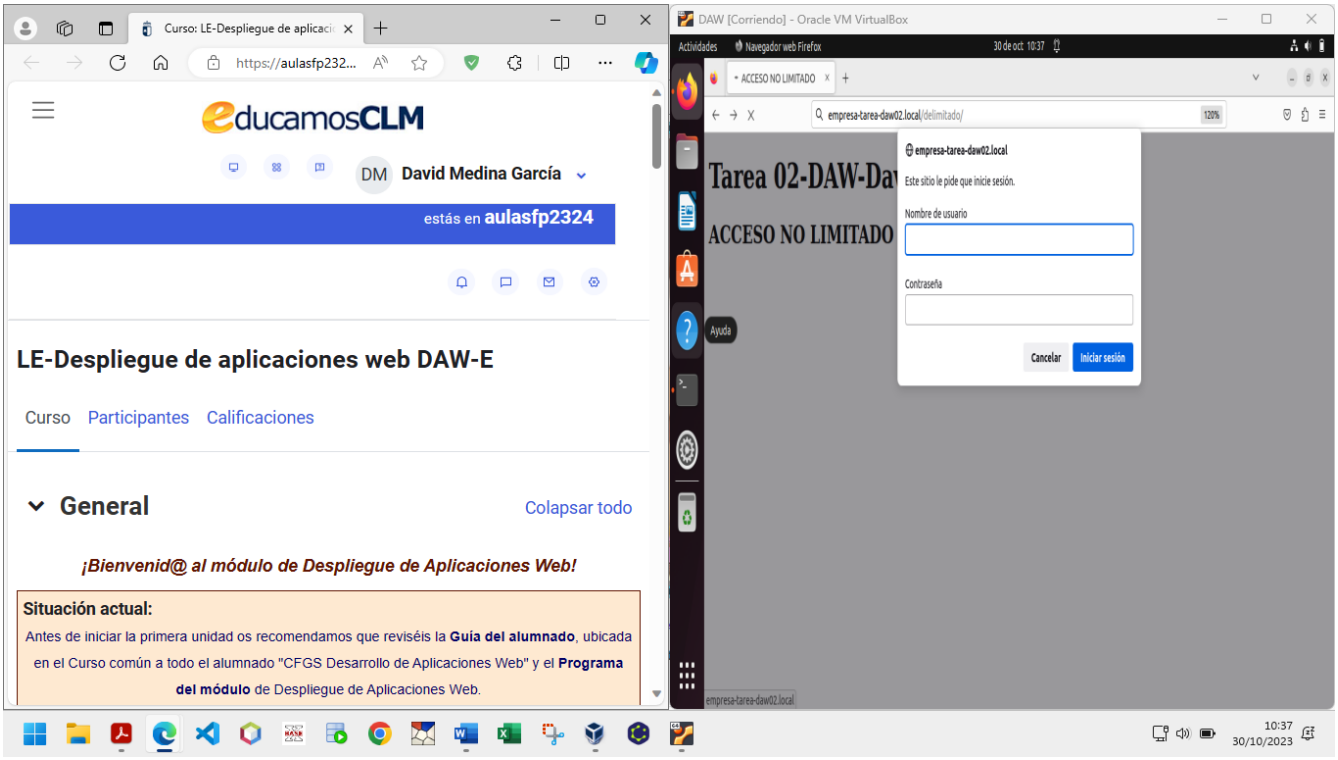
Añadimos el **password** para el usuario **david**
**htpasswd -c /etc/apache2/todo-empresa-tarea-daw02/passwd david**

Habiltamos el módulo **groupfile** y reiniciamos **Apache**
**a2enmod authz_groupfile**
**systemctl reload apache2**

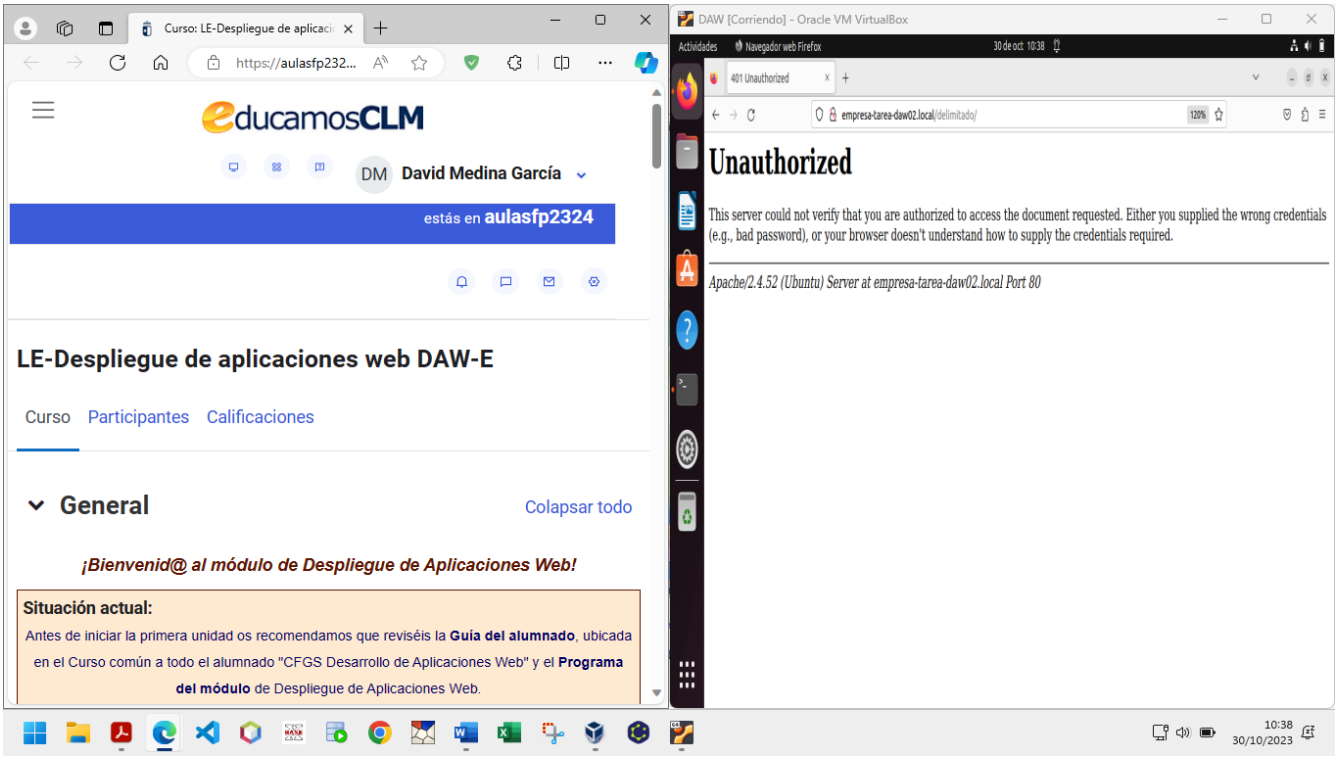
Abrimos la página de acceso no limitado para comprobar que no nos pide ninguna identificación.



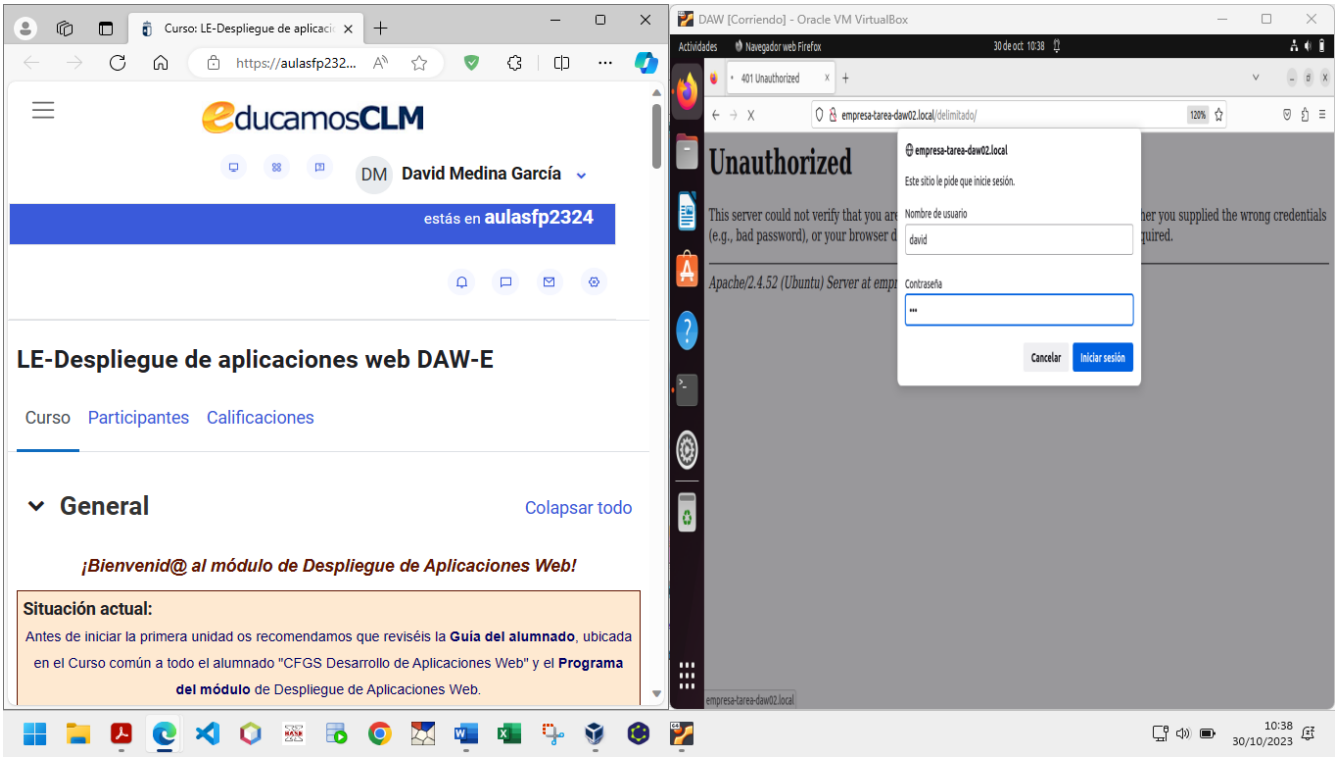
Ahora abrimos la página de acceso limitado y vemos que nos pide una identificación.

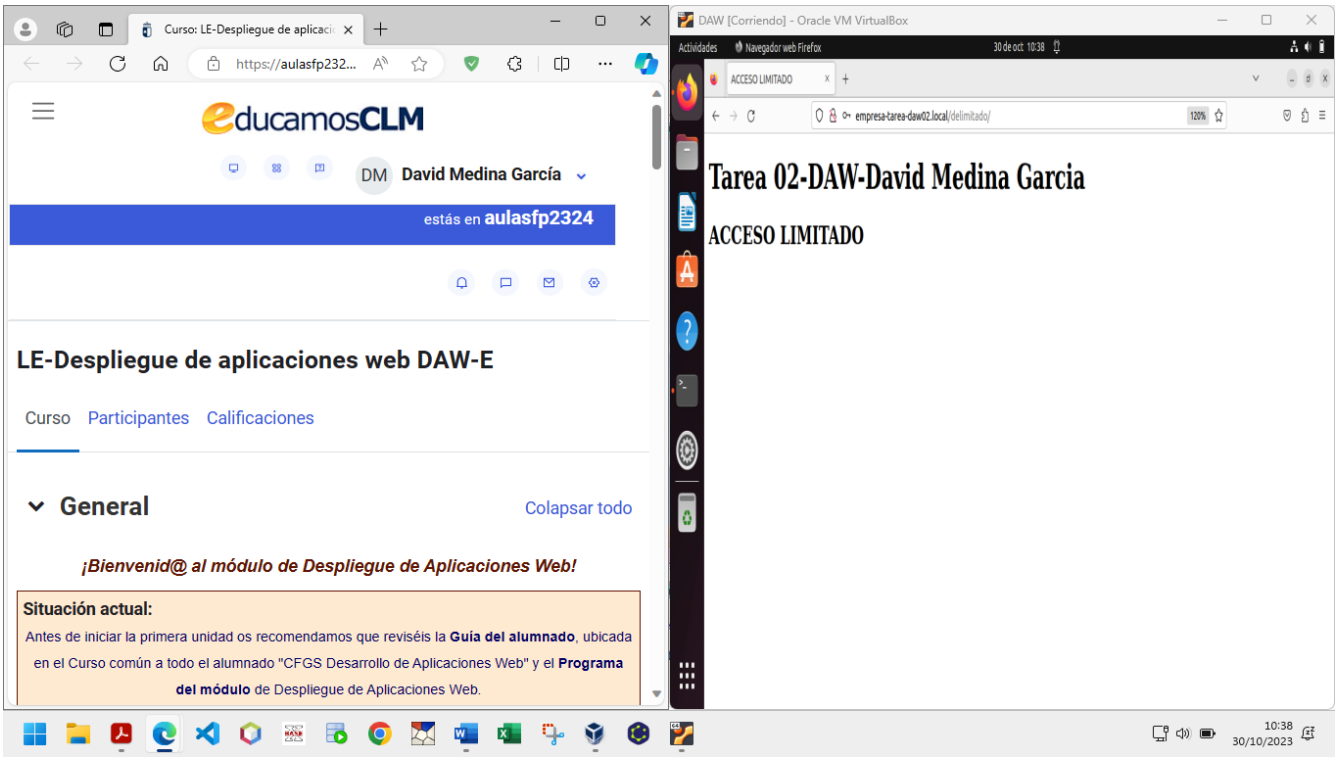



Si no ponemos un usuario y contraseña válidos, no nos dejara acceder a la página.



A continuación introducimos el usuario y contraseña correctos y accedemos a la página



## 5. Permitir el protocolo HTTPS en el virtualhost empresa-tarea-daw02

Vamos a operar con **openssl**, que ya viene instalado en Ubuntu. Creamos el directorio para guardar el certificado y la clave privada de la certificación y nos posicionamos en él.

**mkdir /etc/apache2/tarea-ssl/**

**cd /etc/apache2/tarea-ssl/**

Generamos ambos archivos, tanto la **clave privada** como el **certificado**.

**openssl req -new -nodes -keyout empresa-tarea-daw02-ssl.key -out empresa-tareadaw02-ssl.csr**

Autofirmamos el certificado, por ejemplo con caducidad de un año.

**openssl x509 -in empresa-tarea-daw02-ssl.csr -out empresa-tarea-daw02-ssl.crt -req -signkey empresa-tarea-daw02-ssl.key -days 365**

Creamos el archivo de configuración para el virtualhost empresa-tarea-daw02-ssl

**nano /etc/apache2/sites-available/empresa-tarea-daw02-ssl.local.conf**

y añadimos el contenido al archivo de configuración:

```
<VirtualHost *:443>
    ServerAdmin aaa@empresa-tarea-daw02-ssl.local
    ServerName empresa-tarea-daw02-ssl.local
    ServerAlias www.empresa-tarea-daw02-ssl.local
    DocumentRoot /var/www/todo-empresa-tarea-daw02-ssl/
    SSLEngine on
    SSLCertificateFile /etc/apache2/tarea-ssl/empresa-tarea-daw02-ssl.crt
    SSLCertificateKeyFile /etc/apache2/tarea-ssl/empresa-tarea-daw02-ssl.key
</VirtualHost>
```

Creamos el directorio **todo-empresa-tarea-daw02-ssl** y creamos el **index.html** dentro del directorio:

**mkdir /var/www/todo-empresa-tarea-daw02-ssl/**
**nano /var/www/todo-empresa-tarea-daw02-ssl/index.html**

Definimos el html

```
<!DOCTYPE html>
<html>
    <head>
    <meta http-equiv="Content-Type" content="text/html;charset=utf-8" />
          <title>PAGINA CON SSL</title>
    </head>
    <body>
      <h2>PAGINA CON SSL</h2>
    </body>
</html>
```

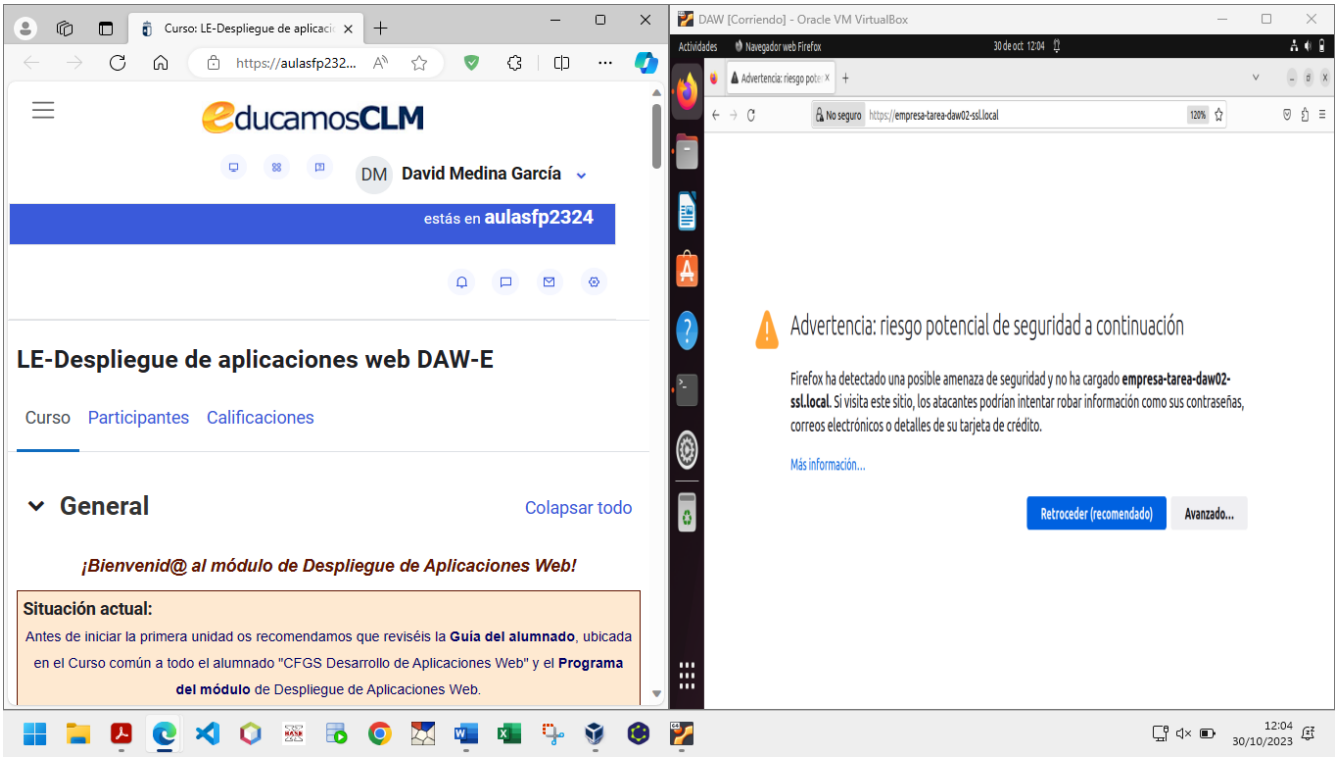
Editamos el archivo **"/etc/hosts**" para redirigir las peticiones a ese dominio a nuestro servidor, con el siguiente comando:

**nano /etc/hosts**
Agregamos la siguiente línea: **127.0.0.1 empresa-tarea-daw02-ssl.local www.empresa-tarea-daw02-ssl.local**

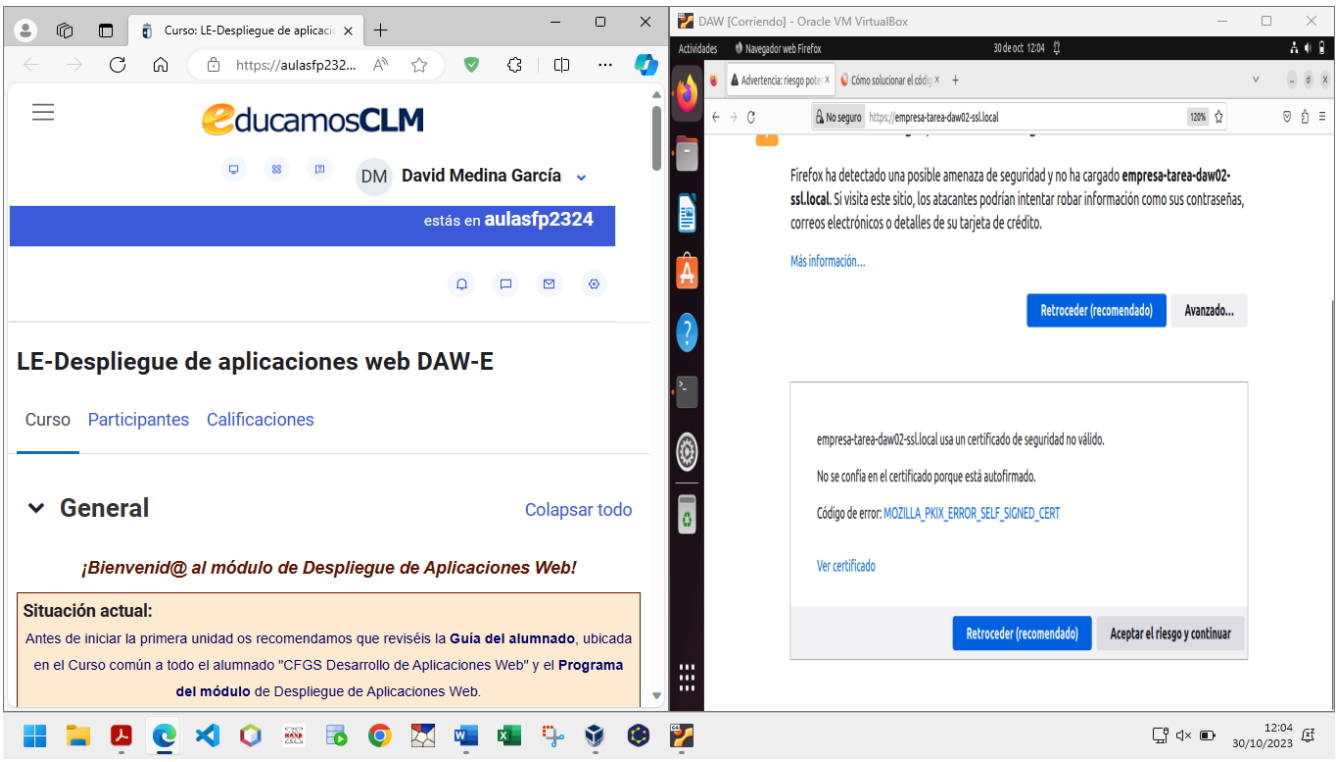
Activamos **ssl** con **a2enmod**, y la configuración con **a2ensite** y reiniciamos **Apache**

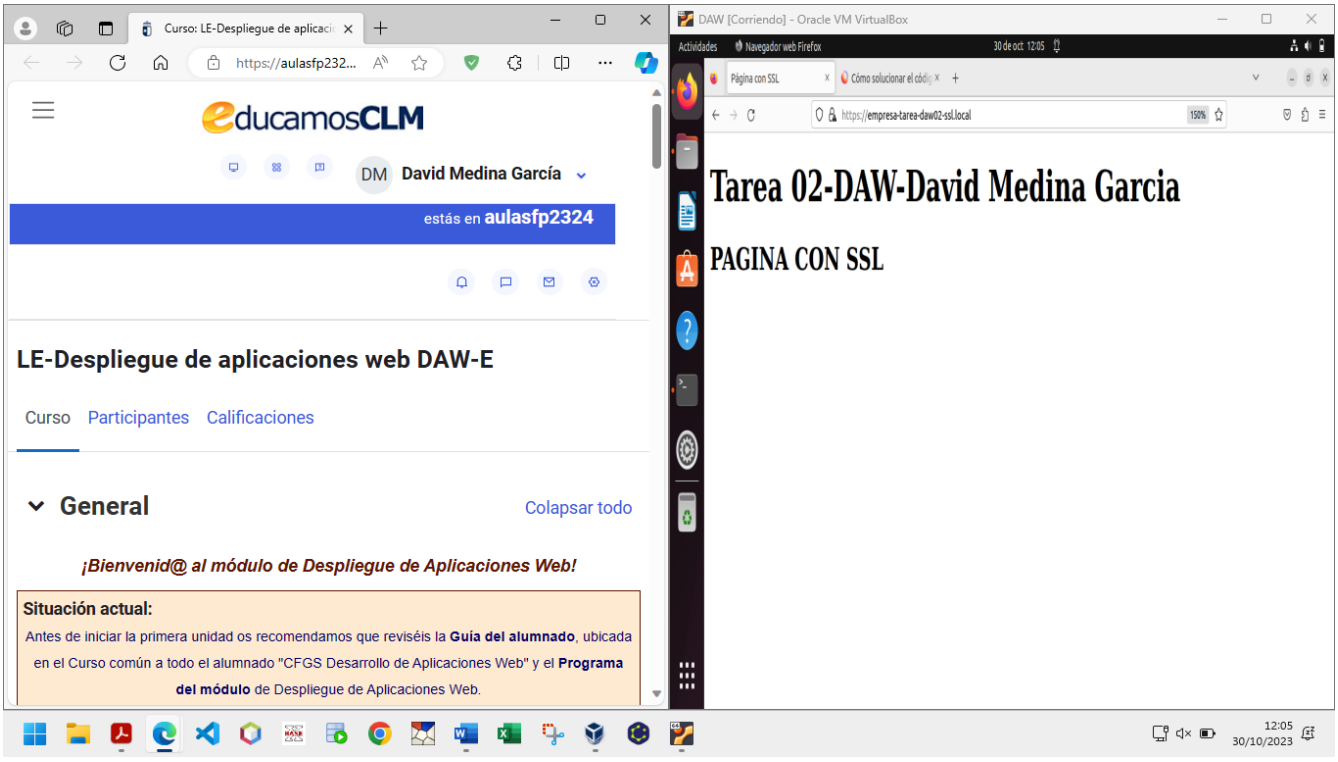
**a2enmod ssl**
**a2ensite empresa-tarea-daw02-ssl.local.conf**
**systemctl reload apache2**

Probamos con **https://empresa-tarea-daw02-ssl.local** y nos muestra la advertencia



Tras añadir la excepción de seguridad nos muestra la página.



6. **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**

Editamos dicho archivo el archivo de configuración **empresa-tarea-daw02.local.conf**

**nano /etc/apache2/sites-available/empresa-tarea-daw02.local.conf**

Añadimos este contenido al final, pero dentro de las etiquetas **VirtualHost**

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

Con la primera línea asignamos el alias **combined** a **logformat**, con el que generaremos registros en el formato:

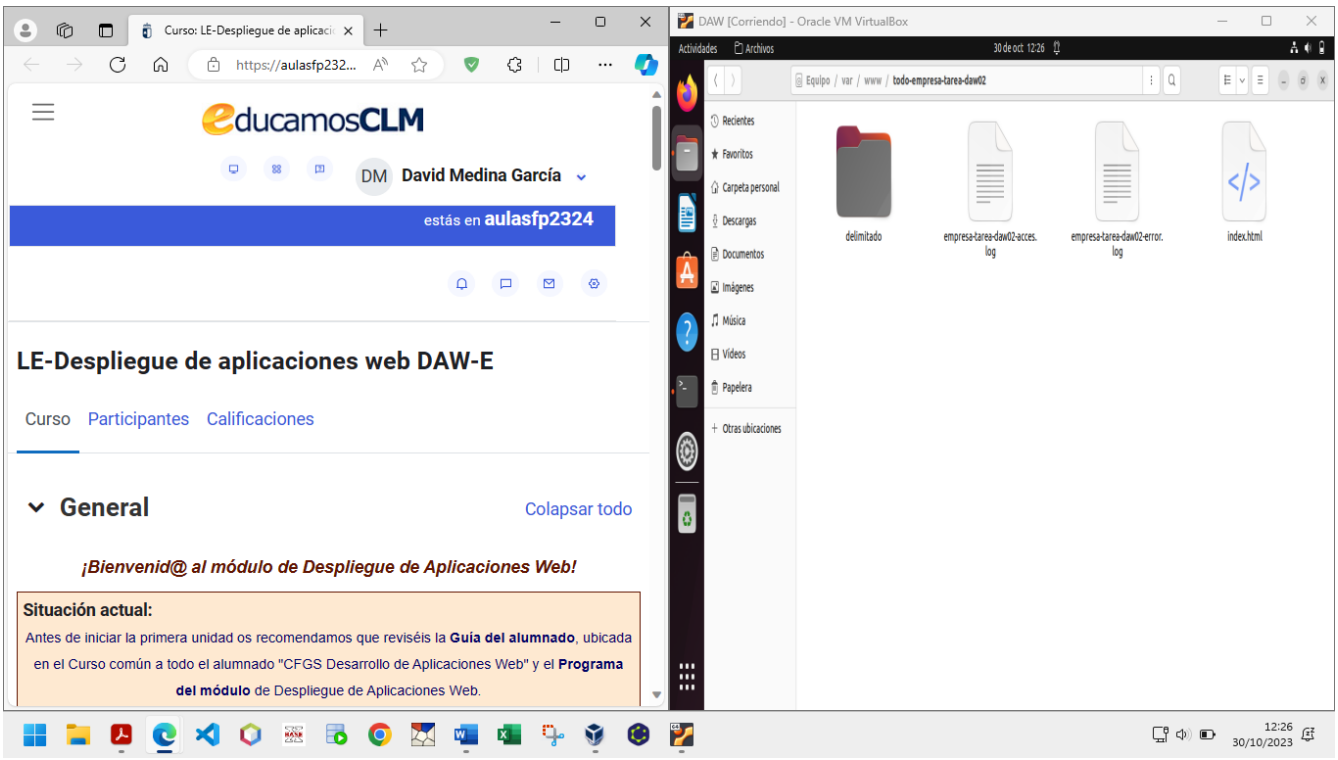
- **%h** host
- **%l** identificación cliente
- **%u** usuario
- **%t** fecha y hora
- **\"%r\"** cliente, recurso, protocolo
- **%>s** Código de estado que el servidor envía de vuelta al cliente. Si el código comienza por 2 fue respondido con éxito, por 3 identifican una redirección, por 4 se trata de un error del cliente y por 5 es un error del servidor.
- **%b** Tamaño del objeto retornado por el cliente.

Si cuando nos tenga que presentar los datos, alguno de ellos no existe, pondrá un guion en el lugar que le corresponda.

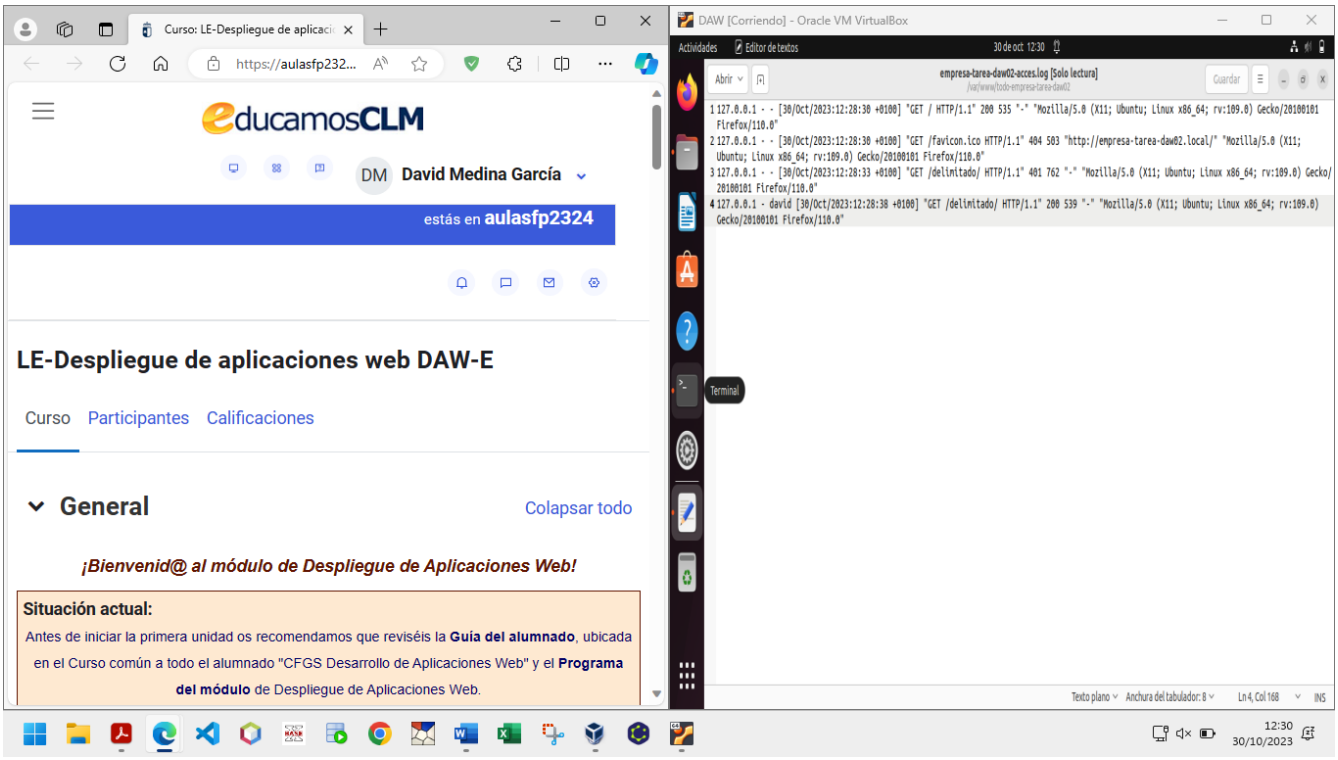
Con la segunda línea indicamos que el fichero de registro de acceso se guardará con el nombre de **empresa-tarea-daw02-access.log** y con el contenido al formato establecido en la línea anterior.

La tercera línea se usa para indicar dónde se ha de guardar el registro de errores, en este caso, en el fichero **empresa-tarea-daw02-error.log** situado.

Aquí vemos como nos genera los archivos:




Aquí el contenido del **empresa-tarea-daw02-access.log**



## 7. Rotar logs por intervalo temporal: cada 24horas.clear

Modificamos estas dos líneas del archivo de configuración **empresa-tarea-daw02.conf**

**CustomLog "|/usr/bin/rotatelogs /var/www/todo-empresa-tarea-daw02/empresatarea-daw02-Access.log 86400" combined**

**ErrorLog "|/usr/bin/rotatelogs /var/www/todo-empresa-tarea-daw02/empresatarea-daw02-error.log 86400"**

Con lo que le indicamos que el fichero del registro de acceso **empresa-tarea-daw02-access.log** lo almacene cada 24 horas (86400 segundos) con **rotatelogs** que se encuentra en **/usr/bin.**

Con la segunda línea, decimos que el fichero de registro de errores **empresa-tareadaw02-error.log** lo almacene cada 24 horas (86400 segundos) en el fichero **rotatelogs** que se encuentra en **/usr/bin**.

Vemos como nos ha rotado log de al día siguiente: