

Tareas Unidad 4

Despliegue de Aplicaciones Web

Autor: Derimán Tejera Fumero

Fecha: 16/10/2024

Enunciado

Tareas Unidad 4: Instalación y administración de servidores FTP.

Se pide la instalación, configuración y administración de un servidor ProFTPD.

Esa documentación se elaborará en el procesador de texto Writer y estará estructurada en cuatro apartados:

1. Instalar un servidor FTP: ProFTPD (proftpd).
2. Crear dos Virtualhosts basado en Nombre que permita el acceso mediante ftp:
 - todo-empresa1-tarea-daw04.local, al directorio del servidor var/ftp/empresa1/
Puerto Port 2121
 - todo-empresa2-tarea-daw04.local, al directorio del servidor var/ftp/empresa2/
Puerto Port 2122No añadir la Directiva AuthUserFile al VirtualHost.
Generar dicha dirección ftp modificando el archivo /etc/hosts
3. Instalar el cifrado TLS Explícito para asegurar la comunicación.
Fichero /etc/proftpd/modules.conf descomentar línea “#LoadModule mod_tls.c”, pasar a “LoadModule mod_tls.c”. Instalar el módulo proftpd-mod-crypto con el comando “aptget install proftpd-mod-crypto”, reiniciar el servicio con “systemctl restart proftpd” o “/etc/init.d/proftpd start”.
4. Conectarse al servidor FTP desde modo gráfico (instalar el cliente FTP gráfico FileZilla en Ubuntu).

NOTAS IMPORTANTES:

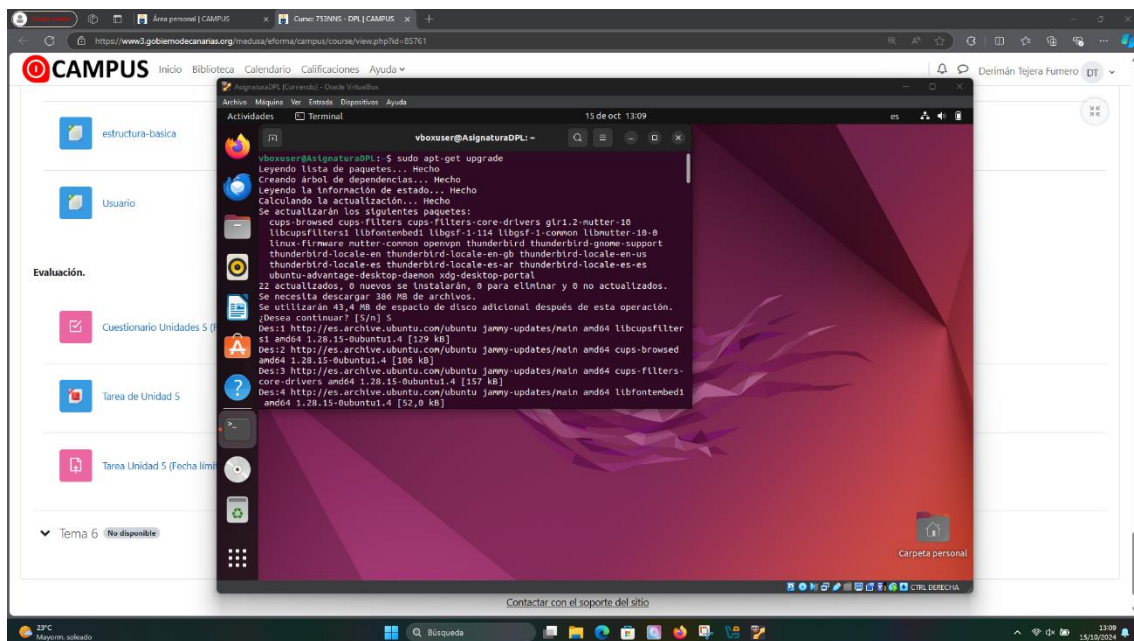
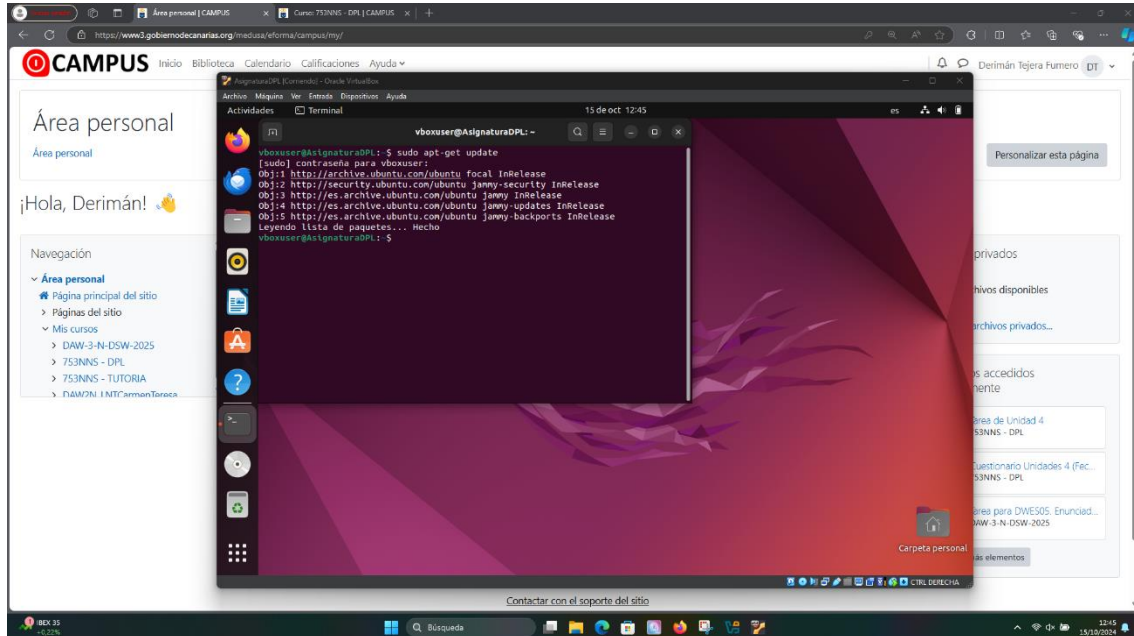
Criterios de Calificación de la Tarea cada Apartado 2,5 puntos.

Para completar esta tarea es necesario entregar la documentación de toda la instalación con las correspondientes capturas de pantalla de los principales pasos realizados, la entrega de cada apartado de la tarea consiste en indicar el archivo a configurar junto con el código necesario para resolver la cuestión correspondiente.

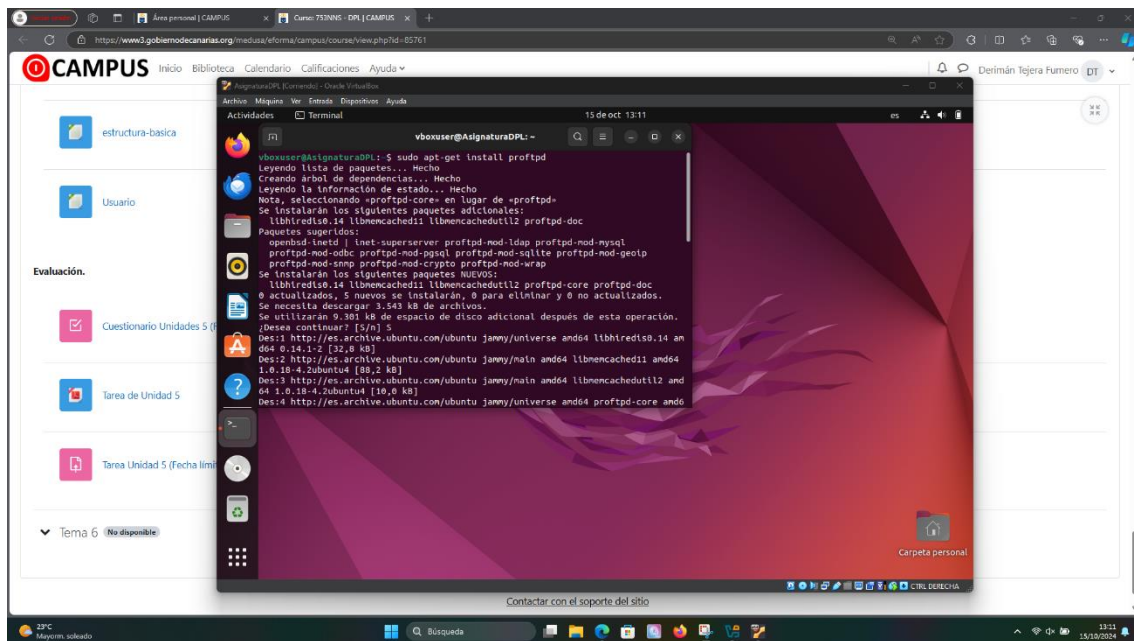
Es importante que las capturas sean de pantalla completa mostrando la hora del sistema, además debe aparecer de fondo en la esquina superior derecha el nombre de tu perfil como usuario de la plataforma Campus.

Apartado 1

Actualizamos el sistema:

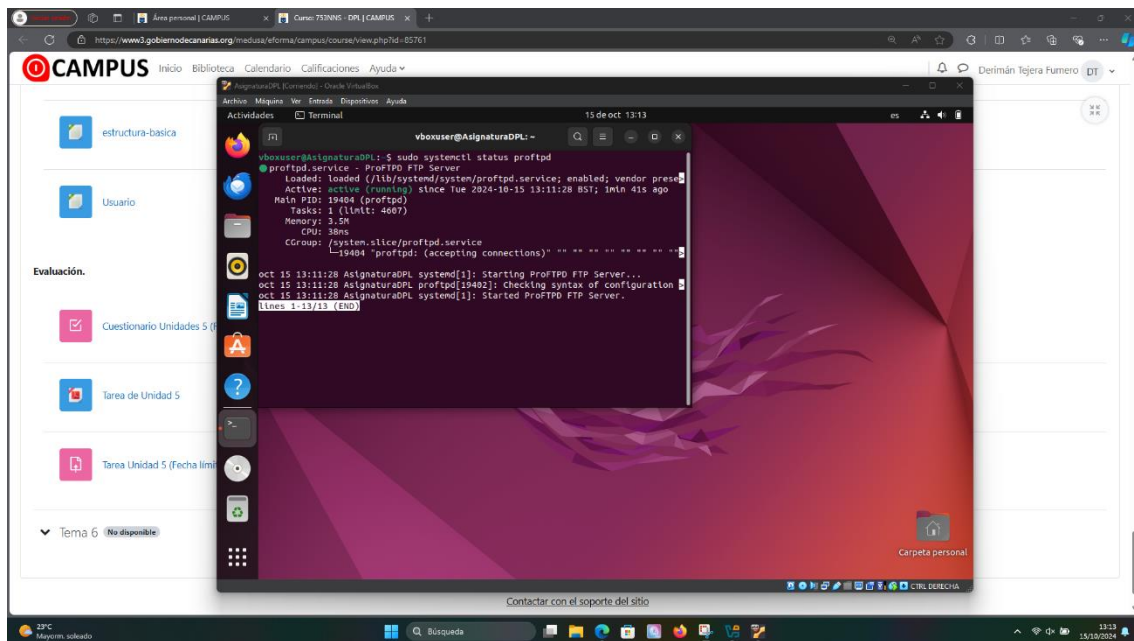


Instalar ProFTPD:



Apartado 2

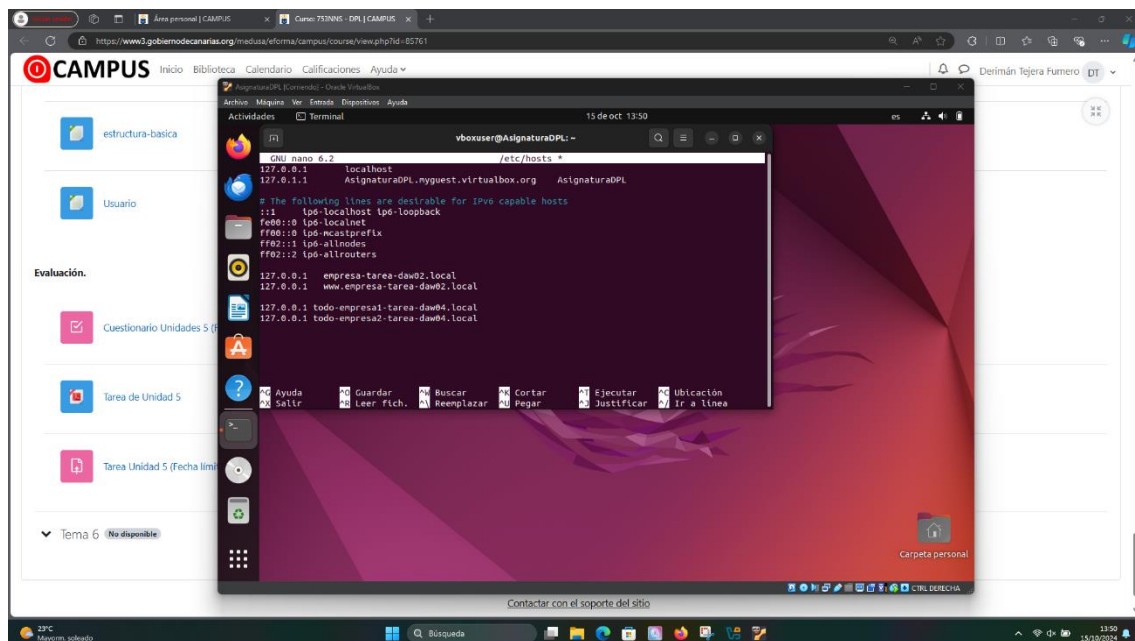
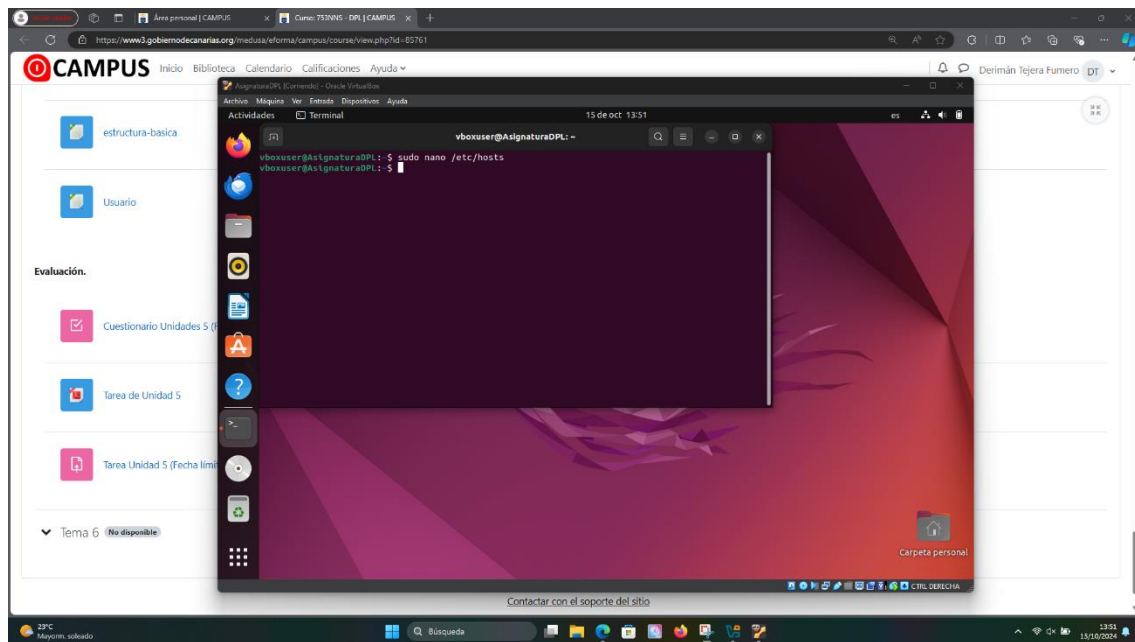
Verificamos el status de ProFTPD:



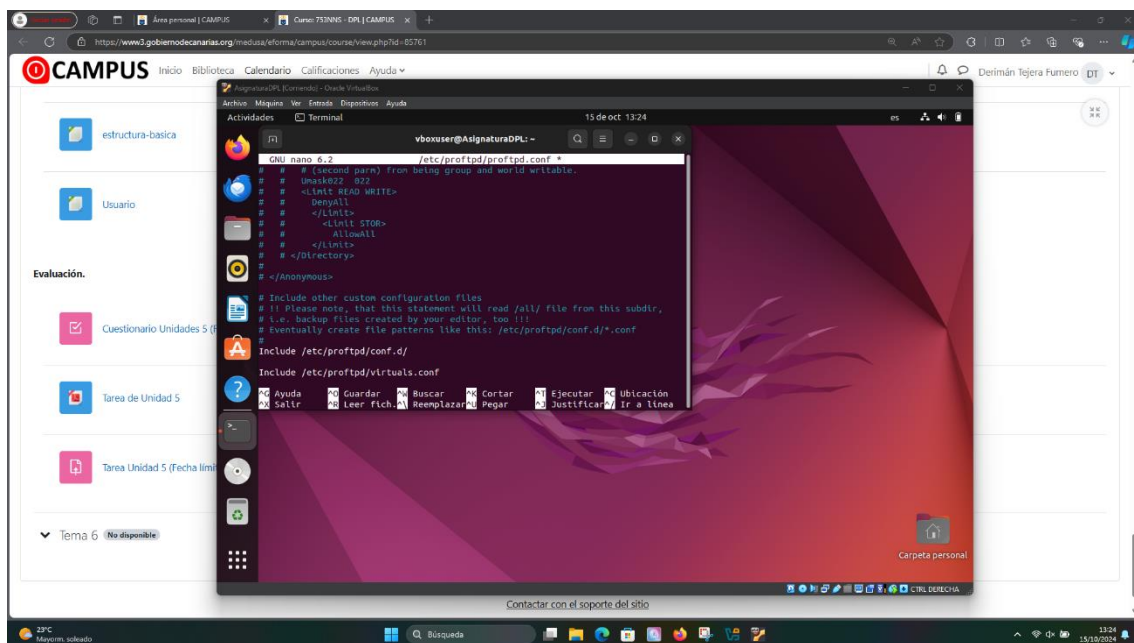
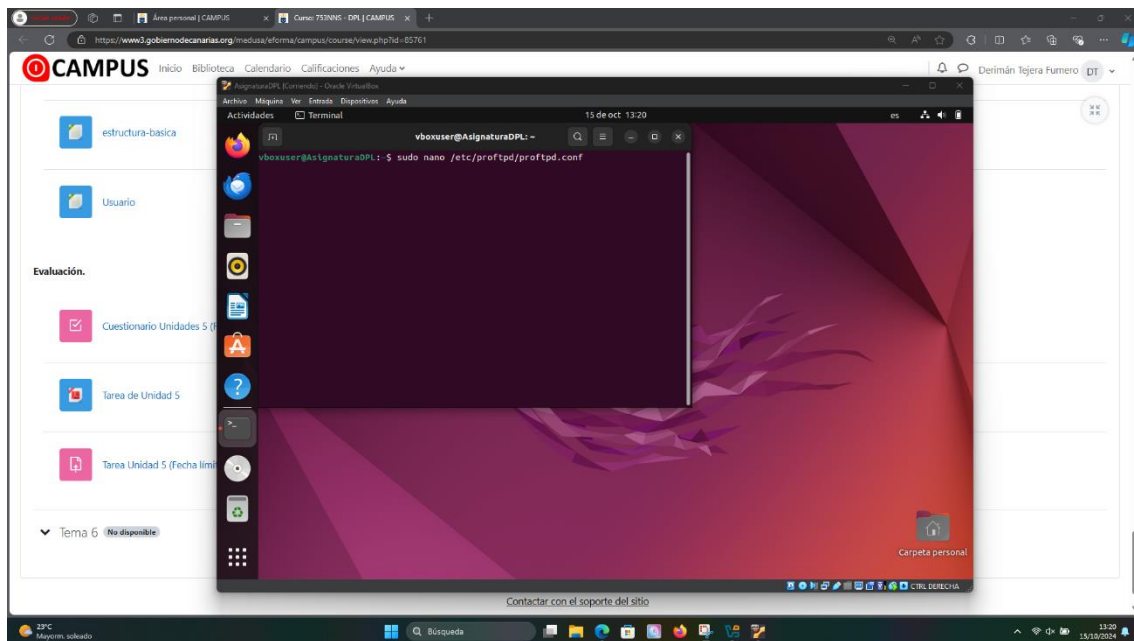
Editar el archivo `/etc/host` para añadir los nombres de los dominios locales al final del archivo:

`127.0.0.1 todo-empresa1-tarea-daw04.local`

`127.0.0.1 todo-empresa2-tarea-daw04.local`



Editar proftpd.conf y añadir al final: `include /etc/proftpd/virtuals.conf`



Editar virtuals.conf y añadir al final:

<VirtualHost todo-empresa1-tarea-daw04.local>

Port 2121

ServerName "Servidor FTP empresa1"

DefaultRoot /var/ftp/empresa1/

RequireValidShell off

</VirtualHost>

<VirtualHost todo-empresa2-tarea-daw04.local>

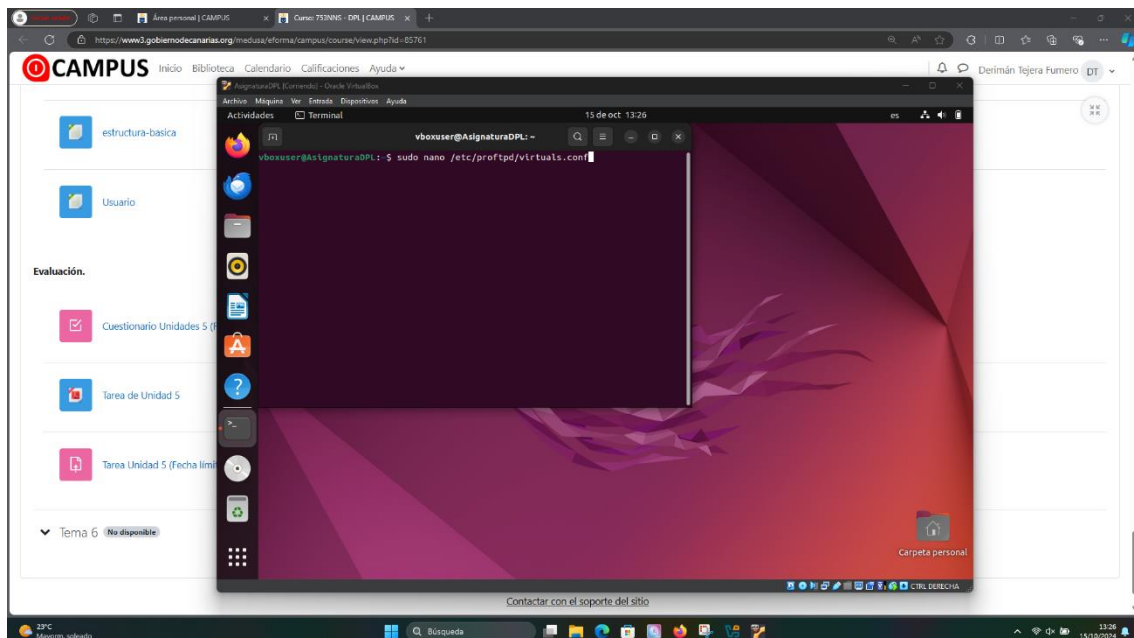
Port 2122

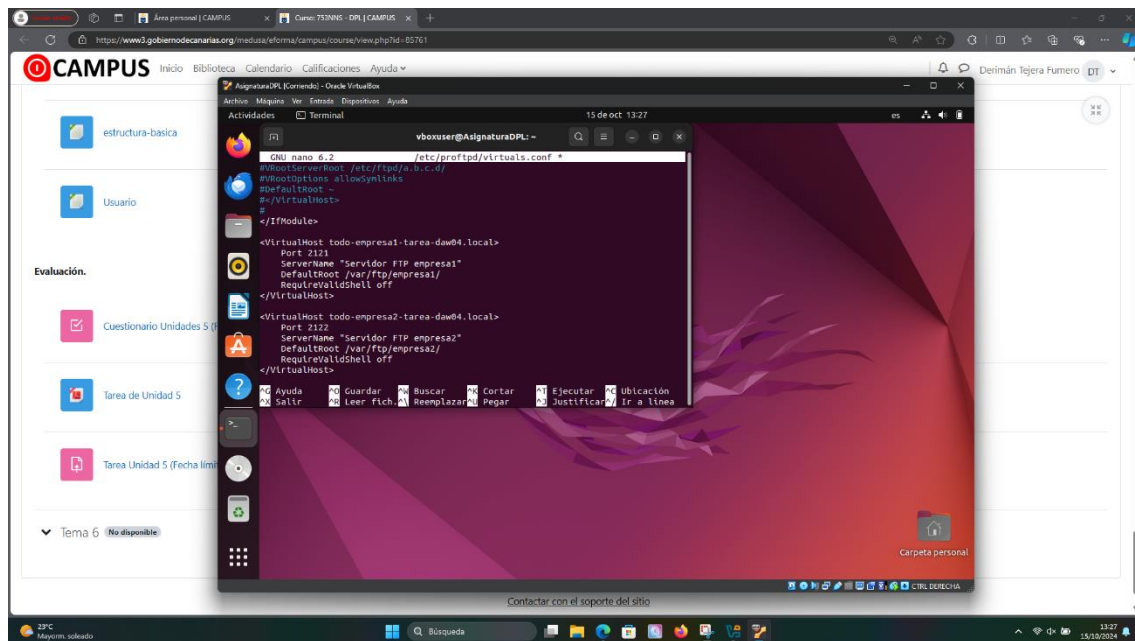
ServerName "Servidor FTP empresa2"

DefaultRoot /var/ftp/empresa2/

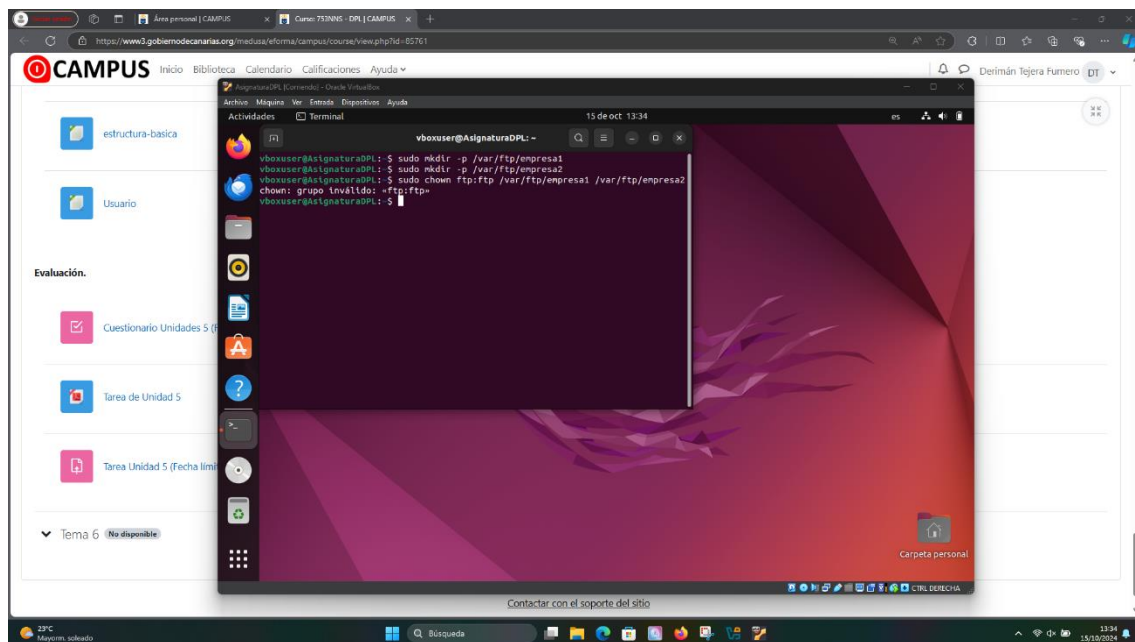
RequireValidShell off

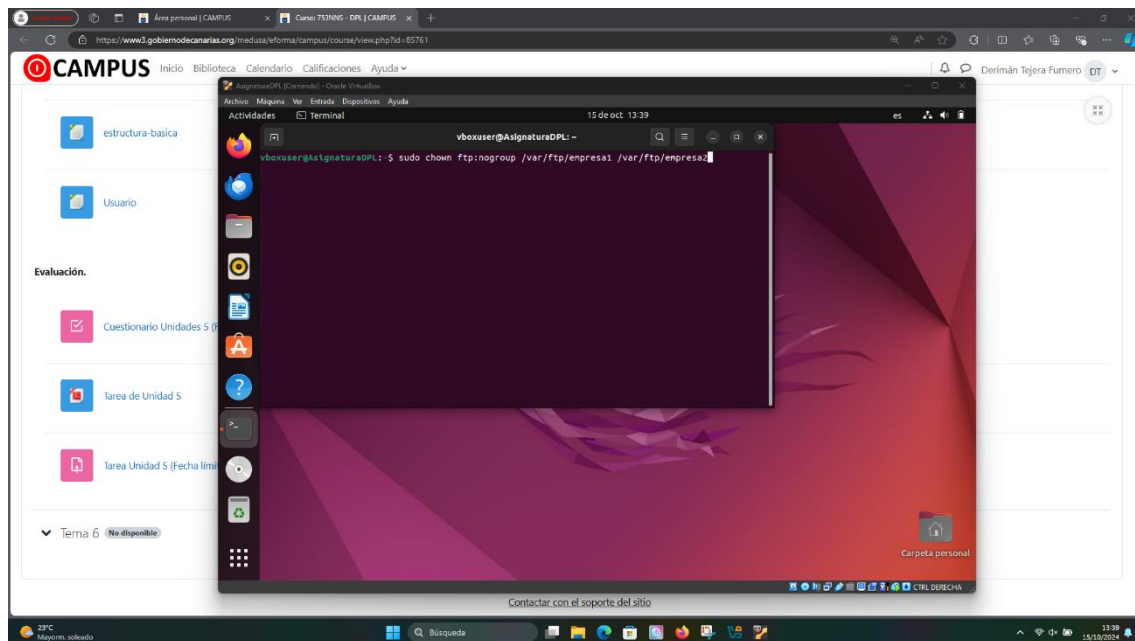
</VirtualHost>



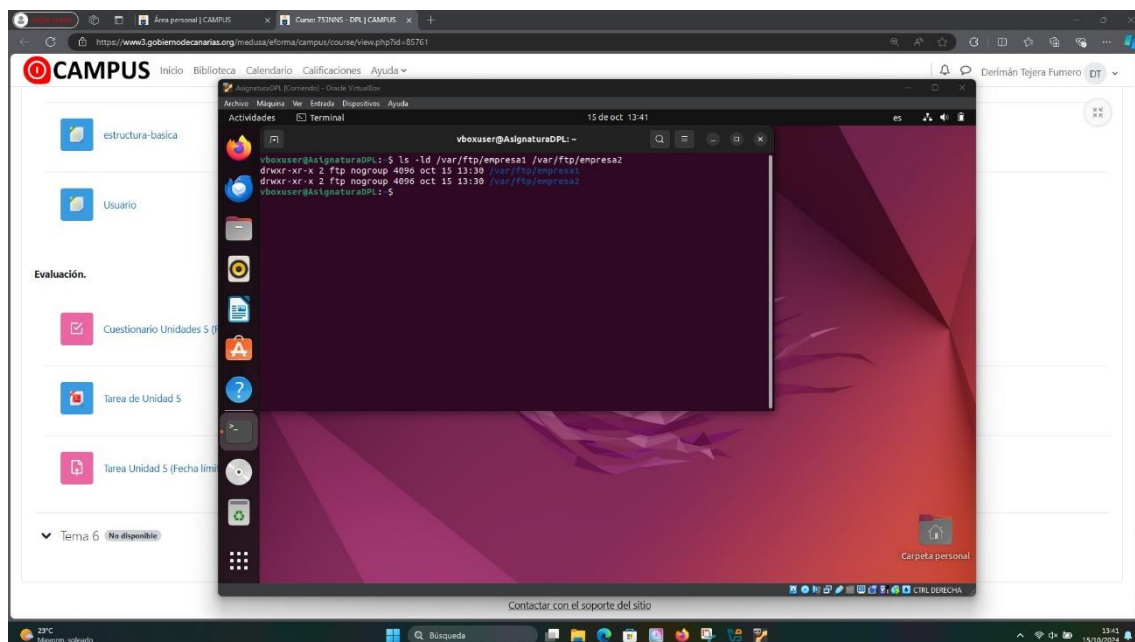


Crear los directorios para los VirtualHosts:

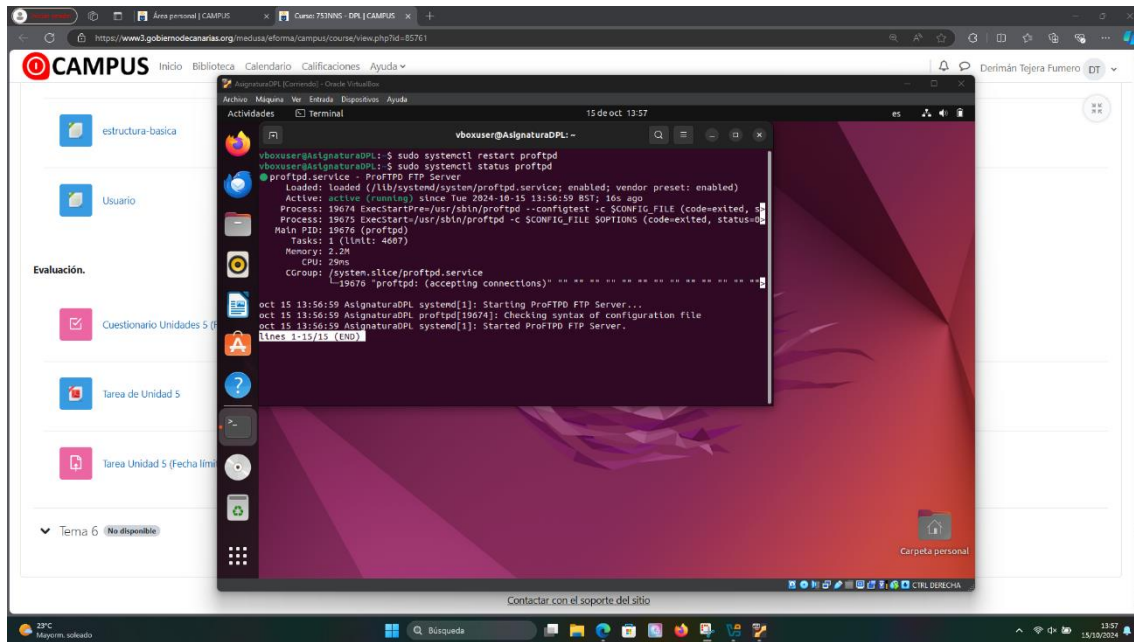




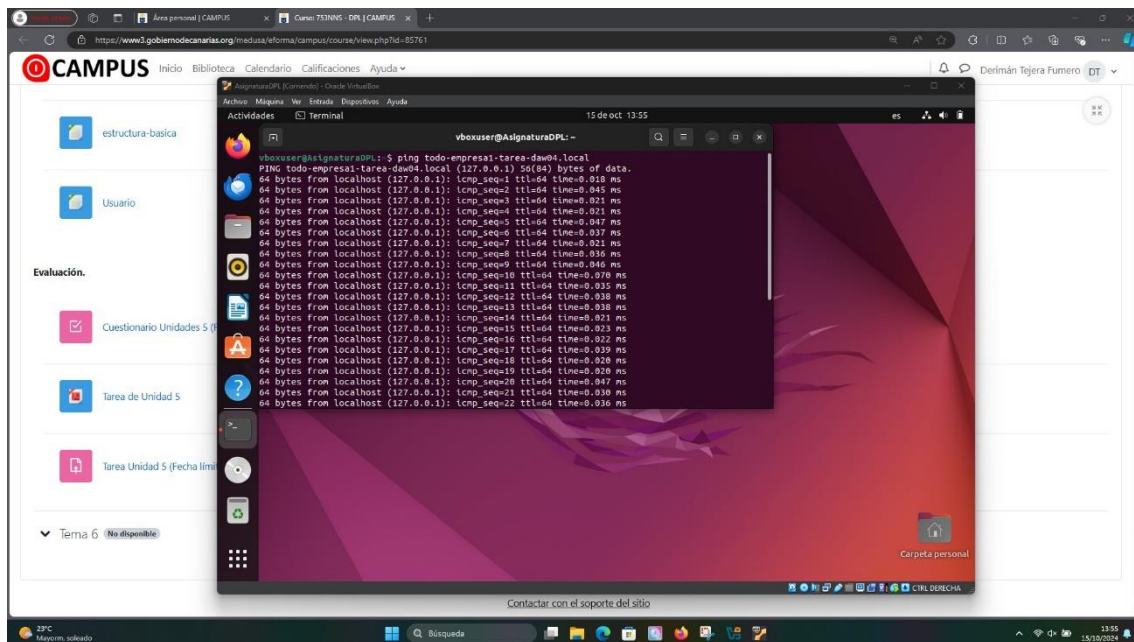
Verificamos los permisos:

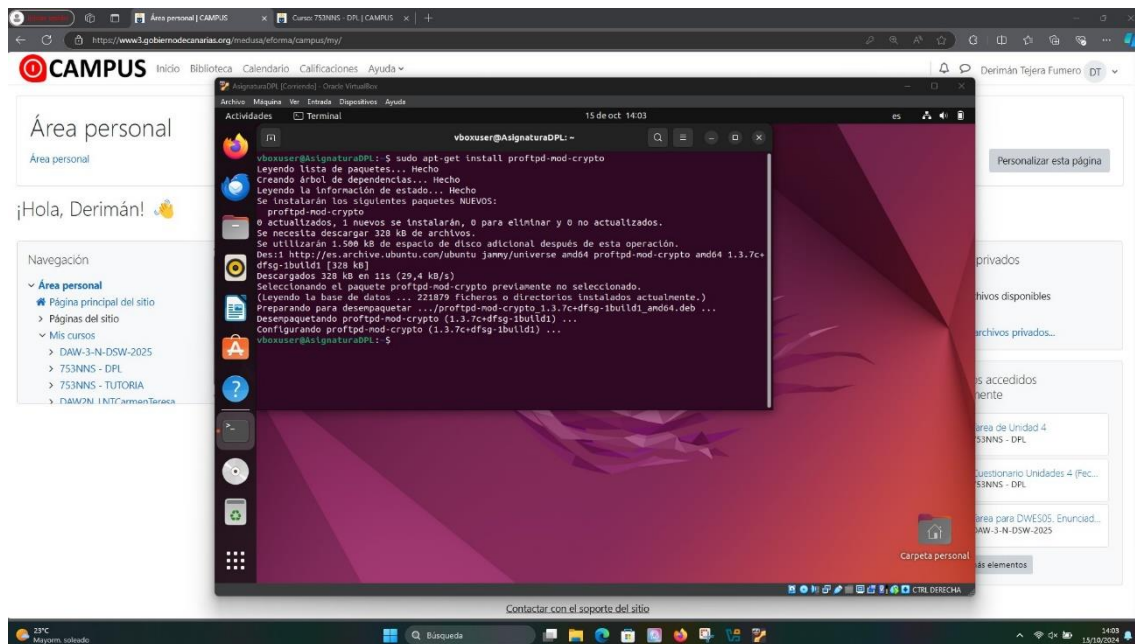


Ahora reiniciamos proftpd para aplicar los cambios:



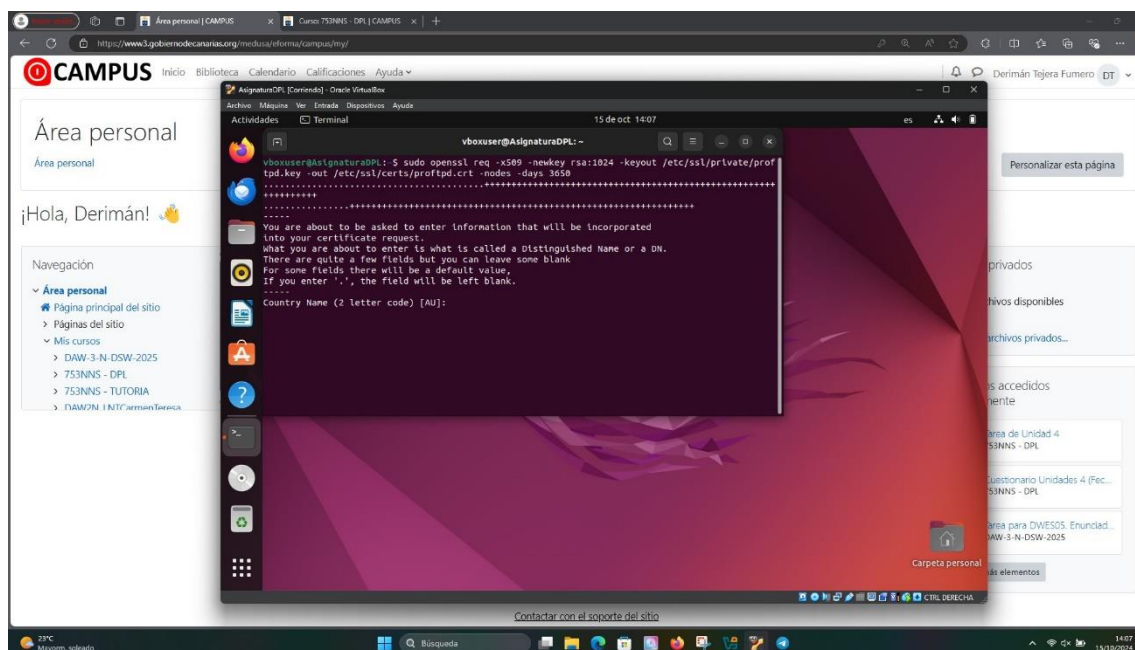
Hacemos ping para verificar que están funcionando:





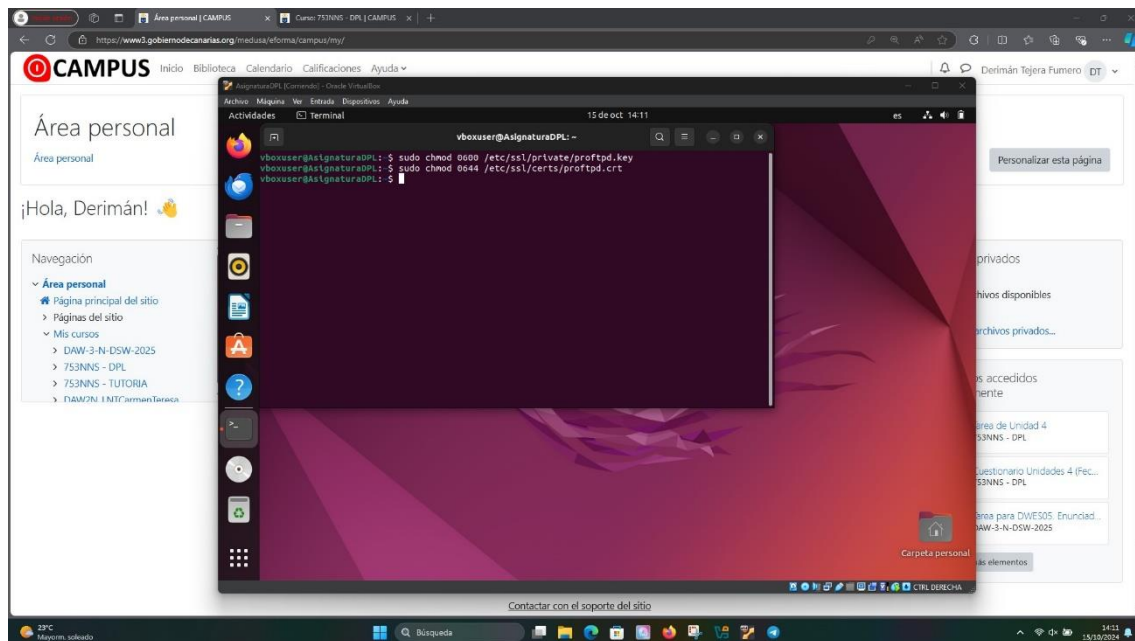
Generamos los certificados TLS utilizando OpenSSL:

```
sudo openssl req -x509 -newkey rsa:1024 -keyout /etc/ssl/private/proftpd.key -out /etc/ssl/certs/proftpd.crt -nodes -days 3650
```

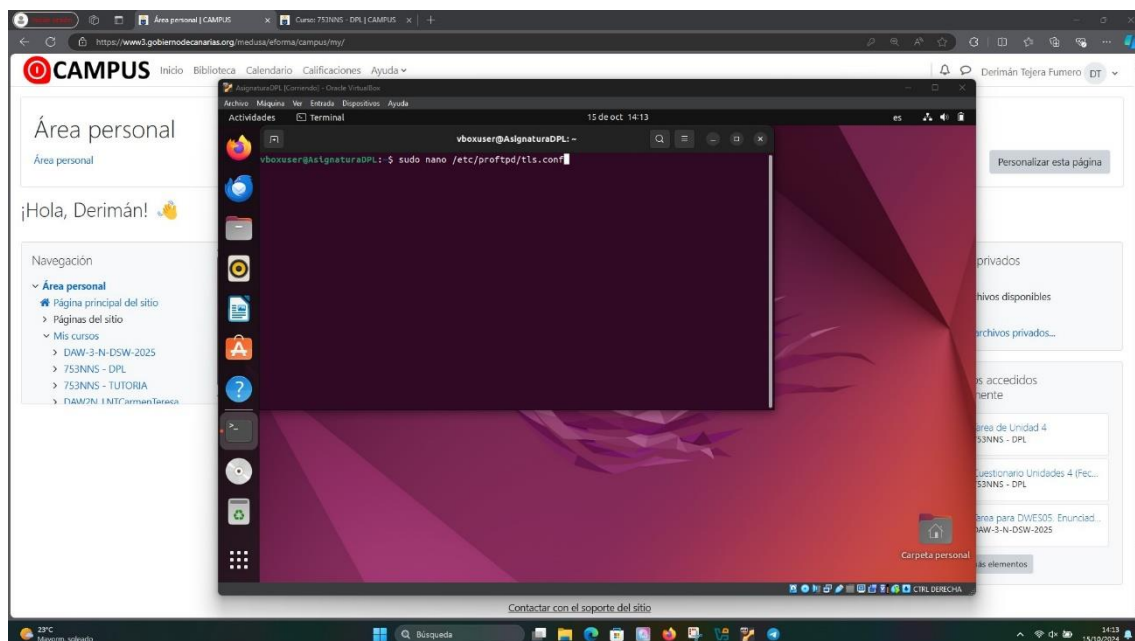


Se van completando los datos que solicitan, para simplificar únicamente se ha rellenado el de Country Name a: **ES**

Modificamos los permisos:



Editamos el archivo `tls.conf` para añadir la configuración necesaria:



TLSEngine on

TLSLog /var/log/proftpd/tls.log

TLSProtocol SSLv23

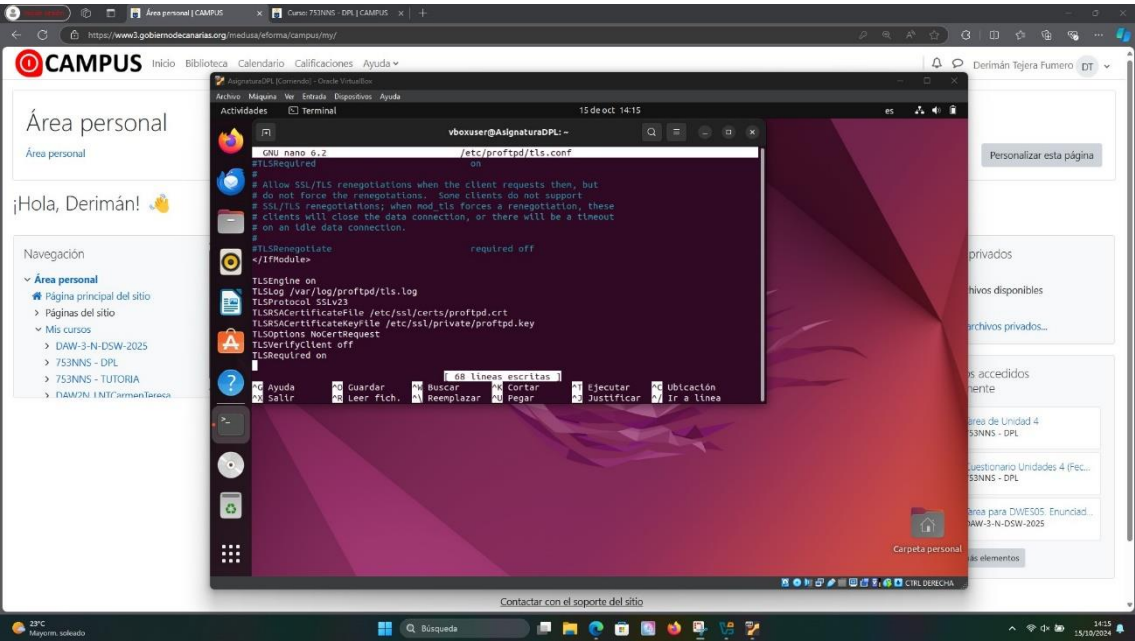
TLSRSACertificateFile /etc/ssl/certs/proftpd.crt

TLSRSACertificateKeyFile /etc/ssl/private/proftpd.key

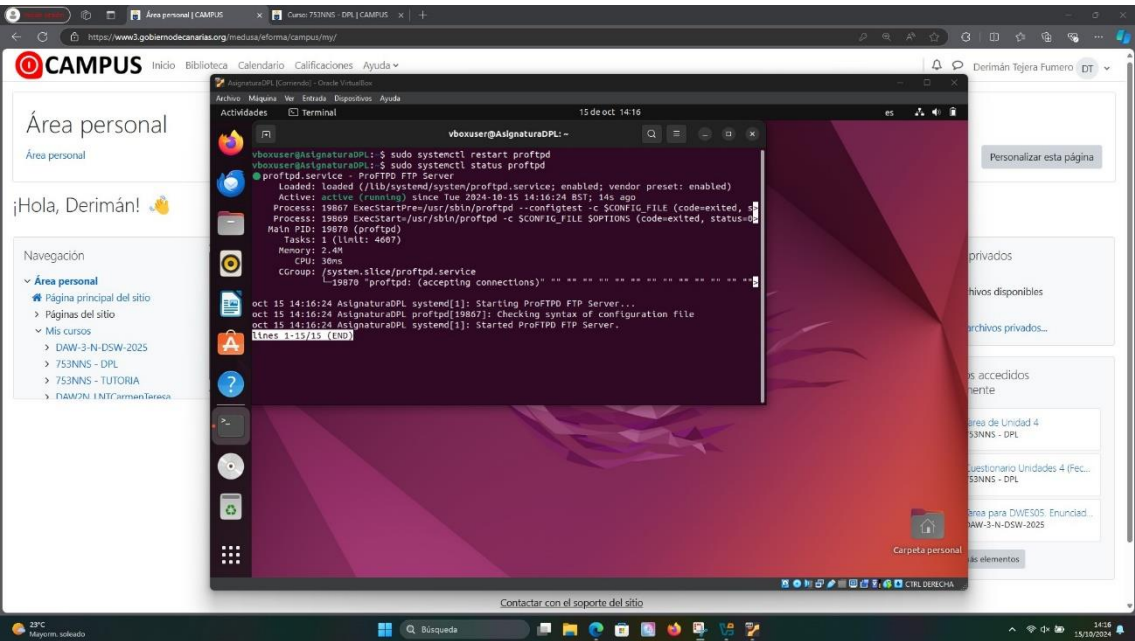
TLSOptions NoCertRequest

TLSVerifyClient off

TLSRequired on

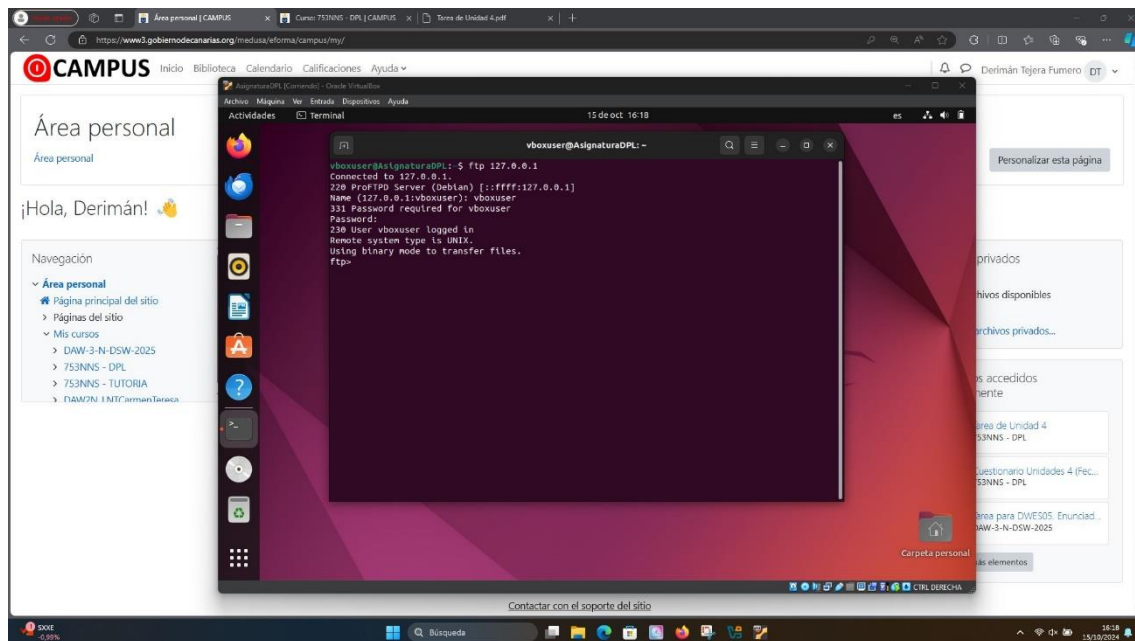


Ahora reiniciamos proftpd para aplicar los cambios:

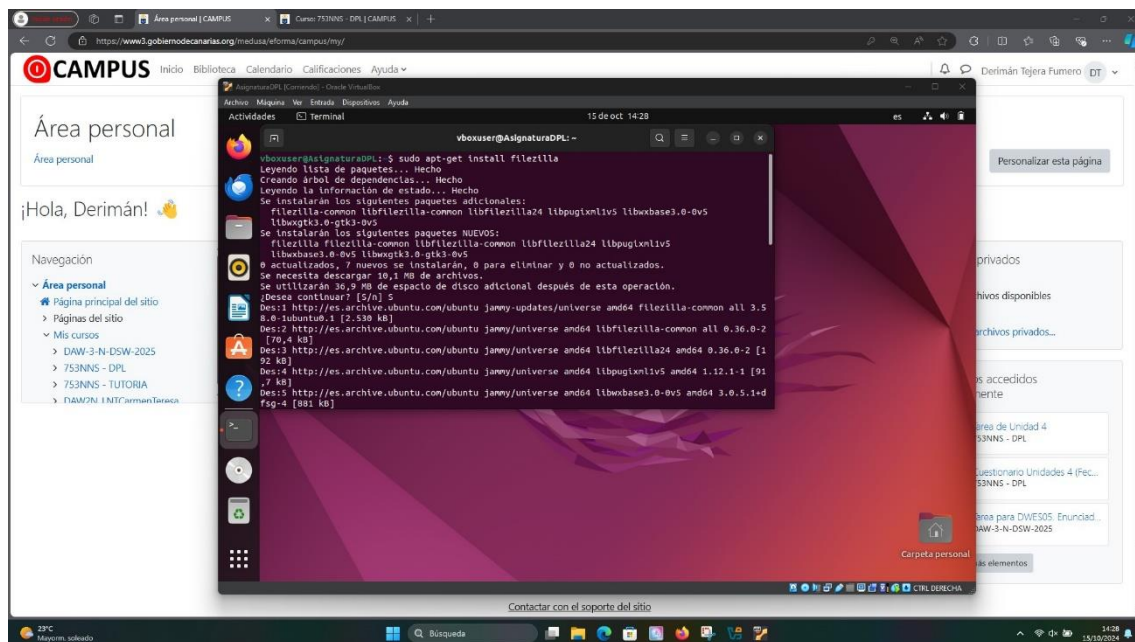


Apartado 4

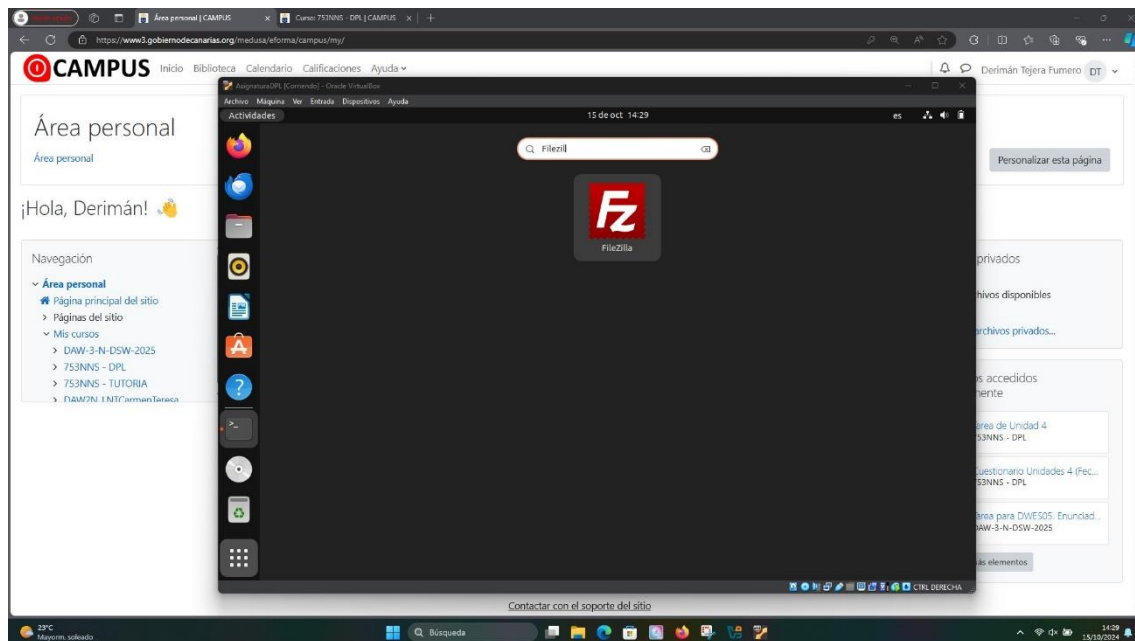
Conexión al servidor a través de la consola:



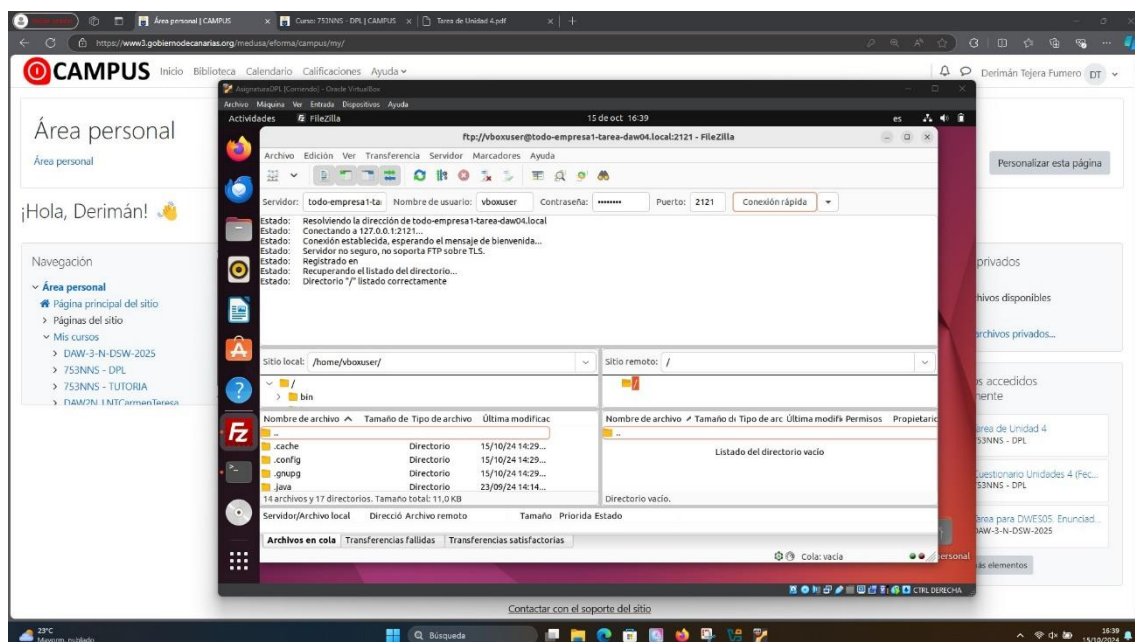
Instalamos el cliente gráfico FileZilla:



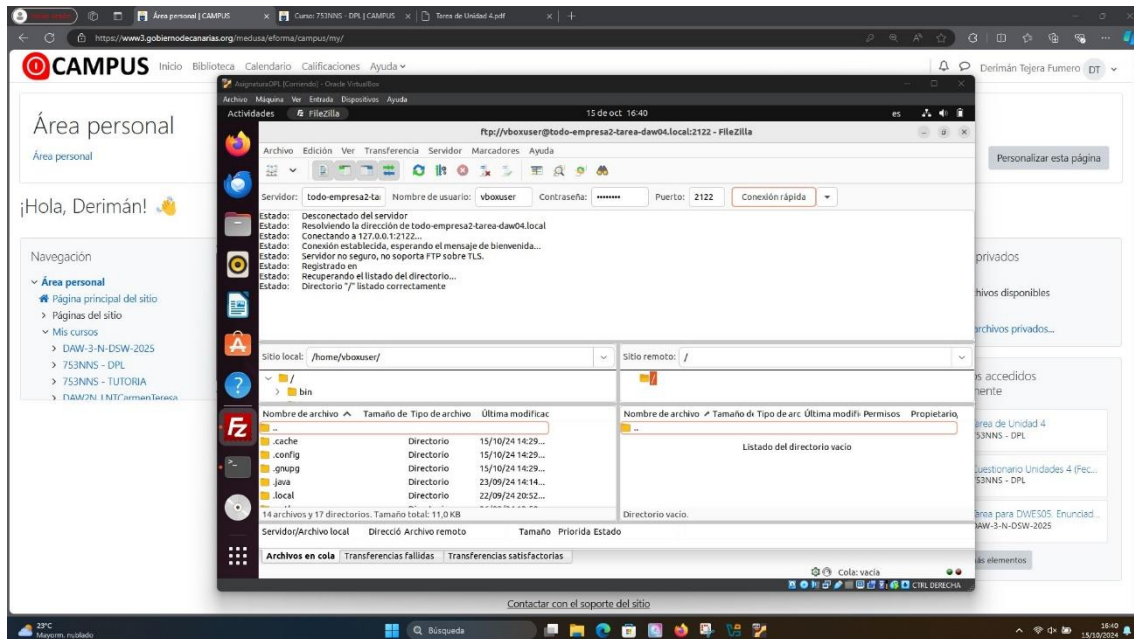
Iniciamos FileZilla:



Conectamos el servidor **todo-empresa1-tarea-daw04.local** usando el puerto 2121:



Conectamos el servidor **todo-empresa2-tarea-daw04.local** usando el puerto 2122:



Anteriormente no funcionaba debido a un error **500 AUTH**, esto finalmente se debió a no añadir los **includes** en el siguiente bloque de código en **virtuals.conf**:

```
<VirtualHost todo-empresa1-tarea-daw04.local>
```

```
Port 2121
```

```
ServerName "Servidor FTP empresa1"
```

```
DefaultRoot /var/ftp/empresa1/
```

```
RequireValidShell off
```

```
AuthUserFile /etc/proftpd/virtuals.passwd
```

```
Include /etc/proftpd/tls.conf
```

```
</VirtualHost>
```

```
<VirtualHost todo-empresa2-tarea-daw04.local>
```

```
Port 2122
```

```
ServerName "Servidor FTP empresa2"
```

```
DefaultRoot /var/ftp/empresa2/
```

```
RequireValidShell off
```

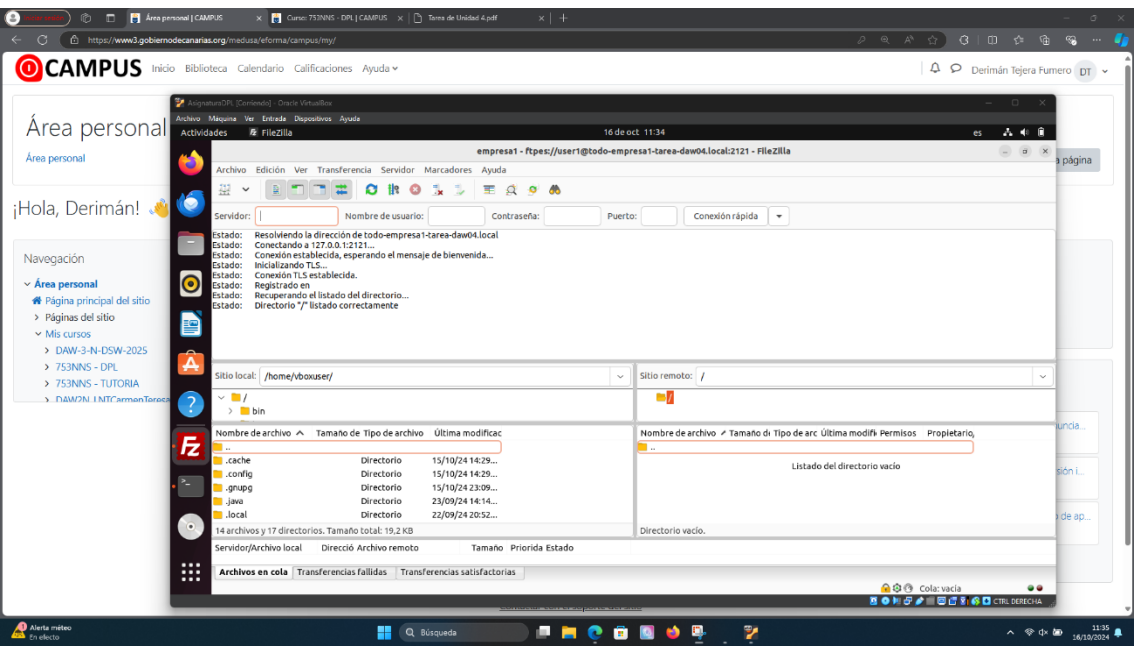
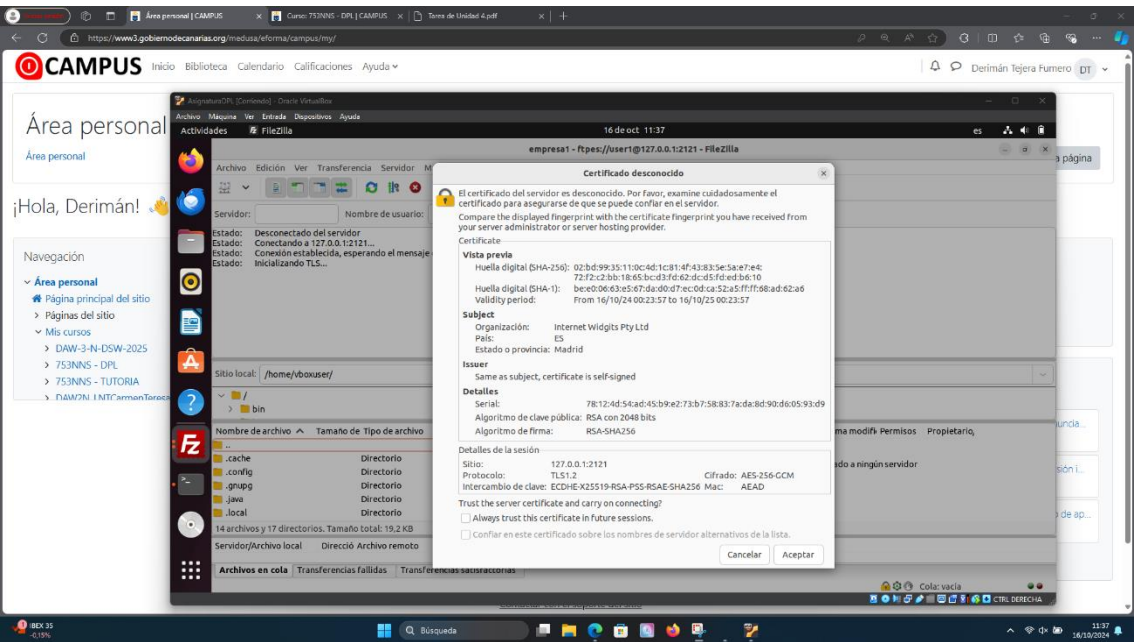
```
AuthUserFile /etc/proftpd/virtuals.passwd
```

```
Include /etc/proftpd/tls.conf
```

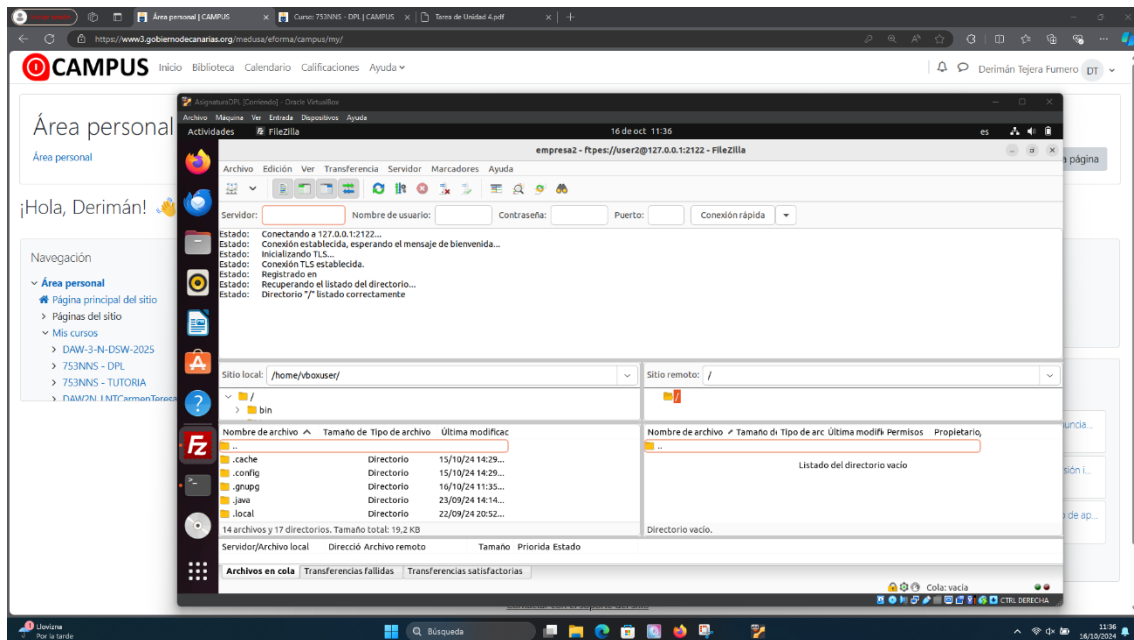
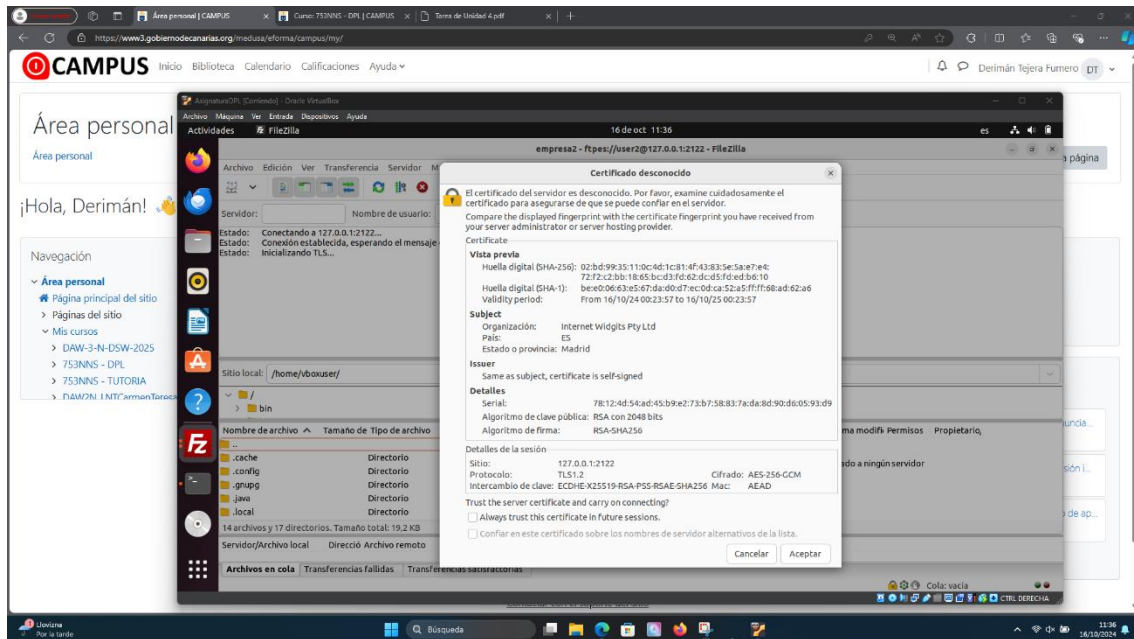
```
</VirtualHost>
```

Guardando y reseteando ProFTPD, ahora si es capaz de conectar usando TLS:

Conexión mediante TLS a **empresa1**:



Conexión mediante TLS a **empresa2**:



FIN

Este es el contenido de tls.conf:

#Contenido actual 16/10/2024 de tls.conf

GNU nano 6.2

/etc/proftpd/tls.conf

```
#
# Proftpd sample configuration for FTPS connections.
#
# Note that FTPS impose some limitations in NAT traversing.
# See http://www.castaglia.org/proftpd/doc/contrib/ProFTPD-mini-HOWTO-TLS.html
# for more information.
#

#<IfModule mod_tls.c>
#TLSEngine                on
#TLSLog                   /var/log/proftpd/tls.log
#TLSProtocol               SSLv23
#
# Server SSL certificate. You can generate a self-signed certificate using
# a command like:
#
# openssl req -x509 -newkey rsa:1024 \
#   -keyout /etc/ssl/private/proftpd.key -out /etc/ssl/certs/proftpd.crt \
#   -nodes -days 365
#
# The proftpd.key file must be readable by root only. The other file can be
# readable by anyone.
#
# chmod 0600 /etc/ssl/private/proftpd.key
# chmod 0640 /etc/ssl/private/proftpd.key
#
#TLRSACertificateFile      /etc/ssl/certs/proftpd.crt
#TLRSACertificateKeyFile   /etc/ssl/private/proftpd.key
#
# CA the server trusts...
#TLSCACertificateFile      /etc/ssl/certs/CA.pem
# ...or avoid CA cert and be verbose
#TLSOptions                NoCertRequest EnableDiags
# ... or the same with relaxed session use for some clients (e.g. FireFtp)
```

```

#TLSOptions          NoCertRequest EnableDiags NoSessionReuseRequired
#
#
# Per default drop connection if client tries to start a renegotiate
# This is a fix for CVE-2009-3555 but could break some clients.
#
#TLSOptions          AllowClientRenegotiations
#
# Authenticate clients that want to use FTP over TLS?
#
#TLSVerifyClient      off
#
# Are clients required to use FTP over TLS when talking to this server?
#
#TLSRequired          on
#
# Allow SSL/TLS renegotiations when the client requests them, but
# do not force the renegotiations. Some clients do not support
# SSL/TLS renegotiations; when mod_tls forces a renegotiation, these
# clients will close the data connection, or there will be a timeout
# on an idle data connection.
#
#TLSRenegotiate       required off
<IfModule mod_tls.c>
    TLSEngine          on
    TLSLog              /var/log/proftpd/tls.log
    TLSProtocol         TLSv1.2
    TLSCipherSuite      HIGH
    TLSRSACertificateFile /etc/proftpd/ssl/proftpd.cert.pem
    TLSRSACertificateKeyFile /etc/proftpd/ssl/proftpd.key.pem
    TLSOptions          NoCertRequest
    TLSVerifyClient     off
    TLSRequired         on
</IfModule>

```

Tener en cuenta que también se utilizó este comando para la generación del certificado:

```
sudo openssl req -x509 -newkey rsa:2048 -keyout /etc/ssl/private/proftpd.key -out  
/etc/ssl/certs/proftpd.crt -nodes -days 365
```