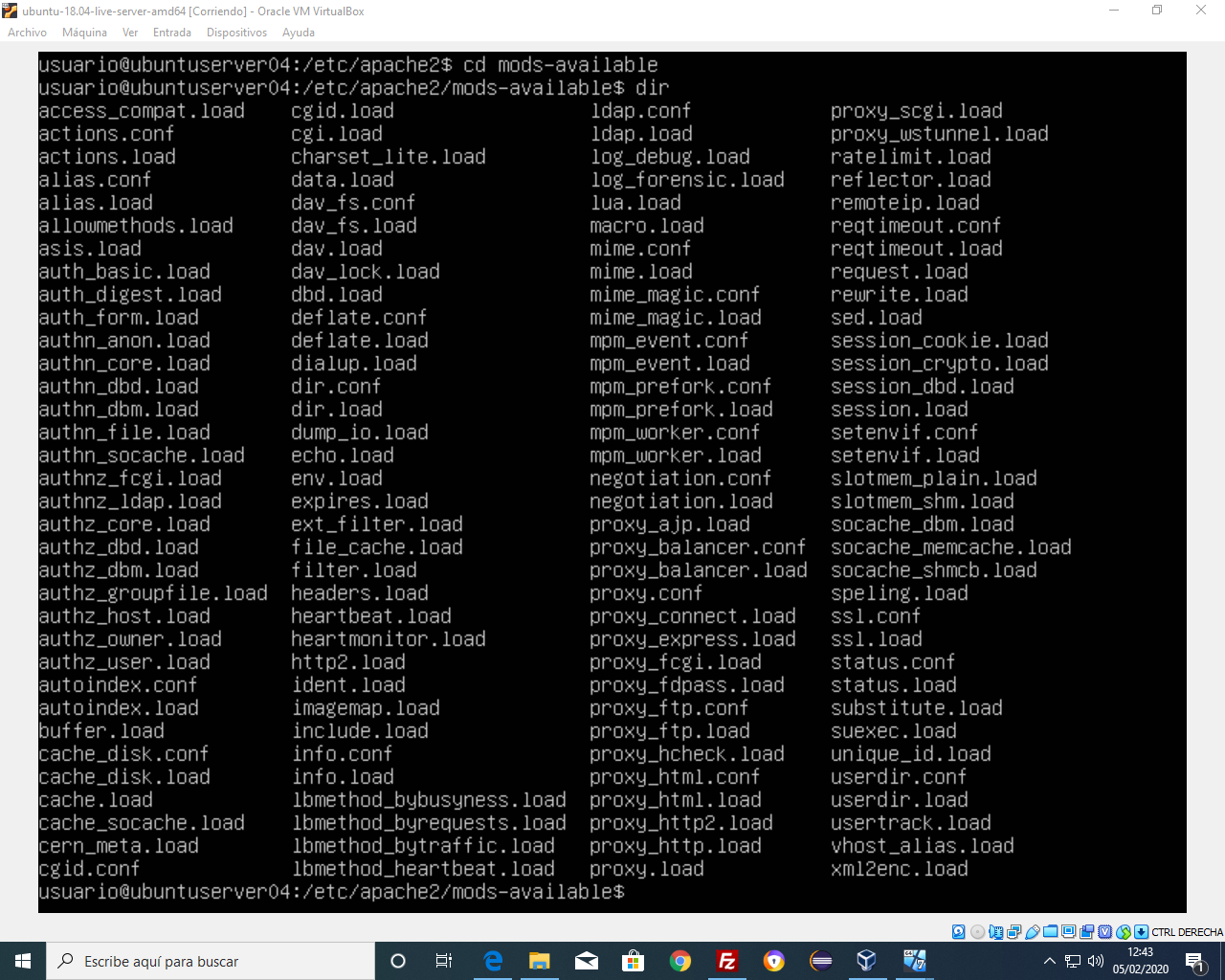
**,Práctica HTTPS POR DEFECTO**

**UBUNTU**

**Realiza la siguiente conﬁguración en el servidor Apache instalado en Ubuntu Server 18.04:**

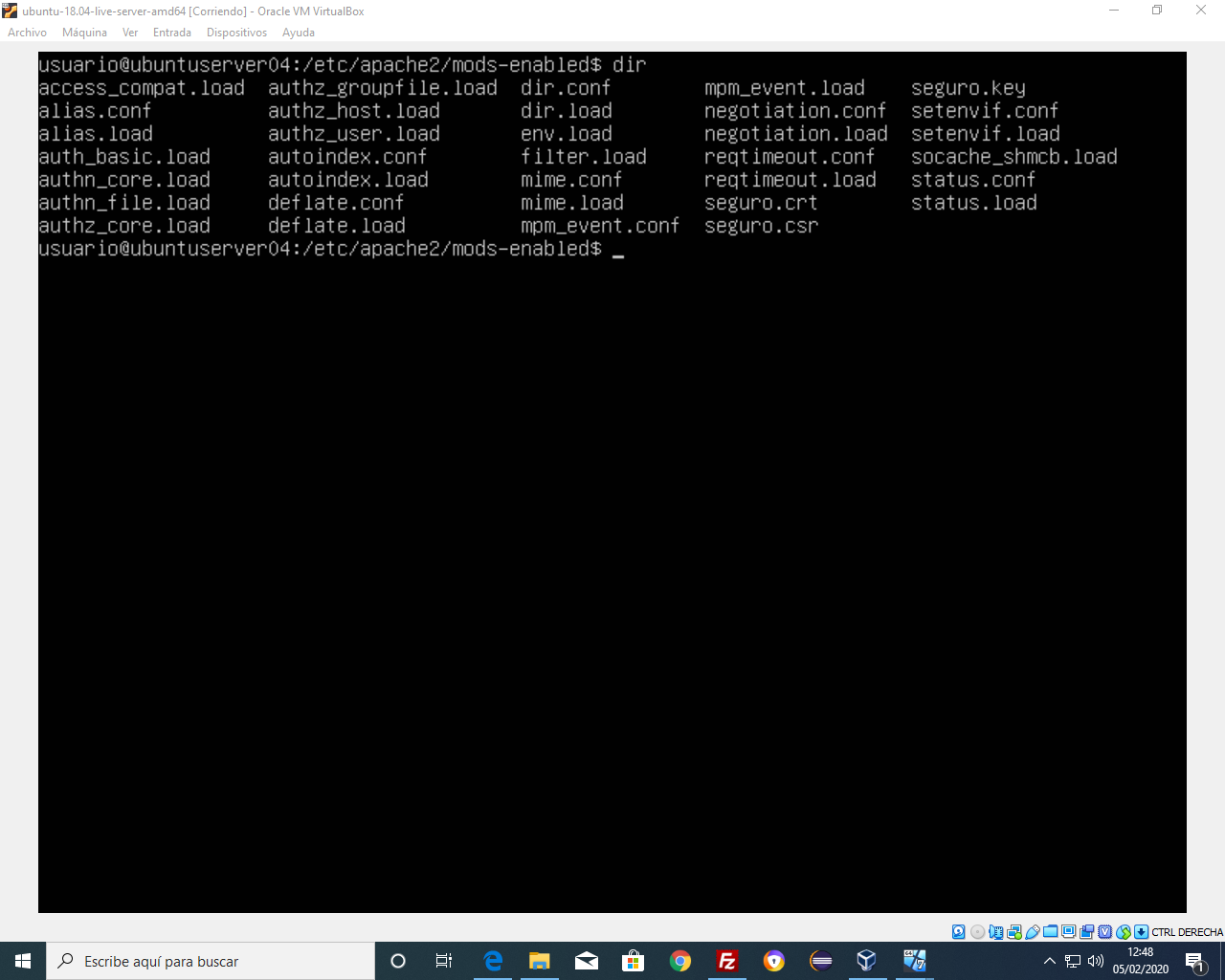
1. Entra en el directorio de módulos disponibles y observa que está mod\_ssl instalado.

*ls -la etc/Apache2/mods-available/ssl.conf*

**

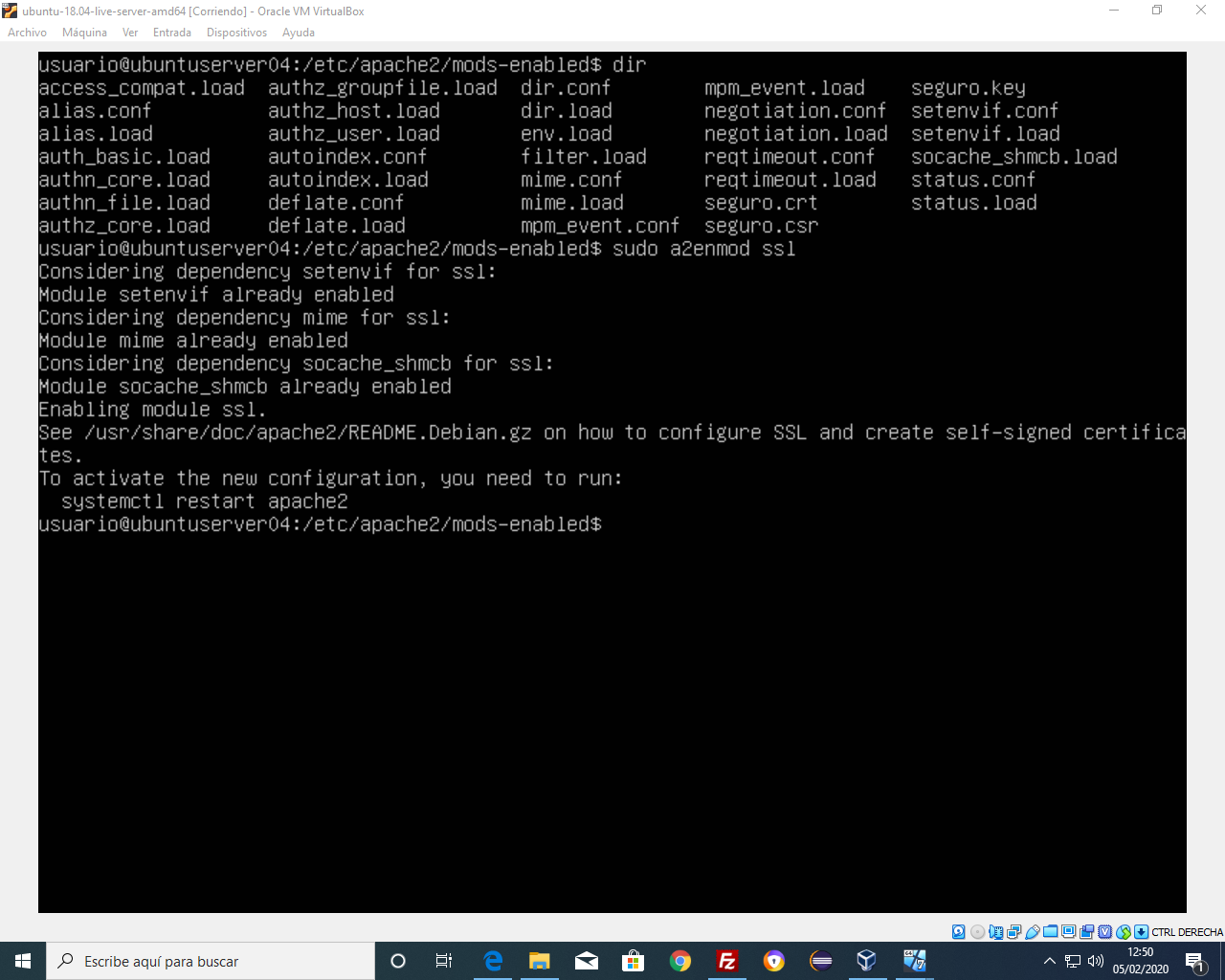
2. Entra en el directorio de módulos habilitados y comprueba que no está habilitado.

ls -la *etc/Apache2/mods-enabled|grep ssl o $cd etc/Apache2/mods-enabled $dir*

**

2.2.- Habilítalo con el comando:

sudo a2enmod ssl



3. Entra en el directorio de sitios disponibles y observa el contenido del sitio ssl por defecto

cd *etc/Apache2/sites-available*

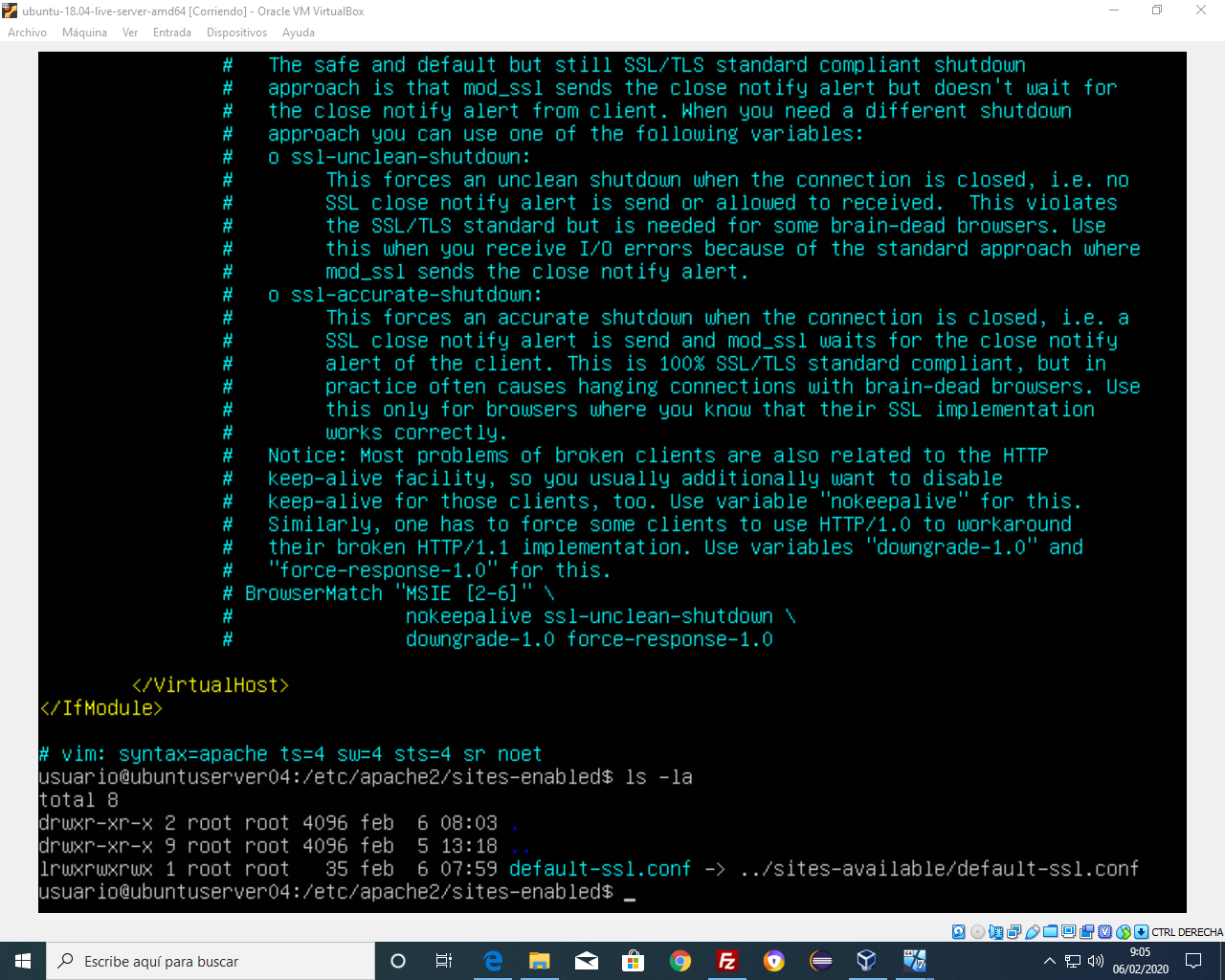
4. Entra en el directorio de sitios habilitados y comprueba que no está habilitado. Habilítalo con el comando:

ls -la *etc/Apache2/sites-enabled|grep ssl*

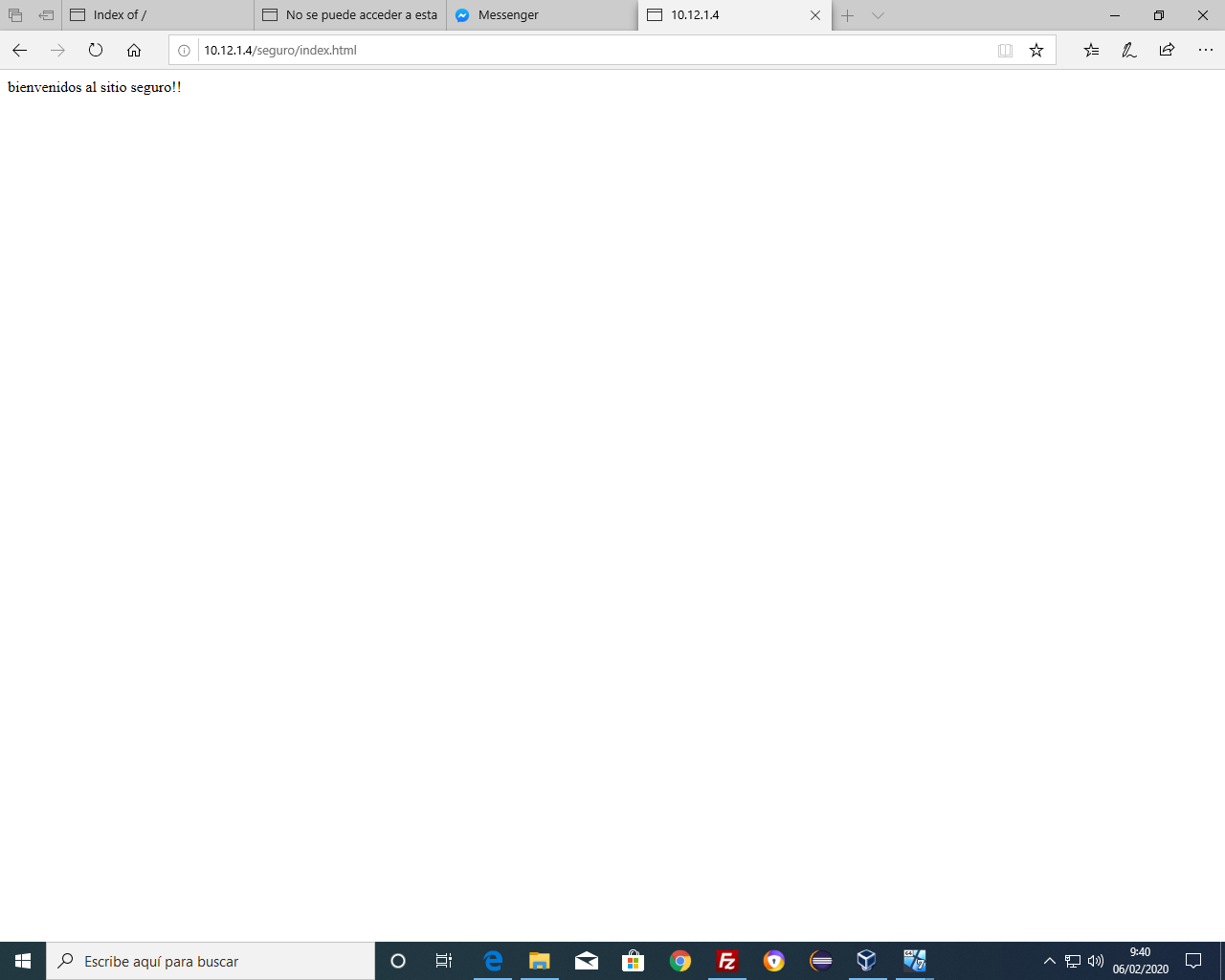
*sudo a2ensite default-ssl*

5. Reiniciamos apache

systemctl restart apache2



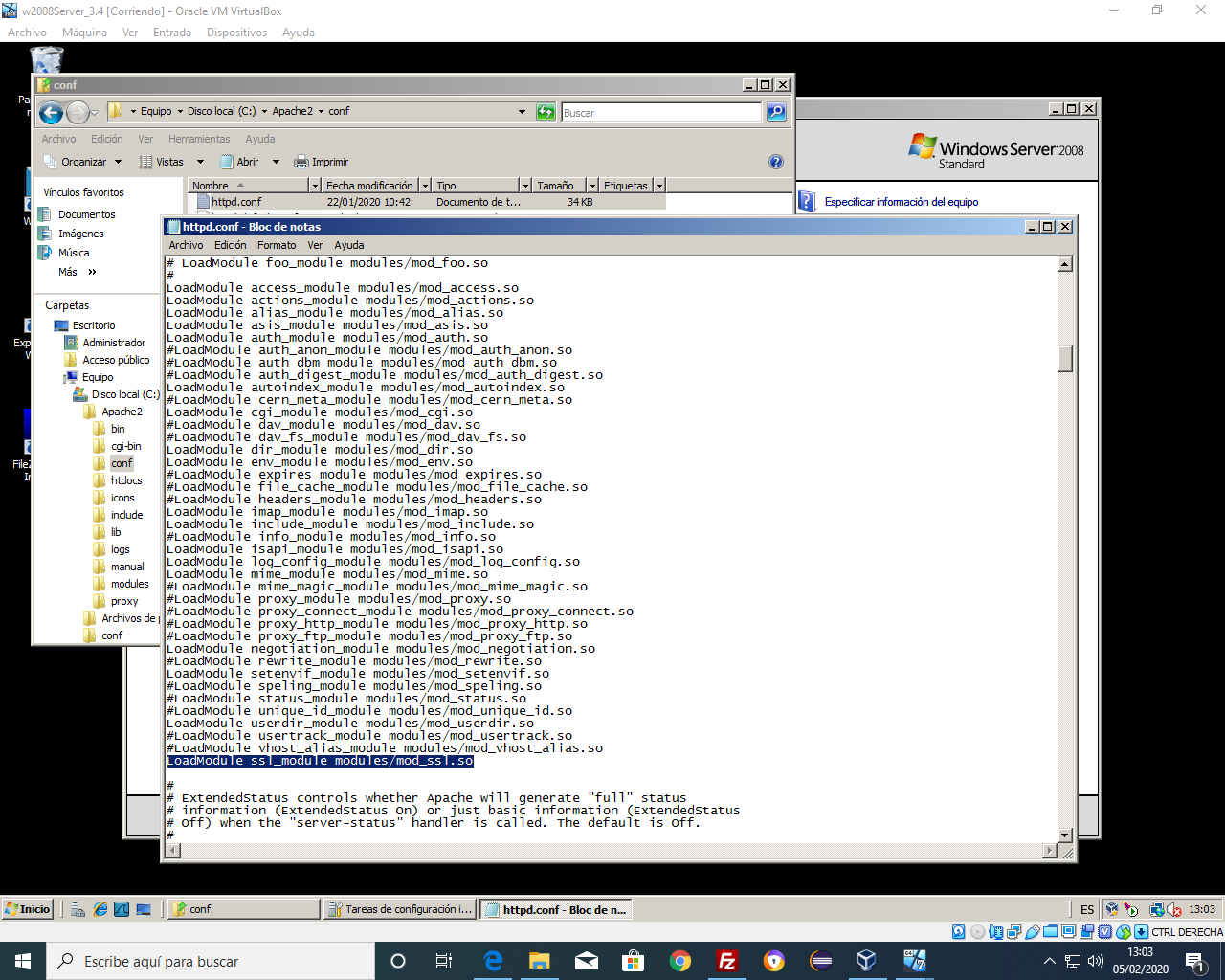
6. Abre el navegador y entra con [https://10.12.1.xx](https://10.12.1.xx/)



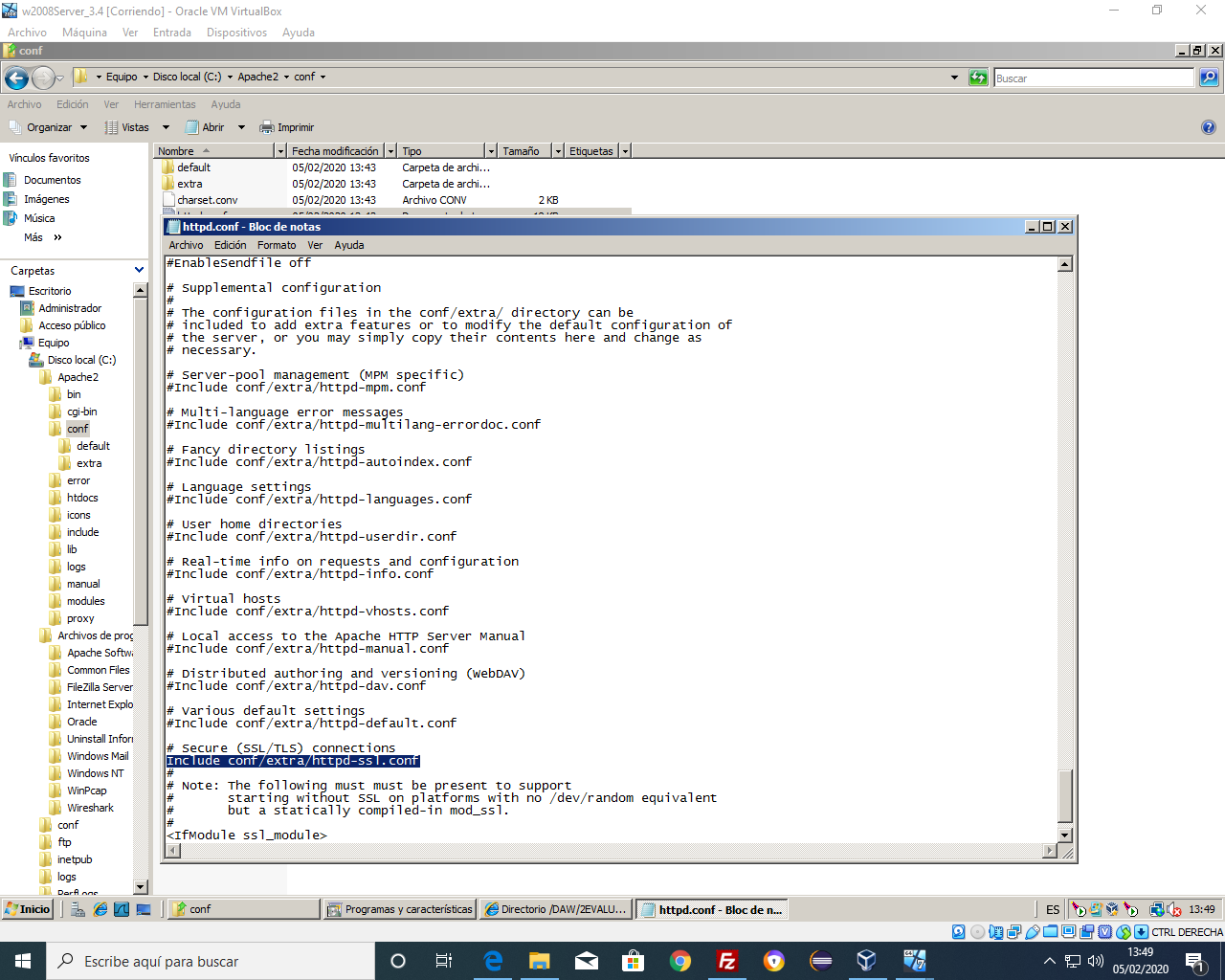
**WINDOWS**

1. Entramos en el archivo de configuración y habilitamos el módulo de ssl si no está ya descomentado.

[C:/Apache2/conf/httpd.conf](../../../../../../../../Apache2/conf/httpd.conf)

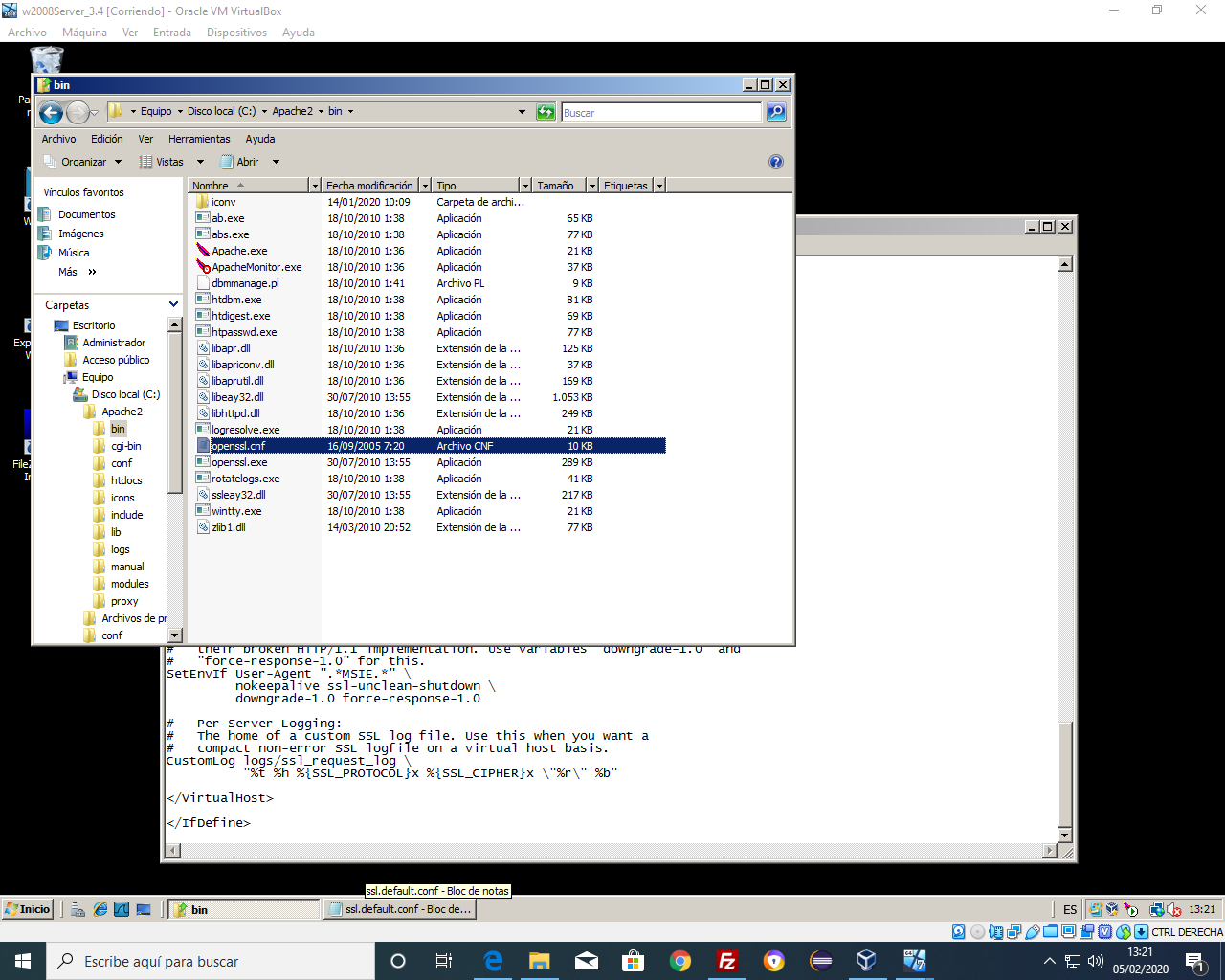


2. También descomentamos el extra del fichero de host virtuales ssl



3. Entramos en el extra en el fichero de de los host virtuales de ssl y observamos su contenido. Las claves no existen.

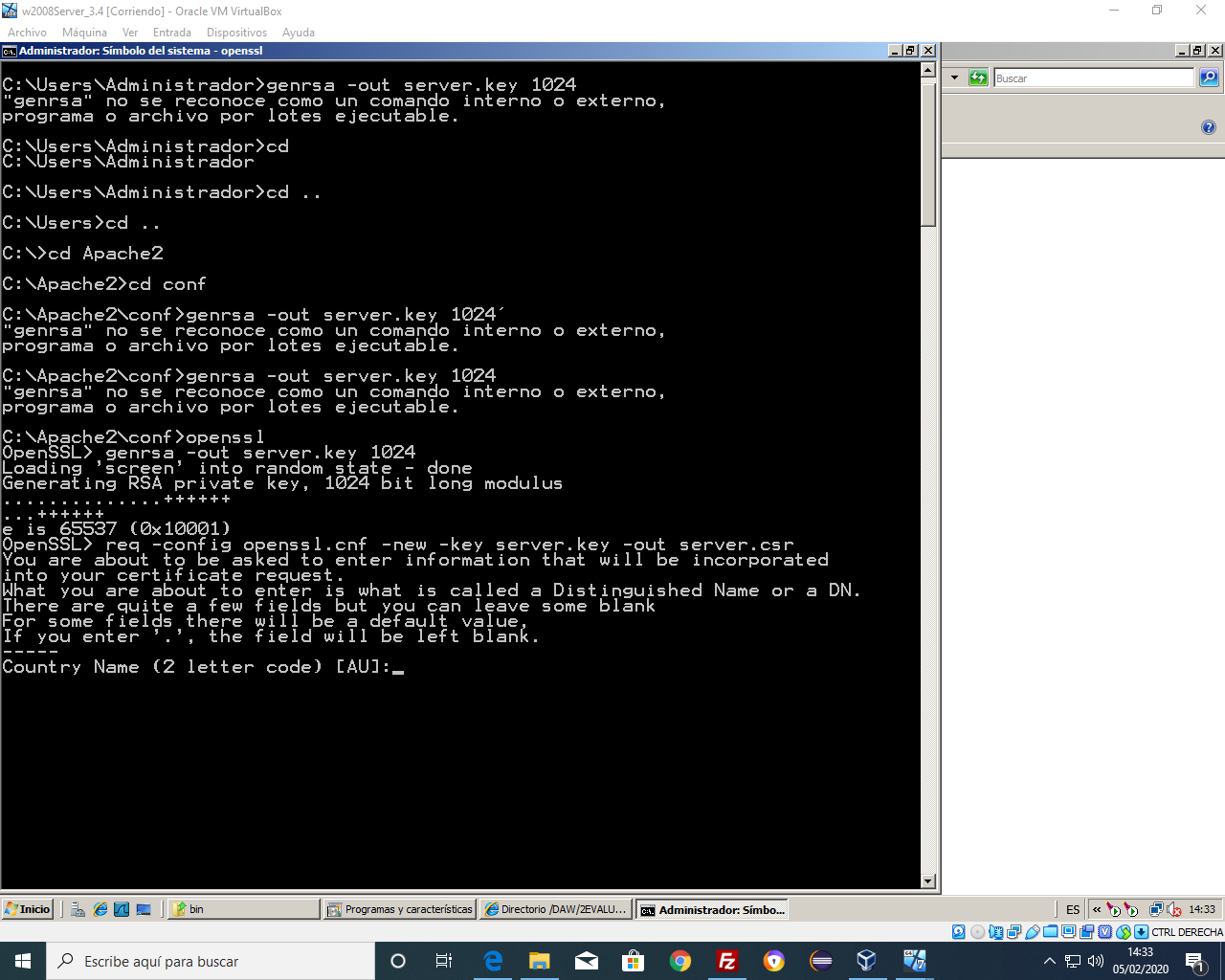
4. Copiamos el archivo openssl.cnf a bin para poder ejecutar openssl desde allí como administrador.



5. Generamos las claves y el certificado openssl

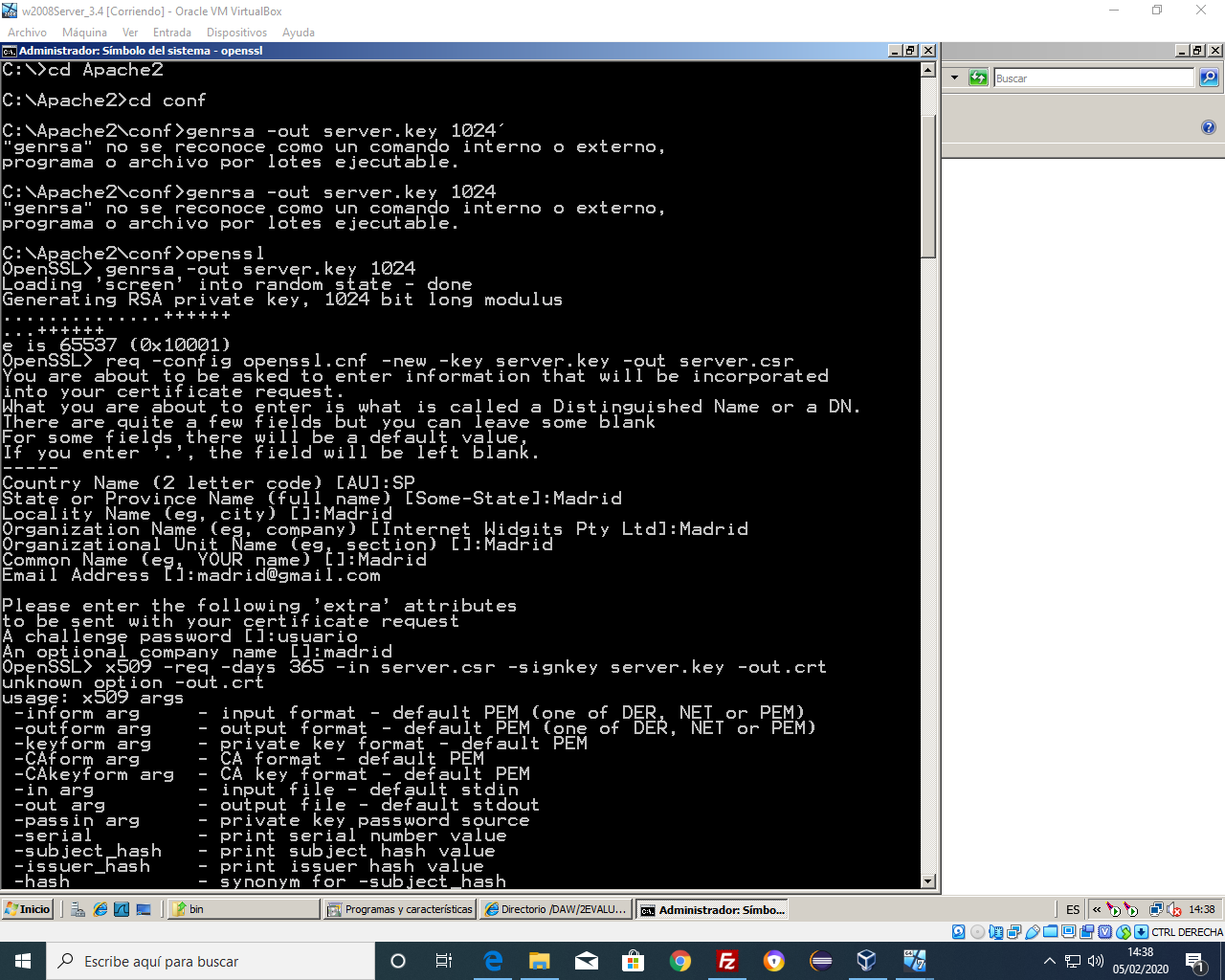
5.1 Creamos el certificado la llave con tamaño 1024 y el certificado asociado de clave privada. Esto da lugar a un fichero csr y un fichero .key.

genrsa -out server.key 1024



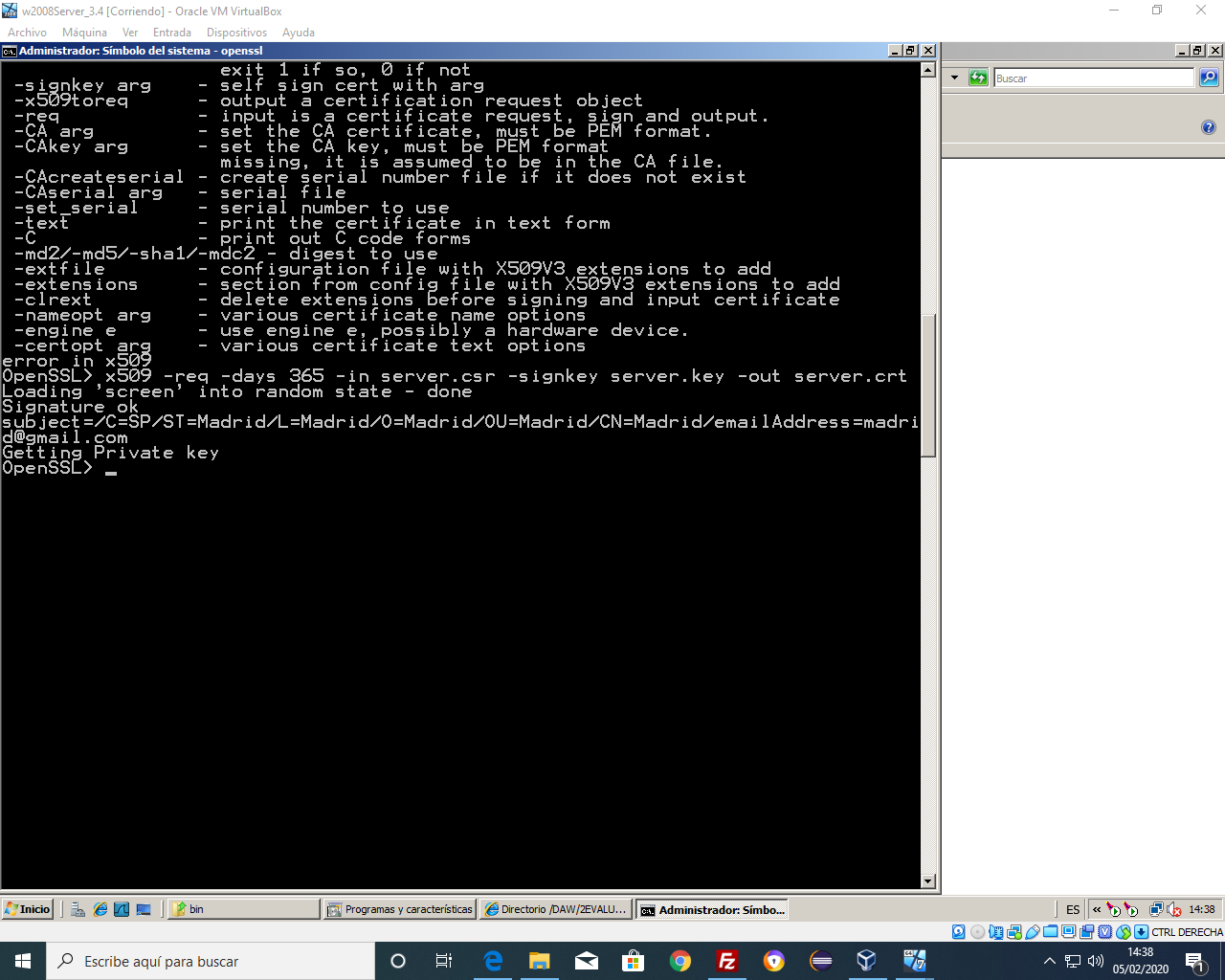
5.2 Creamos el certificado asociado a esa clave (fichero csr), contestando las preguntas que nos indique (darán información al cliente) y recordando la contraseña

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



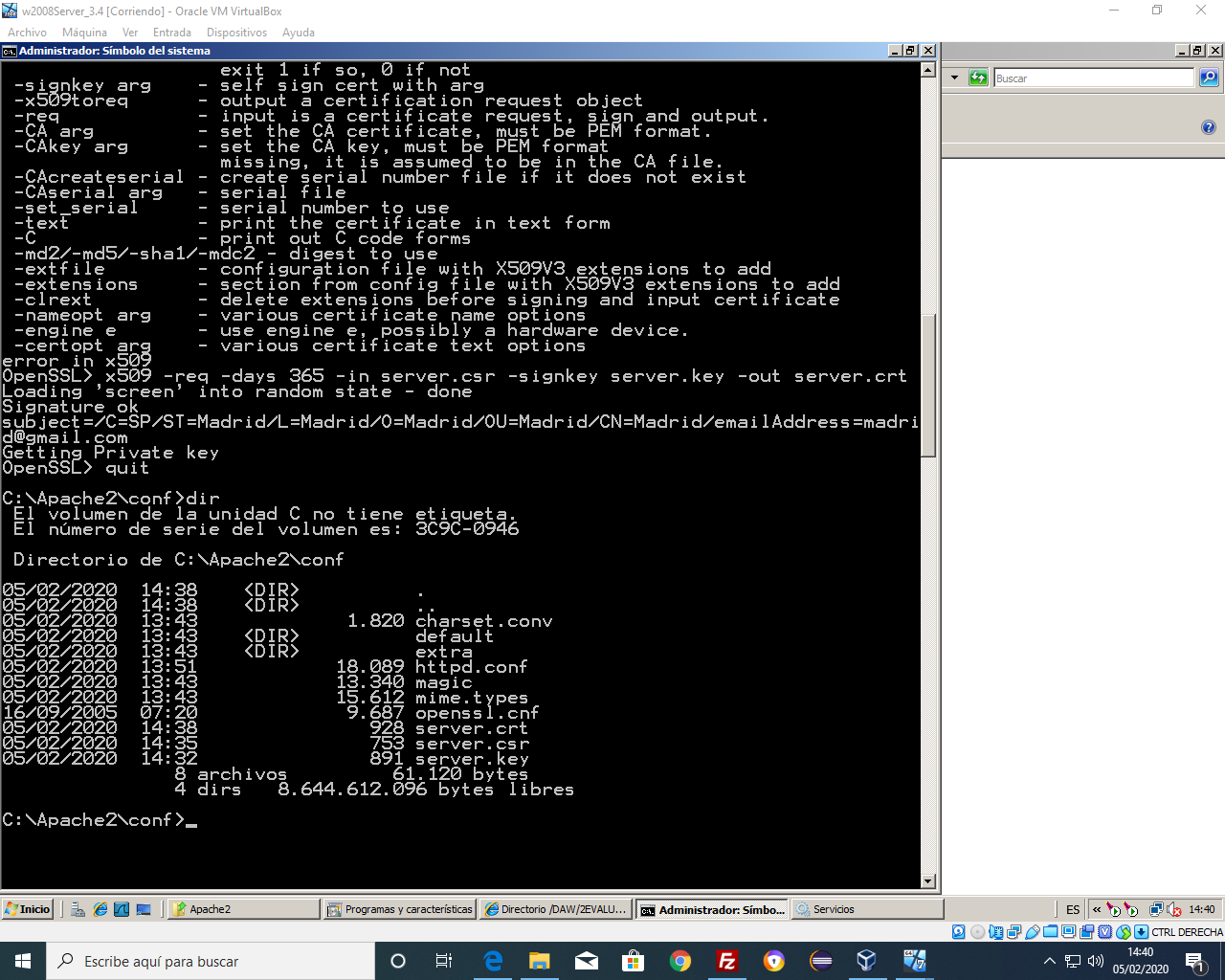
5.3 Creamos el certificado público. Esto nos creará un fichero crt.

x509 -req -days 365 -in server.csr -signkey server.key -out server.crt



5.4. Salimos con quit

6. Comprobamos que existen los ficheros key y crt



7. Copiamos estos ficheros key crt al directorio donde nuestro virtual host ssl los tiene configurados

8. Reiniciamos apache

9. Abre el navegador y entra con [https://127.0.0.1](https://127.0.0.1/) o cualquier dirección de tu servidor

