

## Índice:

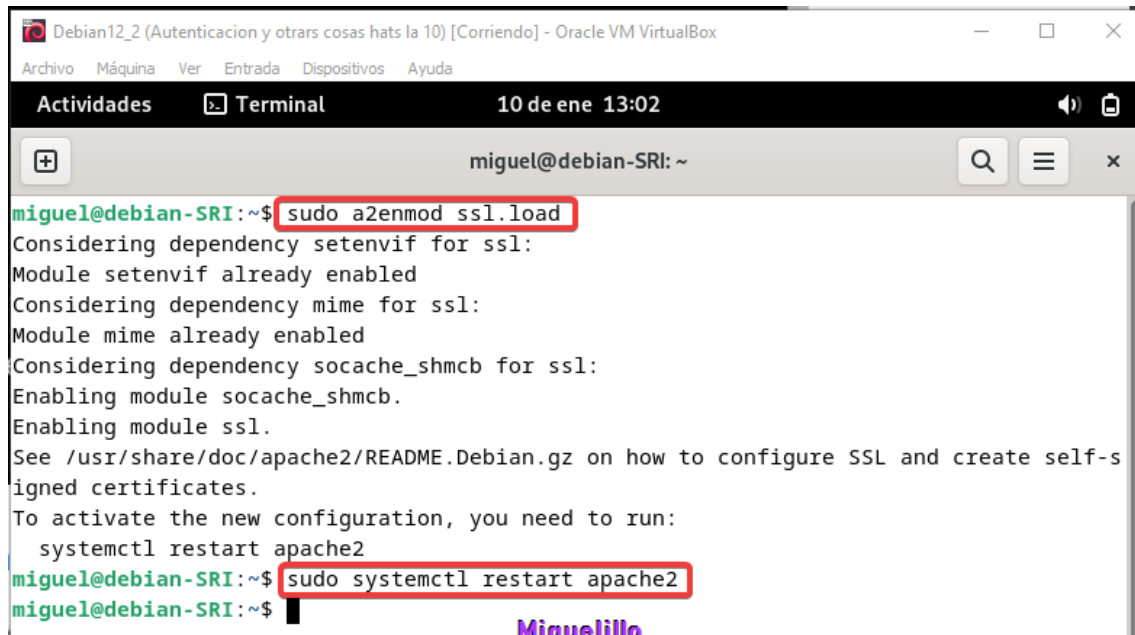
|                                                            |   |
|------------------------------------------------------------|---|
| Ejercicio 1 .....                                          | 2 |
| a) Habilitar SSL y Probarlo .....                          | 2 |
| b) Creación, gestión y configuración de certificados ..... | 5 |

## Ejercicio 1

### a) Habilitar SSL y Probarlo

Solución:

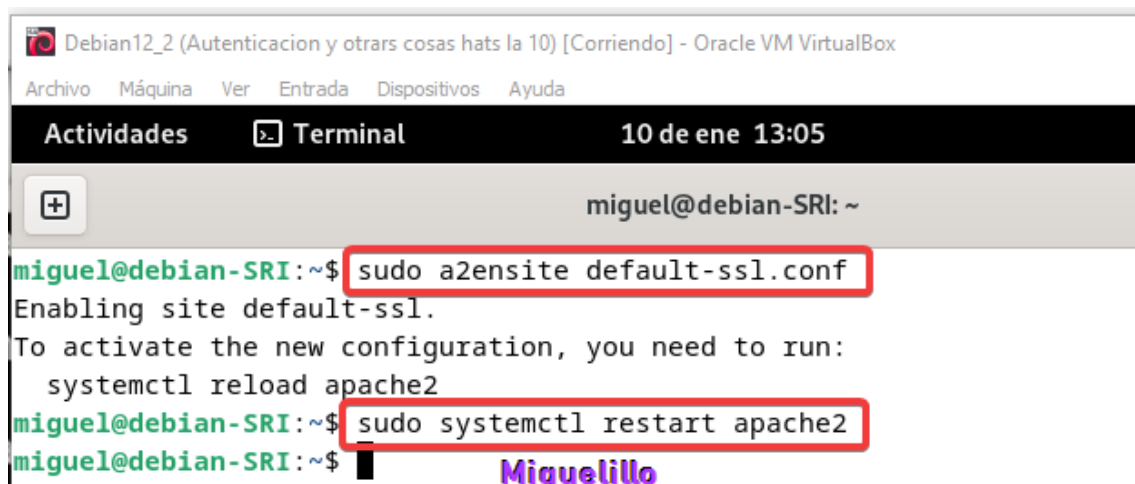
Habilitamos el modulo ssl



```
Debian12_2 (Autenticacion y otras cosas hats la 10) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal  10 de ene 13:02
miguel@debian-SRI: ~
miguel@debian-SRI:~$ sudo a2enmod ssl.load
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-s
igned certificates.
To activate the new configuration, you need to run:
    systemctl restart apache2
miguel@debian-SRI:~$ sudo systemctl restart apache2
miguel@debian-SRI:~$
```

Miguelillo

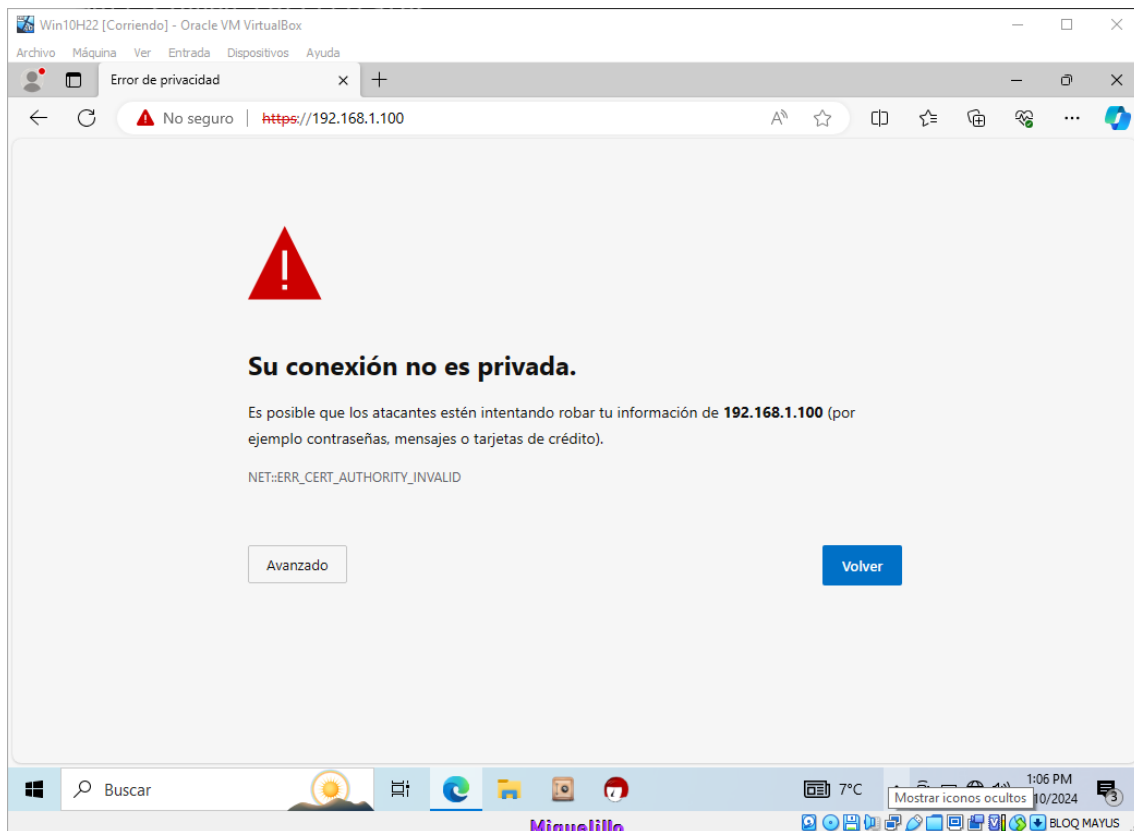
Habilitamos el sitio que trae ssl por defecto



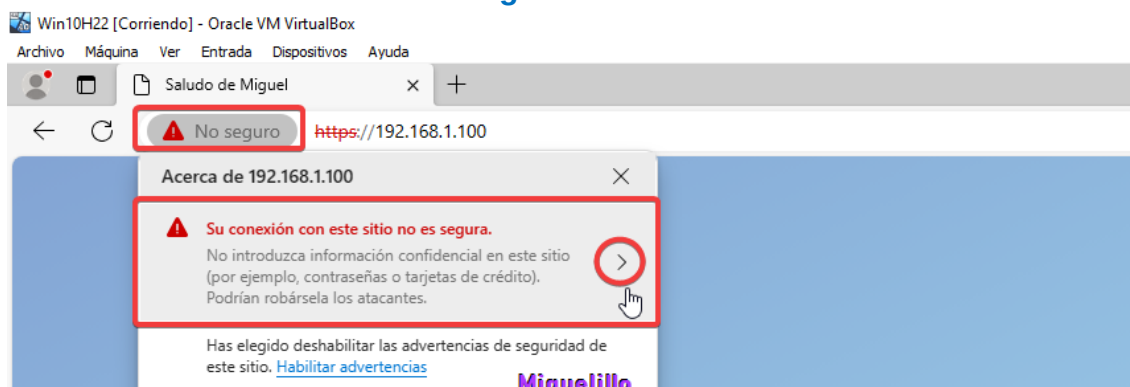
```
Debian12_2 (Autenticacion y otras cosas hats la 10) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal  10 de ene 13:05
miguel@debian-SRI: ~
miguel@debian-SRI:~$ sudo a2ensite default-ssl.conf
Enabling site default-ssl.
To activate the new configuration, you need to run:
    systemctl reload apache2
miguel@debian-SRI:~$ sudo systemctl restart apache2
miguel@debian-SRI:~$
```

Miguelillo

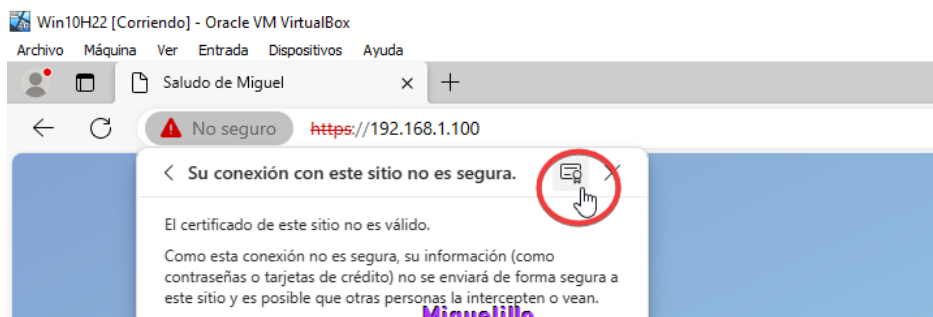
Probamos a acceder y nos dirá que a pesar de ser https no es seguro ya que el certificado no lo ha emitido ninguna entidad certificadora valida que reconozca el navegador en este caso la entidad certificadora es mi propio equipo debian



Podemos ver el certificado dándole a la **Exclamación No Seguro** y a **Su conexión con este sitio no es segura**



Seleccionado el icono nos muestra los certificados



Podemos ver que el nombre del certificado y la entidad certificadora son la misma mi maquina debían, la fecha de emisión y expiración y la huella digital

Win10H22 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Saludo de Miguel

No seguro | <https://192.168.1.100>

### Visor de certificados: debian-SRI

General Detalles

Emitido para

|                          |                                  |
|--------------------------|----------------------------------|
| Nombre común             | debian-SRI                       |
| Organización (O)         | <No forma parte del certificado> |
| Unidad organizativa (UO) | <No forma parte del certificado> |

Emitido por

|                          |                                  |
|--------------------------|----------------------------------|
| Nombre común             | debian-SRI                       |
| Organización (O)         | <No forma parte del certificado> |
| Unidad organizativa (UO) | <No forma parte del certificado> |

Período de validez

|                     |                                             |
|---------------------|---------------------------------------------|
| Emitido el          | miércoles, 8 de noviembre de 2023, 10:49:59 |
| Fecha de expiración | sábado, 5 de noviembre de 2033, 10:49:59    |

Huellas digitales de SHA-256

|               |                                                                  |
|---------------|------------------------------------------------------------------|
| Certificado   | 023321504a21c6b9c33ad10f27fd4d2d8e4bfafe59deee915c871383a55390e  |
| Clave pública | 9e195e6ea18af71b0dda7d11b02ad554a6a894bef39114d5df39e9dfda0fbf59 |

Miguelillo

## b) Creación, gestión y configuración de certificados

**Solución:**

## Creo una carpeta para guardar los certificados



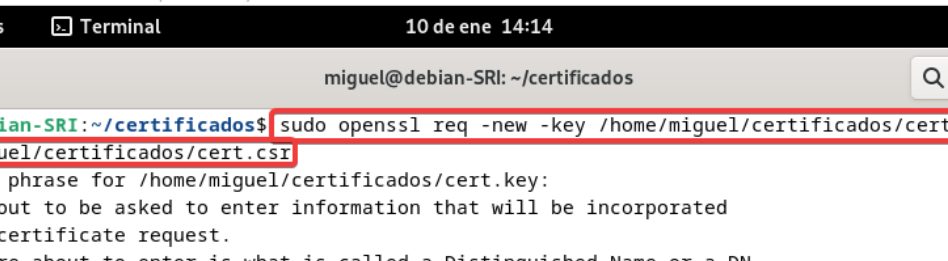
```
Debian12_2 (Autenticacion y otras cosas hats la 10) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal  10 de ene 13:22
miguel@debian-SRI: ~
miguel@debian-SRI:~$ sudo mkdir certificados
[sudo] contraseña para miguel
```

Dentro creamos una llave para generar los certificados



The screenshot shows a terminal window titled "Debian12\_2 (Autenticacion y otras cosas hats la 10) [Corriendo] - Oracle VM VirtualBox". The terminal prompt is "miguel@debian-SRI: ~/certificados". The command being executed is "sudo openssl genpkey -algorithm RSA -out /home/miguel/certificados/cert.key -aes256". The output shows a series of dots and a plus sign, indicating the progress of the key generation. The terminal window has a dark theme and a menu bar with options like "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda".

## Creamos el certificado e introducimos los datos



The screenshot shows a terminal window titled "Debian12\_2 (Autenticación y otras cosas hats la 10) [Corriendo] - Oracle VM VirtualBox". The terminal output shows the execution of the command `sudo openssl req -new -key /home/miguel/certificados/cert.key -out /home/miguel/certificados/cert.csr`. The user is prompted to enter a pass phrase for the key file. Following this, the user provides information for the certificate request, including Country Name (ES), State or Province Name (Ciudad Real), Locality Name (Valdepenas), Organization Name (IES GP), Organizational Unit Name (ASIR), Common Name (Miguel Lillo Romero), and Email Address (miquel@cosa.com).

```
Debian12_2 (Autenticación y otras cosas hats la 10) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 10 de ene 14:14
miguel@debian-SRI: ~/certificados
miguel@debian-SRI:~/certificados$ sudo openssl req -new -key /home/miguel/certificados/cert.key -out /home/miguel/certificados/cert.csr
Enter pass phrase for /home/miguel/certificados/cert.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] ES
State or Province Name (full name) [Some-State] Ciudad Real
Locality Name (eg, city) [] Valdepenas
Organization Name (eg, company) [Internet Widgits Pty Ltd] IES GP
Organizational Unit Name (eg, section) [] ASIR
Common Name (e.g. server FQDN or YOUR name) [] Miguel Lillo Romero
Email Address [] miquel@cosa.com
```

Ahora firmamos el certificado con una validez de 9000 días con la llave que creamos al principio

```
Debian12_2 (Autenticacion y otras cosas hats la 10) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 10 de ene 14:17
miguel@debian-SRI: ~/certificados
miguel@debian-SRI:~/certificados$ sudo openssl x509 -req -in /home/miguel/certificados/cert.csr -signkey
/home/miguel/certificados/cert.key -out /home/miguel/certificados/certificado-firmado.crt
Enter pass phrase for /home/miguel/certificados/cert.key:
Certificate request self-signature ok
subject=C = ES, ST = Ciudad Real, L = Valdepenas, O = IES GP, OU = ASIR, CN = Miguel Lillo Romero, email
Address = miguel@cosa.com
miguel@debian-SRI:~/certificados$
```

Nos creamos un nuevo sitio copiando el sitio ssl por defecto.

```
Debian12_2 (Autenticacion y otras cosas hats la 10) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 10 de ene 13:42
miguel@debian-SRI: /etc/apache2/sites-available
miguel@debian-SRI: /etc/apache2/sites-available$ sudo cp default-ssl.conf miguel-ssl.conf
Miguelillo
```

Configuramos el archivo index por defecto y el directorio por defecto

```
Debian12_2 (Autenticacion y otras cosas hats la 10) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 10 de ene 13:45
miguel@debian-SRI: /etc/apache2/sites-available
GNU nano 7.2 miguel-ssl.conf *
<VirtualHost *:443>
    ServerAdmin webmaster@localhost
    DocumentRoot /home/miguel/html
    DirectoryIndex miguel.html
Miguelillo
```

Habilitamos el motor SSL en caso que no este activado y añadimos las rutas a la llave y al certificado

```
Debian12_2 (Autenticacion y otras cosas hats la 10) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 10 de ene 13:48
miguel@debian-SRI: /etc/apache2/sites-available
GNU nano 7.2 miguel-ssl.conf
SSLEngine on

# A self-signed (snakeoil) certificate can be created by installing
# the ssl-cert package. See
# /usr/share/doc/apache2/README.Debian.gz for more info.
# If both key and certificate are stored in the same file, only the
# SSLCertificateFile directive is needed.
SSLCertificateFile /home/miguel/certificados/certificado-firmado.csr
SSLCertificateKeyFile /home/miguel/certificados/cert.key
# Server Certificate Chain:
Miguelillo
```

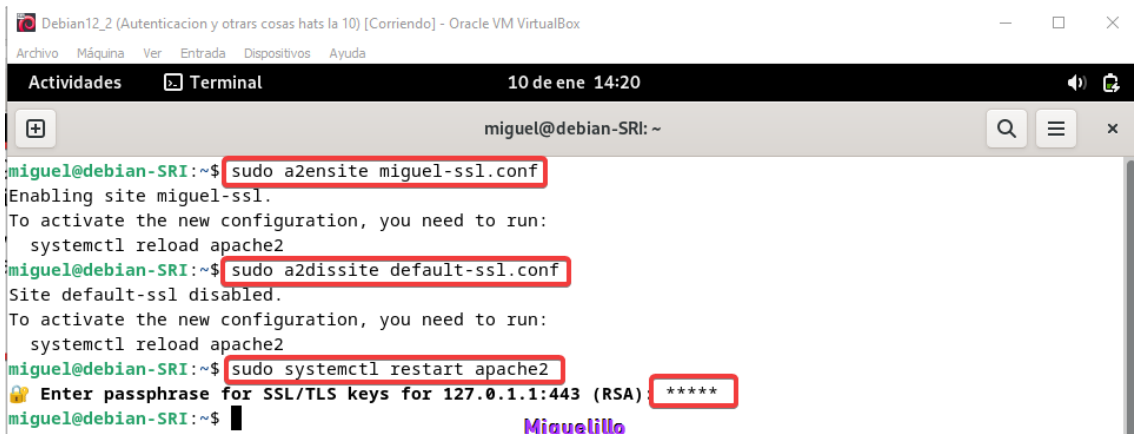
Añadimos el directorio del índice con los permisos para poder acceder



```
Debian12_2 (Autenticacion y otras cosas hats la 10) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal  10 de ene 13:52
miguel@debian-SRI: /etc/apache2/sites-available
GNU nano 7.2  miguel-ssl.conf
<Directory /home/miguel/html/>
    AllowOverrride all
    Order allow,deny
    Allow from all
    Require all granted
</Directory>
```

Miguelillo

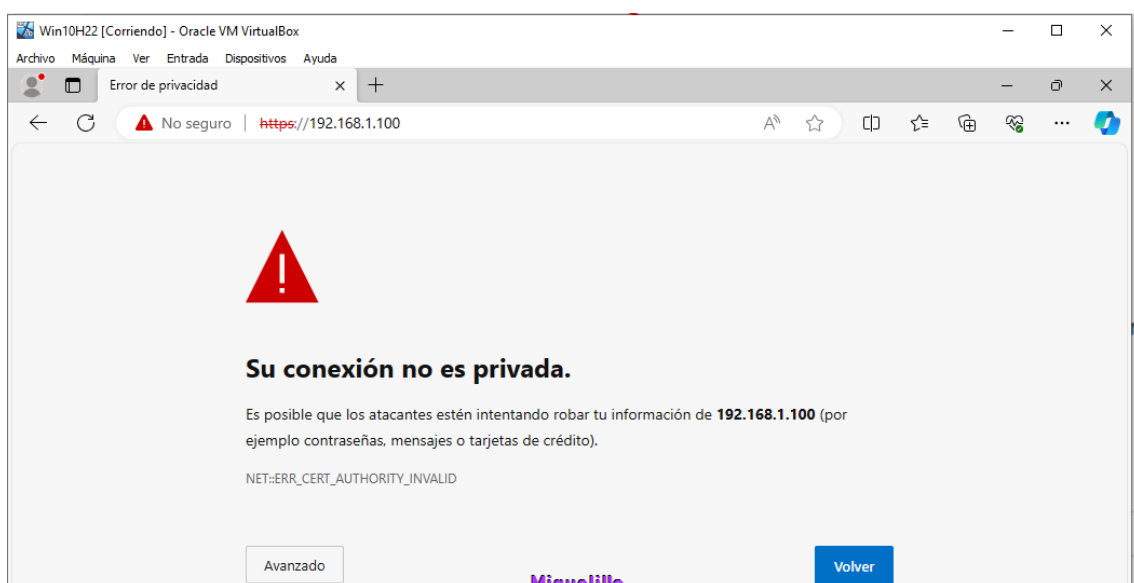
Activamos el sitio deshabilitamos el por defecto e introducimos al reinicial la contraseña de la llave del certificado del sitio



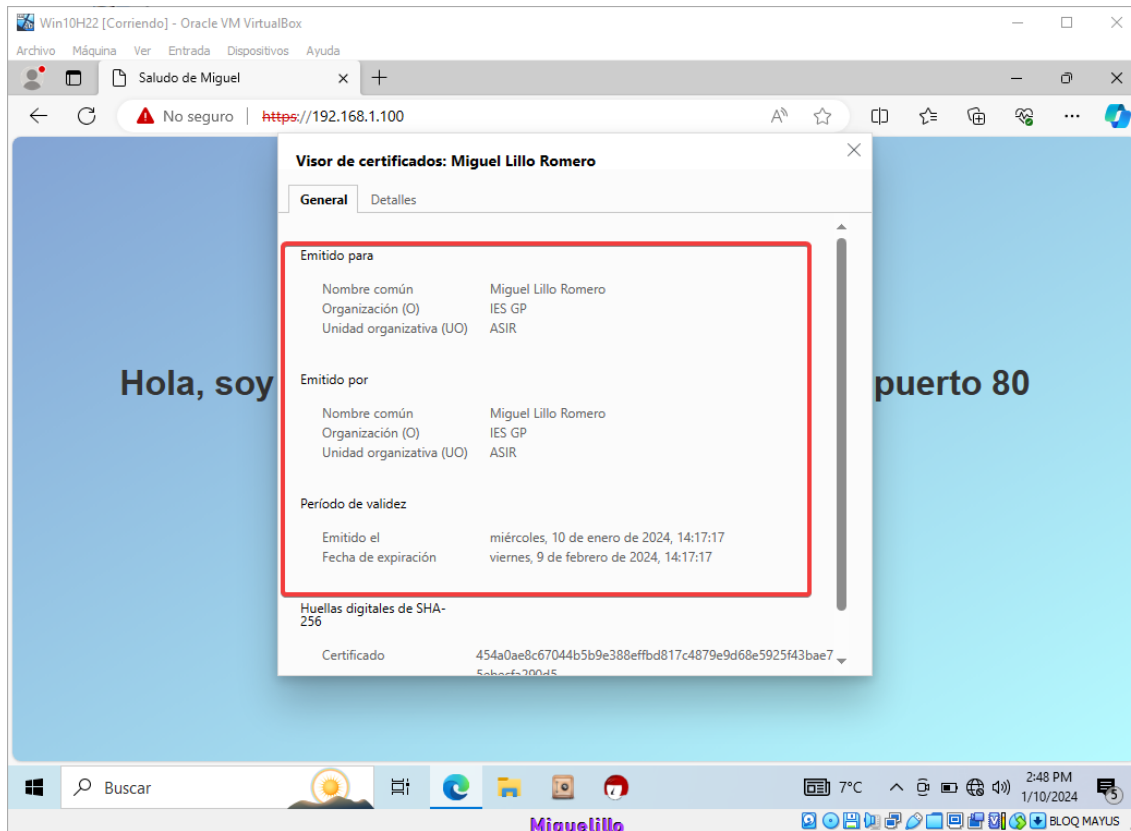
```
Debian12_2 (Autenticacion y otras cosas hats la 10) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal  10 de ene 14:20
miguel@debian-SRI: ~
miguel@debian-SRI:~$ sudo a2ensite miguel-ssl.conf
Enabling site miguel-ssl.
To activate the new configuration, you need to run:
    systemctl reload apache2
miguel@debian-SRI:~$ sudo a2dissite default-ssl.conf
Site default-ssl disabled.
To activate the new configuration, you need to run:
    systemctl reload apache2
miguel@debian-SRI:~$ sudo systemctl restart apache2
Enter passphrase for SSL/TLS keys for 127.0.1.1:443 (RSA) *****
miguel@debian-SRI:~$
```

Miguelillo

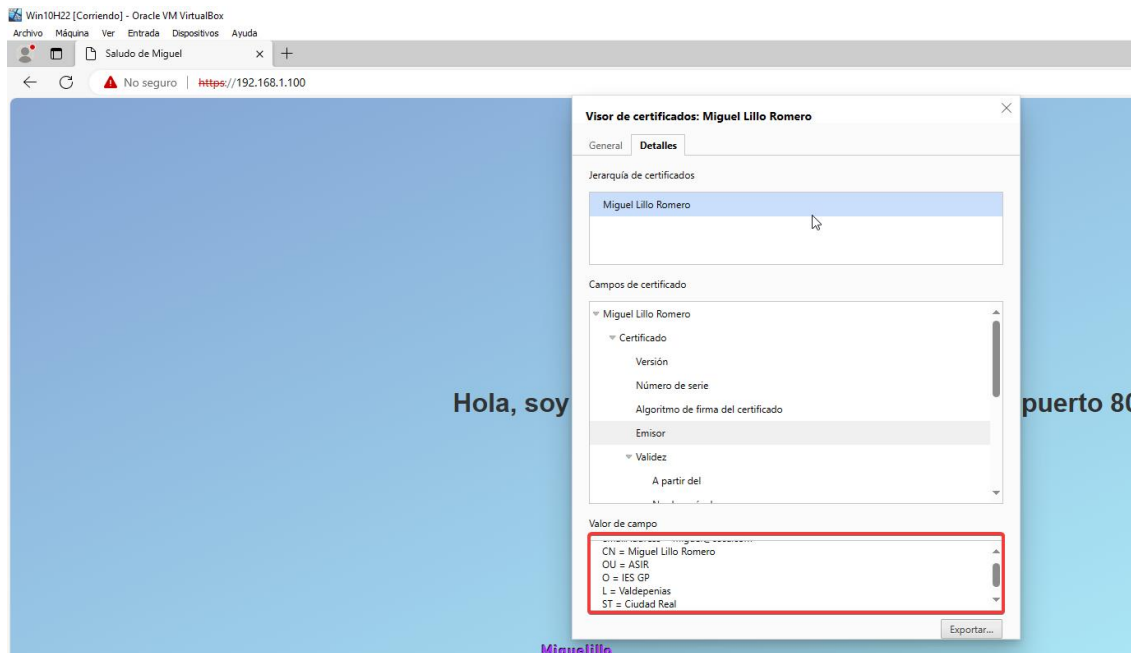
Probamos a acceder nos sigue saliendo que no es seguro



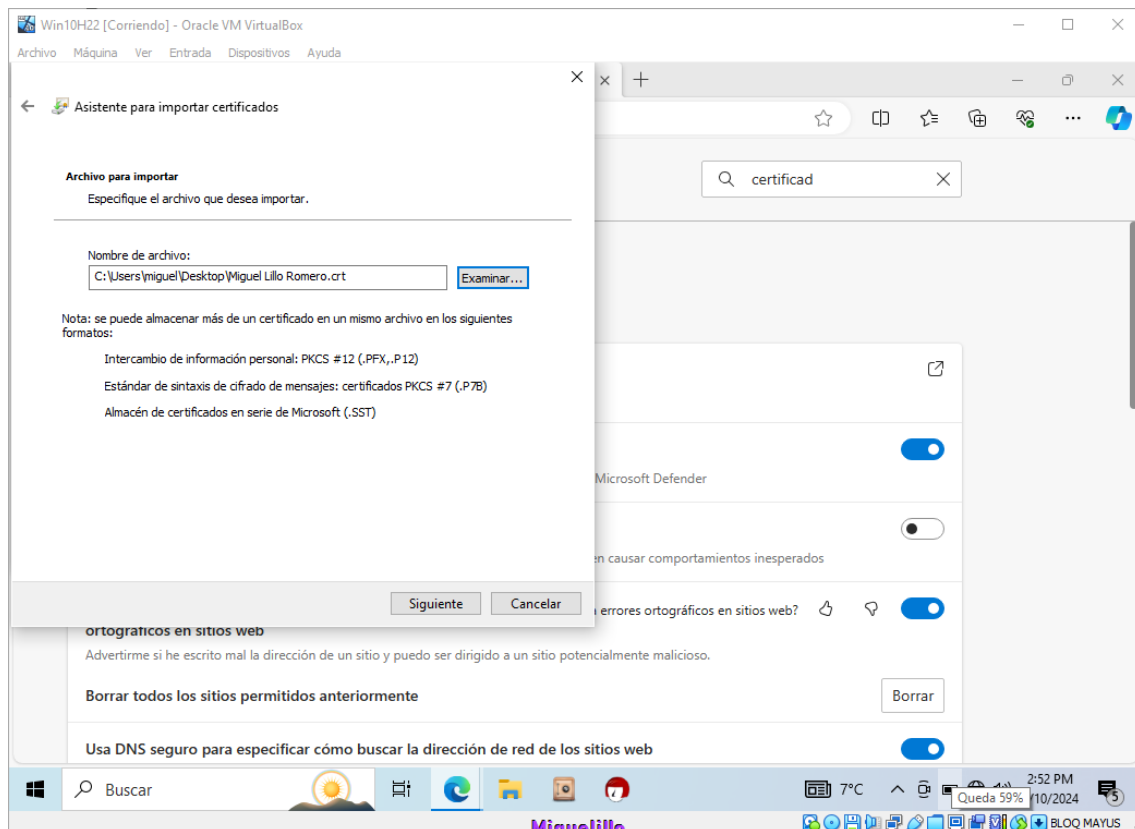
Podemos ver los datos del emisor del certificado, para quien ha sido emitido y la fecha de emisión y de expiración



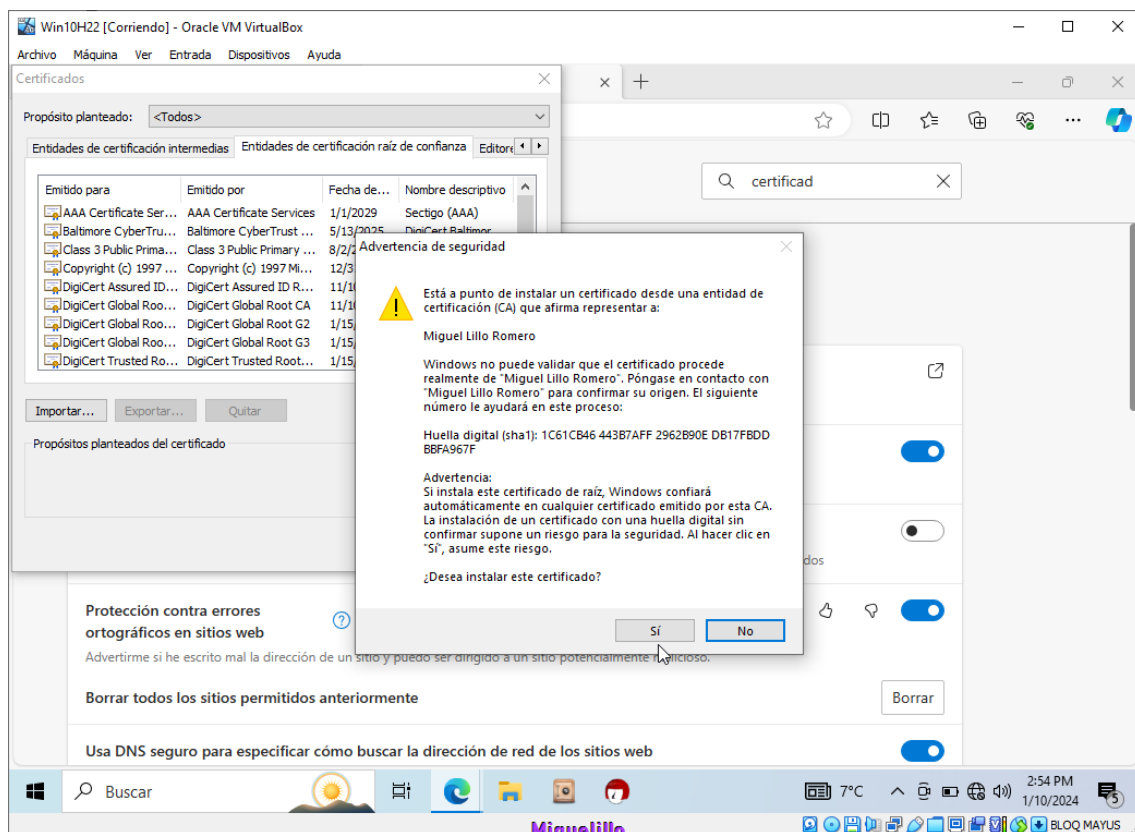
Podemos ver los datos introducidos anteriormente ey exportar el certificado para poder instalarlo



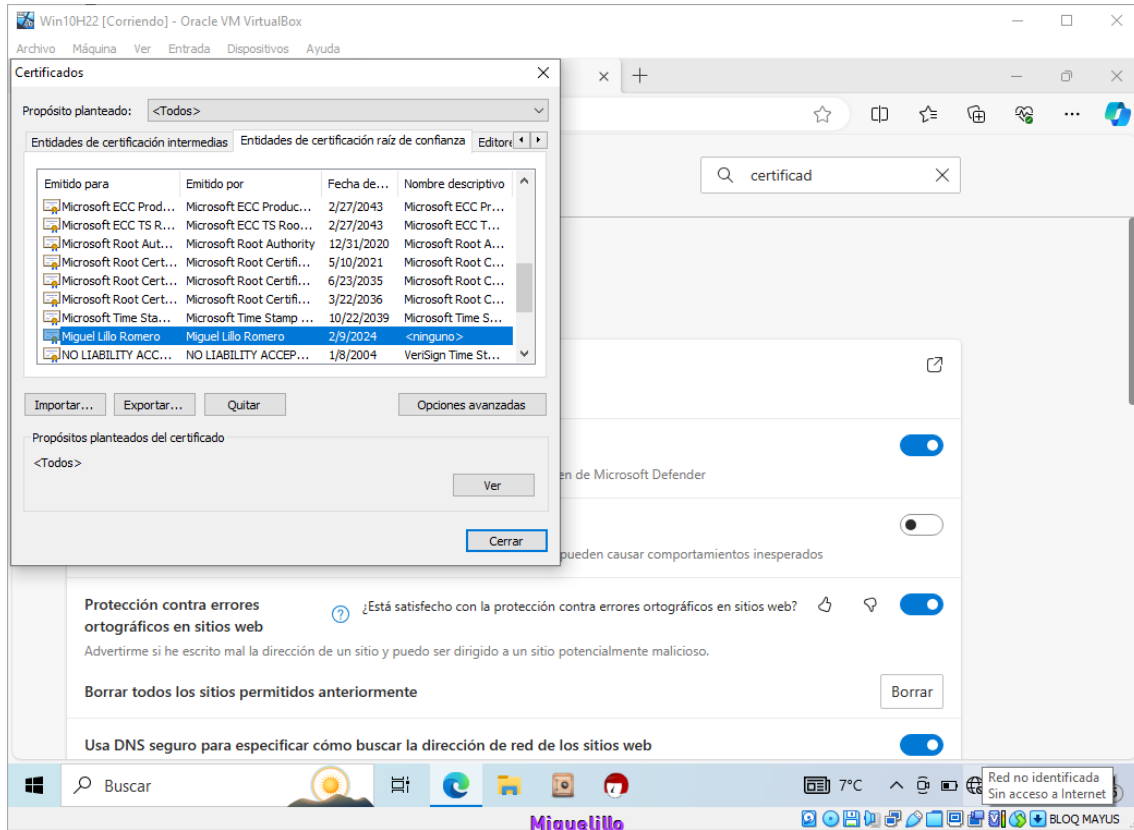
## Le instalamos el certificado para que no aparezca el mensaje del principio



## Lo instalamos



## Comprobamos que se ha instalado



## Aparece que es insegura pero no aparece el mensaje de principio

