|  |  |
| --- | --- |
| ***Despliegue de Aplicaciones Web***  **UD 02. Servidor Web** |  |
| **Practica 2.4: Seguridad Apache** |

Contenido

[Objetivos 1](#_Toc119255157)

[Información básica/Preparación 1](#_Toc119255158)

[Condiciones de entrega. 1](#_Toc119255159)

[Desarrollo 1](#_Toc119255160)

[Paso 1: Activar módulo SSL 1](#_Toc119255161)

[Paso 2: Puerto seguro 2](#_Toc119255162)

[Paso 3: Crear host virtual 2](#_Toc119255163)

[Paso 4: Instalar OpenSSL 4](#_Toc119255164)

[Paso 5: Generar el certificado autofirmado y su clave 4](#_Toc119255165)

[Paso 6: Modificar fichero de configuración de servidor seguro 7](#_Toc119255166)

[Paso 7: Aplicar cambios 8](#_Toc119255167)

[Paso 8: Comprobar funcionamiento 8](#_Toc119255168)

[Paso 9: Comprobar que el certificado es el correcto 9](#_Toc119255169)

# Objetivos

* Instalar servidor HTTPs
* Configurar servidor HTTPs

# Información básica/Preparación

Este laboratorio se llevará a cabo individualmente con la ayuda de uno de tus compañeros en las partes que se te indique.

Se necesitan los siguientes recursos:

* Una computadora con Linux Ubuntu
* Al menos una computadora con Windows

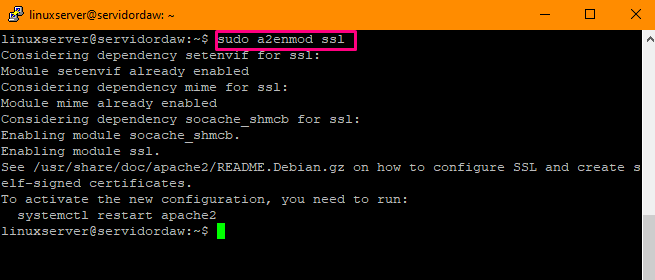
# Condiciones de entrega.

Debes entregar un documento dónde se indique los pasos dados para llevar a cabo la tarea expuesta.

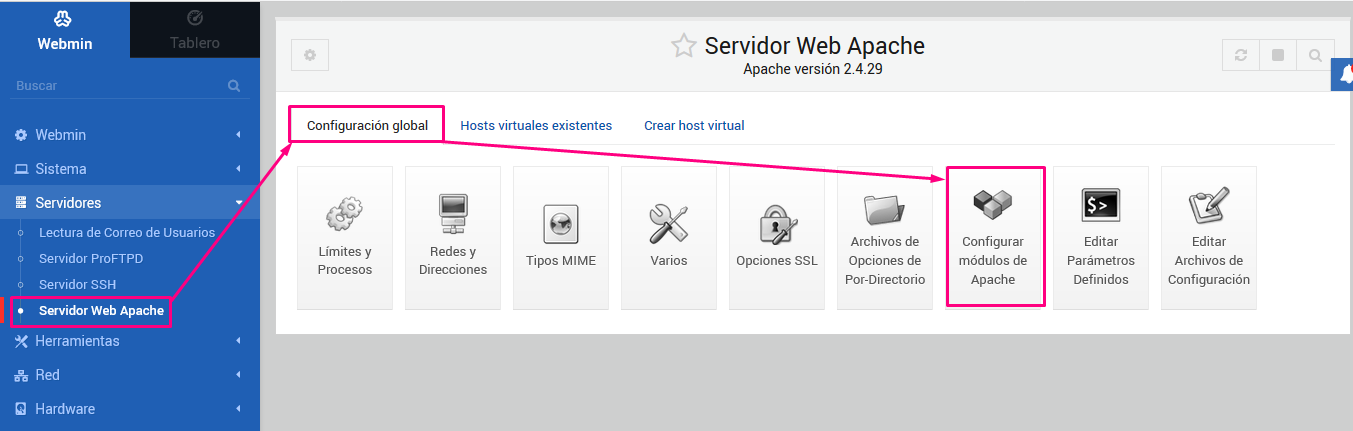
# Desarrollo

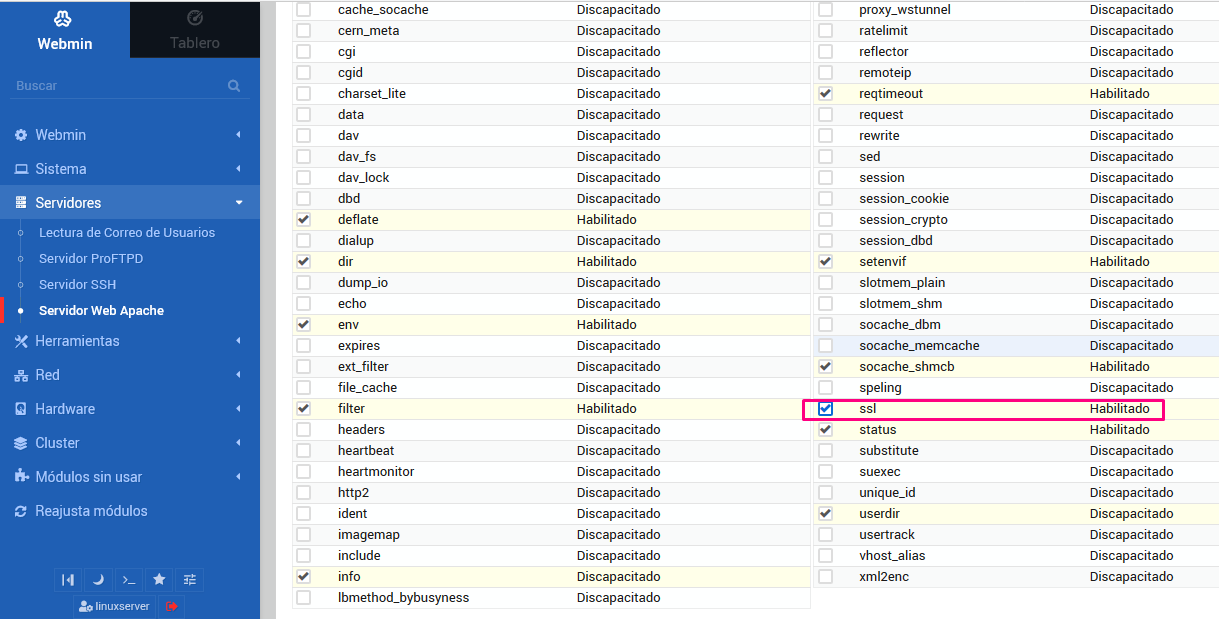
## Paso 1: Activar módulo SSL

Activa el módulo SSL de Apache.



Con Webmin, se podría activar el módulo en





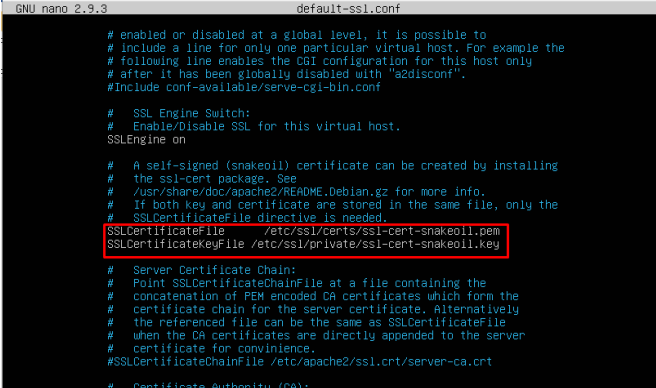
## Paso 2: Puerto seguro

Comprobar que el archivo /etc/apache/ports.conf, hay una directiva <IfModule> donde está incluida la escucha en el puerto 443, ya que el módulo SSL está activado.

## Paso 3: Crear host virtual

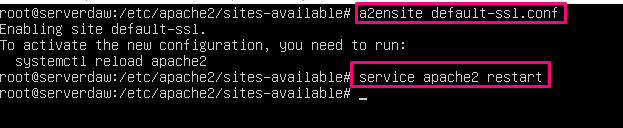
Crear un hosts virtual basado en el hosts virtual por defecto (default-ssl.conf) y con directorio de inicio para documentos /var/www/ssl/htdocs. Crear dicho directorio previamente como usuario root. Crea también un archivo index.html preparado para la prueba de conexión.

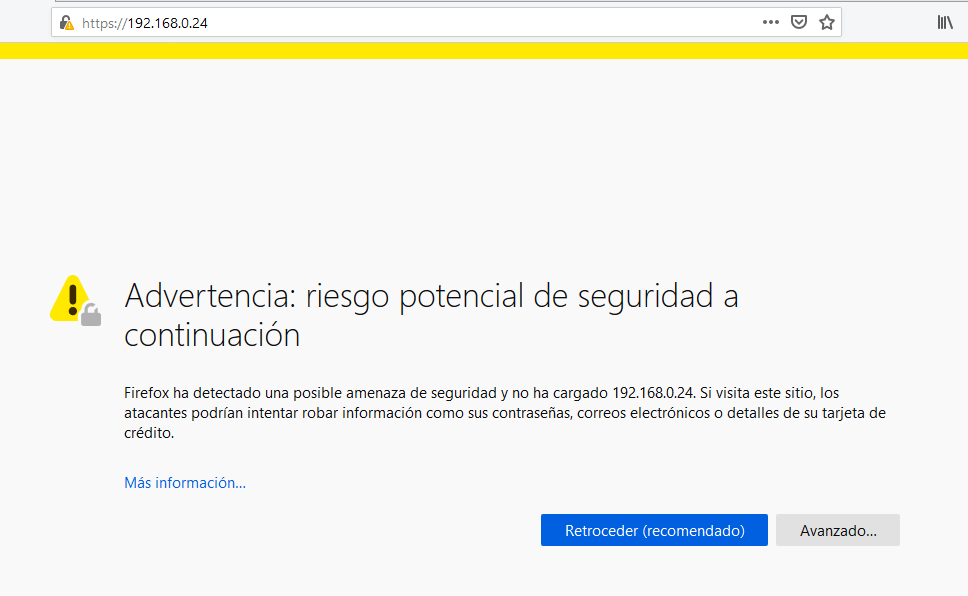
Observamos que es el archivo original, el que viene por defecto, e incluye las rutas para los certificados, siendo uno el certificado de seguridad y otro el archivo key para la clave privada.



En sí, el sistema te crea dos claves: una privada y otra pública y se necesitan ambos archivos para poder crear el servidor seguro.

Una vez activado el módulo y comprobado que los certificados por defecto se encuentran en su ubicación, comprobamos que el navegador detecta un certificado que no es de ninguna entidad certificadora y nos tiene que avisar de ello. Primero habilitamos el servidor seguro con a2ensite default-ssl.conf y reiniciamos el servicio con service apache2 restart.





## Paso 4: Instalar OpenSSL

Primero vamos a instalar openssl, escribimos:

sudo apt-get install openssl

Si vemos que ya está instalado, entonces lo ignoramos y seguimos.



## Paso 5: Generar el certificado autofirmado y su clave

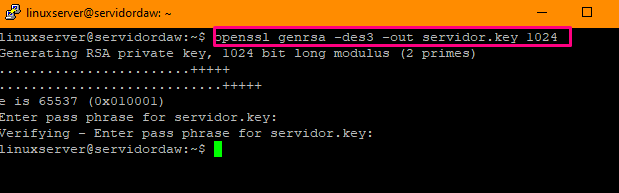
Una vez lo instalemos, debemos crear la clave privada de nuestro servidor que será de 1024 bit.

Sustituye servidor por: servidornombre. (Sustituye la palabra nombre por tu nombre de pila)

openssl genrsa -des3 -out servidor.key 1024

**Si no funcionara con la línea anterior, sustituirla por la siguiente:**

openssl genrsa -des3 -out servidor.key **2048**



**La frase que escribas recuérdala, te la pedirá en el proceso de configuración.**

Ya podemos crear los nuevos certificados. Rellenamos los datos y en Common Name ponemos la IP de nuestro servidor o el dominio.

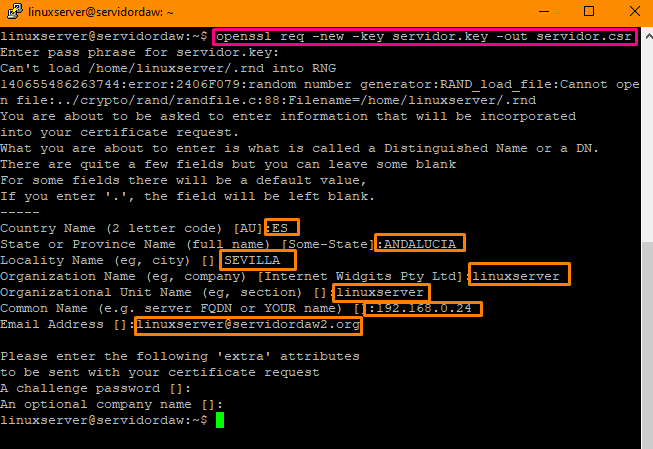
Sustituye servidor por: servidornombre. (Sustituye la palabra nombre por tu nombre de pila)

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

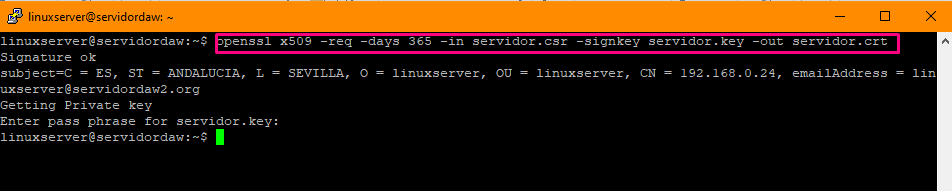
req: este modificador especifica usar la administración de la solicitud de firma de certificados (CSR) X.509, este es un estándar de claves públicas.

Nos aparecerá un asistente en la terminal que nos preguntará por diferentes datos que debemos rellenar:

* **Country Name:** corresponde a un código con las dos letras de nuestro país. Si vivimos en España, por ejemplo, escribimos ES.
* **State or Province Name:** escribimos el nombre de nuestra provincia o estado. Si eres español como yo, se refiere al nombre de tu comunidad autónoma. Por ejemplo, la mía es Andalucía. Por si acaso, para evitar problemas con las tildes y para aumentar la visibilidad, la escribimos en mayúsculas y sin tildes.
* **Locality Name:** escribimos el nombre de nuestra localidad en mayúsculas y sin tildes. SEVILLA
* **Organization Name:** se refiere al nombre de nuestra organización. nombreapellido1.
* **Organizational Unit Name:** se refiere al nombre del sector de nuestra organización. Poner **IESVELAZQUEZ**.
* **Common Name:** este campo es esencial, aquí debemos poner el nombre del dominio de la página web. En mi caso, aun no tenemos dominio así que la IP del servidor.
* **Email Address:** ponemos una dirección de correo personal, esto sirve por si nos tienen que enviar algún correo informativo o si necesitamos que nos contacten.



Le daremos una duración al certificado, en este caso 365 días.



Movemos los certificados a sus directorios correspondientes:

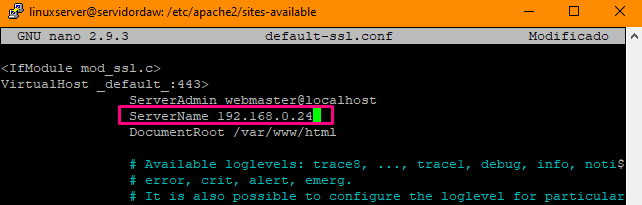




## Paso 6: Modificar fichero de configuración de servidor seguro

Ir al archivo del servidor virtual seguro, en el directorio /etc/apache2/sites-available, editar el archivo del servidor virtual seguro e incluir las directivas siguientes:

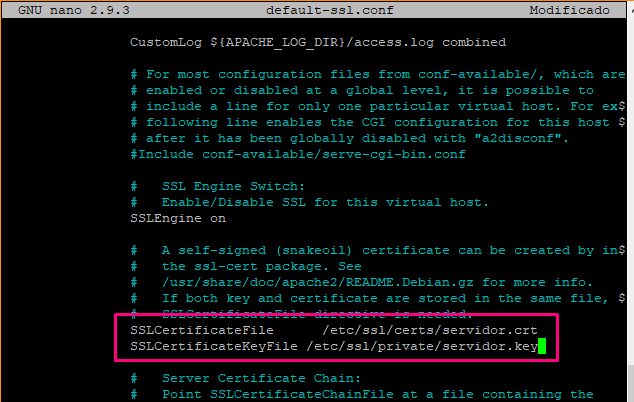
**Si no funcionara con al clave de 1024, quitar la línea de ServerName**



SSLEngine on

SSLCertificateFile /etc/ssl/certs/servidor.crt

SSLCertificateKeyFile /etc/ssl/private/servidor.key

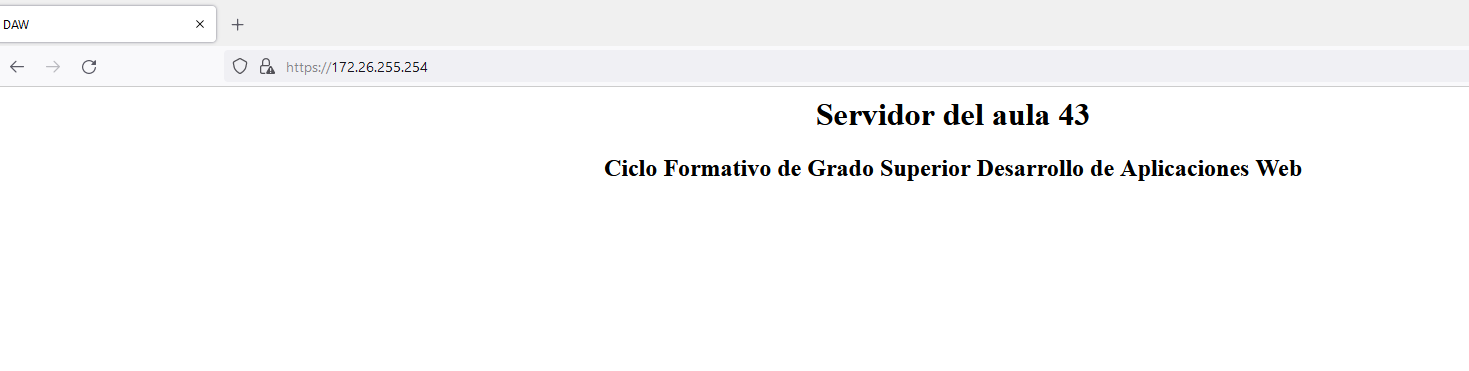


## Paso 7: Aplicar cambios

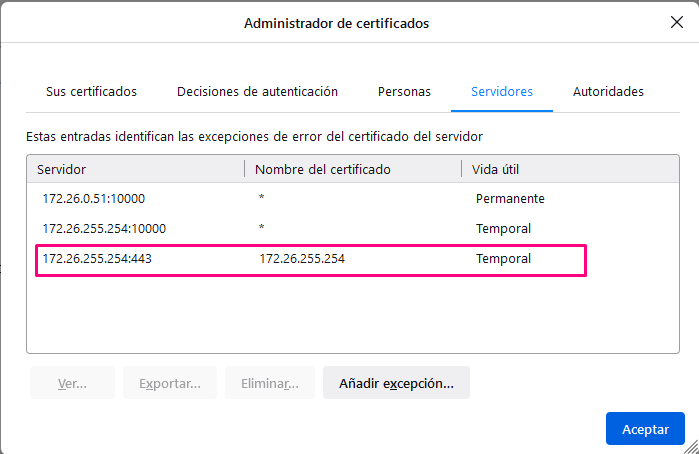


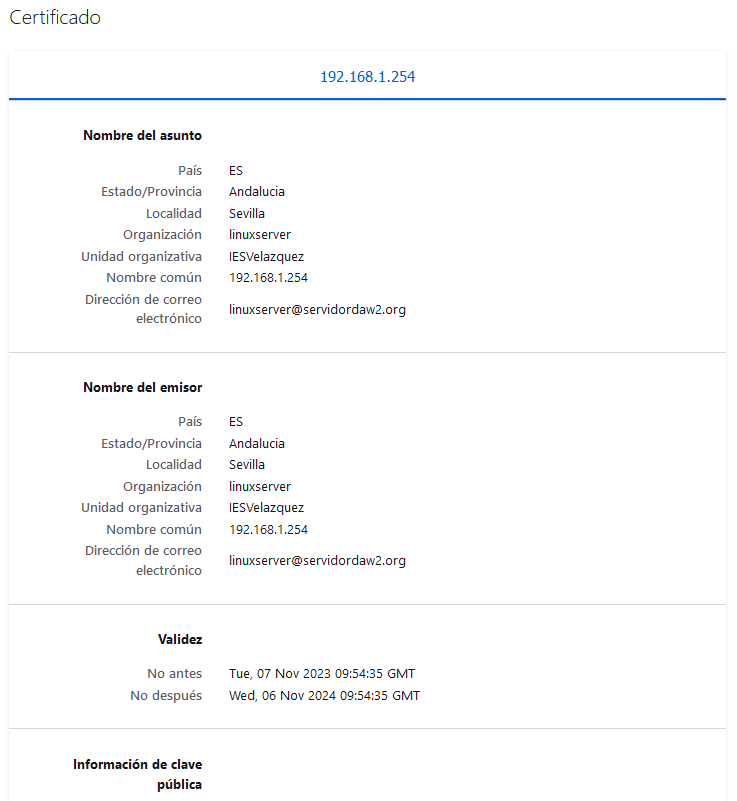
## Paso 8: Comprobar funcionamiento

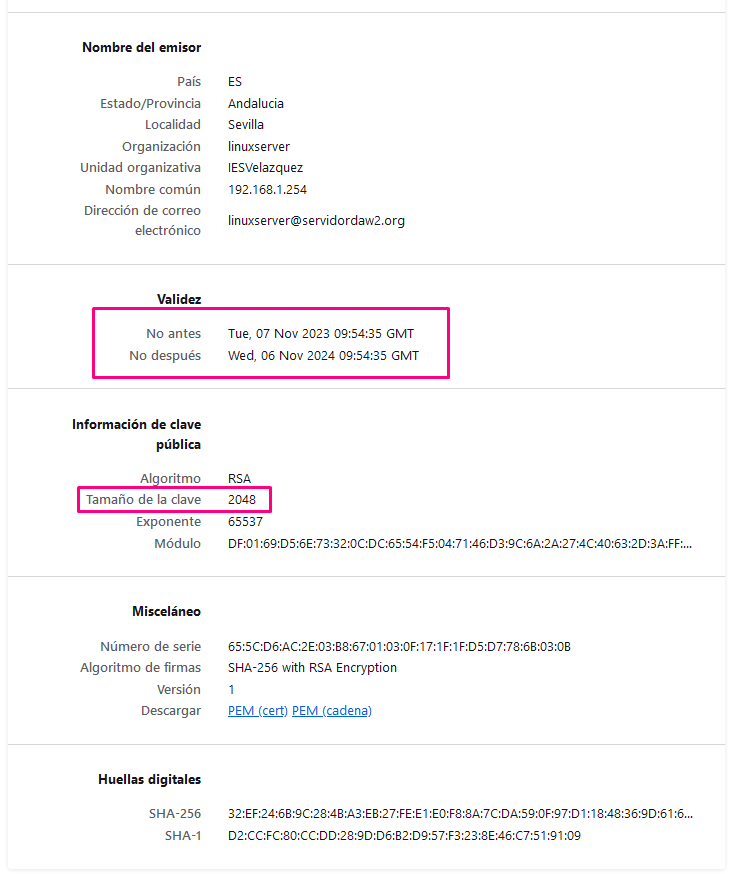
Abrir el navegador de la máquina anfitriona y escribir *https://IP* en la barra de direcciones:



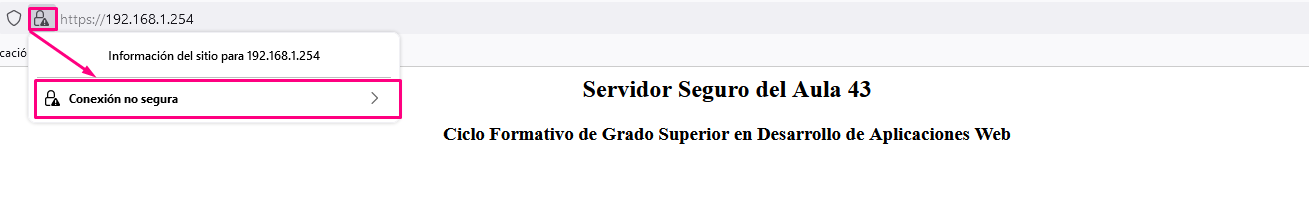
## Paso 9: Comprobar que el certificado es el correcto

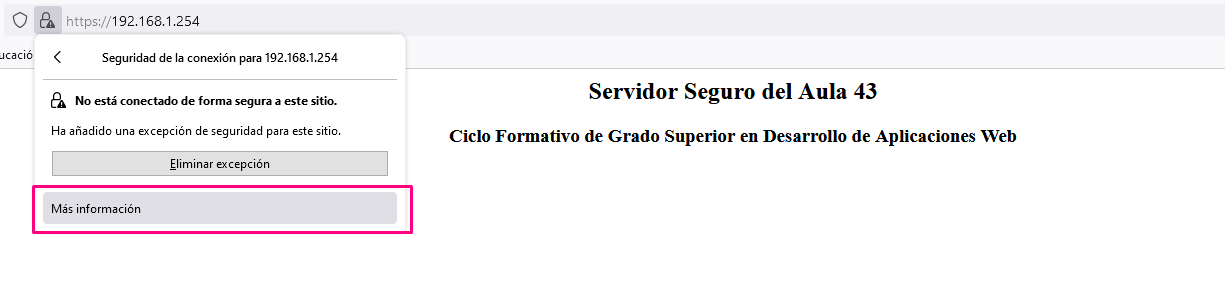


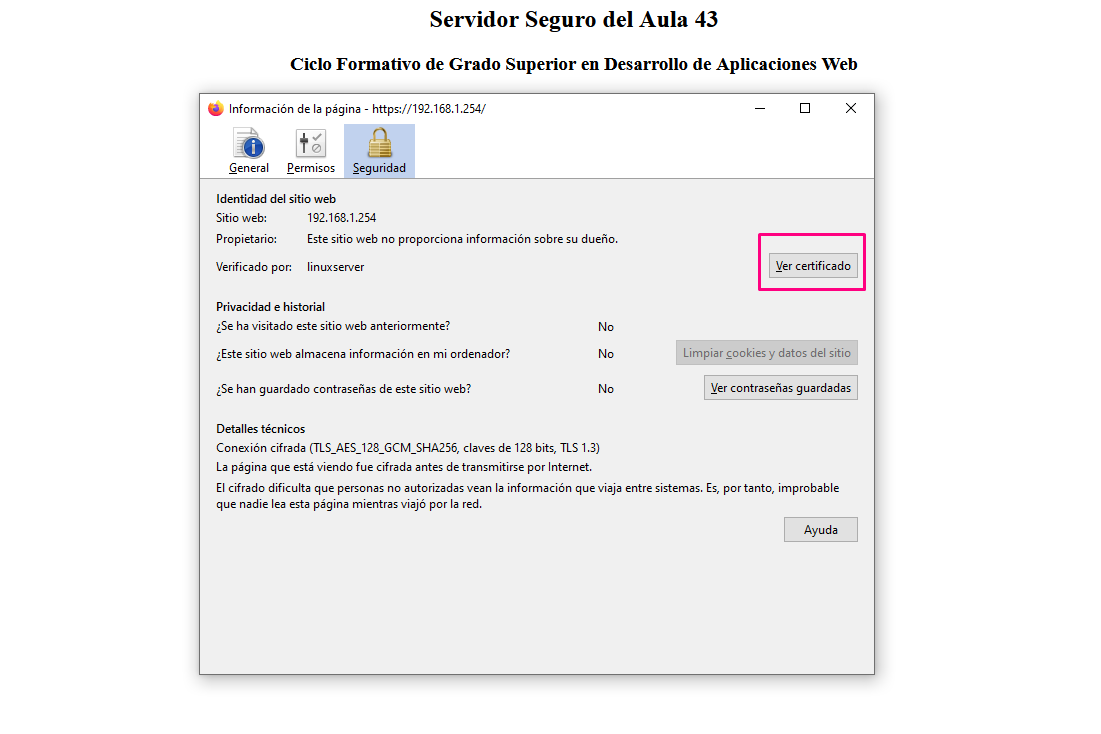




**También puedes conseguir la información del certificado en:**







**Toma capturas de los pasos 1, 2, 3 , 4 5, 6, 7, 8, 9**

|  |  |
| --- | --- |
| • | Crea un fichero que se llame Practica\_2.4\_ Apellido1Apellido2\_Nombre.pdf .    Inserta todas las capturas de pantallas por orden explicando cada una de ellas. |
| • | Una vez terminada la práctica, sube el archivo. |