



## **Práctica 3: Configuración segura de servidores**



# MEDAC

**Juan Esteban Fernández González**

# Índice

- 1.¿Qué es un certificado SSL?**
- 2.Crea un certificado un certificado SSL**
- 3.Instala un certificado SSL en tu servidor Apache o Nginx**
- 4.Explica que son los Virtual Host/Virtual Block con tus propias palabras, así como cualquier documento del servidor que tengas que modificar.**
- 5.Redirecciona todo el tráfico al protocolo HTTPS**
- 6. Muestra el acceso correcto por HTTPS por el navegador.**

- 1. ¿Qué es un certificado SSL?**

Es un archivo de datos que permite conexiones seguras y encriptadas entre un servidor web y un navegador protegiendo la información sensible entre los usuarios durante su transmisión a través de Internet.

- 2. Crea un certificado SSL (autofirmado o validado por una C.A.)**

- **sudo apt install openssl**

```
root@reo:/home/reo# apt install openssl
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
openssl ya está en su versión más reciente (3.0.13-0ubuntu3.4).
fijado openssl como instalado manualmente.
```

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

```
root@reo:/home/reo# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/selfsigned.key -out /etc/ssl/certs/selfsigned.crt
+++++
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]:Andalucía
Locality Name (eg, city) []:Granada
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Medac
Organizational Unit Name (eg, section) []:DNM
Common Name (e.g. server FQDN or YOUR name) []:Esteban
Email Address []:jfg0010@alu.medac.es
```

- 3. Instala un certificado SSL en tu servidor Apache o Nginx.**

- Abrimos el archivo de configuración de Nginx (el mío está en /etc/nginx/sites-available/default) y añadimos o ajustamos las siguientes líneas en el bloque server:

```
GNU nano 2.2 /etc/nginx/sites-available/default
# leave it as reference inside of sites-available where it will continue to be
# updated by the nginx packaging team.
#
# This file will automatically load configuration files provided by other
# applications, such as Drupal or Wordpress. These applications will be made
# available underneath a path with that package name, such as /drupal8.
#
# Please see /usr/share/doc/nginx-doc/examples/ for more detailed examples.
##

# Default server configuration
#
server {
    listen 443 ssl;
    server_name localhost;

    ssl_certificate /etc/ssl/certs/selfsigned.crt;
    ssl_certificate_key /etc/ssl/private/selfsigned.key;

    location / {
        # First attempt to serve request as file, then
        # as directory, then fall back to displaying a 404.
        try_files $uri $uri/ =404;
    }
}
```

#### 4. Explica que son los Virtual Host/Virtual Block con tus propias palabras, así como cualquier documento del servidor que tengas que modificar.

- Son una característica en servidores web, en mi caso Nginx, que permite que un solo servidor físico aloje varios sitios o aplicaciones cada uno con su propio hostname. Puede contener configuraciones como el nombre del servidor, la dirección IP, el puerto, las rutas a los certificados SSL, entre otros.
- Como usé Nginx modifiqué el archivo de configuración del sitio en `/etc/nginx/sites-available/default` para incluir bloques server (osea Virtual Hosts) que especifican cómo manejar el tráfico de las solicitudes HTTP y HTTPS, así como las rutas a los certificados SSL.

#### 5. Redirecciona todo el tráfico al protocolo HTTPS

- Añadimos un bloque de servidor para HTTP (puerto 80) en `/etc/nginx/sites-available/default`

```
server {
    listen 80;
    server_name localhost;

    return 301 https://$host$request_uri;
}
```

#### 6. Muestra el acceso correcto por HTTPS por el navegador.

- Como lo he hecho en Ubuntu Server voy a hacerlo por curl:

```
root@reo:/home/reo# curl -I https://Esteban
HTTPS/1.1 200 OK
Server: nginx/1.24.0 (Ubuntu)
Date: Mon, 28 Oct 2024 15:45:27 GMT
Content-Type: text/html
Content-Length: 615
Last-Modified: Tue, 11 Apr 2023 01:45:34 GMT
Connection: keep-alive
ETag: "6434bbbe-267"
Accept-Ranges: bytes
```

