Pràctica 3: Certificat SSL/TLS

Creación Certificado

Crearemos el certificado autofirmado.

```
iker@ikerserver:~$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -key
out /etc/ssl/private/nginx-selfsigned.key -out /etc/ssl/certs/nginx-selfsigned.c
rt
```

Luego nos dirá que pongamos unos datos.

```
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Valencia
Locality Name (eg, city) []:Gandia
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:Iker
Email Address []:iker@mail.com
```

Automatizar creación del certificado autofirmado

Automatizamos creando un script.

```
iker@ikerserver:~$ sudo cat autofirmado.sh
[sudo] password for iker:
#!/bin/bash
3 set -x
4
5 # Configuramos las variables con los datos que necesita el certificado
6 OPENSSL_COUNTRY="ES"
7 OPENSSL_PROVINCE="Valencia"
8 OPENSSL_LOCALITY="Tavernes de la Valldigna"
9 OPENSSL_ORGANIZATION="IES Jaume II el Just"
10 OPENSSL_ORGUNIT="Departamento de Informatica"
11 OPENSSL_COMMON_NAME="practica-https.local"
12 OPENSSL_EMAIL="emico@ieseljust.com"
13
14 # Creamos el certificado autofirmado
15
16 sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/
ssl/private/nginx-selfsigned.key -out /etc/ssl/certs/nginx-
selfsigned.crt -subj "/C=$OPENSSL_COUNTRY/ST=$OPENSSL_PROVINCE/L=
$OPENSSL_LOCALITY/O=$OPENSSL_ORGANIZATION/OU=$OPENSSL_ORGUNIT/CN=
$OPENSSL_COMMON_NAME/emailAddress=$OPENSSL_EMAIL"
```

Consultar certificado

Consultar información del sujeto del certificado.

```
iker@ikerserver:~$ openssl x509 -in /etc/ssl/certs/nginx-selfsigned.crt -noout -
subject
subject=C = ES, ST = Valencia, L = Gandia, O = Internet Widgits Pty Ltd, CN = Ik
er, emailAddress = iker@mail.com
```

Consultar la fecha de caducidad del certificado.

```
iker@ikerserver:~$ openssl x509 -in /etc/ssl/certs/nginx-selfsigned.crt -noout -
dates
notBefore=Oct 24 08:22:32 2025 GMT
notAfter=Oct 24 08:22:32 2026 GMT
```

Configurar un Block SSL/TSL en Nginx

Configurar el Bloc SSL

Configuramos el sitio seguro ssl.

```
 GNU nano 7.2            /etc/nginx/sites-available/segur
server {
        listen 443 ssl;
        server_name intranet.local;

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

        root /var/www/segur;
        index index.html;

        location / {
                try_files $uri $uri/ =404;
        }
}
```

Creamos el sitio seguro

Creamos el siguiente directorio.

```
iker@ikerserver:~$ sudo mkdir /var/www/segur
```

Creamos el documento de inicio.

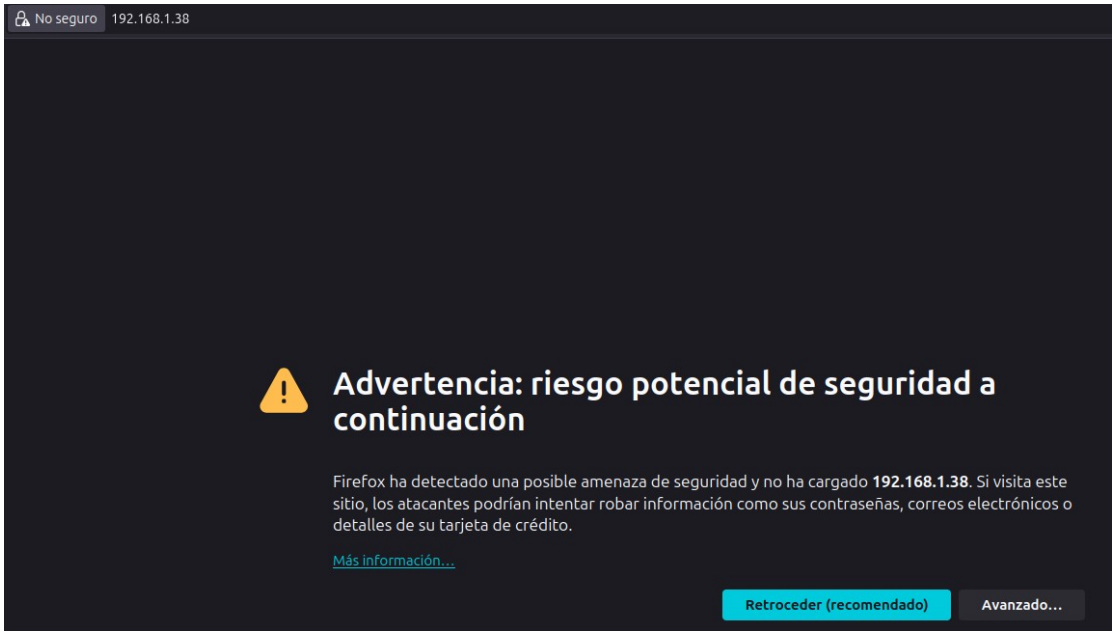
```
 GNU nano 7.2                /var/www/segur/index.html *
<!DOCTYPE html>
<html lang="ca">
<head>
        <meta charset="UTF-8">
        <meta name="viewport" content="width=device-width, initial-scale=1.0">
</head>
<body>
        <h1>PRÀCTICA WEB ESTÀTICA HTTPS</h1>
        <h2>Site Segur Local - intranet</h2>
        <h3>Servidor nginx</h3>
</body>
</html>
```

Aplicamos cambios y reiniciamos el servicio.

```
iker@ikerserver:~$ sudo nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
iker@ikerserver:~$ sudo systemctl reload nginx
```

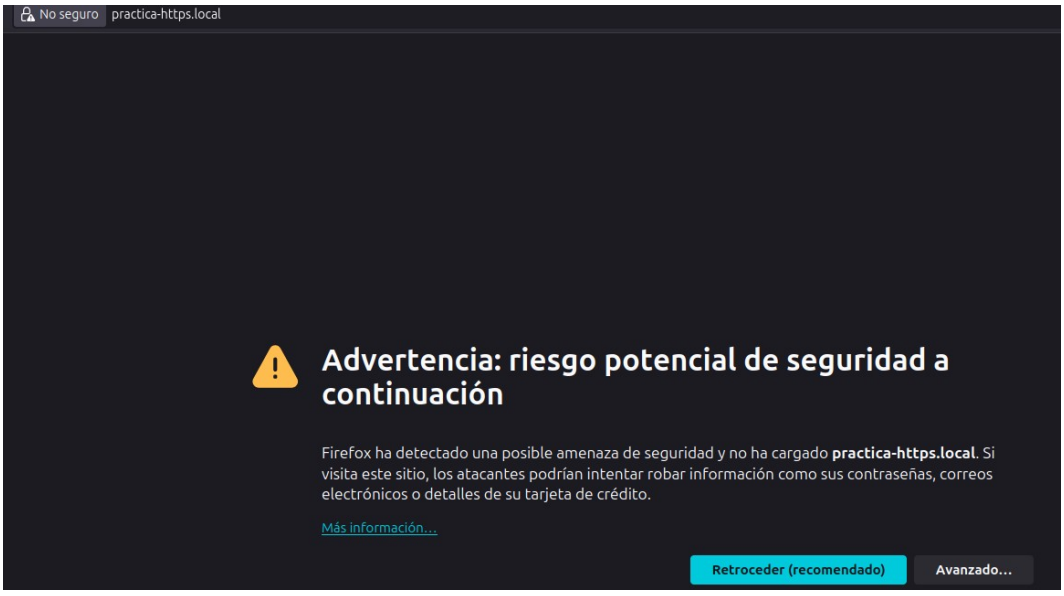
Verificamos el correcto funcionamiento

Desde un cliente accedemos por IP.



Vemos que nos salta una alerta de advertencia, en *Avanzado* aceptamos el riesgo.

Ahora volvemos a entrar con el nombre de la página.



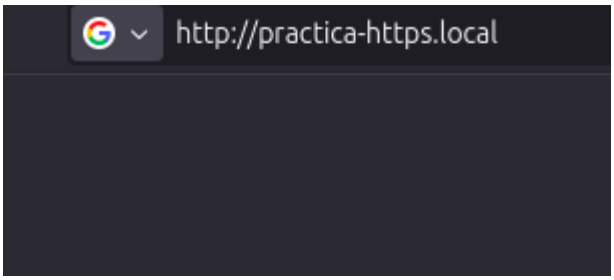
Volvemos a realizar el proceso para acceder.

Block de redirección de HTTP a HTTPS.

En el bloque de por defecto *default* y añadimos las siguientes líneas.

```
 GNU nano 7.2                 /etc/nginx/sites-available/default
server {
        listen 80 default_server;
        server_name practica-https:local;
        return 301 https://practica-https.local ;
        listen [::]:80 default_server;
```

Reiniciamos el servicio y entramos en el navegador pero con el enlace con http.



Y al buscar, vemos que nos redirigió a https.