Utiliza la práctica P.1. para securizar un sitio web:

1. Crea un certificado auto-firmado para: `misnoticias.com`.

// Antes de usar ssl tuve que descargar openssl desde su web oficial y añadir su directorio /bin a la variable de entorno PATH para poder ejecutar sus comandos en powershell. No he usado openssh porque es de esta manera como lo hice en casa.u

// Creamos la carpeta que vamos a usar para esta actividad dentro de misniticias.com

```
PS C:\Apache24\htdocs\misnoticias.com> mkdir miCA


    Directorio: C:\Apache24\htdocs\misnoticias.com


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        15/11/2024     13:58                miCA


PS C:\Apache24\htdocs\misnoticias.com> DIR


    Directorio: C:\Apache24\htdocs\misnoticias.com


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        15/11/2024     13:58                miCA
-a----        15/11/2024     12:34            251 index.html


PS C:\Apache24\htdocs\misnoticias.com> CD .\miCA\
PS C:\Apache24\htdocs\misnoticias.com\miCA>
```

// Generamos clave privada de CA

```
PS C:\Apache24\htdocs\misnoticias.com\miCA> openssl genrsa -out miCA.key 2048
PS C:\Apache24\htdocs\misnoticias.com\miCA> dir


    Directorio: C:\Apache24\htdocs\misnoticias.com\miCA


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        15/11/2024     14:05           1732 miCA.key
```

// Generamos el certificado autofirmado por el CA

```
PS C:\Apache24\htdocs\misnoticias.com\miCA> openssl req -x509 -new -nodes -key miCA.key -sha256 -days 365 -out miCA.pem
>>
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]:España
String too long, must be at most 2 bytes long
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:España
Locality Name (eg, city) []:Málaga
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IES Portada Alta
Organizational Unit Name (eg, section) []:Dpto. de Informática
Common Name (e.g. server FQDN or YOUR name) []:iesportada.org
Email Address []:cperazu.iesportada.org
PS C:\Apache24\htdocs\misnoticias.com\miCA>
```

// Generamos la clave privada del servidor

```
PS C:\Apache24\htdocs\misnoticias.com\miCA> openssl genrsa -out myserver.key 2048
PS C:\Apache24\htdocs\misnoticias.com\miCA> dir


    Directorio: C:\Apache24\htdocs\misnoticias.com\miCA


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        15/11/2024     14:05           1732 miCA.key
-a----        15/11/2024     14:06           1554 miCA.pem
-a----        15/11/2024     14:08           1732 myserver.key


PS C:\Apache24\htdocs\misnoticias.com\miCA>
```

// Solicitud de certificado del servidor

```
PS C:\Apache24\htdocs\misnoticias.com\miCA> openssl req -new -key myserver.key -out myserver.csr
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]:España
Locality Name (eg, city) []:Málaga
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IES Portada Alat
Organizational Unit Name (eg, section) []:Dep. de Informática
Common Name (e.g. server FQDN or YOUR name) []:iesportada.org
Email Address []:cperazu@iesportada.org

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234
An optional company name []:
PS C:\Apache24\htdocs\misnoticias.com\miCA> dir


    Directorio: C:\Apache24\htdocs\misnoticias.com\miCA


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        15/11/2024     14:05           1732 miCA.key
-a----        15/11/2024     14:06           1554 miCA.pem
-a----        15/11/2024     14:10           1146 myserver.csr
-a----        15/11/2024     14:08           1732 myserver.key


PS C:\Apache24\htdocs\misnoticias.com\miCA>
```

// Firma del certificado con la CA

```
PS C:\Apache24\htdocs\misnoticias.com\miCA> openssl x509 -req -in myserver.csr -CA miCA.pem -CAkey miCA.key -CAcreateserial -out myserver.crt -days 365 -sha256
Certificate request self-signature ok
subject=C=ES, ST=Espa┬ña, L=M┬álaga, O=IES Portada Alat, OU=Dep. de Inform┬ática, CN=iesportada.org, emailAddress=cperazu@iesportada.org
PS C:\Apache24\htdocs\misnoticias.com\miCA>
```

```
PS C:\Apache24\htdocs\misnoticias.com\miCA> dir


    Directorio: C:\Apache24\htdocs\misnoticias.com\miCA


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         15/11/2024     14:05           1732 miCA.key
-a----         15/11/2024     14:06           1554 miCA.pem
-a----         15/11/2024     14:11             42 miCA.srl
-a----         15/11/2024     14:11           1530 myserver.crt
-a----         15/11/2024     14:10           1146 myserver.csr
-a----         15/11/2024     14:08           1732 myserver.key


PS C:\Apache24\htdocs\misnoticias.com\miCA>
```

2. Configura Apache para utilizar el certificado y que se responda solo mediante https.

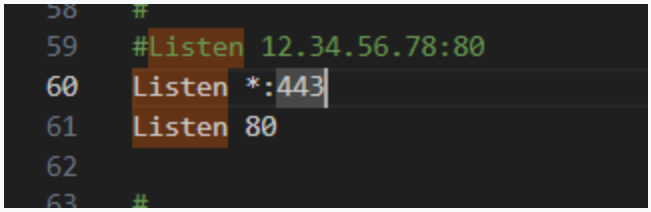
// Descomentamos esta linea para habilitar el https en httpd.conf

```
509   # Virtual hosts
510   Include conf/extra/httpd-vhosts.conf
511
512   # Local access to the Apache HTTP Server Manual
513   #Include conf/extra/httpd-manual.conf
```

// igual con esta:

```
176   #LoadModule speling_module modules/mod_speling.so
177   LoadModule ssl_module modules/mod_ssl.so
178   #LoadModule status_module modules/mod_status.so
179   #LoadModule substitute_module modules/mod_substitute.so
180   #LoadModule unique_id_module modules/mod_unique_id.so
```

// Añadimos la siguiente escucha de puerto



3. Investigación. Busca como se puede generar un certificado auto-firmado que sea válido para un dominio y para un alias de ese dominio. Explica como se haría y pon la ruta a la fuente que has utilizado.

Consideraciones

- Usa openssh, tal y como hemos visto en clase, para generar el certificado, especifica las propiedades como creas oportunas.
- Puedes hacer el ejercicio en Windows, Linux (WSL u otra distribución) o con Docker
- Recuerda que para probar que funciona tendrás que acceder a cada dominio por lo que modifica tu fichero hosts para redireccionar el nombre de dominio a localhost/127.0.0.1 (Si ya lo hiciste antes no tendrás que modificar nada más)

Entrega

- Un zip con la configuración y código generado.
- Un pdf con los pasos realizados con una pequeña descripción sobre los mismos.