ÍNDICE – U02 – A04

1.- Configuración del servidor para que se acceda a todos los sitios con HTTP y HTTPS.

- En el /home del usuario vamos a crear la claves privadas.

```
miadmin@igcdaw:~$ cd /home/miadmin/
miadmin@igcdaw:~$ openssl genrsa 2048 > fichero1.key
Generating RSA private key, 2048 bit long modulus
.........................................+++
........+++
e is 65537 (0x010001)
miadmin@igcdaw:~$ openssl genrsa 2048 > fichero2.key
Generating RSA private key, 2048 bit long modulus
.................................+++
.................................+++
e is 65537 (0x010001)
miadmin@igcdaw:~$ openssl genrsa 2048 > ficherolocal.key
Generating RSA private key, 2048 bit long modulus
.................................+++
.....................+++
e is 65537 (0x010001)
```

- Ahora generamos la solicitud de certificado, haciendo lo mismo para fichero1 y fichero2.

```
miadmin@igcdaw:~$ openssl req -new -key ficherolocal.key  -out ficherolocal.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]:SP
State or Province Name (full name) [Some-State]:Zamora
Locality Name (eg, city) []:Benavente
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:israel.local
Email Address []:israel.garcab@educa.jcyl.es

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:paso
An optional company name []:
```

```
miadmin@igcdaw:~$ openssl req -new -key fichero1.key  -out fichero1.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]:SP
State or Province Name (full name) [Some-State]:Zamora
Locality Name (eg, city) []:Benavente
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:empresa1.com
Email Address []:israel.garcab@educa.jcyl.es

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:paso
An optional company name []:
```

```
miadmin@igcdaw:~$ openssl req -new -key fichero2.key  -out fichero2.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]:SP
State or Province Name (full name) [Some-State]:Zamora
Locality Name (eg, city) []:Benavente
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:empresa2.com
Email Address []:israel.garcab@educa.jcyl.es

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:paso
An optional company name []:
```

- Autofirmaremos los certificados.

```
miadmin@igcdaw:~$ openssl x509 -req -days 365 -in ficherolocal.csr -signkey ficherolocal.key > fiche
rolocal.crt
Signature ok
subject=C = SP, ST = Zamora, L = Benavente, O = Internet Widgits Pty Ltd, CN = israel.local, emailAd
dress = israel.garcab@educa.jcyl.es
Getting Private key
```

```
miadmin@igcdaw:~$ openssl x509 -req -days 365 -in fichero1.csr -signkey fichero1.key > fichero1.crt
Signature ok
subject=C = SP, ST = Zamora, L = Benavente, O = Internet Widgits Pty Ltd, CN = empresa1.com, emailAd
dress = israel.garcab@educa.jcyl.es
Getting Private key
```

```
miadmin@igcdaw:~$ openssl x509 -req -days 365 -in fichero2.csr -signkey fichero2.key > fichero2.crt
Signature ok
subject=C = SP, ST = Zamora, L = Benavente, O = Internet Widgits Pty Ltd, CN = empresa2.com, emailAd
dress = israel.garcab@educa.jcyl.es
Getting Private key
```

- Movemos las claves privadas y los certificados a las carpetas private y certs respectivamente.

```
miadmin@igcdaw:~$ ls
doc           fichero1.csr  fichero2.crt  fichero2.key      ficherolocal.csr  fp
fichero1.crt  fichero1.key  fichero2.csr  ficherolocal.crt  ficherolocal.key
miadmin@igcdaw:~$ pwd
/home/miadmin
miadmin@igcdaw:~$ mv /home/miadmin/ficherolocal.key /etc/ssl/private/
mv: cannot stat '/etc/ssl/private/ficherolocal.key': Permission denied
miadmin@igcdaw:~$ sudo mv /home/miadmin/ficherolocal.key /etc/ssl/private/
[sudo] password for miadmin:
miadmin@igcdaw:~$ sudo mv /home/miadmin/fichero1.key /etc/ssl/private/
miadmin@igcdaw:~$ sudo mv /home/miadmin/fichero2.key /etc/ssl/private/
miadmin@igcdaw:~$ sudo mv /home/miadmin/ficherolocal.crt /etc/ssl/certs/
miadmin@igcdaw:~$ sudo mv /home/miadmin/fichero1.crt /etc/ssl/certs/
miadmin@igcdaw:~$ sudo mv /home/miadmin/fichero2.crt /etc/ssl/certs/
miadmin@igcdaw:~$ ls
doc  fichero1.csr  fichero2.csr  ficherolocal.csr  fp
```

- Vamos a esas carpetas y cambiamos el propietario y los permisos de las claves privadas y los certificados.

```
root@igcdaw:/etc/ssl/private# chown -R root:ssl-cert ficherolocal.key
root@igcdaw:/etc/ssl/private# chown -R root:ssl-cert fichero1.key
root@igcdaw:/etc/ssl/private# chown -R root:ssl-cert fichero2.key
root@igcdaw:/etc/ssl/private# chown -R 640 ficherolocal.key
root@igcdaw:/etc/ssl/private# chown -R 640 fichero1.key
root@igcdaw:/etc/ssl/private# chown -R 640 fichero2.key
root@igcdaw:/etc/ssl/private# cd ../certs/
root@igcdaw:/etc/ssl/certs# chown -R root:root ficherolocal.crt
root@igcdaw:/etc/ssl/certs# chown -R root:root fichero1.crt
root@igcdaw:/etc/ssl/certs# chown -R root:root fichero2.crt
```

- Activaremos el módulo SSL desde la carpeta /etc/apache/mods-available y reiniciamos el servicio.

```
miadmin@igcdaw:/etc/apache2/mods-available$ sudo a2enmod ssl
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-signed certifica
tes.
To activate the new configuration, you need to run:
  systemctl restart apache2
miadmin@igcdaw:/etc/apache2/mods-available$ systemctl restart apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to restart 'apache2.service'.
Authenticating as: miadmin
Password:
==== AUTHENTICATION COMPLETE ===
```

- Vamos a /etc/apache2/sites-available y copiamos el archivo default-ssl.conf en la misma carpeta cambiándolo de nombre.

```
miadmin@igcdaw:/etc/apache2/sites-available$ sudo cp default-ssl.conf israel-ssl.conf
```

- Editamos el nuevo archivo de la siguiente forma.

```
 GNU nano 2.9.3                                israel-ssl.conf

<IfModule mod_ssl.c>
        <VirtualHost *:443>
                ServerName israel.local
                ServerAlias israel.local
                ServerAdmin webmaster@localhost
                DocumentRoot /var/www/israel.local/public_html
                ErrorLog ${APACHE_LOG_DIR}/error.log
                CustomLog ${APACHE_LOG_DIR}/access.log combined
                SSLEngine on
                SSLCertificateFile      /etc/ssl/certs/ficherolocal.crt
                SSLCertificateKeyFile /etc/ssl/private/ficherolocal.key
                <FilesMatch "\.(cgi|shtml|phtml|php)$">
                                SSLOptions +StdEnvVars
                </FilesMatch>
                <Directory /usr/lib/cgi-bin>
                                SSLOptions +StdEnvVars
                </Directory>
        </VirtualHost>
</IfModule>
```

- Copiamos el fichero del sitio renombrándolo para los otros dos sitios.

```
miadmin@igcdaw:/etc/apache2/sites-available$ sudo cp israel-ssl.conf empresa1-ssl.conf
```

```
miadmin@igcdaw:/etc/apache2/sites-available$ sudo cp empresa1-ssl.conf empresa2-ssl.conf
```

- Los editamos de la siguiente forma.

```
 GNU nano 2.9.3                                empresa1-ssl.conf

<IfModule mod_ssl.c>
        <VirtualHost *:443>
                ServerName empresa1.com
                ServerAlias www.empresa1.com
                ServerAdmin webmaster@localhost
                DocumentRoot /var/www/empresa1.com/public_html
                ErrorLog ${APACHE_LOG_DIR}/error.log
                CustomLog ${APACHE_LOG_DIR}/access.log combined
                SSLEngine on
                SSLCertificateFile      /etc/ssl/certs/fichero1.crt
                SSLCertificateKeyFile /etc/ssl/private/fichero1.key
                <FilesMatch "\.(cgi|shtml|phtml|php)$">
                                SSLOptions +StdEnvVars
                </FilesMatch>
                <Directory /usr/lib/cgi-bin>
                                SSLOptions +StdEnvVars
                </Directory>
        </VirtualHost>
</IfModule>
```

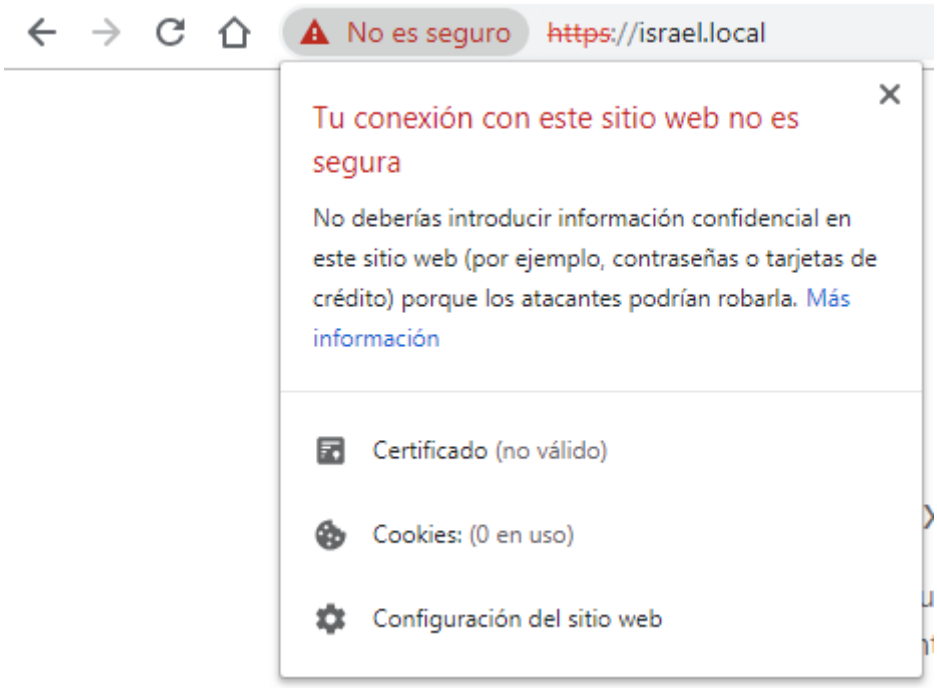
```
 GNU nano 2.9.3                                  empresa2-ssl.conf

<IfModule mod_ssl.c>
        <VirtualHost *:443>
                ServerName empresa2.com
                ServerAlias www.empresa2.com
                ServerAdmin webmaster@localhost
                DocumentRoot /var/www/empresa2.com/public_html
                ErrorLog ${APACHE_LOG_DIR}/error.log
                CustomLog ${APACHE_LOG_DIR}/access.log combined
                SSLEngine on
                SSLCertificateFile      /etc/ssl/certs/fichero2.crt
                SSLCertificateKeyFile /etc/ssl/private/fichero2.key
                <FilesMatch "\.(cgi|shtml|phtml|php)$">
                                SSLOptions +StdEnvVars
                </FilesMatch>
                <Directory /usr/lib/cgi-bin>
                                SSLOptions +StdEnvVars
                </Directory>
        </VirtualHost>
</IfModule>
```

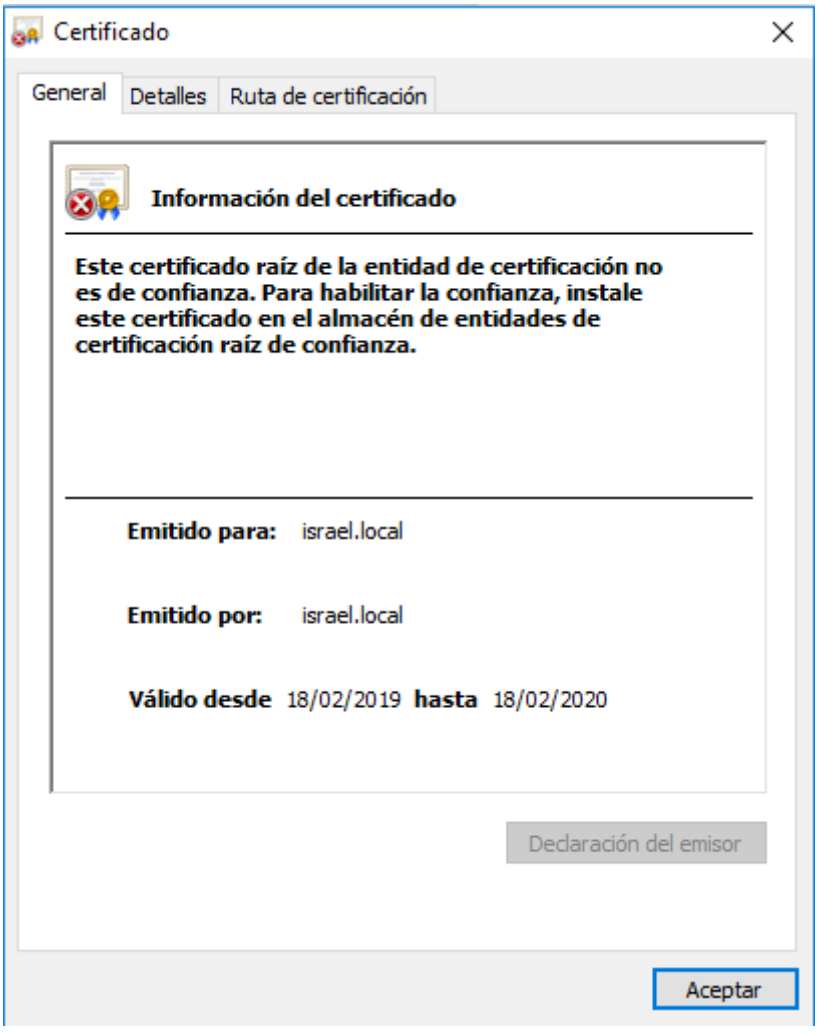
- Checkeamos el fichero, activamos el sitio y reiniciamos el servicio.

```
miadmin@igcdaw:/etc/apache2/sites-available$ sudo a2ensite israel-ssl.conf
Enabling site israel-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
miadmin@igcdaw:/etc/apache2/sites-available$ systemctl reload apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to reload 'apache2.service'.
Authenticating as: miadmin
Password:
==== AUTHENTICATION COMPLETE ===
```

```
miadmin@igcdaw:/etc/apache2/sites-available$ sudo a2ensite empresa1-ssl.conf
Enabling site empresa1-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
miadmin@igcdaw:/etc/apache2/sites-available$ systemctl reload apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to reload 'apache2.service'.
Authenticating as: miadmin
Password:
==== AUTHENTICATION COMPLETE ===
```

- Desde el navegador accedemos a los sitios con https y accederá de forma segura.






No es seguro
https://empresa1.com