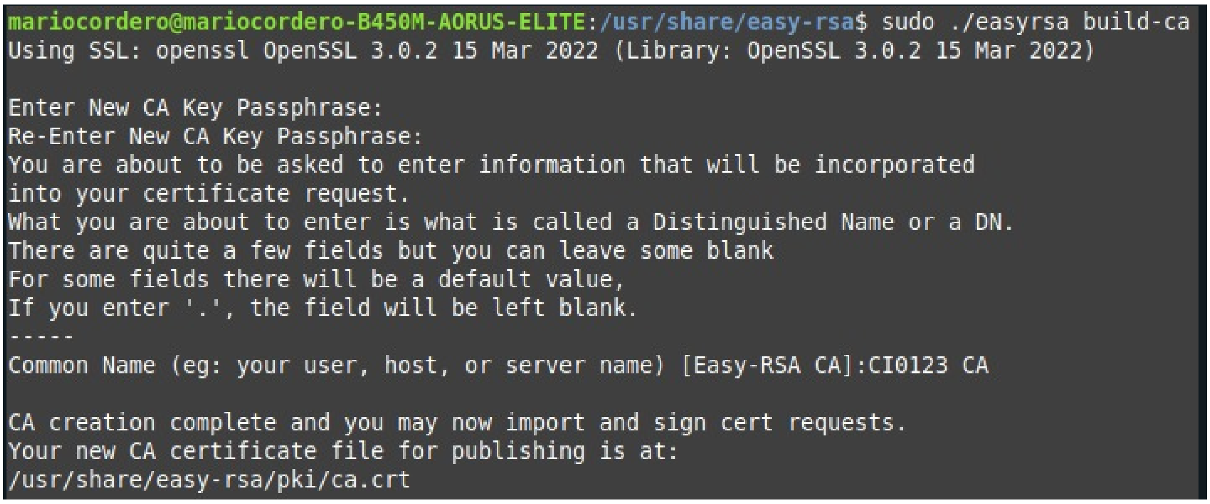
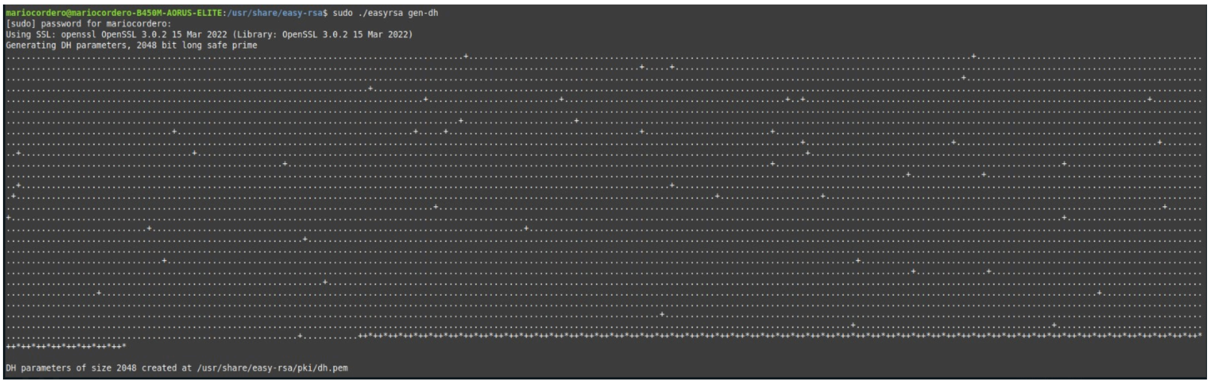
```
mariocordero@mariocordero-B450M-AORUS-ELITE:~/Desktop/PI-Redes$ sudo apt install easy-rsa
[sudo] password for mariocordero:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libccid opensc opensc-pkcs11 pcscd
The following NEW packages will be installed:
  easy-rsa libccid opensc opensc-pkcs11 pcscd
0 upgraded, 5 newly installed, 0 to remove and 250 not upgraded.
Need to get 1 464 kB of archives.
After this operation, 4 960 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu jammy/universe amd64 libccid amd64 1.5.0-2 [83,1 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 pcscd amd64 1.9.5-3ubuntu1 [58,1 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy/universe amd64 opensc-pkcs11 amd64 0.22.0-1ubuntu2 [933 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy/universe amd64 opensc amd64 0.22.0-1ubuntu2 [346 kB]
Get:5 http://archive.ubuntu.com/ubuntu jammy/universe amd64 easy-rsa all 3.0.8-1ubuntu1 [44,1 kB]
Fetched 1 464 kB in 1s (1 129 kB/s)
Selecting previously unselected package libccid.
(Reading database ... 635189 files and directories currently installed.)
Preparing to unpack .../libccid_1.5.0-2_amd64.deb ...
Unpacking libccid (1.5.0-2) ...
Selecting previously unselected package pcscd.
Preparing to unpack .../pcscd_1.9.5-3ubuntu1_amd64.deb ...
Unpacking pcscd (1.9.5-3ubuntu1) ...
Selecting previously unselected package opensc-pkcs11:amd64.
Preparing to unpack .../opensc-pkcs11_0.22.0-1ubuntu2_amd64.deb ...
Unpacking opensc-pkcs11:amd64 (0.22.0-1ubuntu2) ...
Selecting previously unselected package opensc.
Preparing to unpack .../opensc_0.22.0-1ubuntu2_amd64.deb ...
Unpacking opensc (0.22.0-1ubuntu2) ...
Selecting previously unselected package easy-rsa.
Preparing to unpack .../easy-rsa_3.0.8-1ubuntu1_all.deb ...
Unpacking easy-rsa (3.0.8-1ubuntu1) ...
Setting up libccid (1.5.0-2) ...
Setting up pcscd (1.9.5-3ubuntu1) ...
Created symlink /etc/systemd/system/sockets.target.wants/pcscd.socket → /lib/systemd/system/pcscd.socket.
pcscd.service is a disabled or a static unit, not starting it.
Setting up opensc-pkcs11:amd64 (0.22.0-1ubuntu2) ...
Setting up easy-rsa (3.0.8-1ubuntu1) ...
Setting up opensc (0.22.0-1ubuntu2) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for mailcap (3.70+nmu1ubuntu1) ...
Processing triggers for desktop-file-utils (0.26+mint3+victoria) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu3) ...
Processing triggers for libc-bin (2.35-0ubuntu3.7) ...
```

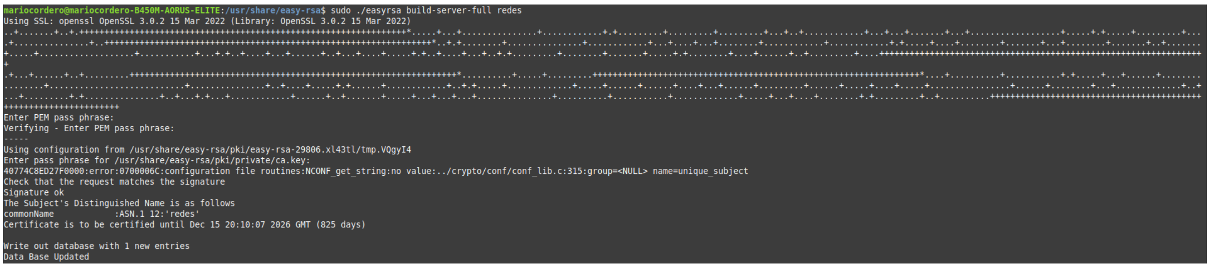
```
mariocordero@mariocordero-B450M-AORUS-ELITE:/usr/share/easy-rsa$ sudo ./easyrsa

Easy-RSA 3 usage and overview

USAGE: easyrsa [options] COMMAND [command-options]

A list of commands is shown below. To get detailed usage and help for a
command, run:
  ./easyrsa help COMMAND

For a listing of options that can be supplied before the command, use:
  ./easyrsa help options

Here is the list of commands available with a short syntax reminder. Use the
'help' command above to get full usage details.

  init-pki
  build-ca [ cmd-opts ]
  gen-dh
  gen-req <filename_base> [ cmd-opts ]
  sign-req <type> <filename_base>
  build-client-full <filename_base> [ cmd-opts ]
  build-server-full <filename_base> [ cmd-opts ]
  revoke <filename_base> [cmd-opts]
  renew <filename_base> [cmd-opts]
  build-serverClient-full <filename_base> [ cmd-opts ]
  gen-crl
  update-db
  show-req <filename_base> [ cmd-opts ]
  show-cert <filename_base> [ cmd-opts ]
  show-ca [ cmd-opts ]
  import-req <request_file_path> <short_basename>
  export-p7 <filename_base> [ cmd-opts ]
  export-p8 <filename_base> [ cmd-opts ]
  export-p12 <filename_base> [ cmd-opts ]
  set-rsa-pass <filename_base> [ cmd-opts ]
  set-ec-pass <filename_base> [ cmd-opts ]
  upgrade <type>

DIRECTORY STATUS (commands would take effect on these locations)
  EASYRSA: /usr/share/easy-rsa
      PKI: /usr/share/easy-rsa/pki
```

```
mariocordero@mariocordero-B450M-AORUS-ELITE:/usr/share/easy-rsa$ sudo ./easyrsa init-pki

init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: /usr/share/easy-rsa/pki
```

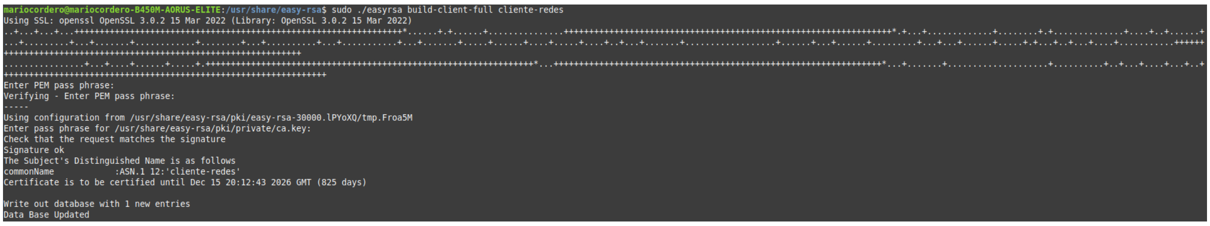

mariocordero@mariocordero-B450M-AORUS-ELITE:/usr/share/easy-rsa$ sudo ./easyrsa build-ca
Using SSL: openssl OpenSSL 3.0.2 15 Mar 2022 (Library: OpenSSL 3.0.2 15 Mar 2022)
Enter New CA Key Passphrase:
Re-Enter New CA Key Passphrase:
You are about to be asked to enter information that will be incorporated
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.

Common Name (eg: your user, host, or server name) [Easy-RSA CA]:CI0123 CA
CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/usr/share/easy-rsa/pki/ca.crt


mariocordero@mariocordero-B450M-AORUS-ELITE:/usr/share/easy-rsa$ sudo ./easyrsa gen-dh
[sudo] password for mariocordero:
Using SSL: openssl OpenSSL 3.0.2 15 Mar 2022 (Library: OpenSSL 3.0.2 15 Mar 2022)
Generating DH parameters, 2048 bit long safe prime
DH parameters of size 2048 created at /usr/share/easy-rsa/pki/dh.pem


mariocordero@mariocordero-B450M-AORUS-ELITE:/usr/share/easy-rsa$ sudo ./easyrsa build-server-full redes
Using SSL: openssl OpenSSL 3.0.2 15 Mar 2022 (Library: OpenSSL 3.0.2 15 Mar 2022)
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

Using configuration from /usr/share/easy-rsa/pki/easy-rsa-29806.xl43tl/tmp.VQgyI4
Enter pass phrase for /usr/share/easy-rsa/pki/private/ca.key:
40774C8ED27F0000:error:0700006C:configuration file routines:NCONF_get_string:no value:../crypto/conf/conf_lib.c:315:group=<NULL> name=unique_subject
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName :ASN.1 12:'redes'
Certificate is to be certified until Dec 15 20:10:07 2026 GMT (825 days)
Write out database with 1 new entries
Data Base Updated


mariocordero@mariocordero-B450M-AORUS-ELITE:/usr/share/easy-rsa$ sudo ./easyrsa build-client-full cliente-redes
Using SSL: openssl OpenSSL 3.0.2 15 Mar 2022 (Library: OpenSSL 3.0.2 15 Mar 2022)
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

Using configuration from /usr/share/easy-rsa/pki/easy-rsa-30000.lPYoXQ/tmp.Froa5M
Enter pass phrase for /usr/share/easy-rsa/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName :ASN.1 12:'cliente-redes'
Certificate is to be certified until Dec 15 20:12:43 2026 GMT (825 days)
Write out database with 1 new entries
Data Base Updated

Nota: soy desarrollador web, ya tenía apache2 instalado en mi PC

```
mariocordero@mariocordero-B450M-AORUS-ELITE:/usr/share/easy-rsa$ sudo apt install openssl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be upgraded:
  openssl
1 upgraded, 0 newly installed, 0 to remove and 251 not upgraded.
Need to get 1 184 kB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssl amd64 3.0.2-0ubuntu1.18 [1 184 kB]
Fetched 1 184 kB in 2s (565 kB/s)
(Reading database ... 635382 files and directories currently installed.)
Preparing to unpack .../openssl_3.0.2-0ubuntu1.18_amd64.deb ...
Unpacking openssl (3.0.2-0ubuntu1.18) over (3.0.2-0ubuntu1.15) ...
Setting up openssl (3.0.2-0ubuntu1.18) ...
Processing triggers for man-db (2.10.2-1) ...
```

```
mariocordero@mariocordero-B450M-AORUS-ELITE:/etc/ssl$ ls
certs  openssl.cnf  private
mariocordero@mariocordero-B450M-AORUS-ELITE:/etc/ssl$ sudo openssl genrsa -out /etc/ssl/private/certificado-redes.key 2048
mariocordero@mariocordero-B450M-AORUS-ELITE:/etc/ssl$ sudo openssl req -new -x509 -key /etc/ssl/private/certificado-redes.key -out /etc/ssl/certs/certificado-redes.crt -days 365
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]:CR
State or Province Name (full name) [Some-State]:San Jose
Locality Name (eg, city) []:Sabanilla
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UCR
Organizational Unit Name (eg, section) []:Mario
Common Name (e.g. server FQDN or YOUR name) []:Mario Cordero
Email Address []:mariogabriel.cordero@ucr.ac.cr
```

Apache usando el certificado:

```
mariocordero@mariocordero-B450M-AORUS-ELITE:/etc/ssl$ sudo a2ensite default-ssl.conf
Site default-ssl already enabled
mariocordero@mariocordero-B450M-AORUS-ELITE:/etc/ssl$ sudo systemctl restart apache2
mariocordero@mariocordero-B450M-AORUS-ELITE:/etc/ssl$ openssl s_client -connect localhost:443 -showcerts
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 C = CR, ST = San Jose, L = Sabanilla, O = UCR, OU = Mario, CN = Mario Cordero, emailAddress = mariogabriel.cordero@ucr.ac.cr
verify error:num=18:self-signed certificate
verify return:1
depth=0 C = CR, ST = San Jose, L = Sabanilla, O = UCR, OU = Mario, CN = Mario Cordero, emailAddress = mariogabriel.cordero@ucr.ac.cr
verify return:1
---
Certificate chain
 0 s:C = CR, ST = San Jose, L = Sabanilla, O = UCR, OU = Mario, CN = Mario Cordero, emailAddress = mariogabriel.cordero@ucr.ac.cr
   i:C = CR, ST = San Jose, L = Sabanilla, O = UCR, OU = Mario, CN = Mario Cordero, emailAddress = mariogabriel.cordero@ucr.ac.cr
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Sep 11 20:42:20 2024 GMT; NotAfter: Sep 11 20:42:20 2025 GMT
-----BEGIN CERTIFICATE-----
MIIEFTCCAv2gAwIBAgIUBZER0kk60qXvcJQKfz/Q3KAI9mcwDQYJKoZIhvcNAQEL
BQAwgZkxCzAJBgNVBAYTAkNSMREwDwYDVQQIDAhTYW4gSm9zZTESMBAGA1UEBwwJ
U2FiYW5pbGxhMQwwCgYDVQQKDANVQ1IxDjAMBgNVBAsMBU1hcmlvMRYwFAYDVQQD
DA1NYXJpbyBDb3JkZXJvMS0wKwYJKoZIhvcNAQkBFh5tYXJpb2dhYnJpZWwuY29y
ZGVyb0B1Y3IuYWMuY3IwHhcNMjQwOTExMjA0MjIwWhcNMjUwOTExMjA0MjIwWjCB
mTELMAkGA1UEBhMCQ1IxETAPBgNVBAgMCFNhbiBKb3NlMRIwEAYDVQQHDAlTYWJh
bmlsbGExDDAKBgNVBAoMA1VDUjEOMAwGA1UECwwFTWFyaW8xFjAUBgNVBAMMDU1h
cmlvIENvcmRlcm8xLTArBgkqhkiG9w0BCQEWHm1hcmlvZ2FicmllbC5jb3JkZXJv
QHVjci5hYy5jcjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJTULLmh
R4ri9Havs0G4SlPjg5zFLd9yiOdSgMz/13eURX8q2XiHHadliJwaoxFjOc6TQJL9
OY/gQsZTNpzPsYHKH/33DzfSLrg/mvNmkp8RASGmF7pGm8OvsCZlFYps3bCNZ8ko
+wysBdh3AfU7plJSI7ohiwMGbUVaBC1+gFzmTcWZrl3falTUGgAGCpu/68ZIbP0+
3NmLngW29p9kXyHpoAIqu0EXK95FKAZplSWKCtPWuMSa8/JkPwozkpLtHk/z5Zh8
lubWGdOJRRKVgbnsMrSjA660/okRTgVm78+oxwqOJY5j3GZLM82cSIlfC12XkfyU
012n+uF2bhgpn5sCAwEAAaNTMFEwHQYDVR0OBBYEFDCvAkCBUyutX1QQNLHJxgPD
JmYdMB8GA1UdIwQYMBaAFDCvAkCBUyutX1QQNLHJxgPDJmYdMA8GA1UdEwEB/wQF
MAMBAf8wDQYJKoZIhvcNAQELBQADggEBADXNY4mrGZeNl2VuwDYo5ueQANC4pKHt
3Sgfu5UYzoONMKQhso4TTvnacuT2oB6iiLwqi6JVzs1FM2wkHeZtjM8PwXHPubxo
3dFSaoiIy2PdfRMqlKrr/Mtk7uxAT7A+3bkFcUomGLl894eatPOqALI8Ek2JZJ8v
wf1of4kG3uaGwxTTlYLh6ESbmjYPhn6yKBHVAwk7IiQXiBCOYsEnQ41JGaFbMU22
QbByXspoofm3M8pvIwqVBJPZBZgJ1eJdNnYp5LksU2TLA2UHrfPX3HtoLo45mzHd
rjglakY7SdqtKGxZDBi4RLtsObCjV0BT6TfBG+T/iOMTRX/AQNzhVhI=
-----END CERTIFICATE-----
---
Server certificate
subject=C = CR, ST = San Jose, L = Sabanilla, O = UCR, OU = Mario, CN = Mario Cordero, emailAddress = mariogabriel.cordero@ucr.ac.cr
issuer=C = CR, ST = San Jose, L = Sabanilla, O = UCR, OU = Mario, CN = Mario Cordero, emailAddress = mariogabriel.cordero@ucr.ac.cr
---
```