- **Instalar el paquete "easy-rsa"**

```
nacho@DESKTOP-51FO8KG:~/Proyecto-Integrados-Bases-de-datos-DIEGOCERDAS-C21988$ sudo apt install easy-rsa
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
easy-rsa is already the newest version (3.0.8-1ubuntu1).
The following packages were automatically installed and are no longer required:
  htop libnl-genl-3-200
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 32 not upgraded.
nacho@DESKTOP-51FO8KG:~/Proyecto-Integrados-Bases-de-datos-DIEGOCERDAS-C21988$
```

- **Iniciar PKI**

```
nacho@DESKTOP-51FO8KG:~/Proyecto-Integrados-Bases-de-datos-DIEGOCERDAS-C21988$ mkdir -p ~/easy-rsa
cp -r /usr/share/easy-rsa/* ~/easy-rsa/
cd ~/easy-rsa
nacho@DESKTOP-51FO8KG:~/easy-rsa$ ./easyrsa init-pki

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

- **Crear la autoridad certificadora [CA]**

```
nacho@DESKTOP-51FO8KG:~/easy-rsa$ ./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 creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/home/nacho/easy-rsa/pki/ca.crt
```

- **Generar la llave de encripción [DS]**

```
nacho@DESKTOP-51FO8KG:~/easy-rsa$ ./easyrsa gen-dh
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 /home/nacho/easy-rsa/pki/dh.pem
```

- ## **Generar la llave para el servidor**


```
nacho@DESKTOP-51FO8KG:~/easy-rsa$ ./easyrsa gen-req server1 nopass
<
Using SSL: openssl OpenSSL 3.0.2 15 Mar 2022 (Library: OpenSSL 3.0.2 15 Mar 2022)
....+........+..+.........+..+...............+...+....+++++++++++++++++++++++++++++++++++++++++++++++*.....+.....+.......+......+....
.+++++++++++++++++++++++++++++++++++++++++*.+..+..+.+.+....+........+...............+.....+.............+.....+..........+++++++++++++++
++++++++++++++++++*...+......+.++++++++++++++++++++++++++++++++++
.........+..+++++++++++++++++++++++++++++++++++++++++++++++*.....+......+.+...++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++*...+..+.+....+........+.....+.+.+....+.+.....++.....+.+...+.....+.+.....+....+....
......................+.....+....+..................+...+.+.....+.......+.+.....+.+.....+.+.....+
...............+......+.+.....++.....+...........+....+...+.+..+.+.....+.......+..............+.......+....+...+..++++++
+.+.+..+.+..+.+++++++++++++++++++++++++++++++++++++++++++++++++++
-----
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) [server1]:Nacho

Keypair and certificate request completed. Your files are:
req: /home/nacho/easy-rsa/pki/reqs/server1.req
key: /home/nacho/easy-rsa/pki/private/server1.key
```

- ## **Generar la llave para el cliente**


```
nacho@DESKTOP-51FO8KG:~/easy-rsa$ ./easyrsa sign-req client cliente1
Using SSL: openssl OpenSSL 3.0.2 15 Mar 2022 (Library: OpenSSL 3.0.2 15 Mar 2022)


You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a client certificate for 825 days:

subject=
    commonName                = Nacho2


Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes
Using configuration from /home/nacho/easy-rsa/pki/easy-rsa-13117.5rK5DT/tmp.TU9G74
Enter pass phrase for /home/nacho/easy-rsa/pki/private/ca.key:
804B117E2D7F0000: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:'Nacho2'
Certificate is to be certified until Jul  6 00:47:54 2027 GMT (825 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /home/nacho/easy-rsa/pki/issued/cliente1.crt

nacho@DESKTOP-51FO8KG:~/easy-rsa$
```

● **Instalar el apache**