


## INDICE

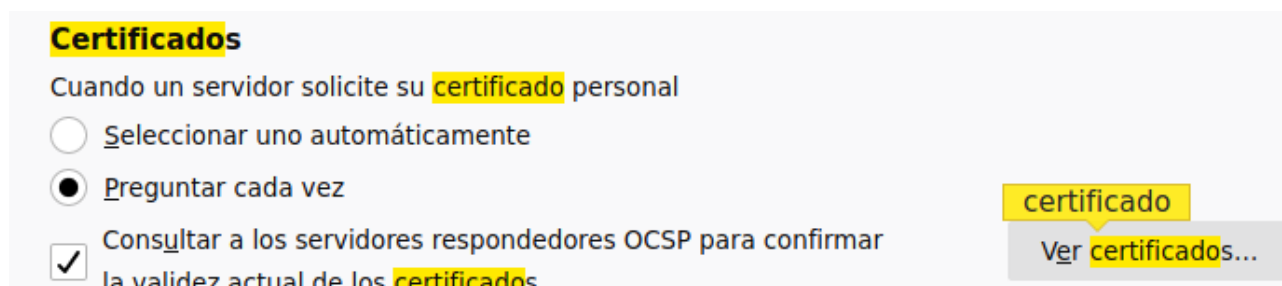
CERTIFICADOS DIGITALES. HTTPS.....	1
Tarea 1: Instalación del Certificado.....	1
Tarea 2: Validación del certificado.....	4
Tarea 3: Firma electrónica.....	5
Tarea 4: Autenticación.....	7
DGT.....	7
Datos Sanitarios.....	8
HTTPS/SSL.....	9
Tarea 1: Certificado autofirmado.....	9

## CERTIFICADOS DIGITALES. HTTPS

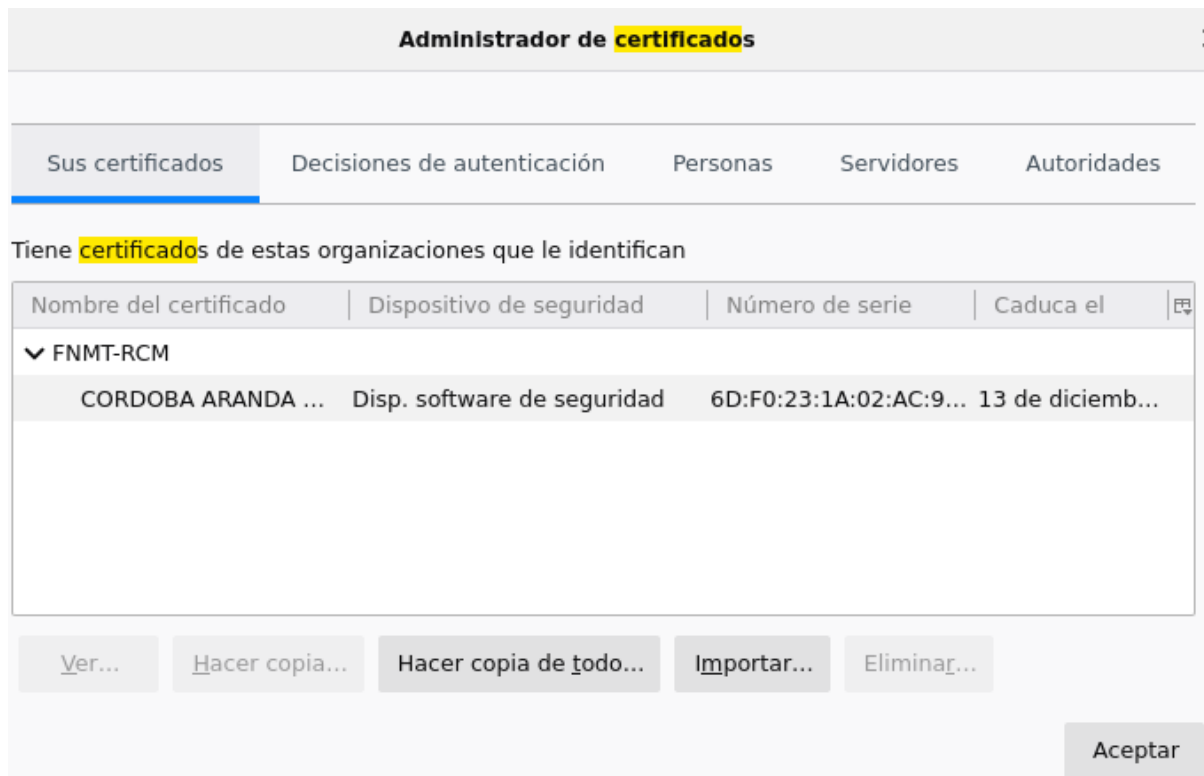
### Tarea 1: Instalación del Certificado

**1. Una vez que hayas obtenido tu certificado, explica brevemente como se instala en tu navegador favorito.**

Una vez obtenido el certificado, nos vamos a nuestro navegador (Firefox)y abrimos el menú de opciones  y en la sección **Preferencias** existe un buscador en el que insertaremos la palabra **certificado**, esto nos llevará a la siguiente pantalla.

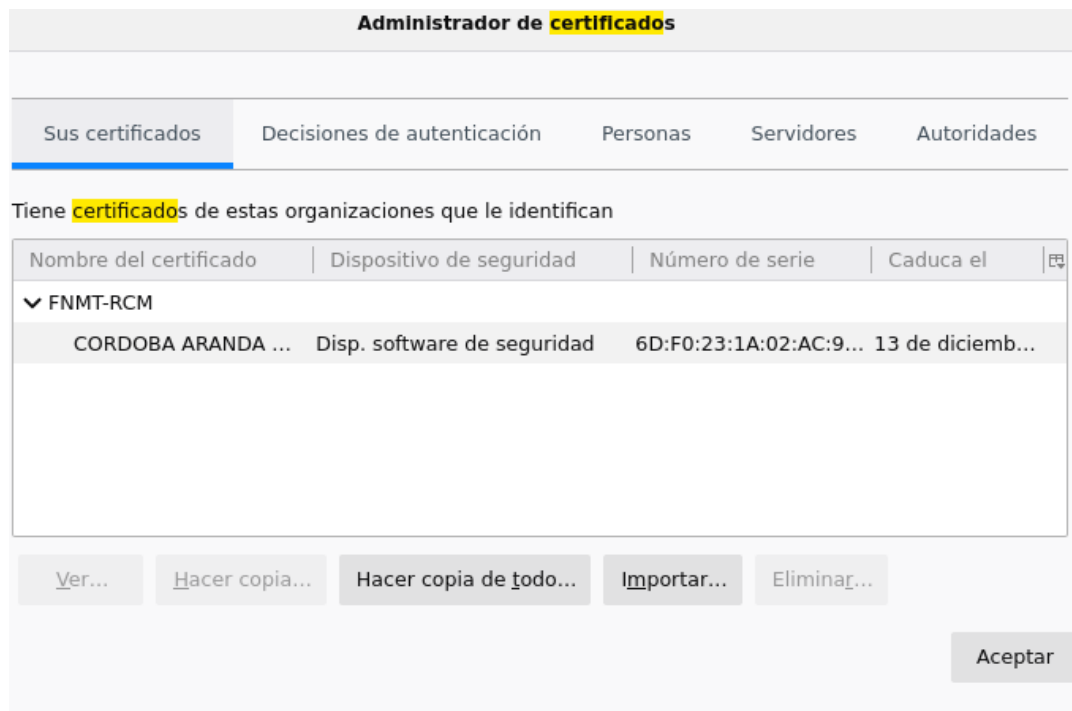


El siguiente paso es clicar en el recuadro **Ver Certificados** para pasar a la siguiente pantalla.



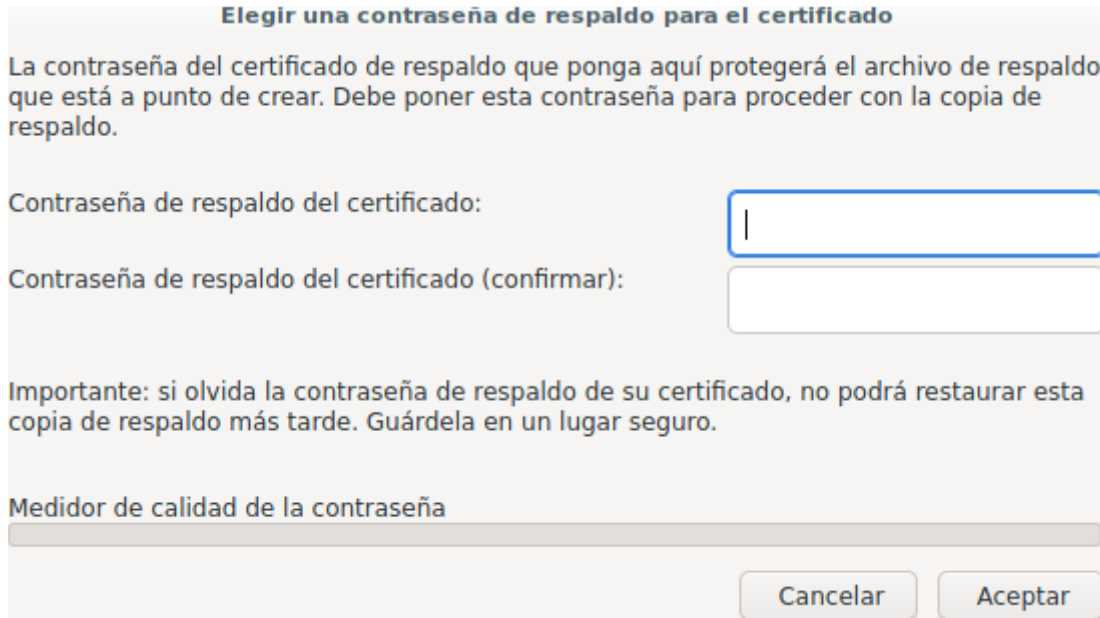
Una vez llegado a este punto es clicar en **Importar** y seleccionar la ruta donde se encuentre nuestro certificado.

**2. Muestra una captura de pantalla donde se vea las preferencias del navegador donde se ve instalado tu certificado.**



3. ¿Cómo puedes hacer una copia de tu certificado?, ¿Como vas a realizar la copia de seguridad de tu certificado?. Razona la respuesta.

Pues en la misma pantalla de **Administrador de Certificados** existe una opción llamada **Hacer copia**, seleccionamos la ruta donde queremos hacer la copia de seguridad y nos pedirá una contraseña.



The screenshot shows a dialog box with the title "Elegir una contraseña de respaldo para el certificado". The main text reads: "La contraseña del certificado de respaldo que ponga aquí protegerá el archivo de respaldo que está a punto de crear. Debe poner esta contraseña para proceder con la copia de respaldo." Below this, there are two input fields: "Contraseña de respaldo del certificado:" and "Contraseña de respaldo del certificado (confirmar):". The first field has a blue border and contains a single character. Below the input fields, there is a warning: "Importante: si olvida la contraseña de respaldo de su certificado, no podrá restaurar esta copia de respaldo más tarde. Guárdela en un lugar seguro." At the bottom, there is a "Medidor de calidad de la contraseña" (password quality meter) and two buttons: "Cancelar" and "Aceptar".

Una vez introducida la contraseña veremos en nuestra ruta que está creado nuestra **Copia de Seguridad** de nuestro certificado.

La copia de seguridad de mi certificado la he realizado con mi navegador Firefox porque es la manera más fácil de hacerlo.

## Tarea 2: Validación del certificado

1. Instala en tu ordenador el software [autofirma](#) y desde la página de VALIDe valida tu certificado. Muestra capturas de pantalla donde se comprueba la validación.

**Certificado válido**

**Nombre/Apellid. Responsable:** MIGUEL CORDOBA ARANDA  
**NIF Responsable:** 49092319S

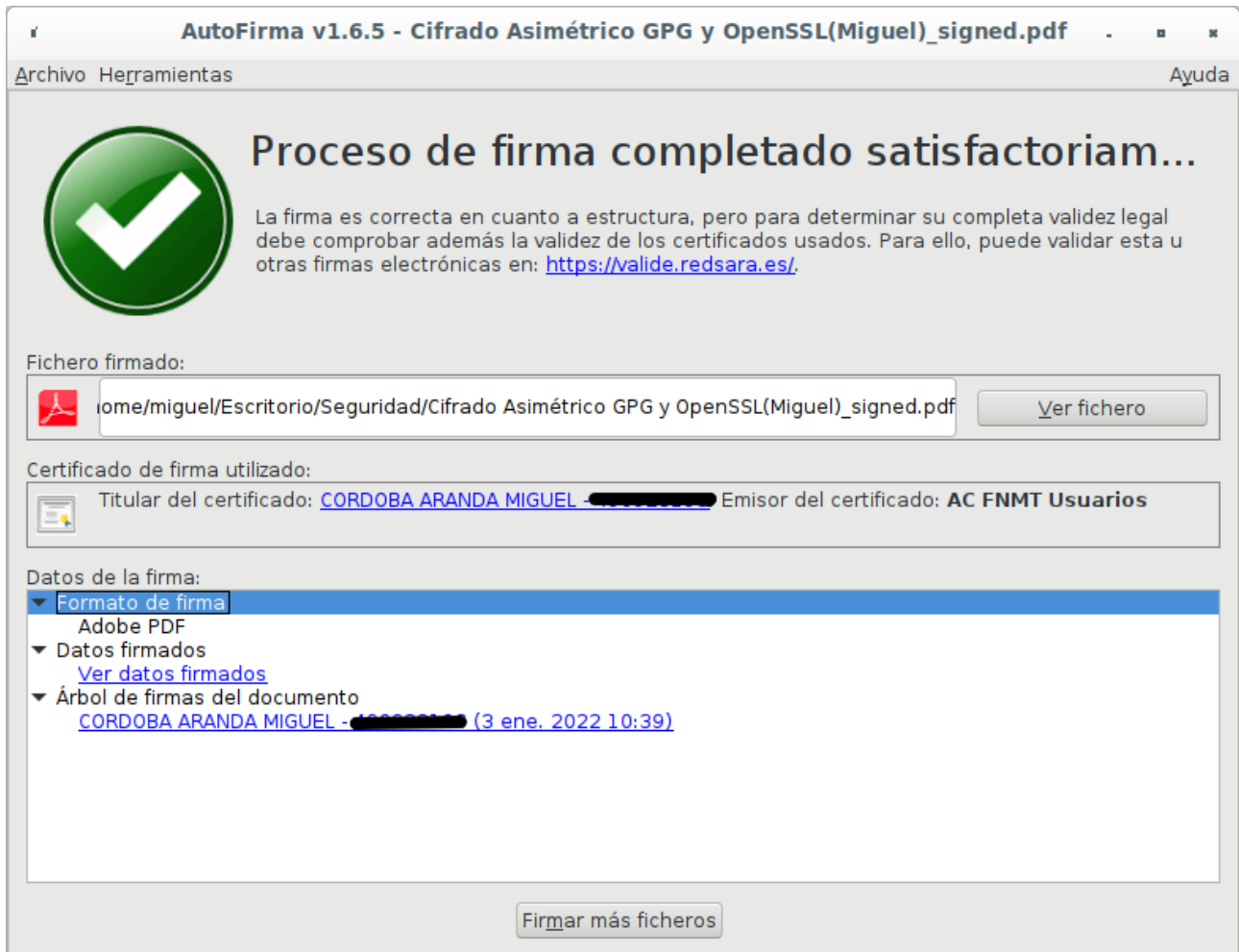
**■ Información del certificado**  
**Apellidos del responsable:** CORDOBA ARANDA  
**Clasificación:** 0  
**Email:** miguelcor.rrss@gmail.com  
**Extensión del uso del certificado:** KeyPurposeld 0: E-mail protection KeyPurposeld 1: TLS Web client authentication  
**ID Emisor:** CN=AC FNMT Usuarios,OU=Ceres,O=FNMT-RCM,C=ES  
**ID Política:** MITYC  
**NIF Responsable:** [REDACTED]  
**Nombre/Apellid. Responsable:** MIGUEL CORDOBA ARANDA  
**Nombre del responsable:** MIGUEL  
**Número de serie:** [REDACTED]  
**Organización emisora:** FNMT-RCM  
**País:** ES  
**Política:** 1.3.6.1.4.1.5734.3.10.1,0.4.0.194112.1.0  
**Primer apellido del responsable:** CORDOBA  
**Segundo apellido del responsable:** ARANDA  
**Asunto:** CN=CORDOBA ARANDA MIGUEL - [REDACTED],SN=CORDOBA ARANDA,givenName=MIGUEL,serialNumber=IDCES-[REDACTED],C=ES  
**Tipo de certificado:** FNMT PF SW EIDAS - SHA256  
**Uso del certificado:** digitalSignature | nonRepudiation | keyEncipherment  
**Válido desde:** 2021-12-13 lun 13:42:33 +0100  
**Válido hasta:** 2025-12-13 sáb 13:42:33 +0100  
**Versión política:** 23

**Observaciones:** El certificado es válido, incluyendo su estado de revocación  
**Hora de Consulta** 27-dic-2021 02:19:18 PM GMT+0100

## Tarea 3: Firma electrónica

1. Utilizando la página VALIDe y el programa autofirma, firma un documento con tu certificado y envíalo por correo a un compañero.

Para firmar un fichero, he iniciado la herramienta **Autofirma** indicándole el fichero y el certificado digital.



Y luego lo he enviado vía Whatsapp.

2. Tu debes recibir otro documento firmado por un compañero y utilizando las herramientas anteriores debes visualizar la firma (Visualizar Firma) y (Verificar Firma). ¿Puedes verificar la firma aunque no tengas la clave pública de tu compañero?.

Si. Puedo verificarla perfectamente.

**Validar Certificado**  
**Realizar firma**  
**Validar Firma**  
**Validar Sede Electrónica**  
**Visualizar Firma**  
**Faqs**

 **Resultado de Validar Firma**

 **Firma válida**  
**Firmantes:**

- MARIA JESUS BOHIGUEZ PEREZ

[Descargar Justificante](#)

Y el justificante es el siguiente:

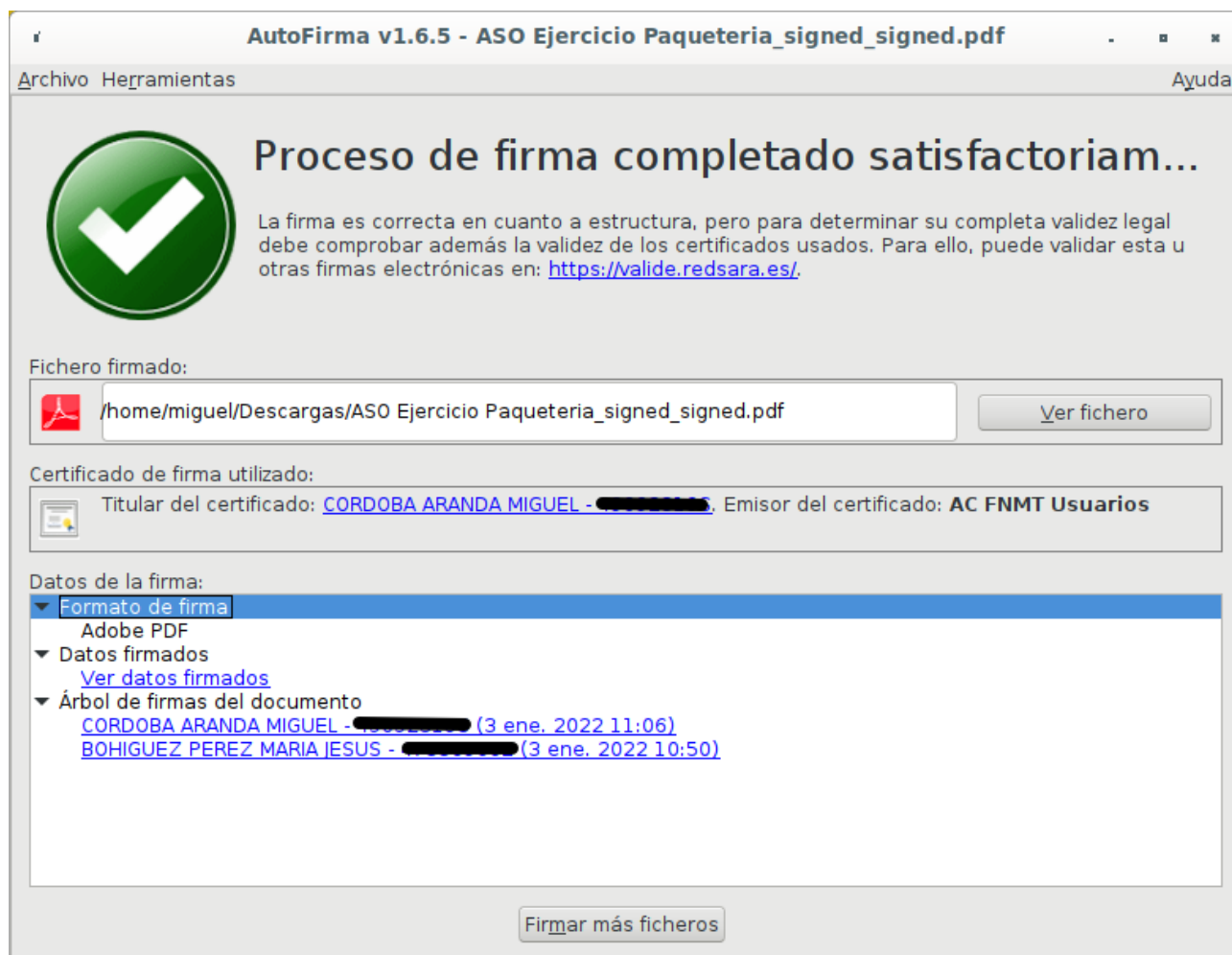


- sudo apt list –upgradable
- Con este comando podremos ver lo siguiente:
  - Los paquetes que se pueden actualizar.
  - Las versiones actuales de los paquetes.
  - Las versiones nuevas de los paquetes.

**¿Es necesario estar conectado a internet para hacer la validación de la firma?. Razona tus respuestas.**

No es necesario porque la herramienta **Autofirma** te permite ver la firma del documento.

- Entre dos compañeros, firmar los dos un documento, verificar la firma para comprobar que está firmado por los dos.



## Tarea 4: Autenticación


- Utilizando tu certificado accede a alguna página de la administración pública (cita médica, becas, puntos del carnet,...). Entrega capturas de pantalla donde se demuestre el acceso a ellas.

### DGT



 miguelcor.rrss@gmail.com

 003465497776

 CALLE VICENTE ALEIXANDRE , NU: 3 , ES: 3 , PLA: BJ , PTA: L 41701 DOS HERMANAS  
SEVILLA



## PERMISOS



### ¿Qué debes saber?

Consulta tus permisos y autorizaciones, su vigencia, y más información de tu interés como cuando te toca renovar tu carnet.



### Permisos

1



### Puntos

15

## Datos Sanitarios

**Miguel Cordoba Aranda**

20/07/1990

Nº historia de salud de Andalucía (NUHSA)

████████████████████

DNI

████████████████████

### Prestación farmacéutica

Porcentaje de aportación: 40% (TSI 003)

### Información asistencial

Consulta de medicina de familia

Jose Antonio Rodas Peral

Consulta de enfermería

INMACULADA DIAZ SALAZAR ALBARRAN


Centro de atención primaria

Santa Ana (Dos Hermanas C)

Calle ANTONIA DIAZ (1ª planta), 19.

41701 - Dos hermanas (Sevilla)

 Todos los días de 08:00 a 20:00

 955019951



# HTTPS/SSL

## Tarea 1: Certificado autofirmado

El alumno que hace de Autoridad Certificadora deberá entregar una documentación donde explique los siguientes puntos:

1. Crear su autoridad certificadora (generar el certificado digital de la CA). Mostrar el fichero de configuración de la AC.

```
HOME = .
oid_section = new_oids
openssl_conf = default_conf

[ new_oids ]
tsa_policy1 = 1.2.3.4.1
tsa_policy2 = 1.2.3.4.5.6
tsa_policy3 = 1.2.3.4.5.7
#####
[ ca ]
default_ca = CA_default # The default ca section
#####
[ CA_default ]
dir = /var/ca # Where everything is kept
certs = $dir/certsdb # Where the issued certs are kept
new_certs_dir = $certs # default place for new certs.
database = $dir/index.txt # database index file.
certificate = $dir/cacert.pem # The CA certificate
private_key = $dir/private/cakey.pem # The private key
serial = $dir/serial # The current serial number
crldir = $dir/crl
crlnumber = $dir/crlnumber # the current crl number
crl = $crldir/crl.pem # The current CRL
RANDFILE = $dir/private/.rand
x509_extensions = usr_cert # The extensions to add to the cert
copy_extensions = copy
name_opt = ca_default # Subject Name options
cert_opt = ca_default # Certificate field options
default_days = 365 # how long to certify for
default_crl_days = 30 # how long before next CRL
default_md = sha1 # use public key default MD
preserve = no # keep passed DN ordering
policy = policy match
```

```
[ policy_match ]
countryName           = match
stateOrProvinceName   = match
organizationName       = match
organizationalUnitName = optional
commonName             = supplied
emailAddress           = optional

[ policy_anything ]
countryName           = optional
stateOrProvinceName   = optional
localityName          = optional
organizationName       = optional
organizationalUnitName = optional
commonName             = supplied
emailAddress           = optional
#####
[ req ]
default_bits           = 2048
default_keyfile         = privkey.pem
distinguished_name      = req_distinguished_name
attributes              = req_attributes
x509_extensions         = v3_ca # The extensions to add to the self signed cert
req_extensions          = v3_req
string_mask = utf8only
```

```
[ req_distinguished_name ]
countryName                = Nombre Pais (2 Letras)
countryName_default        = ES
countryName_min            = 2
countryName_max            = 2
stateOrProvinceName        = Estado o Provincia (Nombre Completo)
stateOrProvinceName_default = Sevilla
localityName               = Localidad (ciudad)
localityName_default       = Dos Hermanas
0.organizationName         = Nombre de la Organizacion (compañia)
0.organizationName_default = Miguelito S.A
commonName                 = Nombre
commonName_max             = 64
emailAddress               = Correo
emailAddress_max           = 64

[ req_attributes ]
challengePassword          = Cambiar de Contraseña (4-20 caracteres)
challengePassword_min      = 4
challengePassword_max      = 20

[ usr_cert ]
basicConstraints=CA:FALSE
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer
nsComment            = "Certificado Generado OpenSSL"
# PKIX recommendations harmless if included in all certificates.
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer

[ v3_req ]
subjectAltName = email:move

[ v3_ca ]
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer:always
basicConstraints = CA:true

[ crt_ext ]
authorityKeyIdentifier=keyid:always
```

```

[ proxy_cert_ext ]
basicConstraints=CA:FALSE
nsComment              = "Certificado Generado OpenSSL"
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer
proxyCertInfo=critical,language:id-ppl-anyLanguage,pathlen:3,policy:foo
#####
[ tsa ]
default_tsa = tsa_config1      # the default TSA section

[ tsa_config1 ]
dir           = ./demoCA                # TSA root directory
serial        = $dir/tsaserial          # The current serial number (mandatory)
crypto_device = builtin                 # OpenSSL engine to use for signing
signer_cert   = $dir/tsacert.pem        # The TSA signing certificate
certs         = $dir/cacert.pem         # Certificate chain to include in reply
signer_key    = $dir/private/tsakey.pem # The TSA private key (optional)
signer_digest = sha256                  # Signing digest to use. (Optional)
default_policy = tsa_policy1            # Policy if request did not specify it
other_policies = tsa_policy2, tsa_policy3 # acceptable policies (optional)
digests       = sha1, sha256, sha384, sha512 # Acceptable message digests (mandatory)
accuracy      = secs:1, millisecs:500, microsecs:100 # (optional)
clock_precision_digits = 0              # number of digits after dot. (optional)
ordering      = yes                    # Is ordering defined for timestamps?
tsa_name      = yes                    # Must the TSA name be included in the reply?
ess_cert_id_chain = no                 # Must the ESS cert id chain be included?
ess_cert_id_alg = sha1                 # algorithm to compute certificate

[default_conf]
ssl_conf = ssl_sect

[ssl_sect]
system_default = system_default_sect

[system_default_sect]
MinProtocol = TLSv1.2
CipherString = DEFAULT@SECLEVEL=2

```

2. Debe recibir el fichero CSR (Solicitud de Firmar un Certificado) de su compañero, debe firmarlo y enviar el certificado generado a su compañero.
3. ¿Qué otra información debes aportar a tu compañero para que éste configure de forma adecuada su servidor web con el certificado generado? .

El alumno que hace de administrador del servidor web, debe entregar una documentación que describa los siguientes puntos:

1. Crea una clave privada RSA de 4096 bits para identificar el servidor.

Para crear una clave privada he usado el comando `#openssl genrsa -des3 -out CA.key 4096`.

```

debian@CA:~/CA$ openssl genrsa -des3 -out CA.key 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
.....+++++
e is 65537 (0x010001)
Enter pass phrase for CA.key:
Verifying - Enter pass phrase for CA.key:

```

