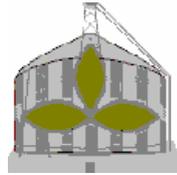
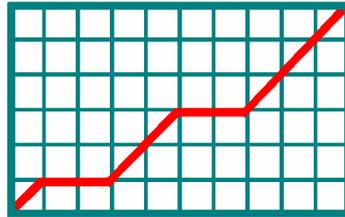


*Alejandro Eguinoa Arteaga y Asoc. S.R.L.*



**AGROACOPIO**

**OPENSSL Y**  
**CERTIFICADO AFIP**

**OPENSSL Y CERTIFICADO AFIP****INDICE**

INTRODUCCIÓN-----	03
INSTALACION DEL VISUAL C++ REDISTRIBUIBLE-----	03
INSTALACION DEL OPENSSL-----	07
COMO GENERAR EL ARCHIVO .CSR-----	13
CONVERTIR EL CERTIFICADO .CRT EN .PFX-----	17
ANEXO I -----	28
PASO 1: INGRESO A LA PAGINA DE AFIP-----	29
PASO 2: HABILITAR “ADMINISTRACIÓN DE CERTIFICADOS DIGITALES”-----	30
PASO 3: SELECCIONAR EL CONTRIBUYENTE-----	34
PASO 4: AGREGAR ALIAS-----	35
PASO 5: SUBIR ARCHIVO .CSR-----	35
PASO 6: DESCARGAR ARCHIVO .CRT-----	36

## INTRODUCCIÓN

Para poder trabajar con Facturación Electrónica, previamente se debe generar un certificado digital por medio de un utilitario llamada OpenSSL, y luego hacer autorizar ese certificado por la AFIP. Se presupone que ya se posee clave fiscal de nivel acorde a los servicios que se utilizan (NIVEL 3), tramitada en una dependencia de AFIP. A continuación se describen los pasos para crear y autorizar el certificado. Para más información ver [Página principal de Factura Electrónica \(AFIP\)](#).

## INSTALACION DEL VISUAL C++ REDISTRIBUIBLE

Para instalar el Visual C++ redistribuible, que es un requisito previo a la instalación del OPENSSL. Se puede bajar desde el siguiente link:

<http://www.microsoft.com/downloads/en/details.aspx?familyid=9B2DA534-3E03-4391-8A4D-074B9F2BC1BF&displaylang=en>

Una vez que accedemos al link, vemos la siguiente ventana:

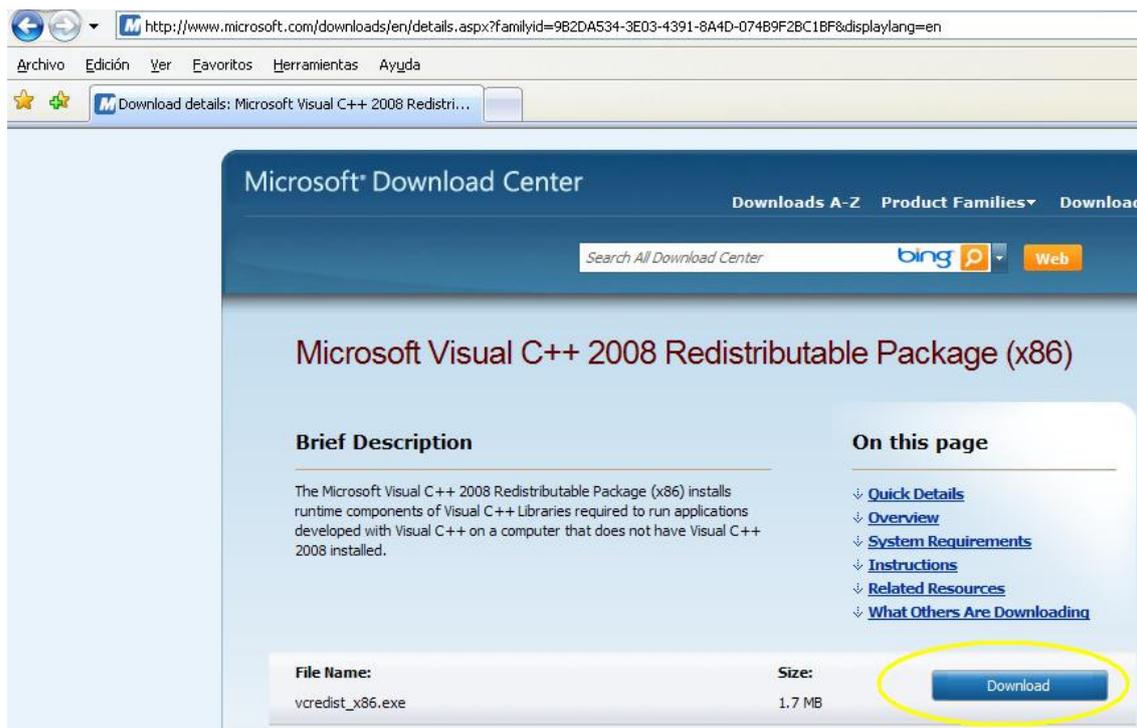


imagen 1

Hacemos click en “Download” y vemos lo siguiente:



imagen 2

Hacemos click en “Guardar” y seleccionamos una carpeta temporal donde guardar el archivo de instalación del Visual C++ redistribuible, como se ve aquí (en el ejemplo se utiliza la carpeta TEMP):

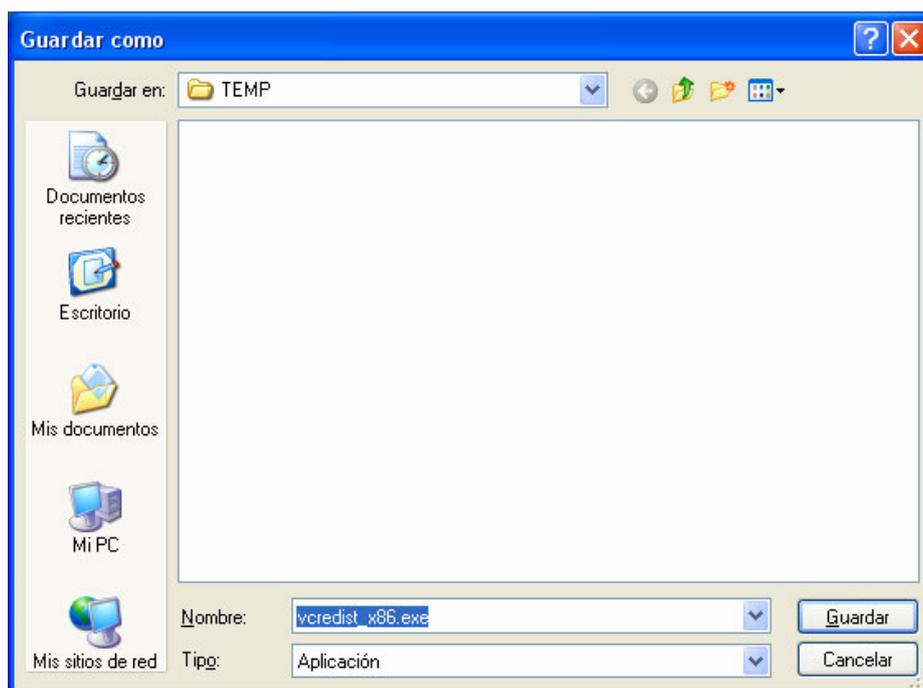


imagen 3

Luego en una ventana de “Mi PC” ingresamos a la carpeta elegida y ejecutamos con doble click el archivo de nombre **vcredist\_x86.exe**:

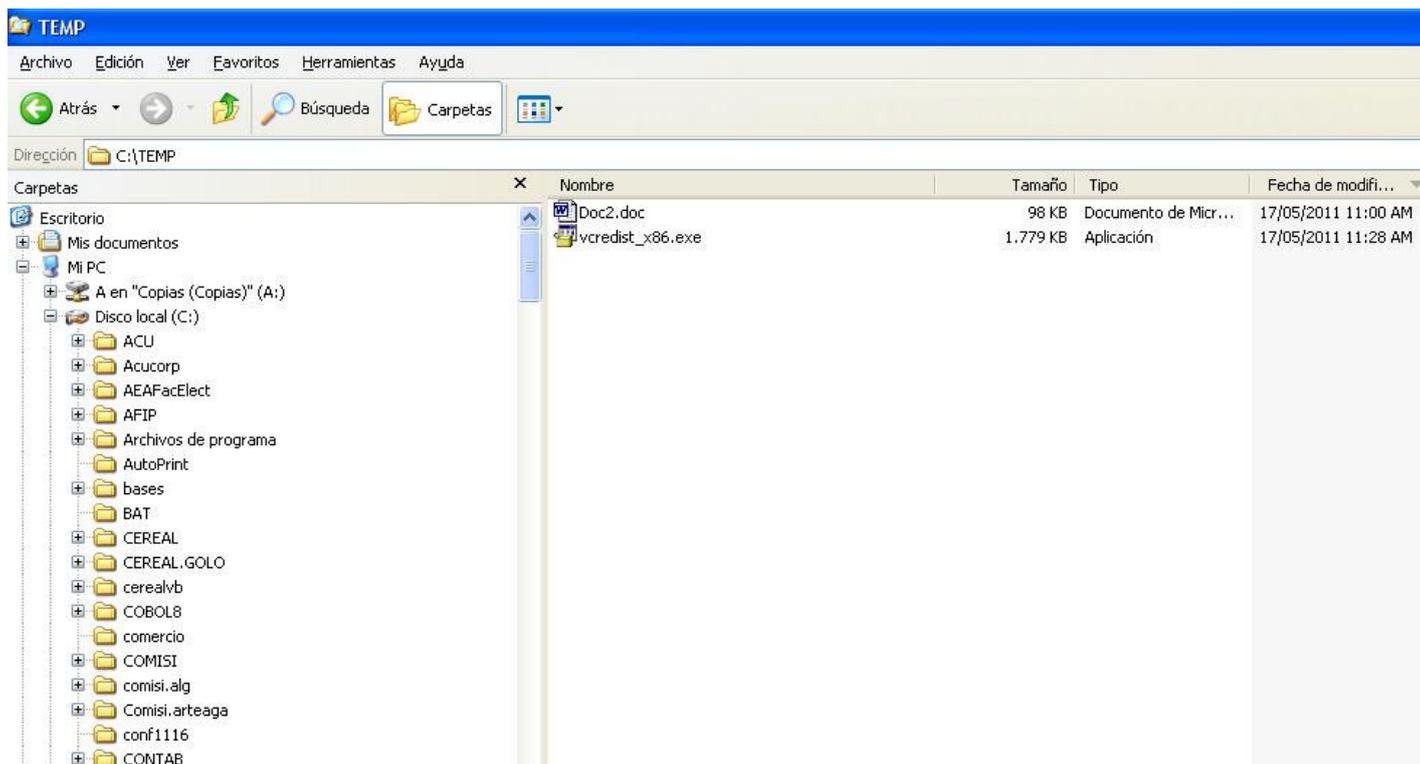


imagen 4

Al comenzar la instalación del Visual C++ redistribuible, lo primero que podemos observar es una advertencia, hacer click en el botón “Ejecutar”, luego vemos la pantalla de presentación de la instalación:



imagen 5

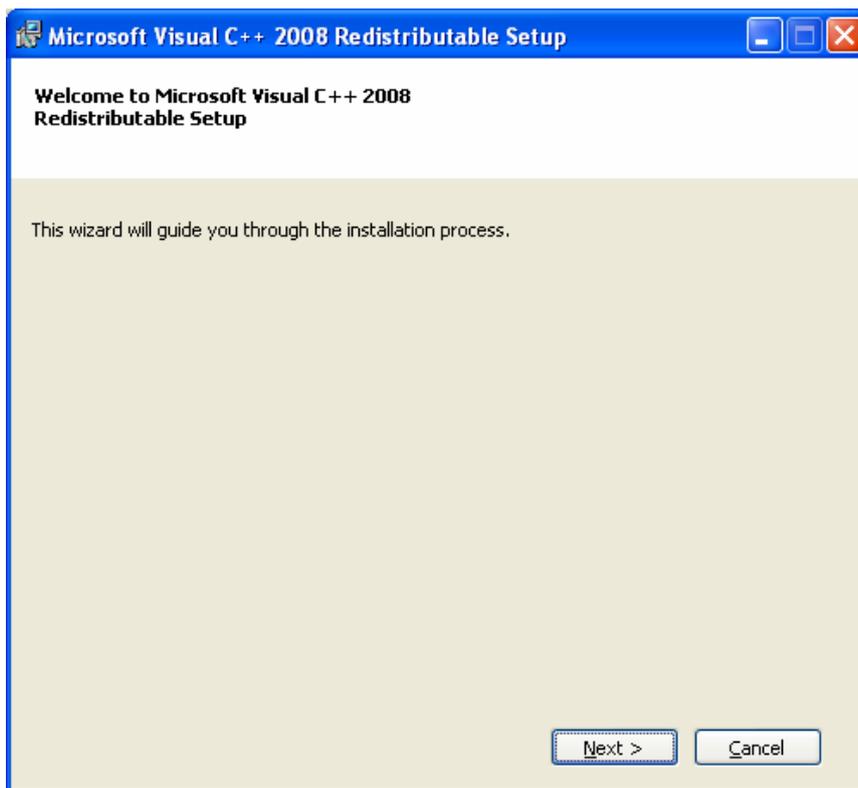


imagen 6

Hacer click en “Next” para continuar, así vemos la próxima ventana:

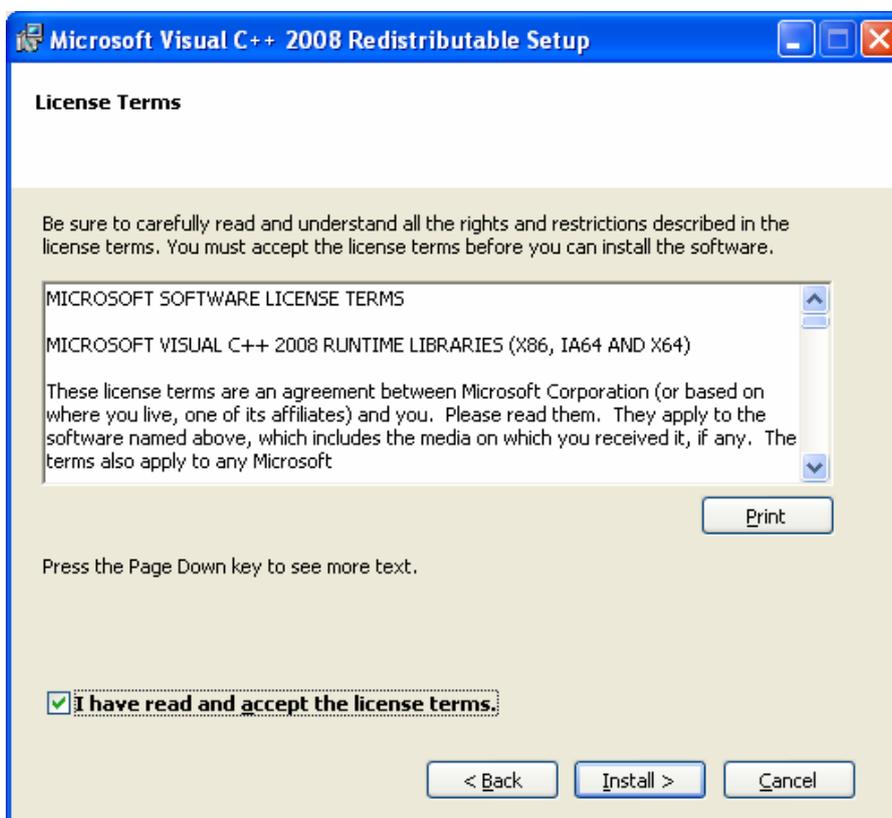


imagen 7

Tildar la casilla “I have read and accept the license terms” y hacer click en “Install”. Luego veremos la siguiente ventana:

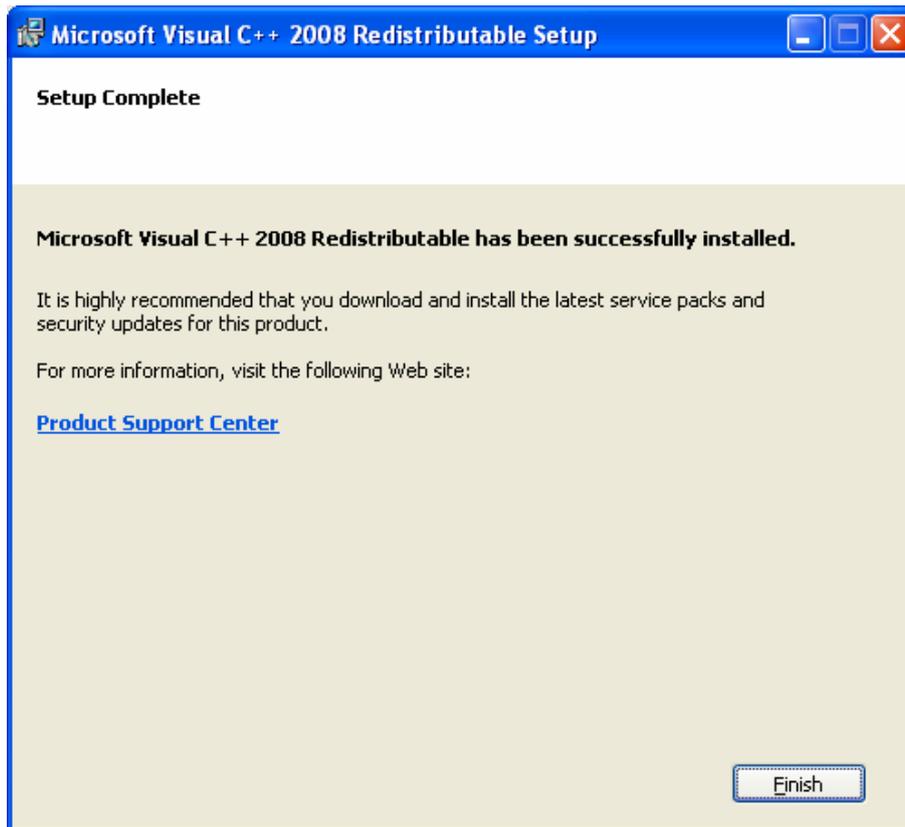


imagen 8

Hacer click en “Finish” para terminar la instalación.

## INSTALACION DEL OPENSLL

Para bajar e instalar OpenSSL para Windows. Un vínculo desde el cual se puede bajar directamente el OpenSSL es [http://www.nsis.com.ar/soft/Win32OpenSSL-0\\_9\\_8i.exe](http://www.nsis.com.ar/soft/Win32OpenSSL-0_9_8i.exe) , una vez ejecutado el vínculo, automáticamente vamos a ver la siguiente ventana:

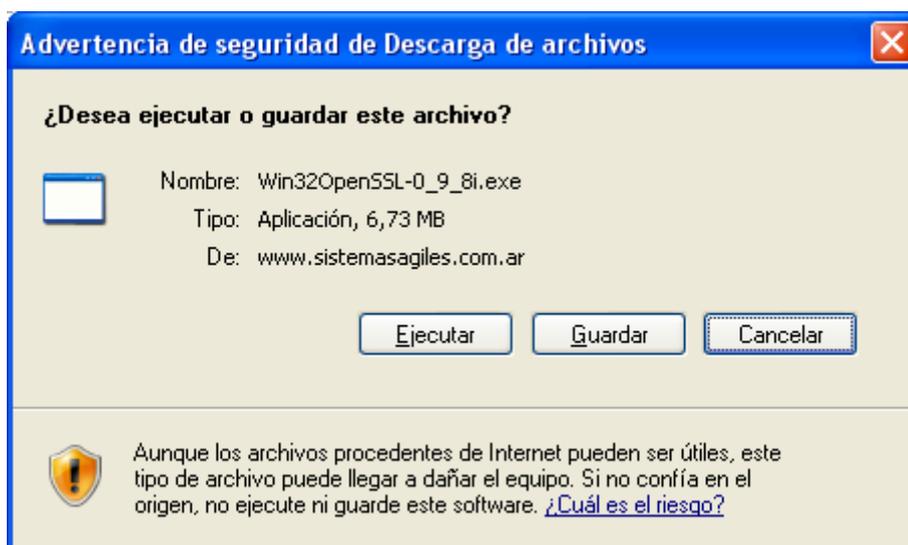


imagen 9

Hacer click en el botón “Guardar”, y elegir como destino alguna carpeta temporal de la PC, como se ve en el siguiente ejemplo (se usa TEMP), luego click nuevamente en el botón “Guardar”:

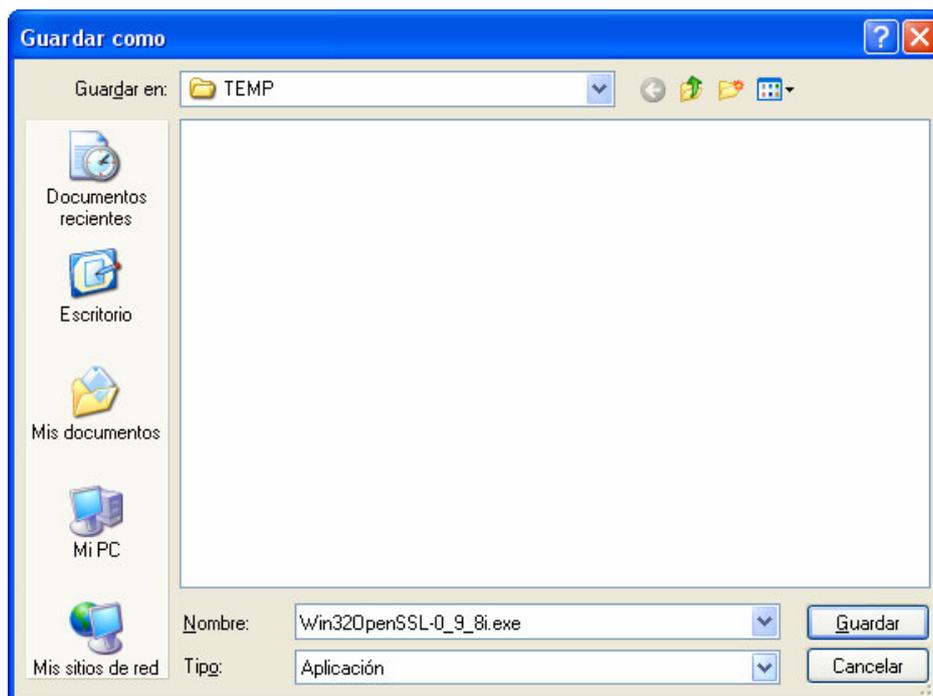


imagen 10

Abrir una ventana de “Mi PC”, ingresar a la carpeta temporal donde guardamos el archivo, y ejecutar con doble click el que tiene el nombre **Win32OpenSSL-0\_9\_8i.exe**

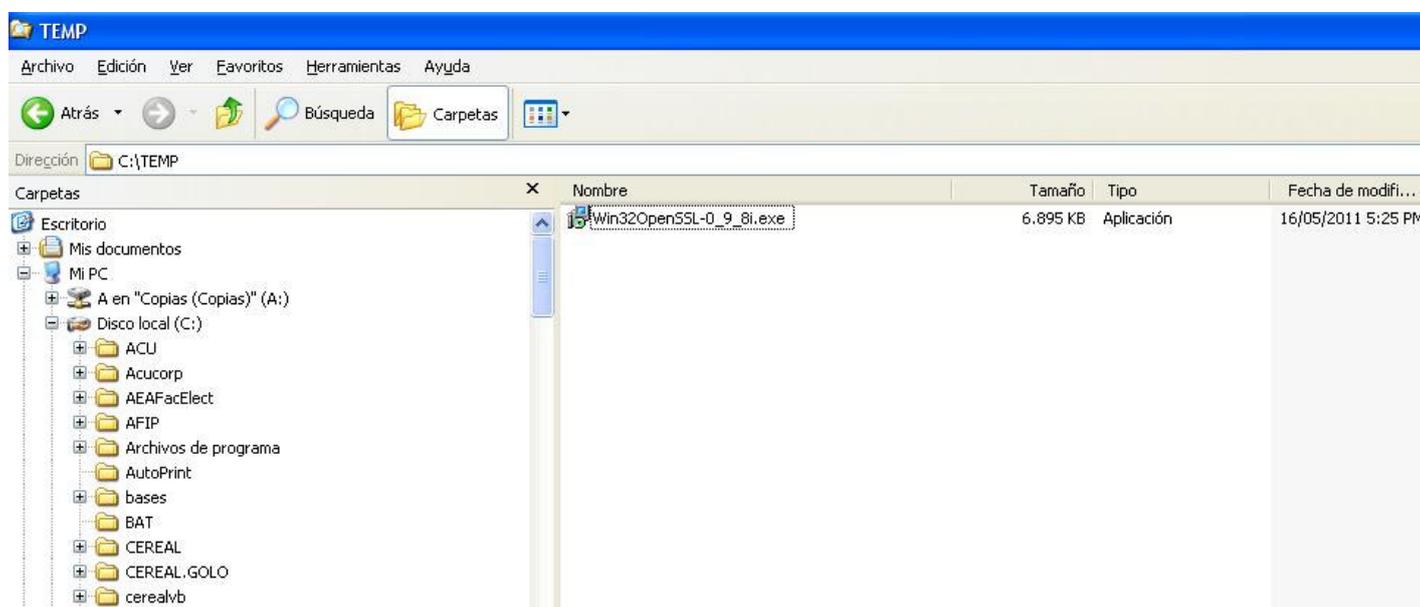


imagen 11

Al comenzar la instalación del OPENSSE, lo primero que podemos ver es la ventana de advertencia de Windows, si es así, hacer clic en el botón “ejecutar” y continuar con la instalación.

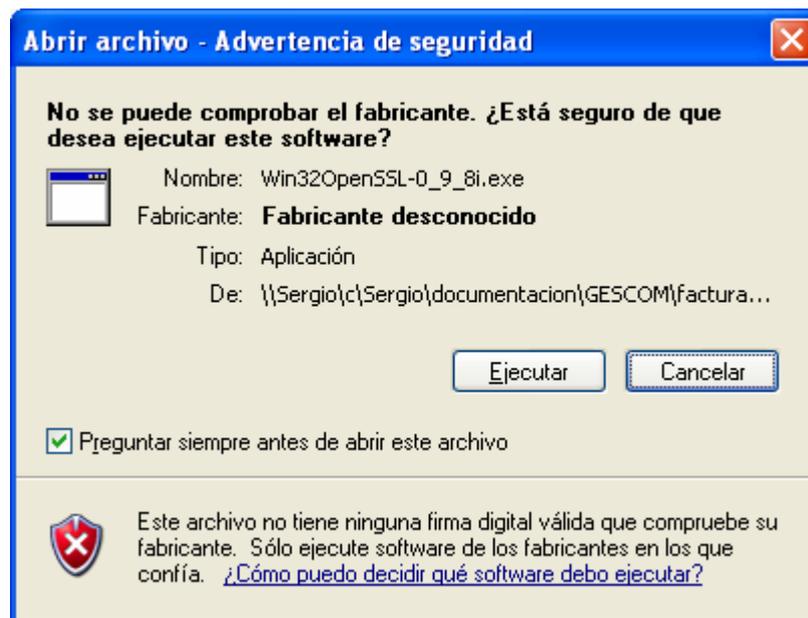


imagen 12

Luego vamos a observar la pantalla de presentación de la instalación del OPENSSL, como se ve a continuación:

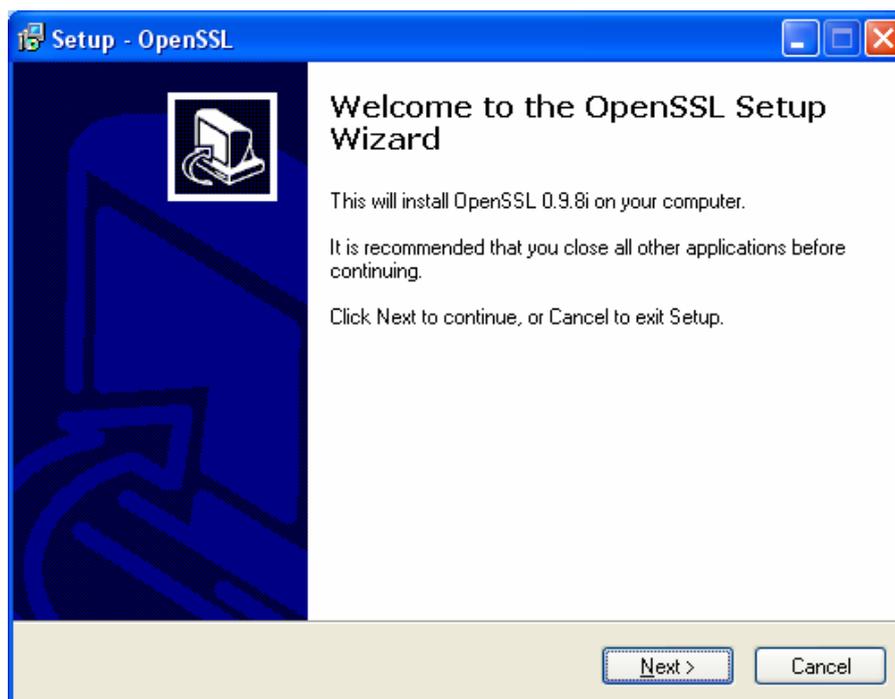


imagen 13

Al hacer click en el botón “Next”, aparece una ventana como la siguiente:

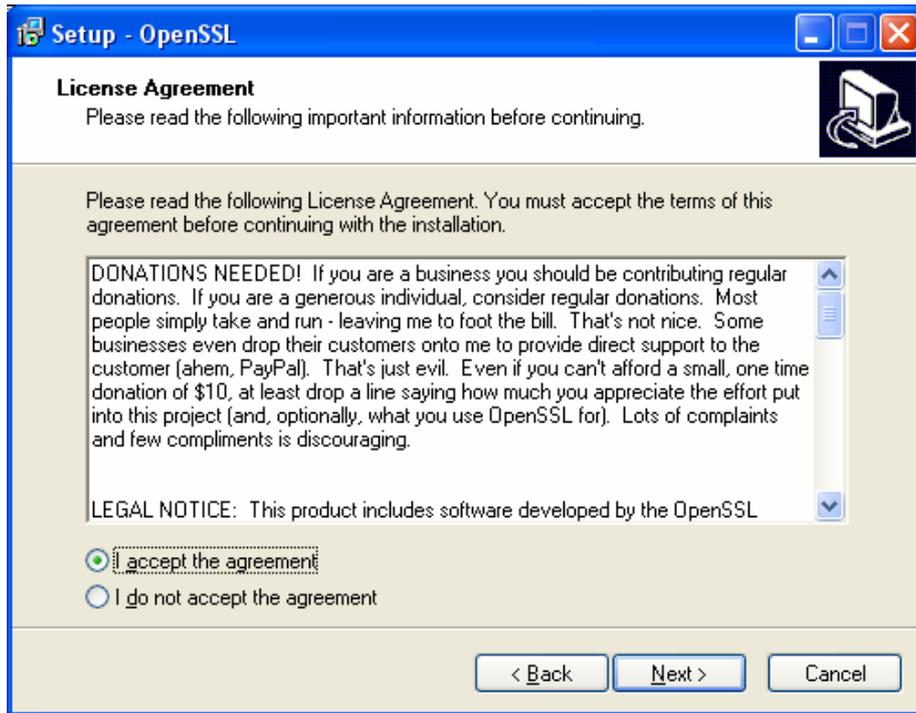


imagen 14

Tildar la opción “I accept the agreement” y hacer click nuevamente en el botón “Next” para ver la siguiente ventana:

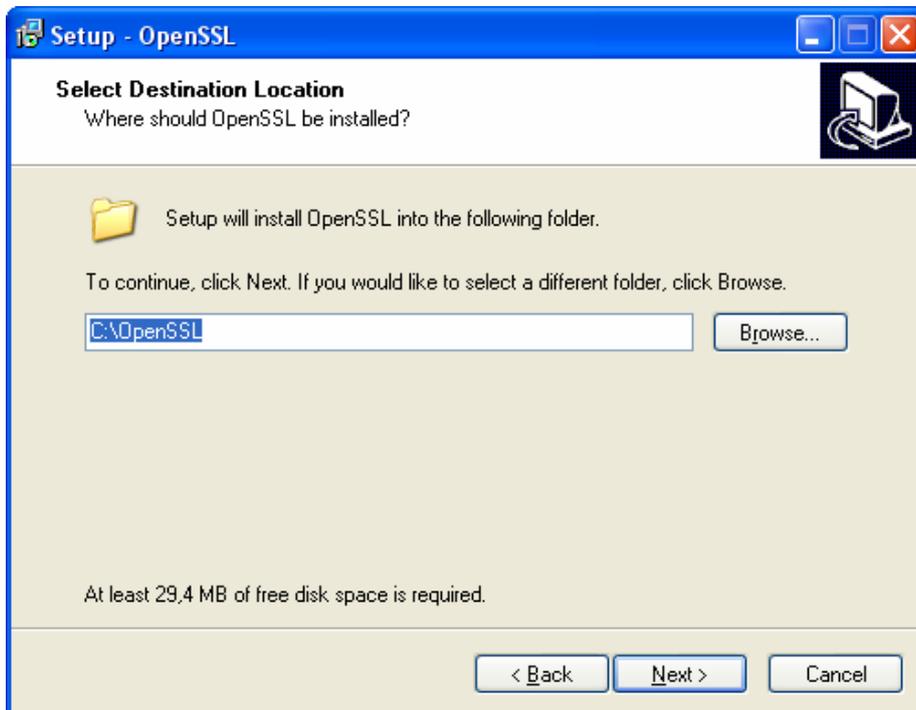


imagen 15

Dejar como carpeta destino para la instalación la que propone la ventana, y hacer click en el botón “Next”. Vemos la siguiente ventana:

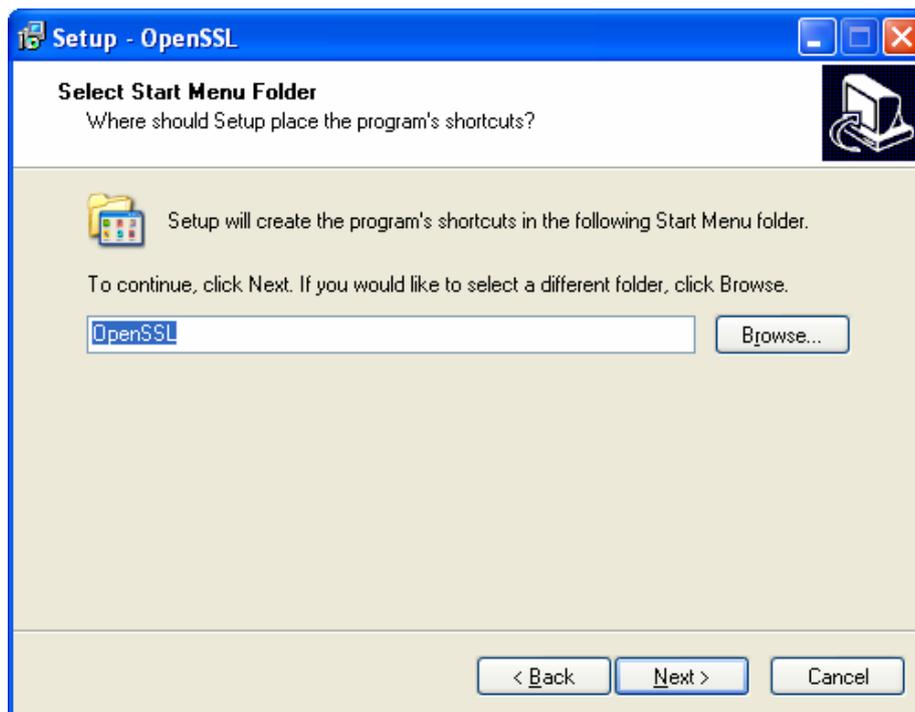


imagen 16

Dejar lo que propone y hacer click en “Next” para ver la siguiente ventana:

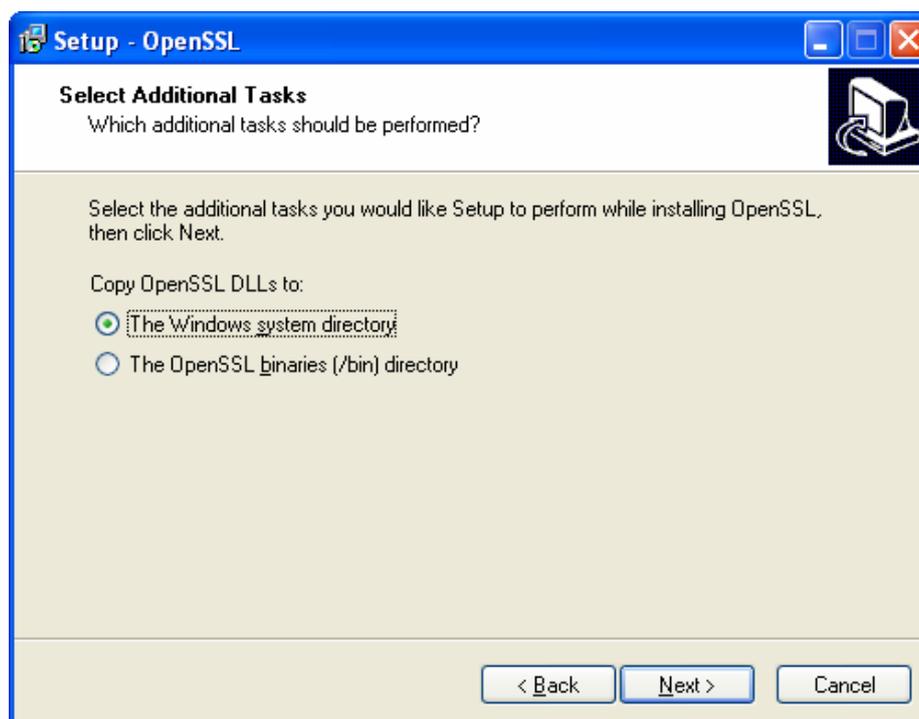


imagen 17

Dejar el valor que propone, es decir el tilde en “The Windows system directory”, hacer click en “Next” . Vamos a ver la última ventana de la instalación, que es una confirmación de todo lo seleccionado previamente:

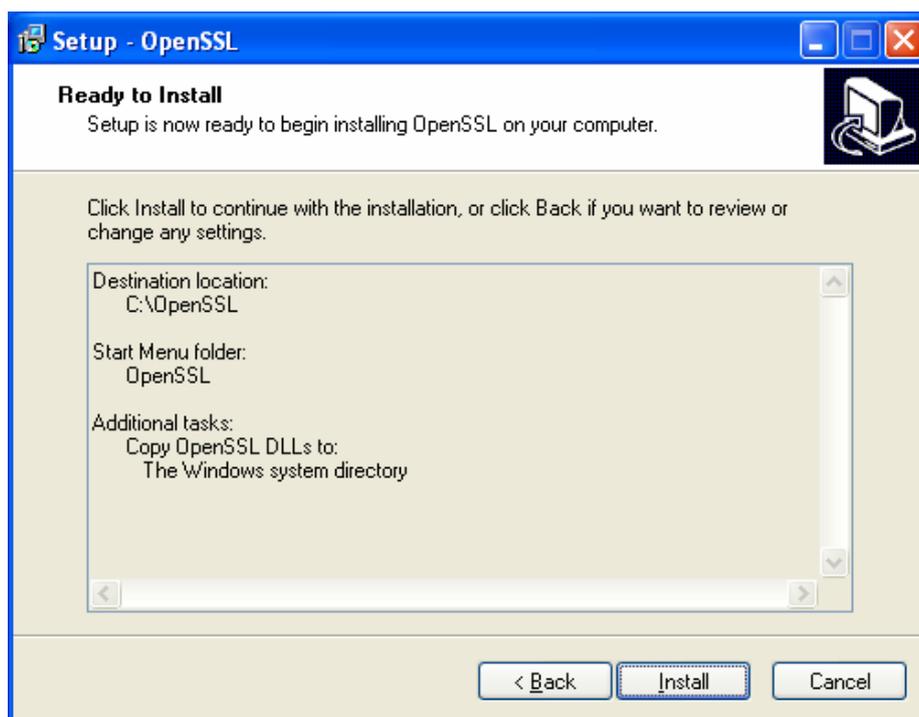


imagen 18

Hacer click en el botón “Install” para finalizar la instalación.

Si al finalizar aparece la siguiente ventana, asegurarse de destildar todas las opciones, como se ve en nuestro ejemplo:

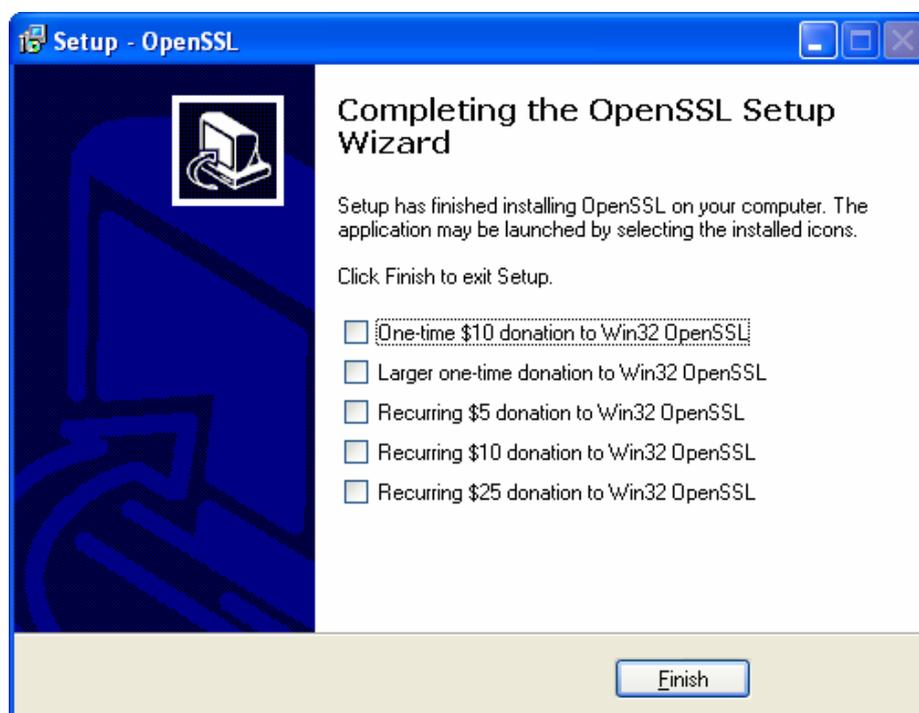


imagen 19

Luego hacer clic en “Finish” para completar el proceso.

## COMO GENERAR EL ARCHIVO .CSR

Una vez instalados los programas necesarios, el próximo paso será generar el certificado digital. Para tal fin, seguir las siguientes instrucciones:

- Ingresar por línea de comando (MSDOS) al directorio de OpenSSL C:\OpenSSL\bin>  
**Si es Windows 7 ingresar a “Símbolo del Sistema” ejecutándolo como Administrador.**
- Generar la clave privada con los siguientes comandos:

**set RANDFILE=.rnd (este se ejecuta solo si tienen windows 7,8 o 10  
para que no de el error “unable to write ‘random state’”)**

**Openssl genrsa -out privada.key 2048**

El comando crea un archivo en la carpeta \OPENSSL\BIN llamado privada.key

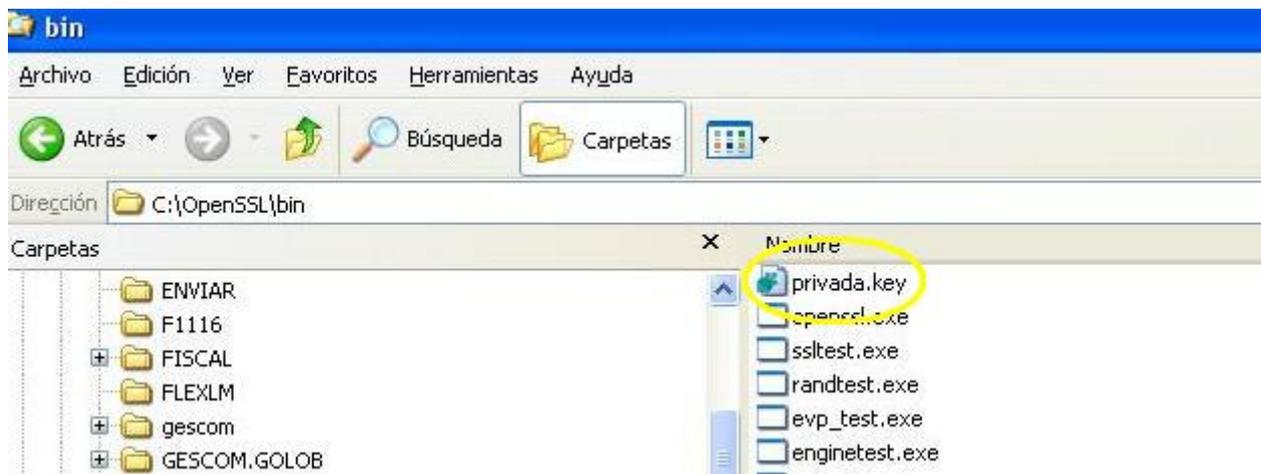


imagen 20

**OBS:** conviene hacer un respaldo del archivo generado que contiene la clave privada (archivo llamado **privada.key** que se encuentra en \OPENSSL\BIN) para evitar futuros inconvenientes, ya que será vital para los futuros pasos y no debe faltar.

- Editar con algún editor de texto estándar el archivo C:\OpenSSL\bin\openssl.cfg:

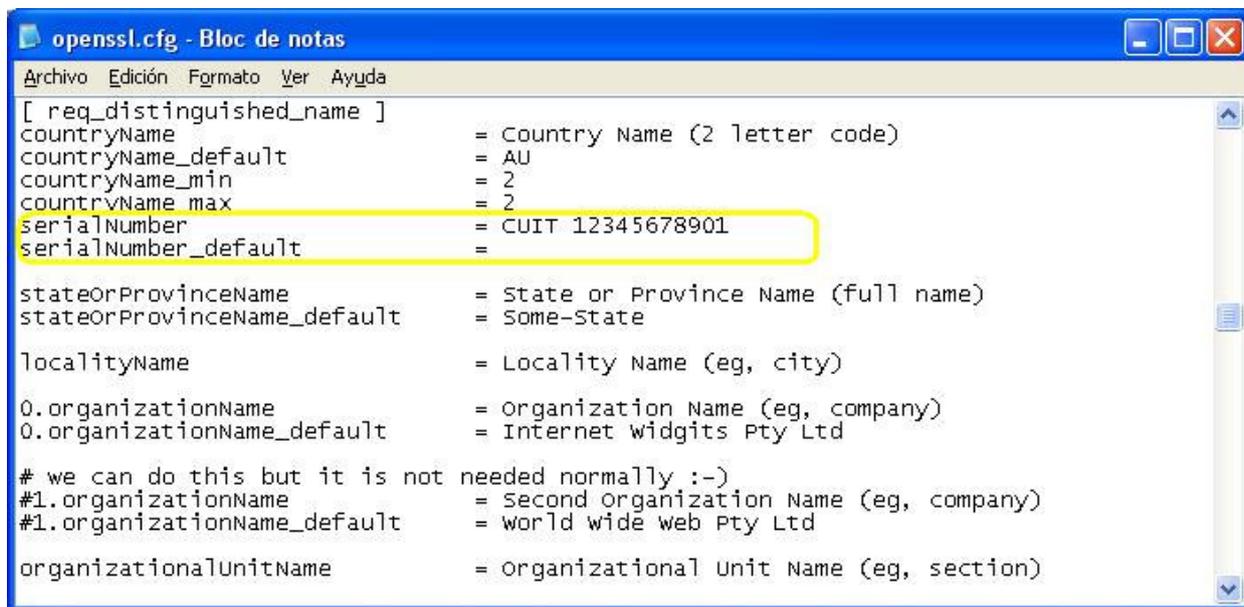
En la sección **[req\_distinguished\_name]** del archivo agregar/modificar las líneas:

**serialNumber = (Poner aquí la palabra CUIT seguido del numero de CUIT de la empresa)**

**serialNumber\_default =**

(OBS: Es importante que la primer letra de “serial” sea minúscula)

En la siguiente pantalla podemos ver un ejemplo de lo dicho:



```

openssl.cfg - Bloc de notas
Archivo Edición Formato Ver Ayuda
[ req_distinguished_name ]
CountryName           = Country Name (2 letter code)
CountryName_default   = AU
CountryName_min       = 2
CountryName_max       = 2
serialNumber          = CUIT 12345678901
serialNumber_default  =

stateOrProvinceName   = State or Province Name (full name)
stateOrProvinceName_default = Some-State

localityName          = Locality Name (eg, city)

0.organizationName    = Organization Name (eg, company)
0.organizationName_default = Internet Widgits Pty Ltd

# we can do this but it is not needed normally :-
#1.organizationName   = Second Organization Name (eg, company)
#1.organizationName_default = World wide Web Pty Ltd

organizationalUnitName = Organizational Unit Name (eg, section)

```

imagen 21

Guardar los cambios y cerrar el archivo.

- Generar el pedido (CSR: certificate signing request) ejecutando desde la línea de comando:

**openssl req -new -sha256 -key privada.key -out pedido.csr (despues del 1-11-2016)**

Al ejecutar el comando, nos va a solicitar por pantalla algunos datos. Los campos obligatorios son:

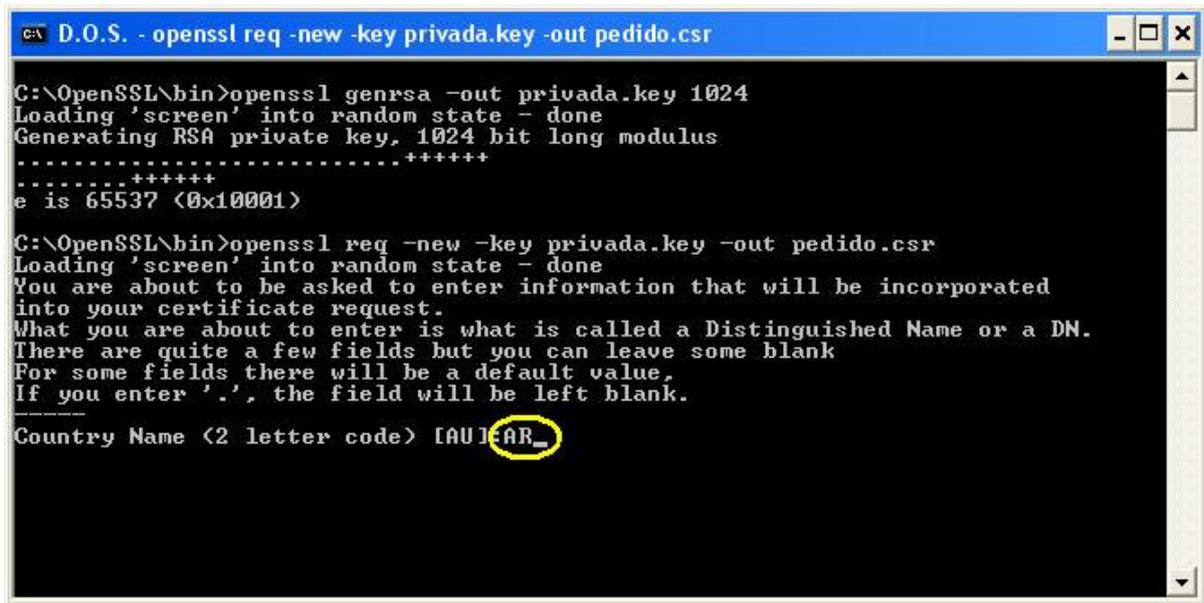
```

CountryName      (AR)
SerialNumber     (CUIT, sin guiones)
OrganizationName (Razon Social de la Empresa)
CommonName      (Persona o Sistema)

```

Veamos un ejemplo ejemplo (con el comando de antes del 1/11/2016, ver según fecha si corresponde el otro):

El primero que se pide es "Country Name (2 letter code) [AR]:" , allí tenemos que ingresar la sigla **AR** como se ve en la pantalla:



```
D.O.S. - openssl req -new -key privada.key -out pedido.csr

C:\OpenSSL\bin>openssl genrsa -out privada.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....+++++
.....+++++
e is 65537 (0x10001)

C:\OpenSSL\bin>openssl req -new -key privada.key -out pedido.csr
Loading 'screen' into random state - done
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]:AR
```

imagen 22

Luego, la aplicación solicita el número de CUIT, como se ve a continuación:



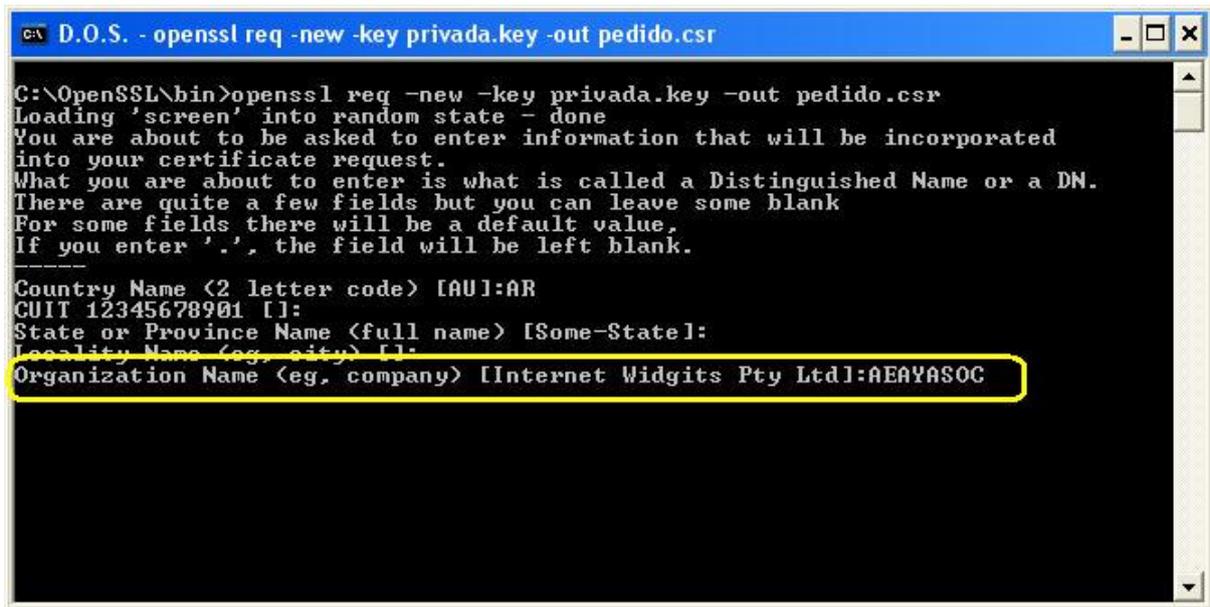
```
D.O.S. - openssl req -new -key privada.key -out pedido.csr

C:\OpenSSL\bin>openssl req -new -key privada.key -out pedido.csr
Loading 'screen' into random state - done
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]:AR
CUIT 12345678901 []:
```

imagen 23

Ingresar el número de CUIT sin guiones.

Los dos siguientes se pueden dejar en blanco. Luego pide el nombre de la empresa que es obligatorio, se ve en pantalla "Organization Name ...." . Debemos ingresar la razon social de la empresa tal cual figura en la consulta de inscripción en AFIP. Ejemplo:



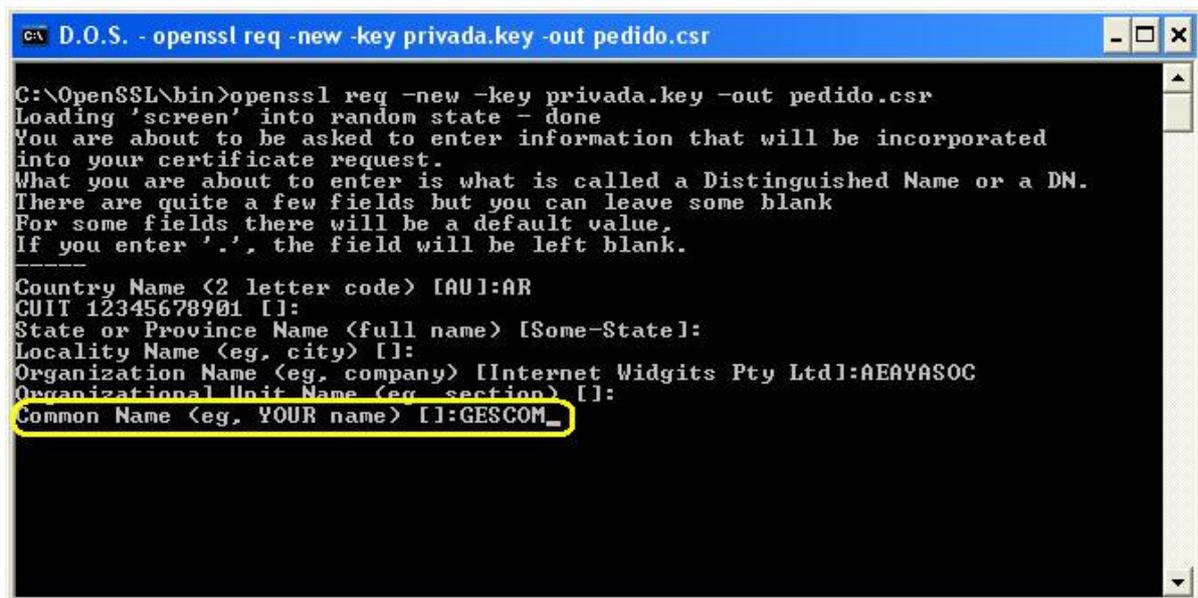
```

C:\OpenSSL\bin>openssl req -new -key privada.key -out pedido.csr
Loading 'screen' into random state - done
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]:AR
CUIT 12345678901 []:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:AEAYASOC

```

imagen 24

Luego se solicita el dato “Common Name ....” ingresar aquí el nombre del servicio, aplicación u unidad operativa, por ej: **GESCOM**



```

C:\OpenSSL\bin>openssl req -new -key privada.key -out pedido.csr
Loading 'screen' into random state - done
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]:AR
CUIT 12345678901 []:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:AEAYASOC
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:GESCOM_

```

imagen 25

Finalmente, se solicitan otros datos que nos son obligatorios, dejarlos en blanco, dar ENTER hasta que concluya el comando.

Una vez que haya generado correctamente su archivo .CSR, puede usarlo para obtener su certificado digital X.509.

Para el caso del entorno de Producción de podrá obtener el certificado interactivamente usando el servicio "Administración de Certificados Digitales" del menú de trámites con Clave Fiscal en el portal [www.afip.gob.ar](http://www.afip.gob.ar). (Para saber los pasos para obtener el certificado de la pagina de AFIP, ver **ANEXO I**)

Una vez autorizados a usar el WebServices de Negocio de AFIP, la empresa quedara registrada en el servicio de autorización de AFIP como entidad autorizada para usar el WebServices de Negocio.

## CONVERTIR EL CERTIFICADO .CRT EN .PFX

Una vez obtenido el certificado (PASO3), recibiremos de AFIP un archivo adjunto con extensión \*.crt. Este es el certificado a usar. Pero **ATENCIÓN** el certificado devuelto por AFIP es **extensión \*.crt** y el runtime de NET y el OCX esperan un **certificado extensión \*.pfx**. De lo contrario recibiremos un error de conexión similar a: "La contraseña de red especificada no es válida". o bien "la clave no existe".

Para poder usar el certificado es necesario convertirlo. A continuación se explican los pasos para convertirlo (primeramente debemos convertir el certificado \*.crt a la extensión \*.p12. y de esta extensión a \*.pfx)

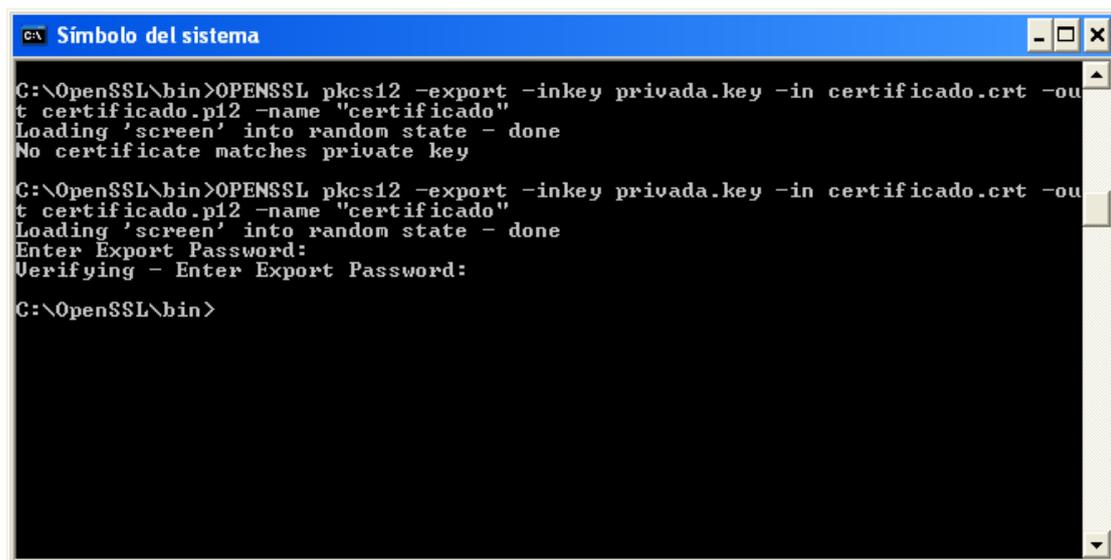
Para convertir el certificado del formato crt al formato p12 :

- Guardar el archivo \*.crt enviado por AFIP en la carpeta OPENSSL\BIN
- Ingresar por línea de comando (MSDOS) al directorio de OpenSSL C:\OpenSSL\bin>
- Ejecutar el siguiente comando:

```
openssl pkcs12 -export -inkey privada.key -in x.crt -out x.p12 -name "x"
```

Reemplazando las letras x (que estan en color rojo) por el nombre del certificado recibido de AFIP. Solo reemplazar las letras x, dejar comillas, guiones y puntos como están (**si al ejecutar el comando solicita una contraseña o clave no ingresar nada. pulsar Enter directamente**).

La pantalla sera similar a esta:



```

C:\OpenSSL\bin>OPENSSL pkcs12 -export -inkey privada.key -in certificado.crt -out
t certificado.p12 -name "certificado"
Loading 'screen' into random state - done
No certificate matches private key

C:\OpenSSL\bin>OPENSSL pkcs12 -export -inkey privada.key -in certificado.crt -ou
t certificado.p12 -name "certificado"
Loading 'screen' into random state - done
Enter Export Password:
Verifying - Enter Export Password:

C:\OpenSSL\bin>

```

imagen 26

(en este ejemplo nuestro archivo se llama **certificado.crt** pero puede tener otro nombre)

Esto nos dejará en la carpeta OPENSSL\BIN un archivo de extensión p12 como se ve en el siguiente ejemplo:

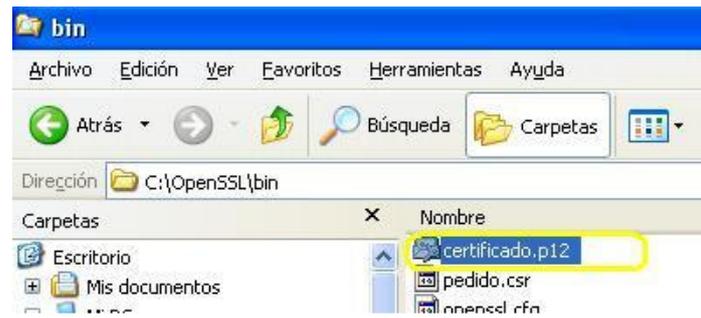


imagen 27

Este archivo de extensión p12 debemos convertirlo a extensión .pfx desde el panel de control.

Los pasos y las pantallas corresponden a Windows XP. En algunos Windows las pantallas son similares aunque en algunos casos (por configuración de permisos o por el control UAC) la conversión pide una contraseña. En estos casos seguir igualmente la guía pero creando una contraseña.

- Ir a Panel de Control.
- Ir a Opciones de Internet.

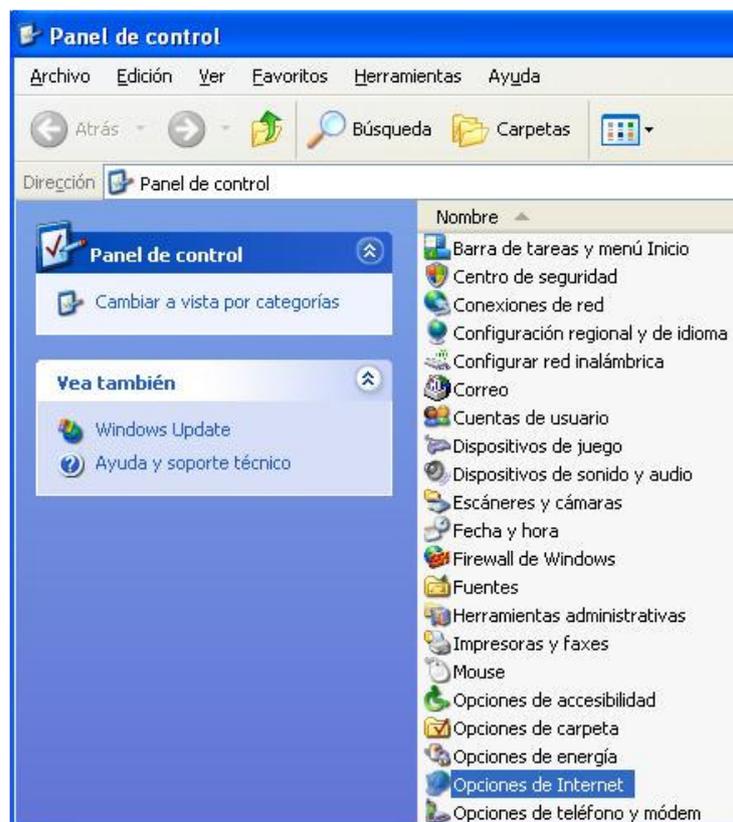


imagen 28

- Ir a solapa "contenido"
- Seleccionar el botón "certificados"

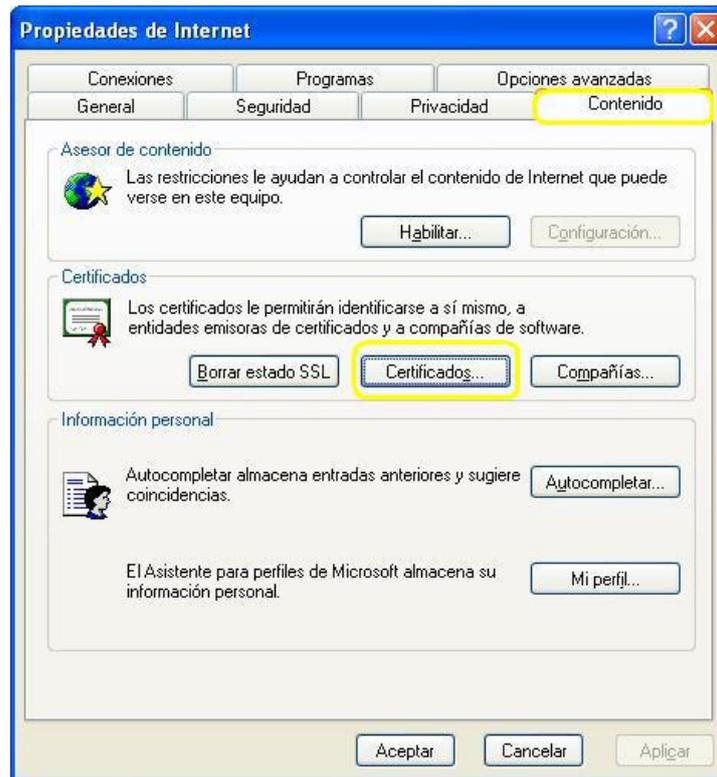


imagen 29

- Ir a solapa "personal" (la primera).
- Seleccionar el botón "importar".

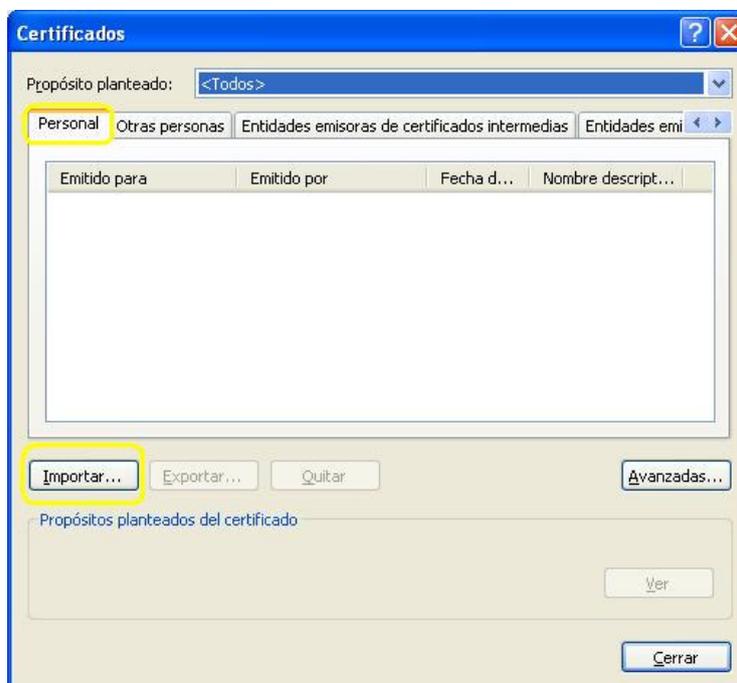


imagen 30

- En la pantalla del asistente seleccionar "siguiente". Nos pedirá donde está el archivo \*.p12 para convertir a \*.pfx. Seleccionar el botón "examinar". Antes de navegar hasta la carpeta donde está el archivo \*.p12 (generalmente c:\openssl\bin) indicar en "tipo de archivo" que estamos buscando un archivo \*.p12 como muestra esta pantalla:



imagen 31

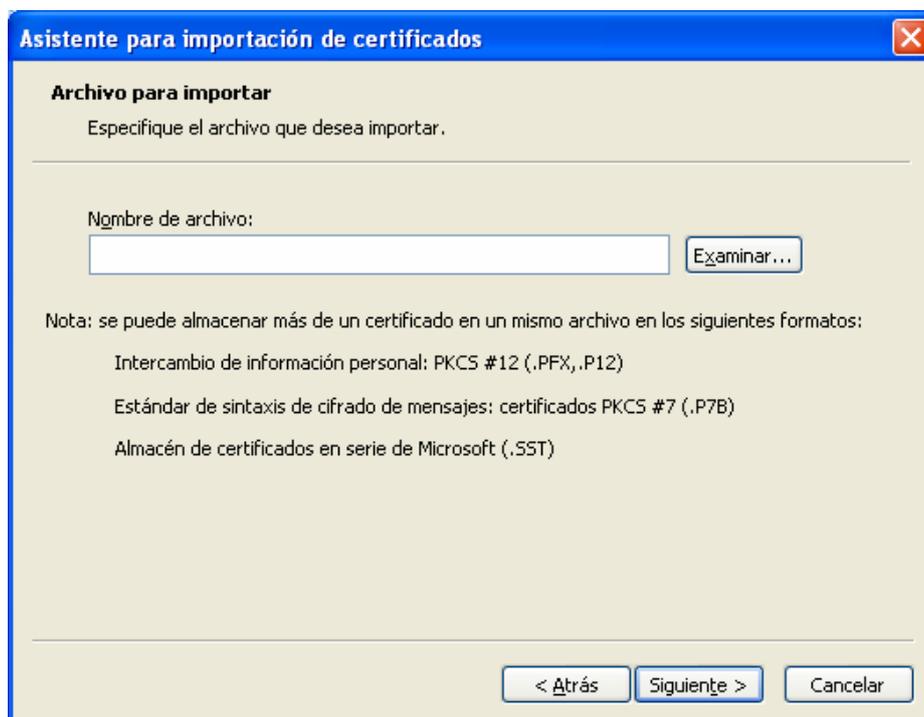


imagen 32

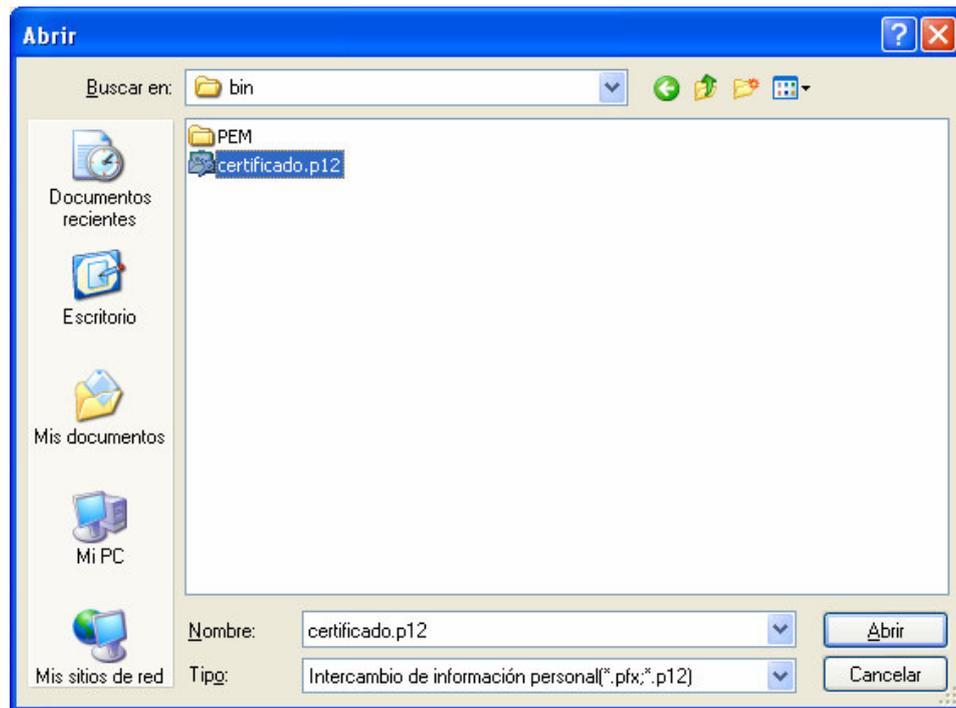


imagen 33

- Seleccionar el archivo \*.p12 y aceptar (en nuestro ejemplo es certificado.p12).
- En el asistente seleccionar "siguiente".

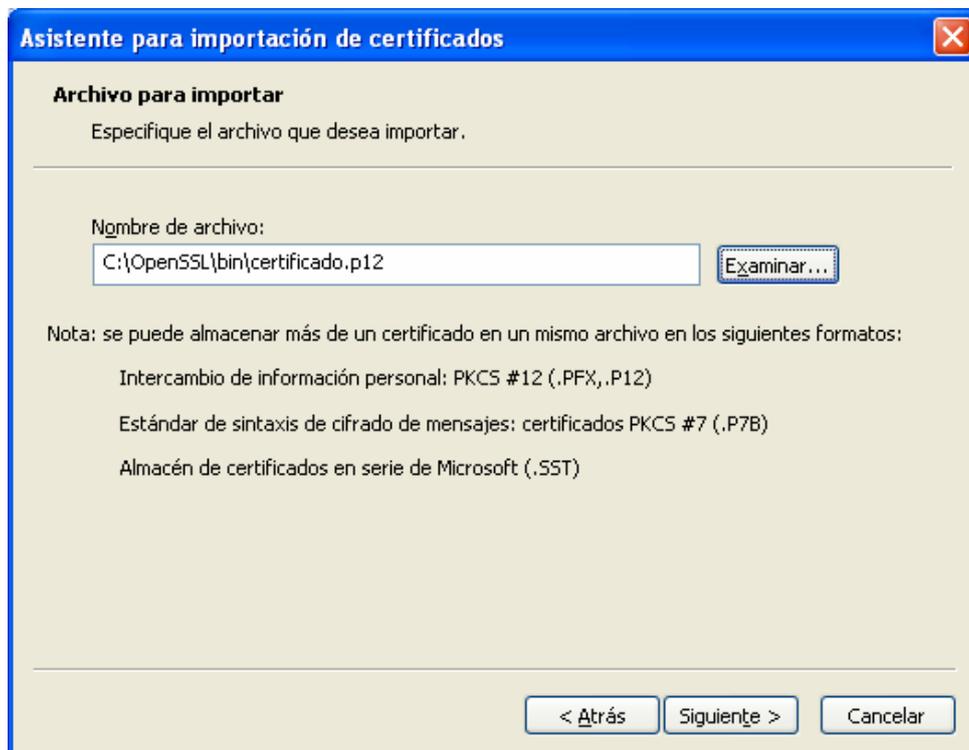


imagen 34

- Nos pedirá una contraseña. No colocar nada (excepto que específicamente se quiera proteger el archivo de certificados con una contraseña o el propio Windows obligue a hacerlo, en este caso, crear una contraseña y marca como exportable. Debe quedar algo como esto:

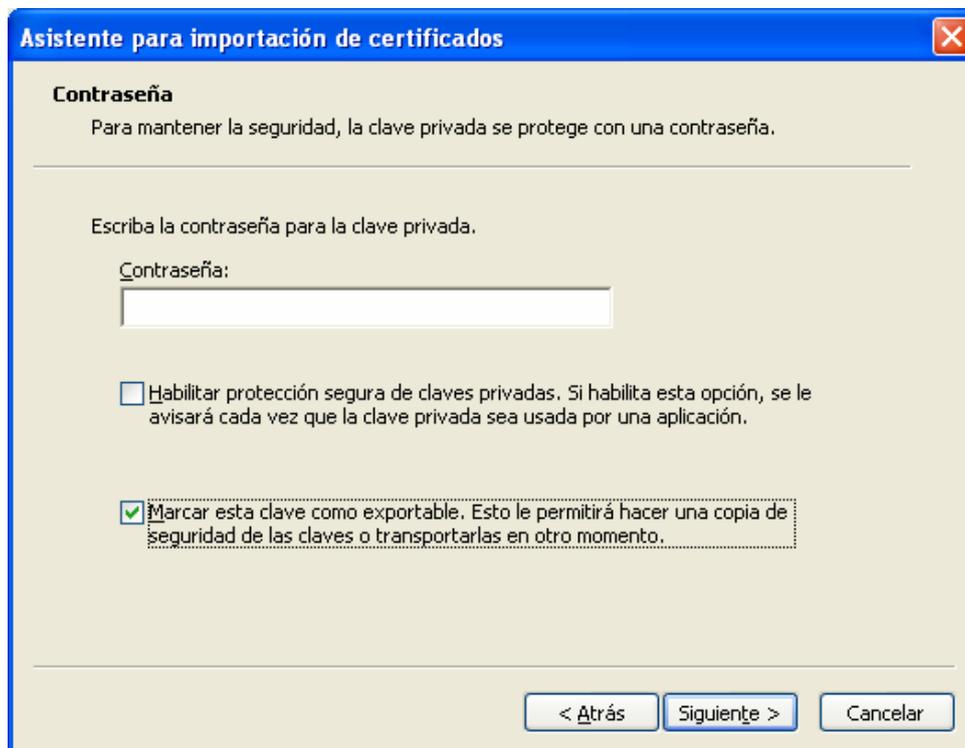


imagen 35

- Seleccionar "siguiente". Nos pedirá en que lugar se guarda el certificado. Dejarlo en "personal" y seleccionar "siguiente".

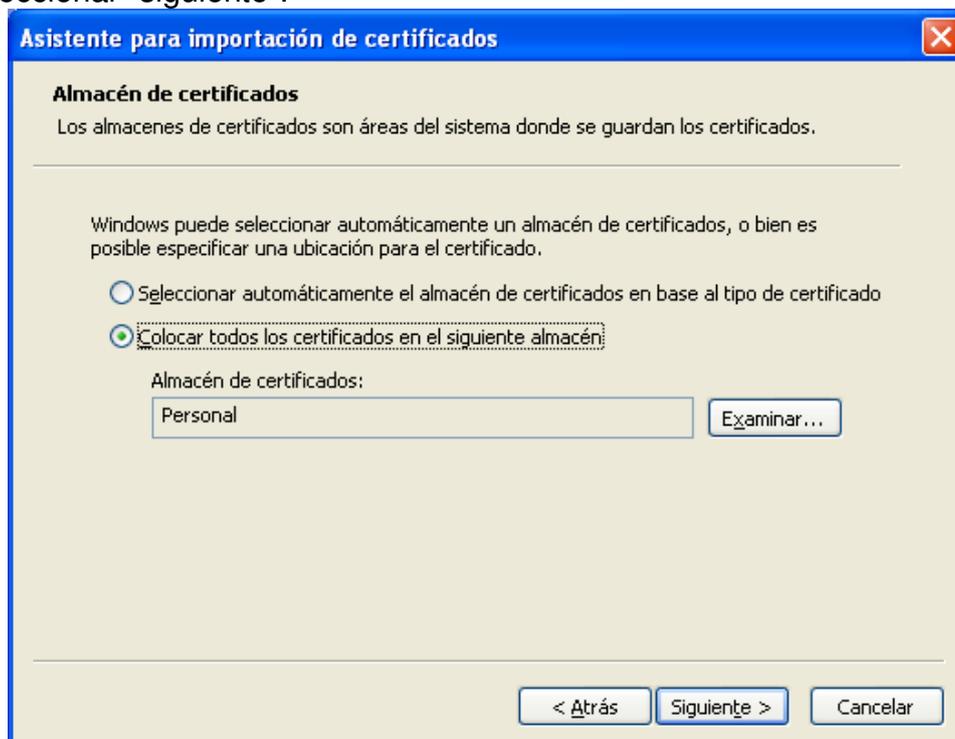


imagen 36

- Luego seleccionar "Finalizar". Windows muestra el mensaje de importación correcta.

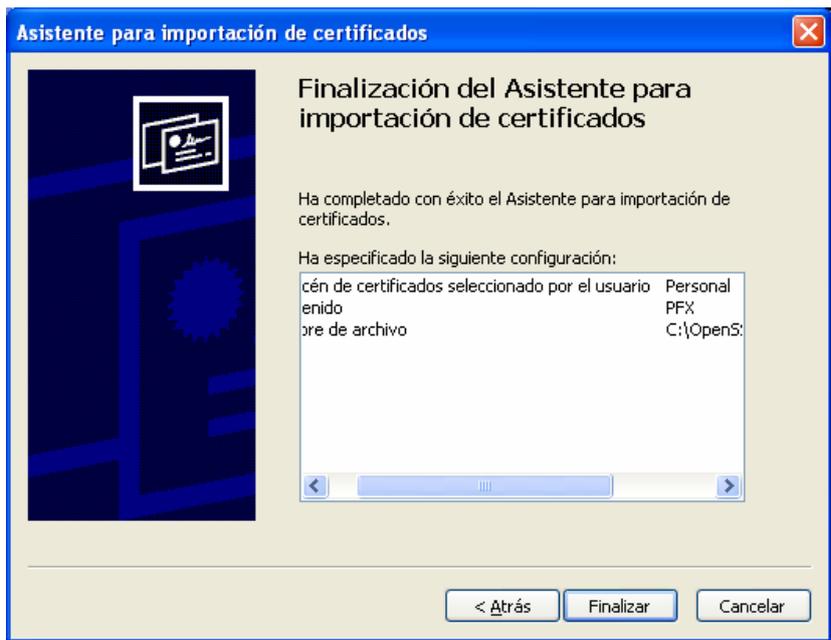


imagen 37



imagen 38

- Luego de Aceptar el mensaje, debe quedar algo como esto:

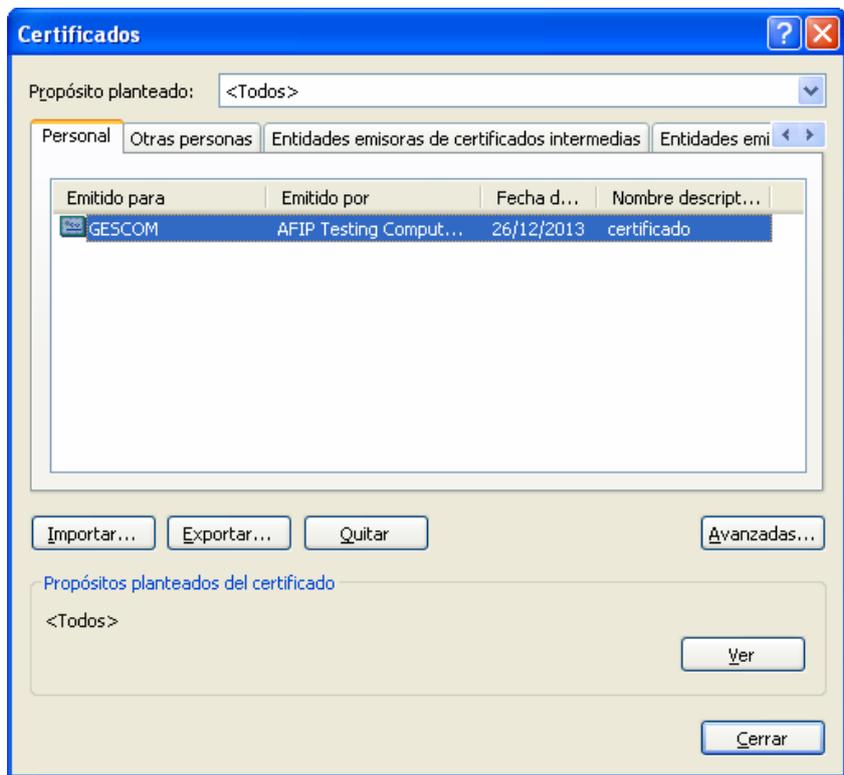


imagen 39

- En esta pantalla seleccionar el botón "exportar". Aparece el asistente.



imagen 40

- En el asistente seleccionar "siguiente".
- Elegir "exportar la clave privada". Debe quedar como esto:



imagen 41

- Seleccionar "siguiente".
- En la pantalla que aparece dejar las opciones como están.

En algunos Windows puede coincidir con esta pantalla:



imagen 42

En otros Windows la pantalla puede ser como la siguiente (dejar tildadas las opciones que se muestran):

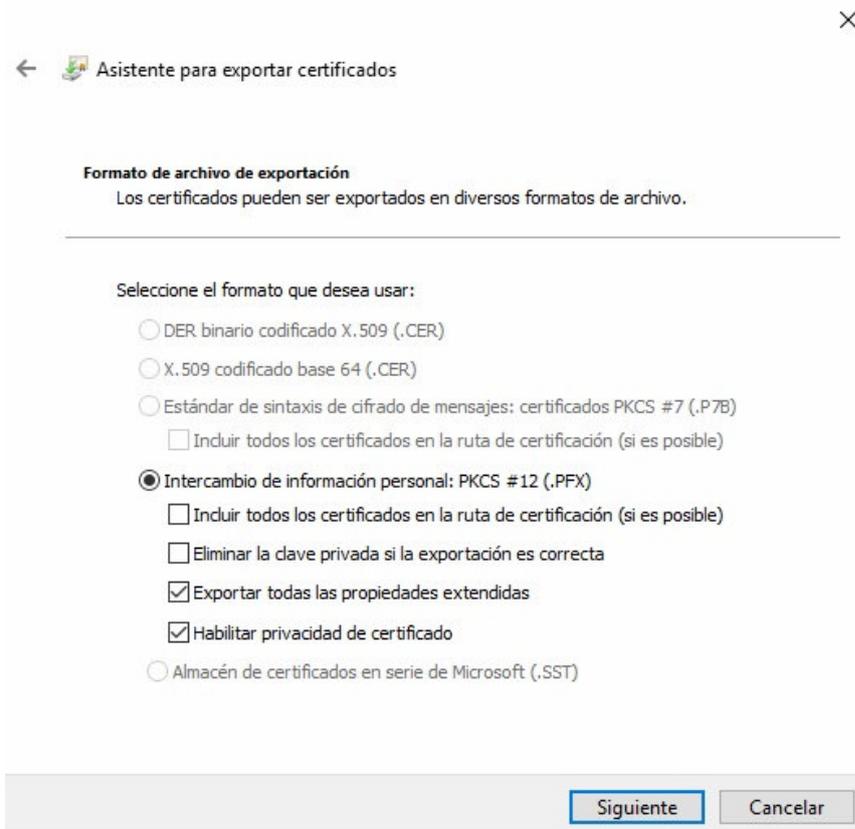


imagen 43

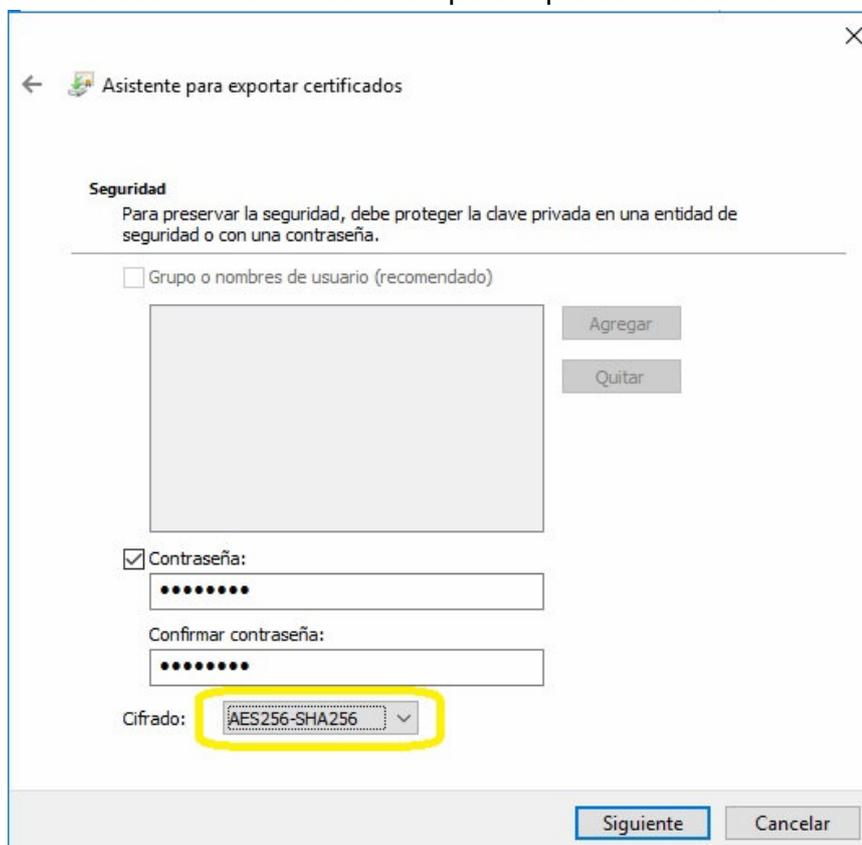
- Seleccionar "siguiente". Nos pedirá contraseña. no colocar nada salvo que el Windows no nos permita continuar, en ese caso colocar **aeayasoc**.



The screenshot shows a Windows dialog box titled "Asistente para exportación de certificados". The "Contraseña" (Password) section is active. It contains the following text: "Para mantener la seguridad, debe proteger la clave privada por medio de una contraseña." Below this, it says "Escriba y confirme una contraseña." There are two input fields: "Contraseña:" and "Confirmar contraseña:". At the bottom, there are three buttons: "< Atrás", "Siguiente >", and "Cancelar".

imagen 44

En algunos Windows la ventana puede ser como la que se muestra a continuación. En ese caso seleccionar en el cuadro de "cifrado" la opción que se muestra en la imagen.



The screenshot shows a Windows dialog box titled "Asistente para exportar certificados". The "Seguridad" (Security) section is active. It contains the following text: "Para preservar la seguridad, debe proteger la clave privada en una entidad de seguridad o con una contraseña." Below this, there is a checkbox for "Grupo o nombres de usuario (recomendado)". There is a large empty box for selecting a security entity, with "Agregar" and "Quitar" buttons. Below that, there is a checked checkbox for "Contraseña:" with two input fields for "Contraseña:" and "Confirmar contraseña:". At the bottom, there is a "Cifrado:" dropdown menu with "AES256-SHA256" selected and highlighted with a yellow box. At the bottom right, there are "Siguiente" and "Cancelar" buttons.

imagen 45

- Seleccionar "siguiente". Nos pedirá donde guardar el archivo (debemos ingresar el nombre del archivo) \*.pfx. en la carpeta que lo guardemos (por ejemplo c:\OPENSSL\BIN\certificado.pfx).

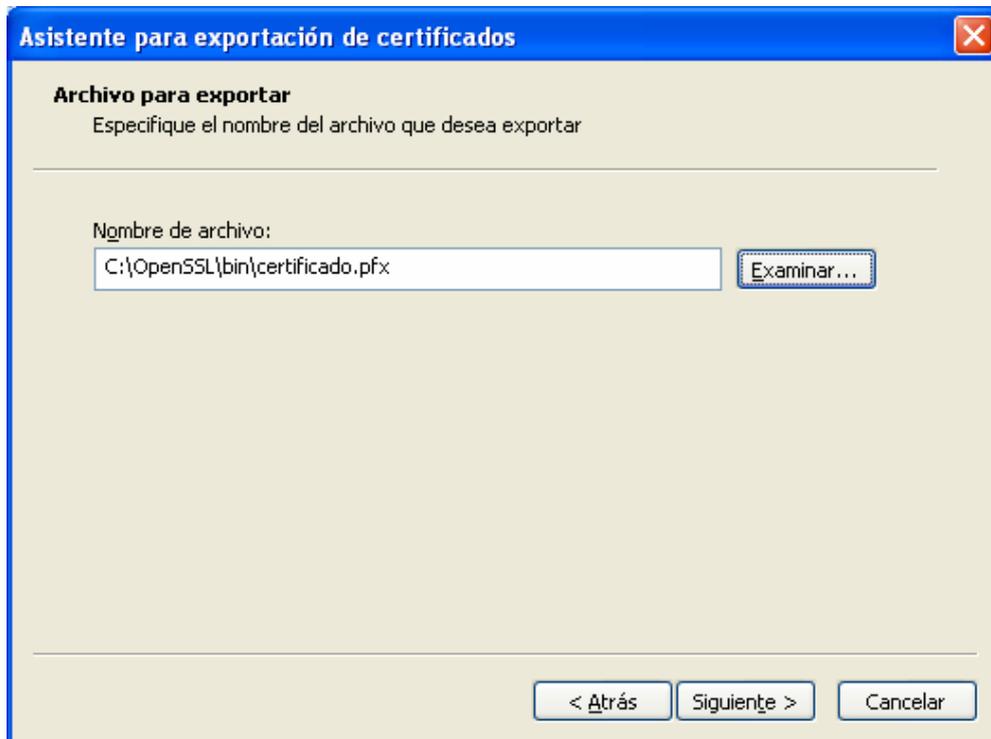


imagen 46

- Finalmente vemos la pantalla del asistente. Seleccionar "Finalizar":



imagen 47

- Vamos a ver el siguiente mensaje, y con esto concluye la exportación:



imagen 48

- Al volver a la pantalla de CERTIFICADOS, seleccionar “Cerrar”.

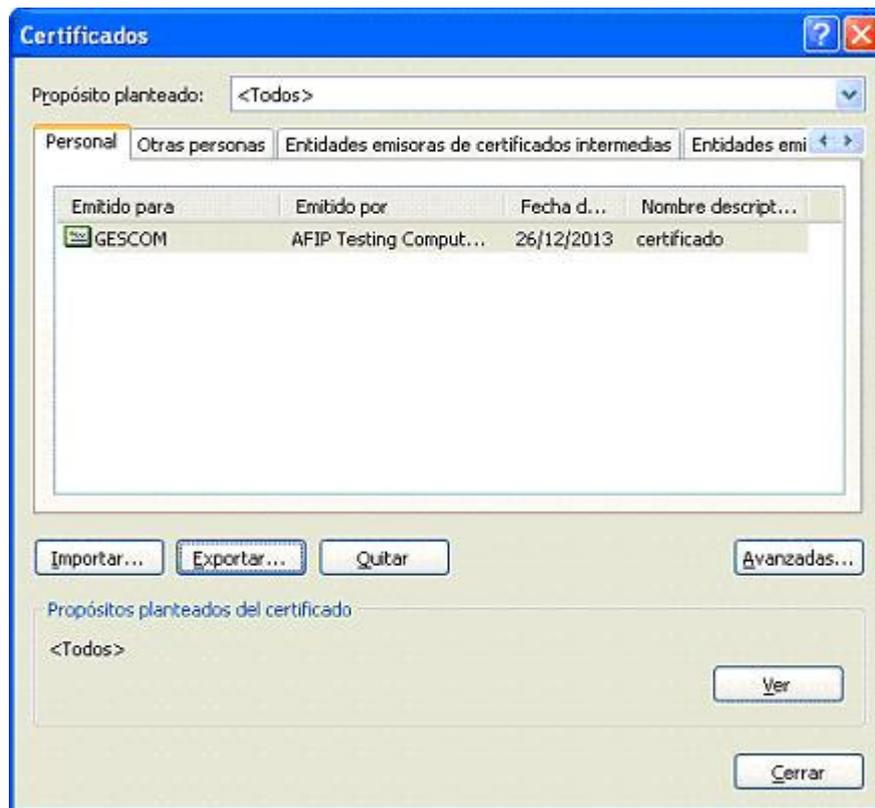


imagen 49

En caso de inconvenientes, los servidores de la AFIP responderán con un mensaje que identifica el problema:

- ns1:coe.notAuthorized Computador no autorizado a acceder los servicios de AFIP: el certificado no es válido o no está correctamente asociado al ambiente en el cual se intenta usar (ej. certificado de homologación usado en producción). Revisar el proceso de generación y asociación del certificado.
- ns1:cms.cert.expired Certificado expirado: los certificados poseen una fecha de vencimiento que varía según el ambiente para el cual fueron creados y la fecha de emisión. Generar y asociar nuevamente el certificado.

OBS: Sincronización de Clocks: La fecha y hora del computador que se comunica con los servicios Web de AFIP deberá estar sincronizada. Dicha sincronización se podrá realizar a través del protocolo NTP con el servidor “time.afip.gov.ar” u otro servidor que preste dicho servicio.

## ANEXO I – SOLICITAR Y OBTENER CERTIFICADO DIGITAL DE AFIP PARA FACTURACIÓN ELECTRÓNICA EN MODO PRODUCCIÓN (REAL)

Este documento describe el procedimiento para habilitar el consumo de Servicio Web de la AFIP, particularmente los correspondientes al servicio de Factura Electrónica (WSFE).

Para poder llevar a cabo este procedimiento, tanto la empresa que operará el Servicio Web como la empresa que facturará, deberán gestionar la obtención de una **Clave Fiscal de Nivel 3**, cuyo trámite deberá realizarse en una agencia de AFIP.

El siguiente Anexo tiene como objetivo mostrar los distintos pasos para la obtención de un certificado digital válido solamente para el entorno de producción.

### PASO 1: INGRESO A LA PAGINA DE AFIP

Ingresar al portal de AFIP ([www.afip.gov.ar](http://www.afip.gov.ar)) y presionar el botón < ir > sin completar ningún dato:



imagen 50

Se abre una nueva ventana con la página de acceso. Ingresar su “CUIT / CUIL / CDI” y “clave” y seleccionar “INGRESAR”:

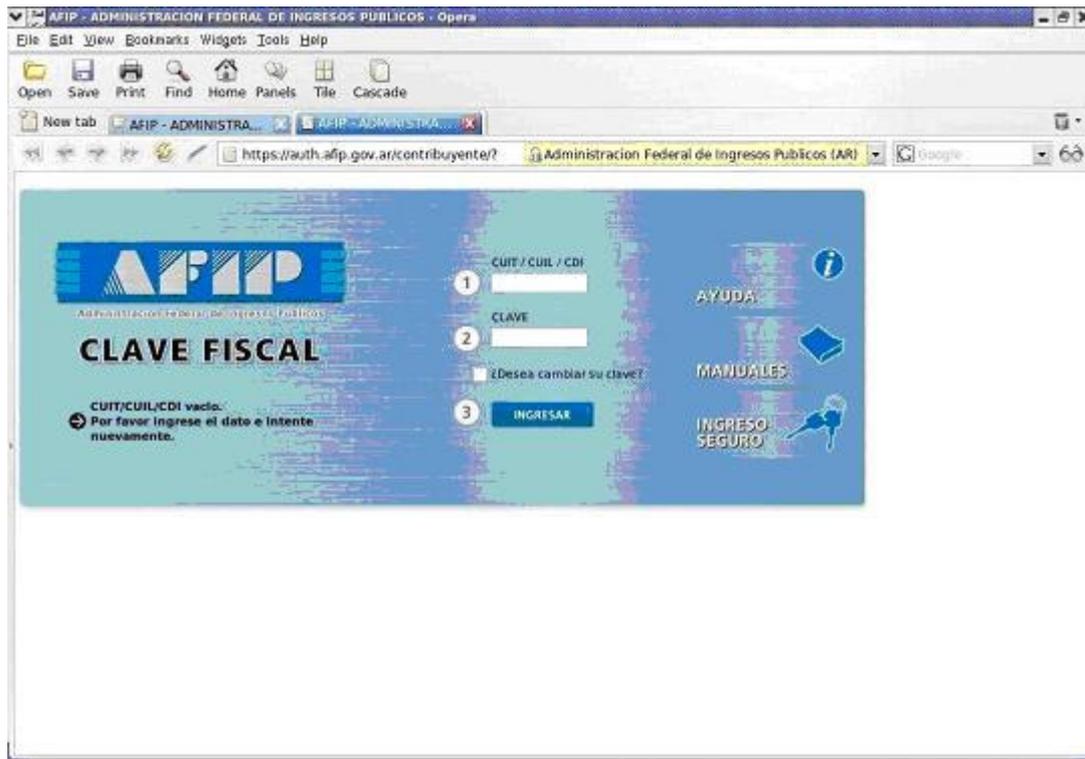


imagen 51

## PASO 2: HABILITAR “ADMINISTRACIÓN DE CERTIFICADOS DIGITALES”

Luego en la siguiente lista de servicios seleccionar:

- Si está habilitado, seleccionar el servicio “Administración de Certificados Digitales”.
- Si el servicio “Administración de Certificados Digitales” no está habilitado, se debe seleccionar el servicio “Administrador de Relaciones de Clave Fiscal” (para poder habilitarlo).



imagen 52

Si la opción es b) para poder habilitar el servicio “Administración de Certificados Digitales” se debe realizar lo siguiente:

- Clickear en “Nueva Relacion”:

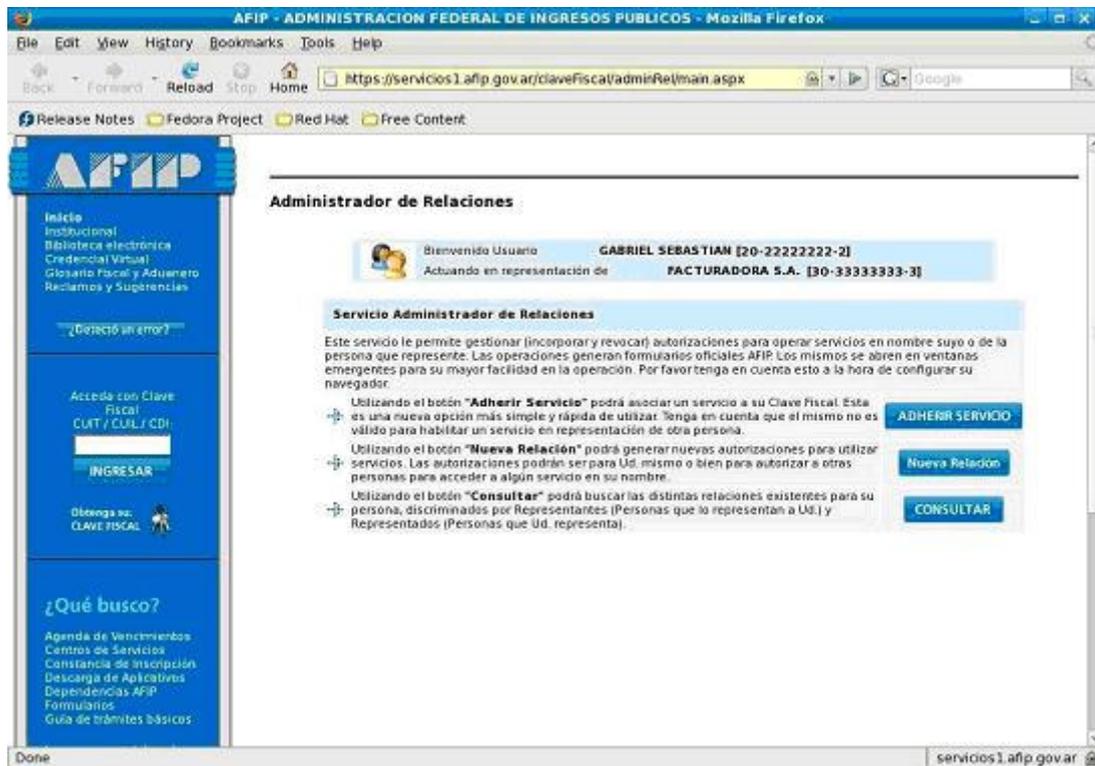


imagen 53

- Clickear en “BUSCAR” para seleccionar el servicio:

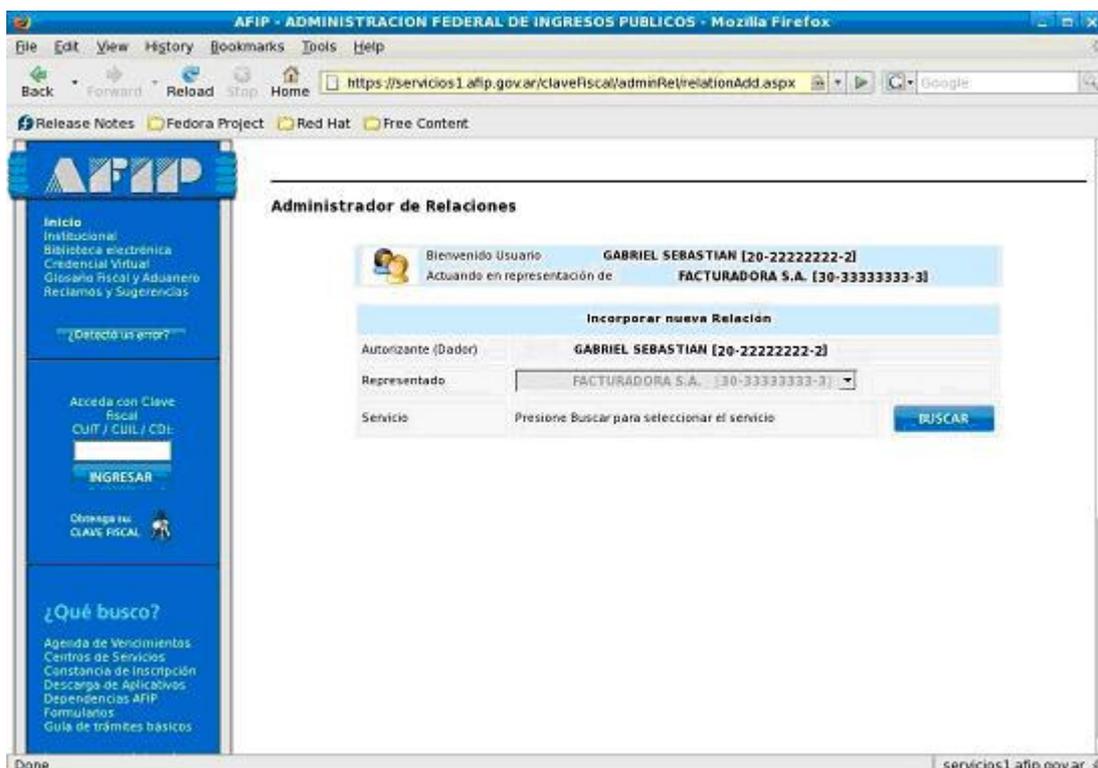


imagen 54

- Seleccionar el servicio “Administración de Certificados Digitales”:

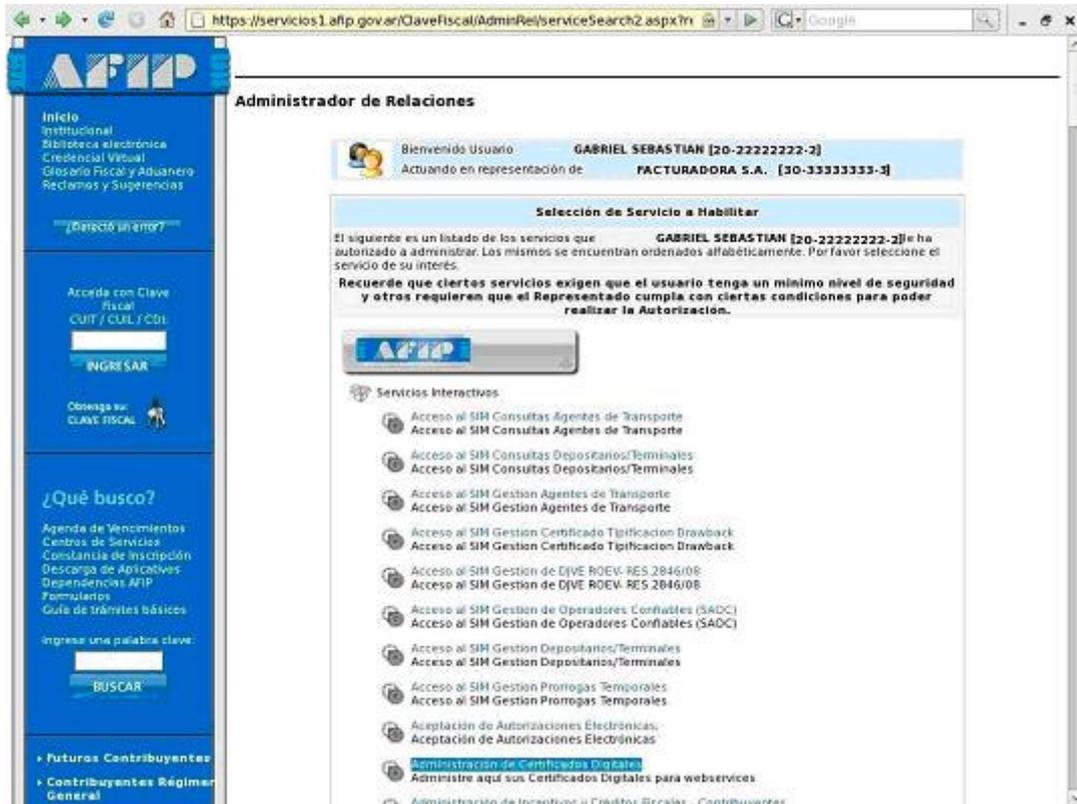


imagen 55

- Clickear en “BUSCAR” para seleccionar el Representante:

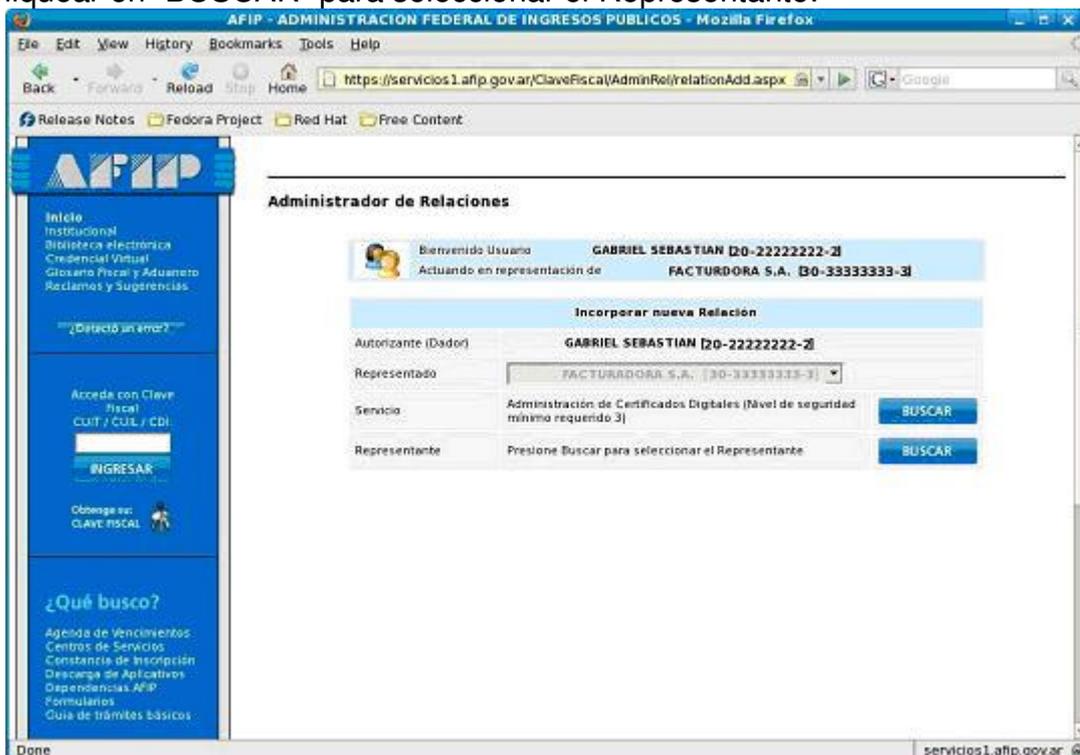


imagen 56

- Ingresar CUIT/CUIL/CDI del Representante y clicar en “BUSCAR”:

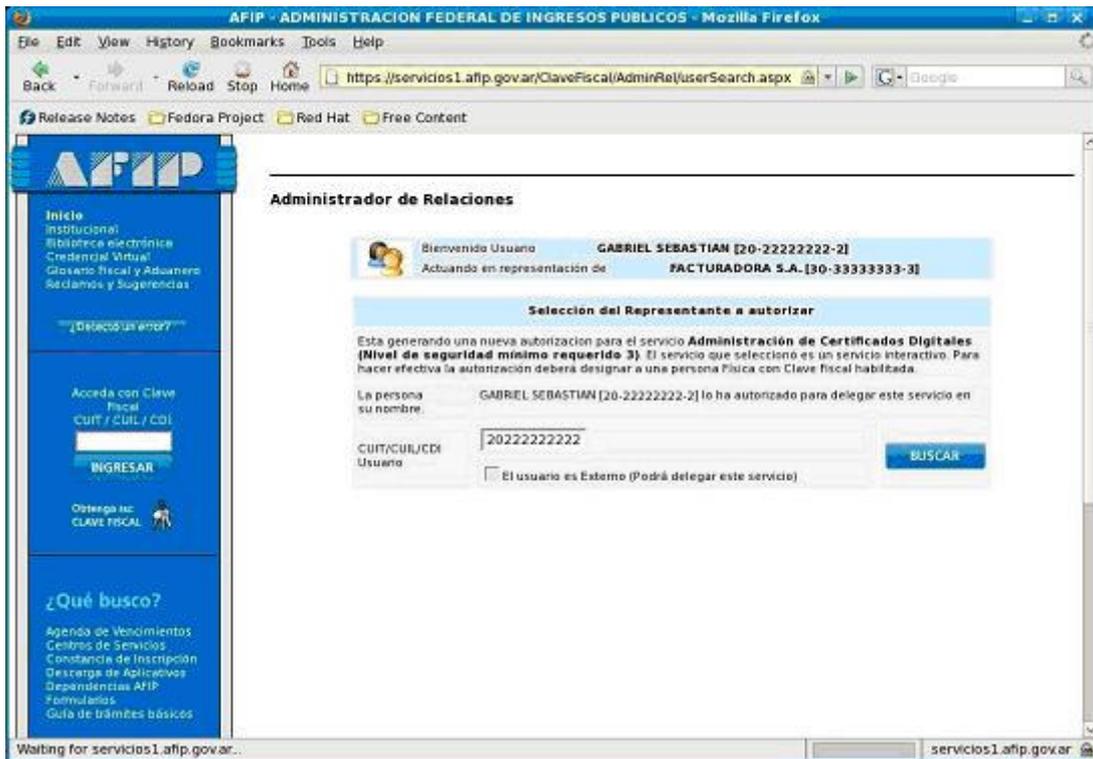


imagen 57

- Clicar en “CONFIRMAR”:

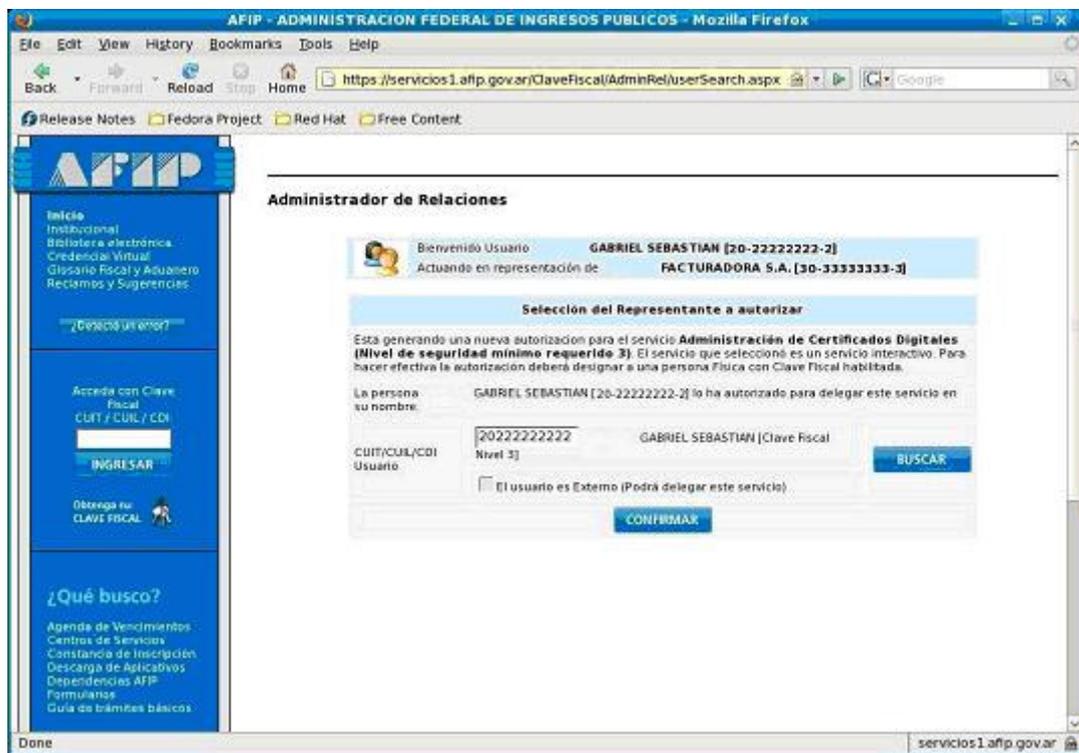


imagen 58

- Clicar en “CONFIRMAR”:

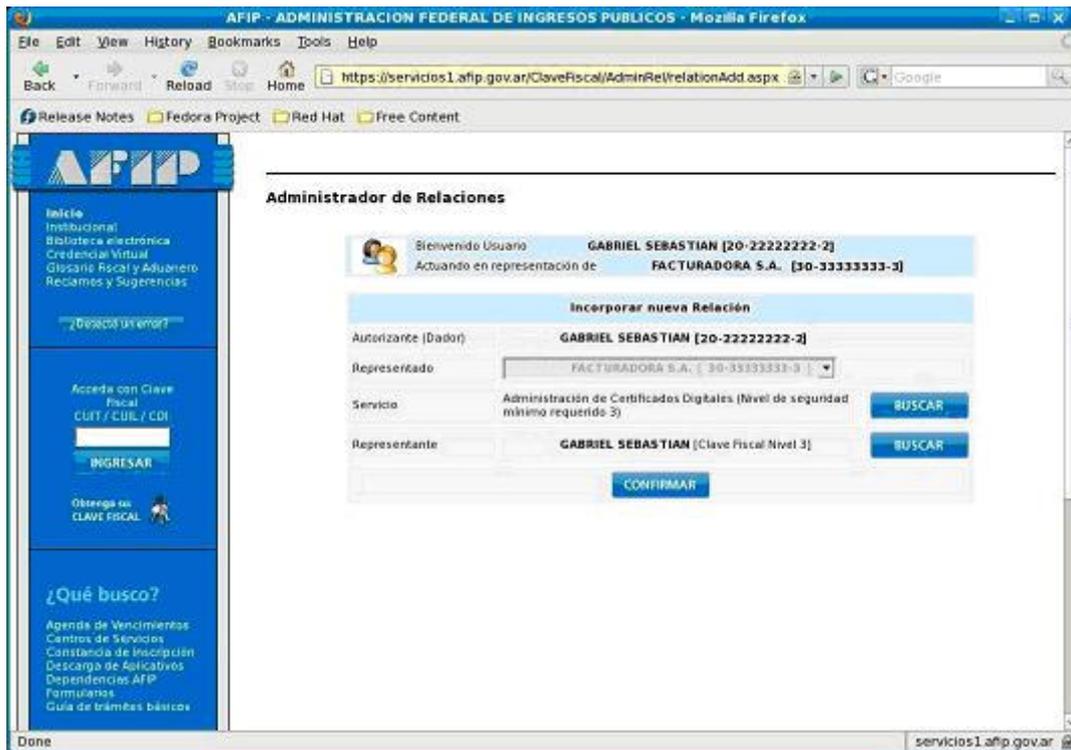


imagen 59

- Salir del sistema y volver a ingresar para poder visualizar y seleccionar el servicio “Administración de Certificados Digitales” en la lista de servicios.
- En caso de no visualizar el servicio en la lista, debe aceptar la relación utilizando el servicio “Aceptación de Designación”.

### PASO 3: SELECCIONAR EL CONTRIBUYENTE

Una vez que ingresamos en “Administración de Certificados Digitales”, seleccionar el contribuyente para el que va a operar el servicio (si representa a más de un contribuyente):

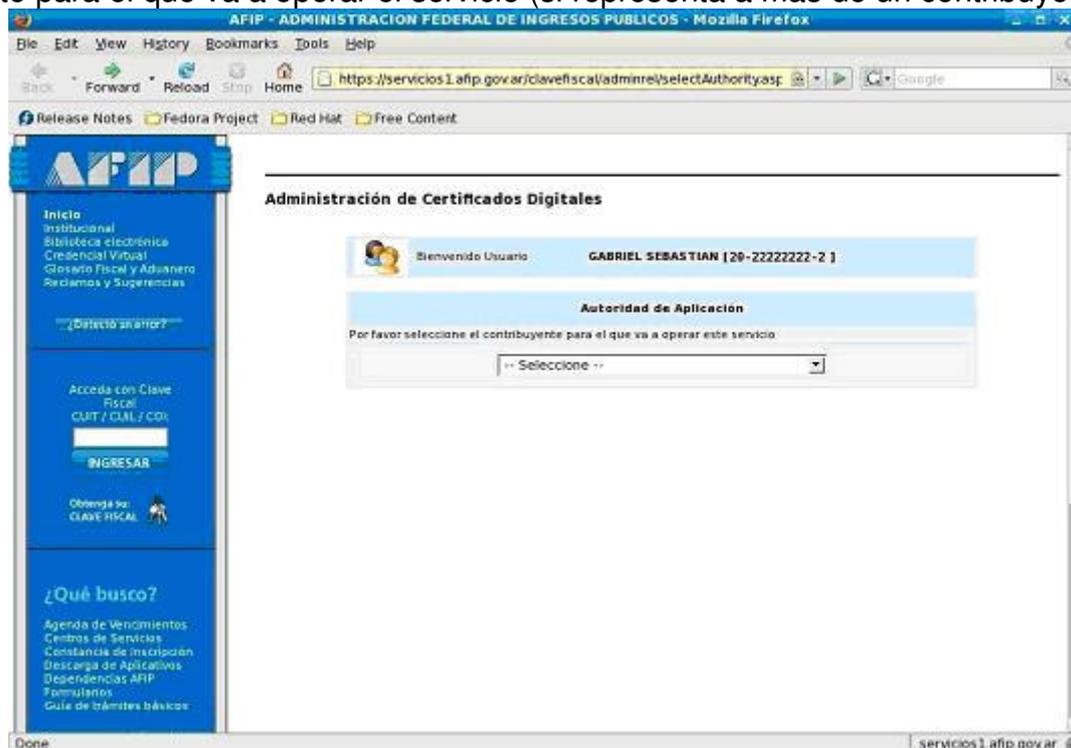


imagen 60

## PASO 4: AGREGAR ALIAS

Clicar en “Agregar alias”:

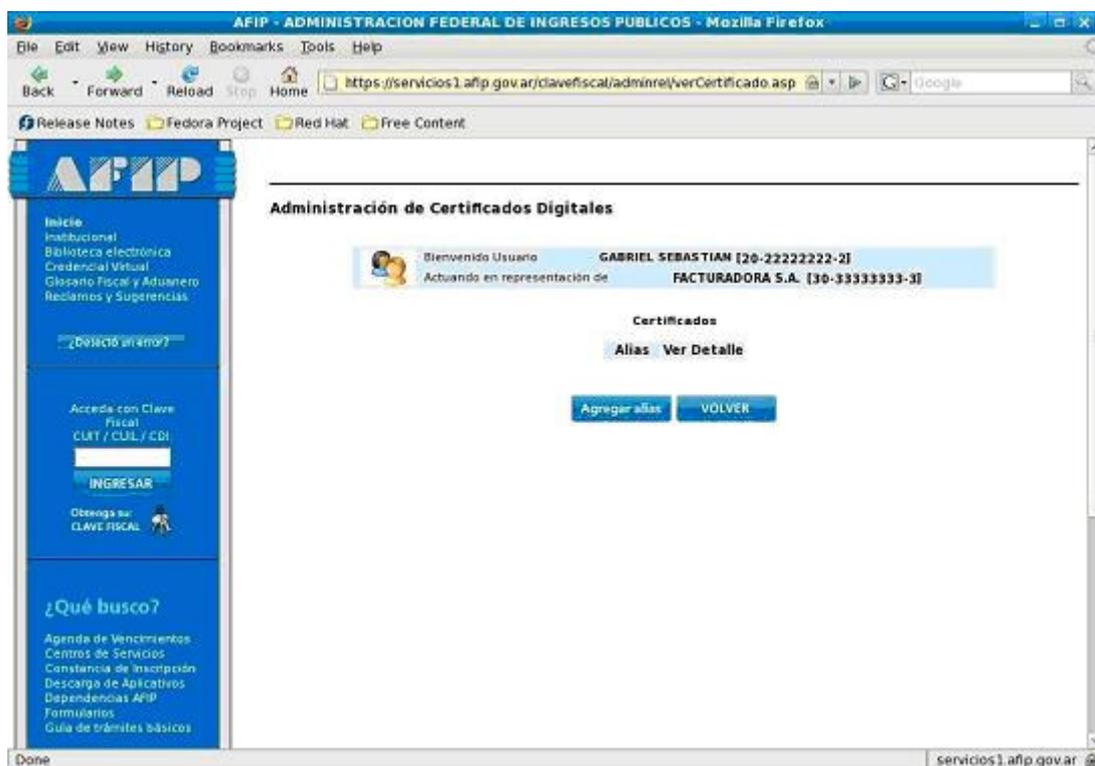


imagen 61

## PASO 5: SUBIR ARCHIVO PEDIDO.CSR

Elegir un nombre para el alias y subir el archivo PEDIDO.CSR generado en los pasos previos con los comandos del OPENSSE (en nuestro ejemplo habíamos generado el archivo pedido.csr en la carpeta \OPENSSE\BIN). Luego clicar en “Agregar alias”:

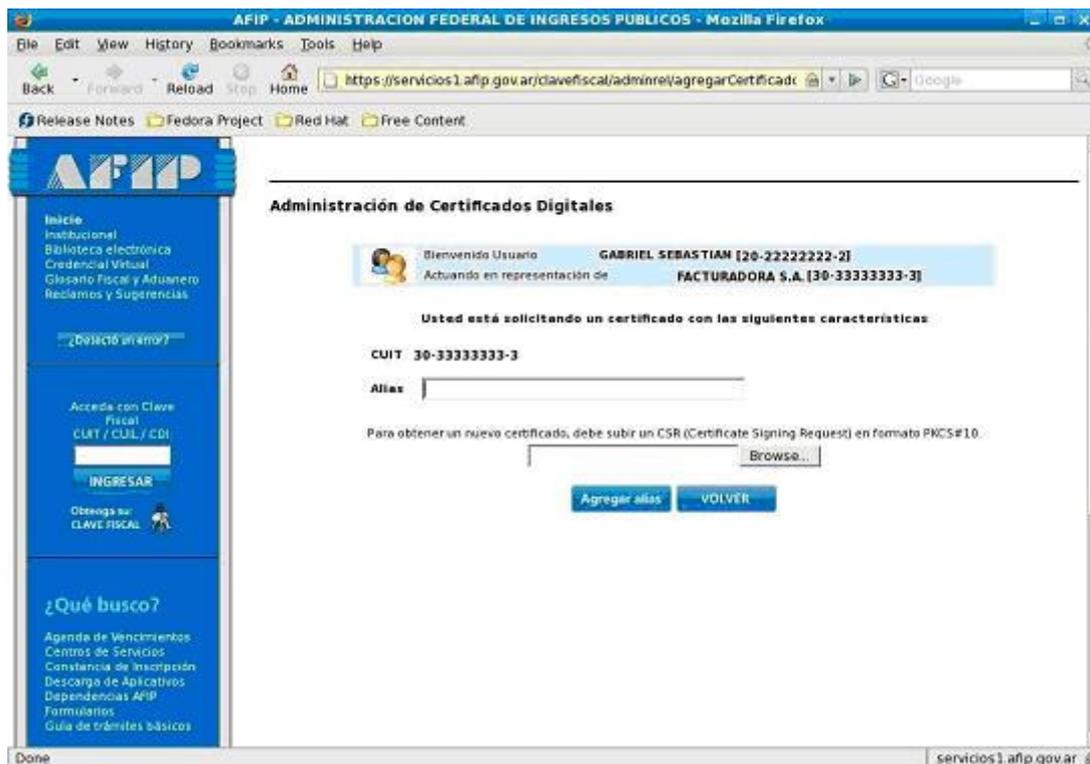


imagen 62

## PASO 6: DESCARGAR ARCHIVO .CRT

Clicar en “Ver” (link ubicado a la derecha del alias generado) para poder visualizar y descargar a su PC el certificado, que será un archivo con extensión **crt** que nos va a permitir continuar con la habilitación y utilización de los servicios Web de AFIP.