

Objetivo del documento

El presente instructivo indica los requisitos de software necesarios para la firma y visualización, del SNE y de un correo electrónico.

Contenido

1.	SNE y Firma Electrónica Avanzada	2
2.	Firma Electrónica Avanzada con Token	2
	2.1 CORREO URUGUAYO	2
	2.2 ABITAB (ID DIGITAL)	2
3.	Firma Electrónica Avanzada con Cédula de Identidad.....	3
4.	Aplicación Soporte Notarial Electrónico	3
	4.1 Requisitos de software de los equipos clientes para trabajar con la aplicación de Soporte Notarial Electrónico	3
	4.2 El uso de Java por parte de la aplicación	4
	4.3 Visualización del Soporte Notarial Electrónico y Verificación de firmas	6
5.	Configuraciones para el envío de correos firmados	20
	5.1 Para cliente de correo Thunderbird	20
	5.2 Para cliente de correo Outlook	42

1. SNE y Firma Electrónica Avanzada

Para el uso de la firma digital se deberá contar con un dispositivo criptográfico (de aquí en adelante token o cédula de identidad).

2. Firma Electrónica Avanzada con Token

Una vez adquirido el token, éste debe ser instalado apropiadamente en las computadoras con el software y driver correspondiente provistos por el vendedor del dispositivo. En esta instalación tendremos la oportunidad de generar una contraseña de carácter personal, la cual se utilizará para efectivizar la firma de los documentos y/o correos electrónicos.

El siguiente paso es solicitar la emisión de la firma digital mencionada ante una de las dos entidades emisoras de este tipo certificados digitales de firma electrónica avanzada; las mismas son Abitab y el Correo Uruguayo.

2.1 CORREO URUGUAYO

Para la gestión ante el Correo Uruguayo es recomendable utilizar Internet Explorer y son necesarios estos requisitos: [ver aquí](#), una vez verificado esto proseguir a realizar la solicitud: [ver aquí](#), se pedirán varios datos para completar y como último paso de esta etapa le pedirá que imprima el resumen de la solicitud. Con esa hoja impresa deberá concurrir a un local del Correo, realizar el pago y firmar el contrato. En los próximos 3 días recibirá un correo electrónico con un link para finalizar la instalación de la firma digital en el token.

En este sitio encontrará la resolución de los errores más comunes que se pueden presentar: [ver aquí](#)

2.2 ABITAB (ID DIGITAL)

Para la gestión ante Abitab es recomendable utilizar Internet Explorer y es necesario como requisito, contar con los siguientes certificados instalados: Autoridad de Certificación de Firma Electrónica Avanzada – Homologada y Autoridad de Certificación Raíz Nacional, [ver aquí](#). Una vez hecho esto proseguir a realizar la solicitud que encontrará en el menú Firma Electrónica Avanzada >> Persona Física, se pedirán varios datos para completar y como último paso de esta etapa le pedirá que imprima el resumen de la solicitud. Con esa hoja impresa deberá concurrir a un local de Abitab, realizar el pago y firmar el contrato. En los próximos 3 días recibirá un correo electrónico con un link para finalizar la instalación de la firma digital en el token.

En este sitio encontrará la información de contacto de soporte técnico en caso de tener algún inconveniente: [ver aquí](#)

Es importante tener en cuenta que las 2 etapas de las que consta la gestión de la firma digital, deben ser realizadas en la misma computadora. Es decir, generar la solicitud para ir a pagar y luego seguir las instrucciones que vienen en el correo que se recibe dentro de las 72 horas.

3. Firma Electrónica Avanzada con Cédula de Identidad

Para poder firmar los documentos deberá contar con la nueva cédula que contiene un chip con firma electrónica avanzada.

Para la operación con esta cédula será necesario:

- un lector de tarjetas inteligentes homologado por el Ministerio del Interior (por ejemplo los que provee Macroseguridad, marca Feitian) y el respectivo driver instalado en su computadora
- tener instalado el certificado Autoridad de Certificación de Raíz Nacional: [ver aquí](#)
- tener instalado el certificado Autoridad Certificadora del Ministerio del Interior: [ver aquí](#)

4. Aplicación Soporte Notarial Electrónico

4.1 Requisitos de software de los equipos clientes para trabajar con la aplicación de Soporte Notarial Electrónico

Los programas necesarios para el correcto funcionamiento son: Mozilla Firefox, Acrobat Reader XI o posterior y Java.

A continuación verán los links de descarga de cada uno de los productos.

Mozilla Firefox, versión 30:

<https://www.mozilla.org/es-ES/firefox/new/>

Google Chrome, última versión disponible:

<https://www.google.es/chrome/browser/desktop/>

Acrobat Reader, versión XI o posterior:

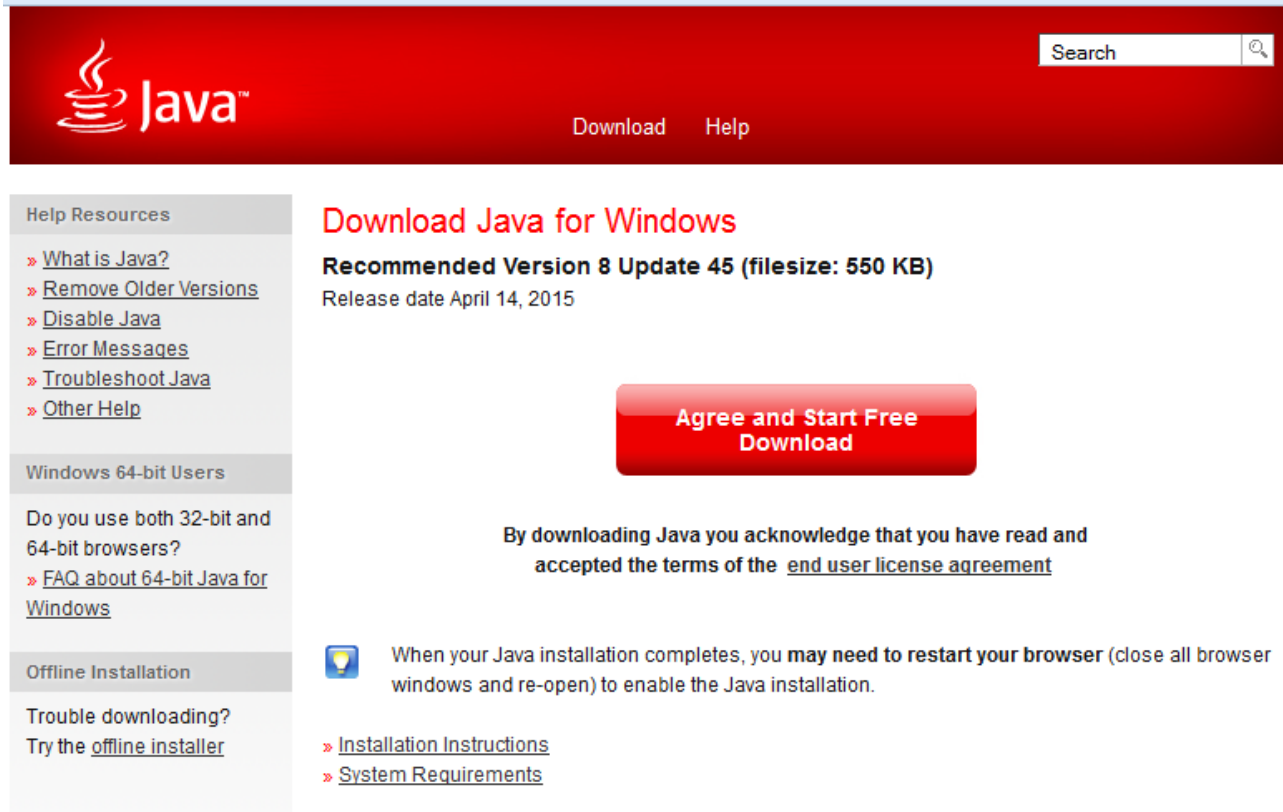
<http://get.adobe.com/es/reader/otherversions/>

Java, versión 8.45:

<http://java.com/es/download/>

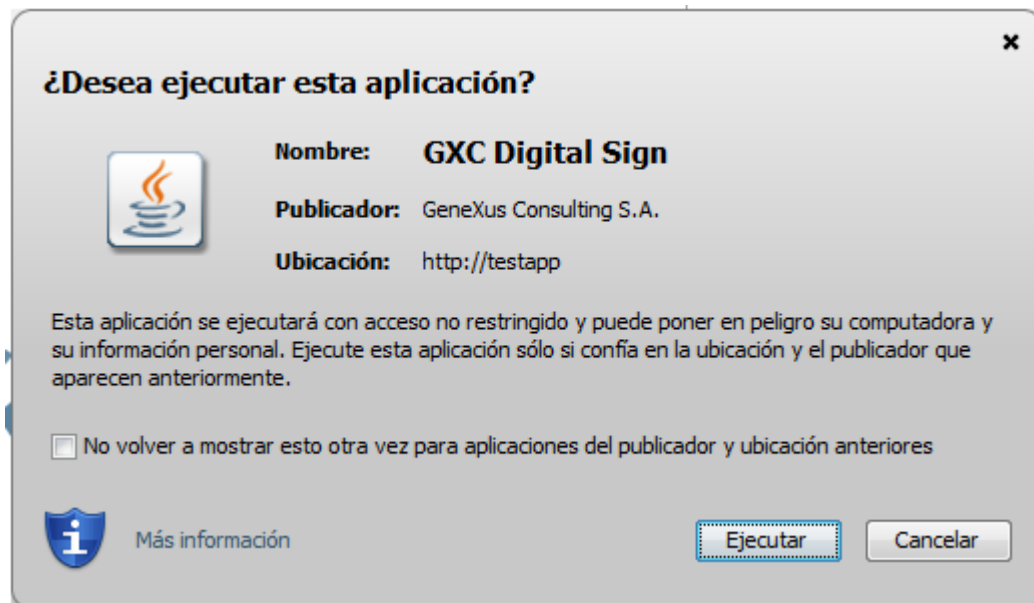
4.2 El uso de Java por parte de la aplicación

Después de redactar el documento se hace click en el botón Continuar. Aquí se ejecuta el applet de Java que prepara el documento para ser firmado, en caso de no haber hecho la instalación según recomienda el punto anterior, se nos direccionará al sitio web del fabricante para su descarga, como lo muestra la siguiente captura.



The screenshot shows the Java website's download page for Windows. At the top, there is a red navigation bar with the Java logo on the left, a search box, and links for 'Download' and 'Help'. Below the navigation bar, the main content area is divided into a left sidebar and a main content area. The sidebar contains sections for 'Help Resources' (with links like 'What is Java?', 'Remove Older Versions', 'Disable Java', 'Error Messages', 'Troubleshoot Java', and 'Other Help'), 'Windows 64-bit Users' (with a link to 'FAQ about 64-bit Java for Windows'), and 'Offline Installation' (with a link to 'Try the offline installer'). The main content area features the heading 'Download Java for Windows' in red, followed by 'Recommended Version 8 Update 45 (filesize: 550 KB)' and 'Release date April 14, 2015'. A prominent red button with white text says 'Agree and Start Free Download'. Below this, a disclaimer states: 'By downloading Java you acknowledge that you have read and accepted the terms of the [end user license agreement](#)'. A lightbulb icon is followed by a note: 'When your Java installation completes, you may need to restart your browser (close all browser windows and re-open) to enable the Java installation.' At the bottom of the main content area, there are two links: 'Installation Instructions' and 'System Requirements'.

La primera vez que se utiliza la aplicación y genera un documento para ser firmado, nos saldrá la siguiente consulta. En esta ventana deberemos marcar la casilla “No volver a mostrar esto...” y click en Ejecutar.

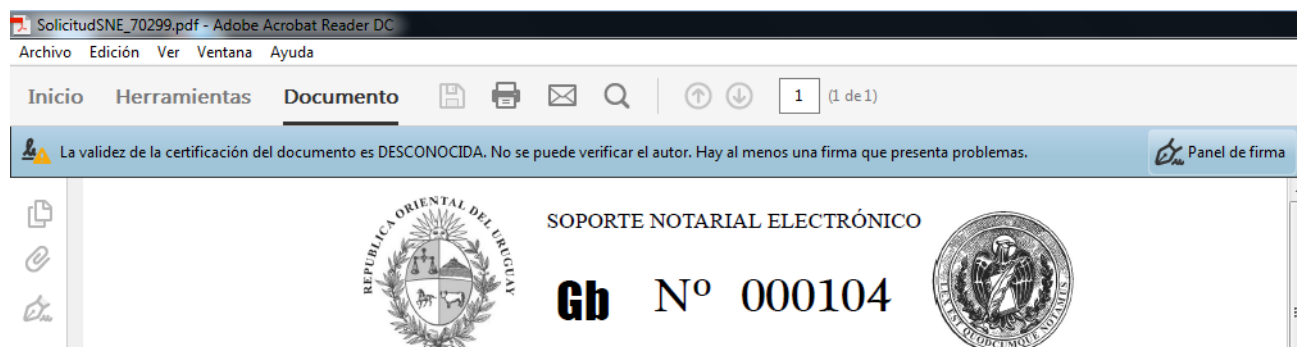


4.3 Visualización del Soporte Notarial Electrónico y Verificación de firmas

El destinatario del documento deberá chequear que el mismo esté firmado por la Caja Notarial y por el escribano actuante. Ambas firmas deben ser Firmas Electrónicas Avanzadas y por lo tanto, se debe validar que estén emitidas por una entidad certificadora que dependa de la Raíz Nacional Agestic.

Para poder visualizar correctamente la jerarquía de certificaciones y las propiedades de la firma se deberá proceder de la forma siguiente.

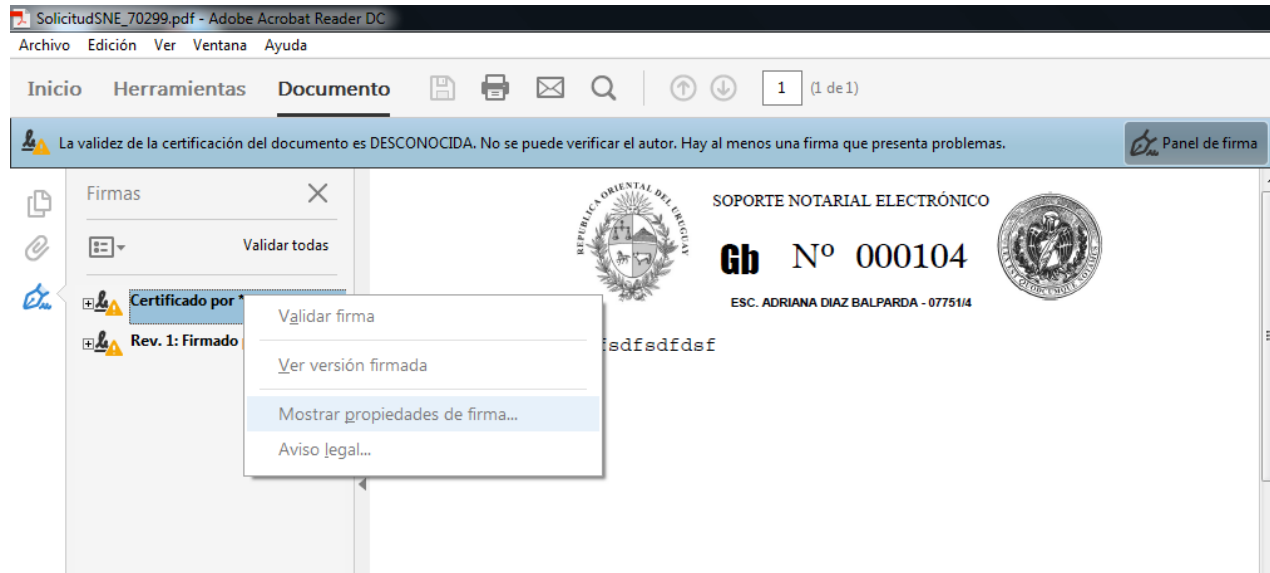
La primera vez que se descargue y abra el archivo PDF, notaremos que en la parte superior del mismo aparecerá una leyenda como la que se muestra dónde nos alerta de que la validez de la certificación del documento es desconocida.



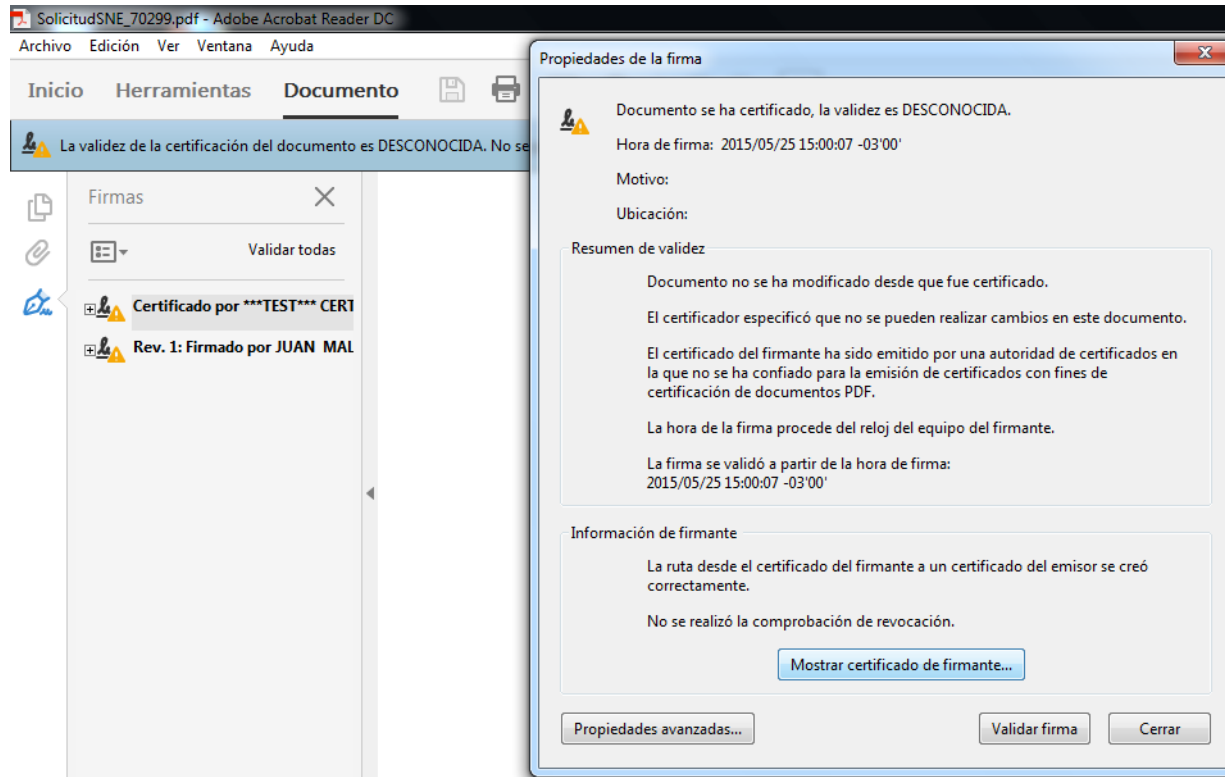
Deberemos por única vez, configurar el Acrobat Reader para que confíe en las firmas electrónicas de las entidades emisoras y del escribano en cuestión, para poder visualizar el documento sin las advertencias de seguridad.

Para esto debemos hacer click en el botón Panel de Firma que está a la derecha de la leyenda de alerta.

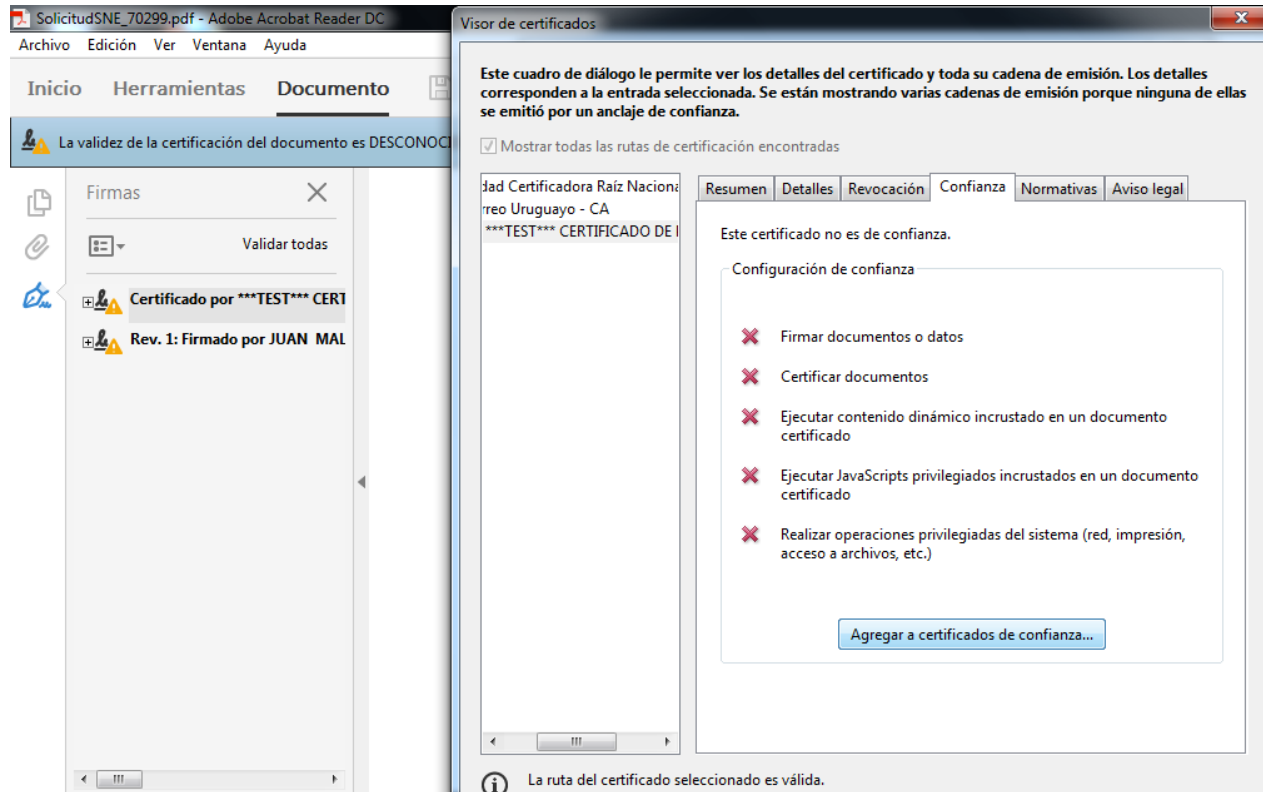
Veremos dos firmas, la de la Caja Notarial (que en este caso dice Test por ser una firma con un certificado de persona jurídica de prueba) y la del escribano. Sobre la firma de la Caja Notarial hacemos click derecho >> Mostrar propiedades de firma...



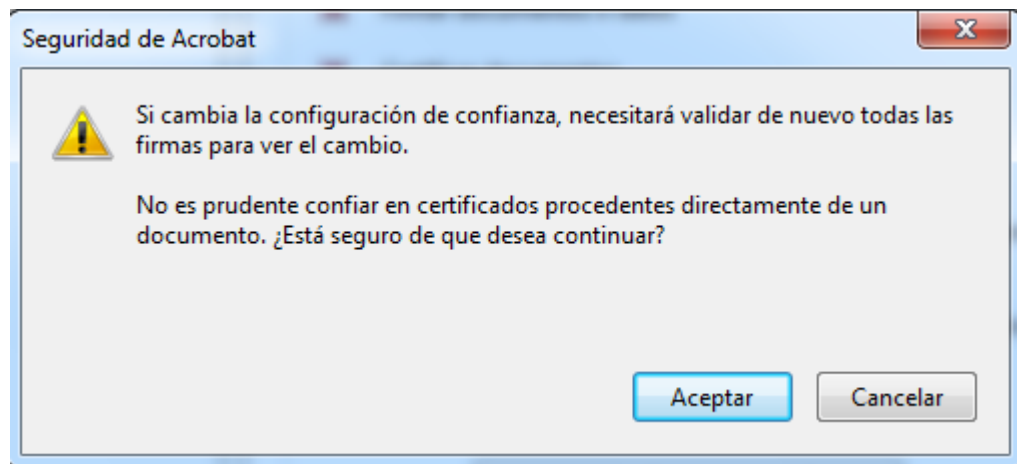
En el siguiente cuadro de diálogo hacemos click en el botón Mostrar certificado de firmante...



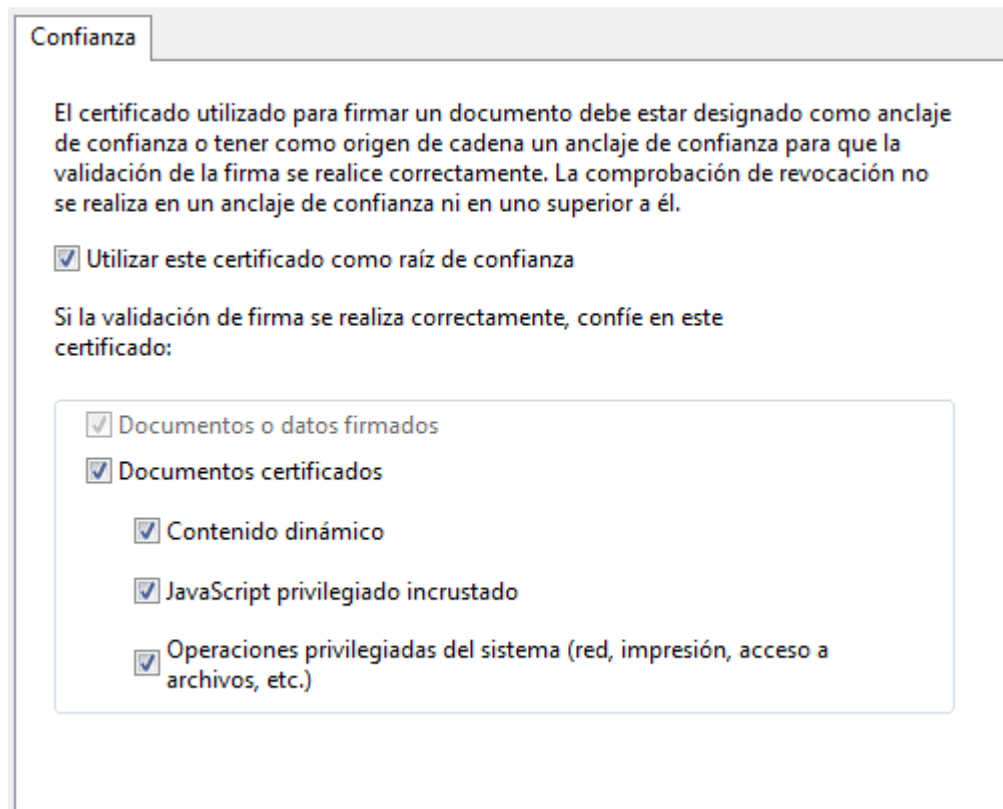
Nos posicionamos en la pestaña Confianza >> Click en Agregar a certificados de confianza



Confirmamos la advertencia de seguridad



Debemos marcar todas las opciones como muestra la siguiente captura.



The screenshot shows a dialog box titled "Confianza" (Trust). It contains the following text and options:

El certificado utilizado para firmar un documento debe estar designado como anclaje de confianza o tener como origen de cadena un anclaje de confianza para que la validación de la firma se realice correctamente. La comprobación de revocación no se realiza en un anclaje de confianza ni en uno superior a él.

Utilizar este certificado como raíz de confianza

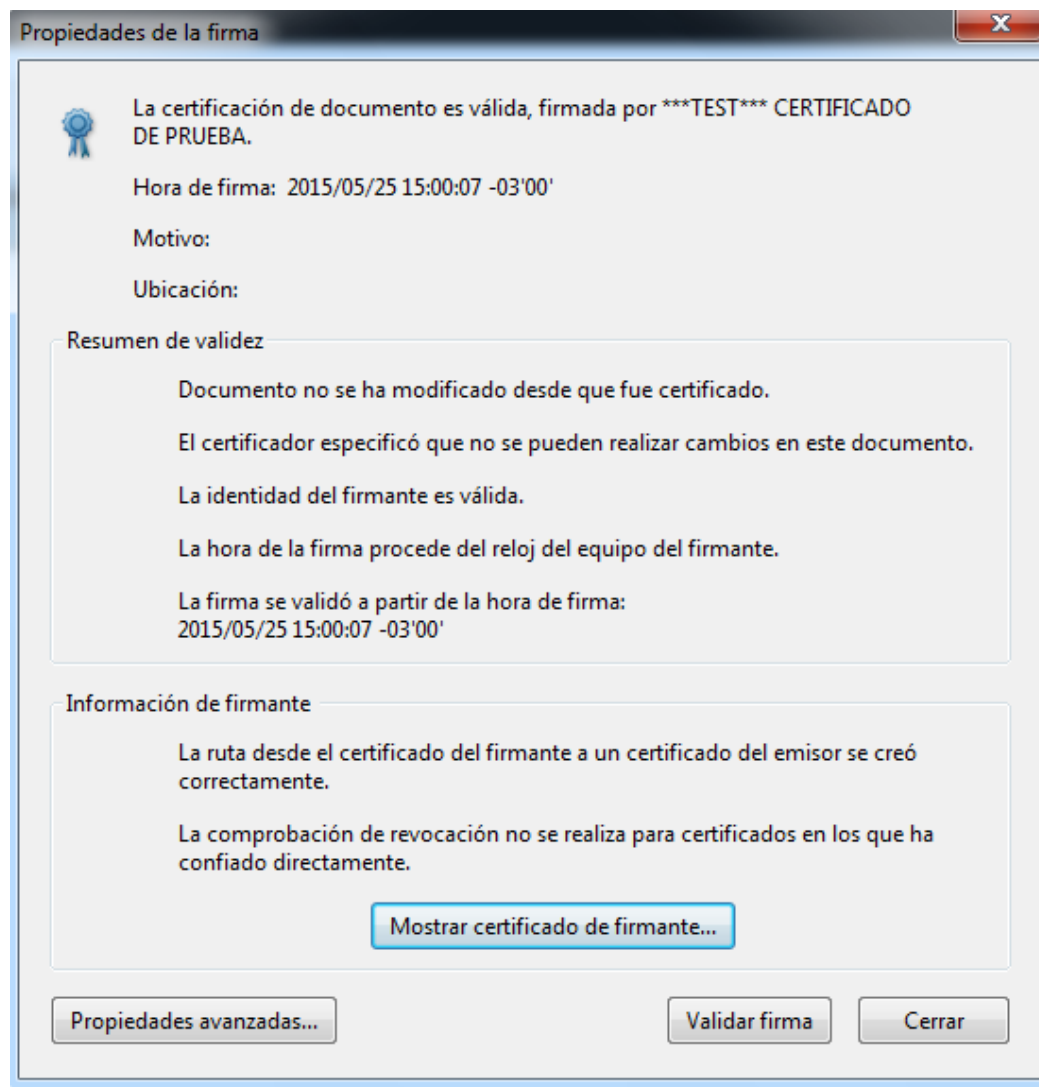
Si la validación de firma se realiza correctamente, confíe en este certificado:

- Documentos o datos firmados
- Documentos certificados
 - Contenido dinámico
 - JavaScript privilegiado incrustado
 - Operaciones privilegiadas del sistema (red, impresión, acceso a archivos, etc.)

Damos click en Aceptar para cerrar el cuadro de diálogo Confianza.

Damos click en Aceptar para cerrar el cuadro de diálogo Visor de Certificados.

En el siguiente cuadro de diálogo hacemos click en el botón Validar firma y veremos el detalle de la firma validando la identidad del firmante.



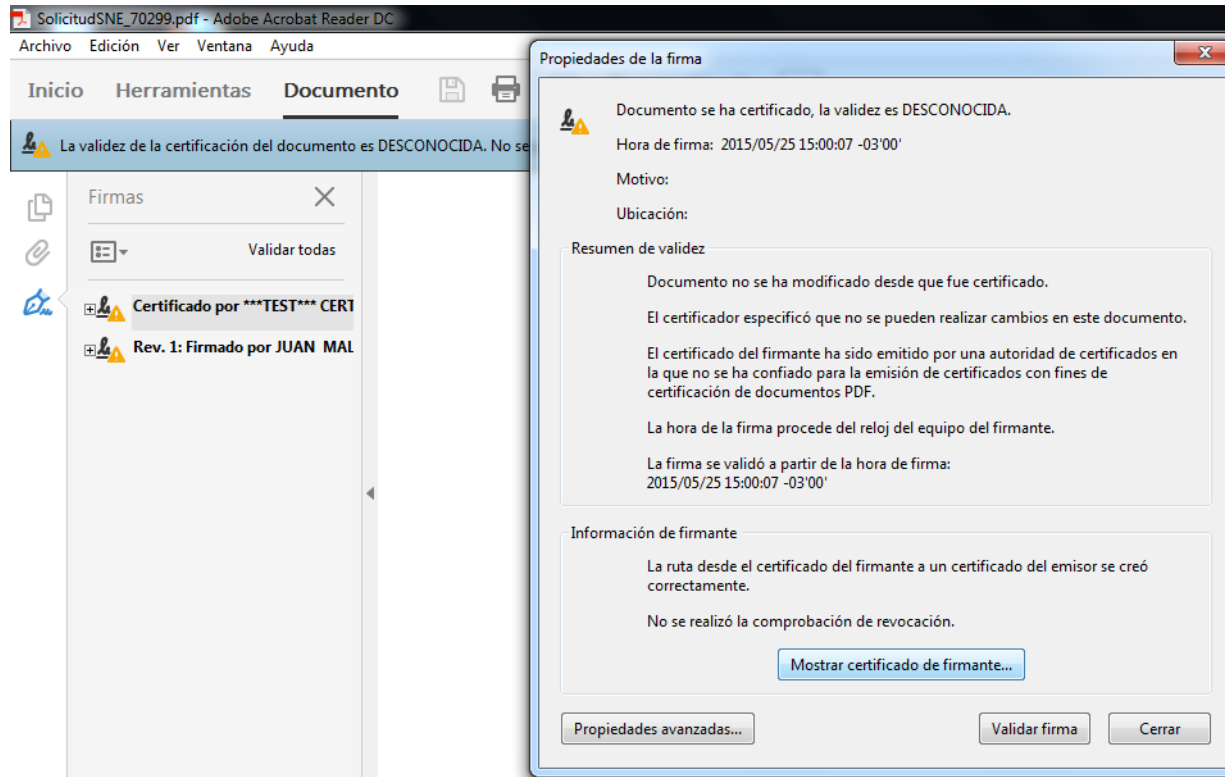
Notarán que el ícono correspondiente a la firma de la entidad ha cambiado por una cocarda y sin advertencia.

Ahora resta repetir el mismo procedimiento para la firma correspondiente al escribano firmante.

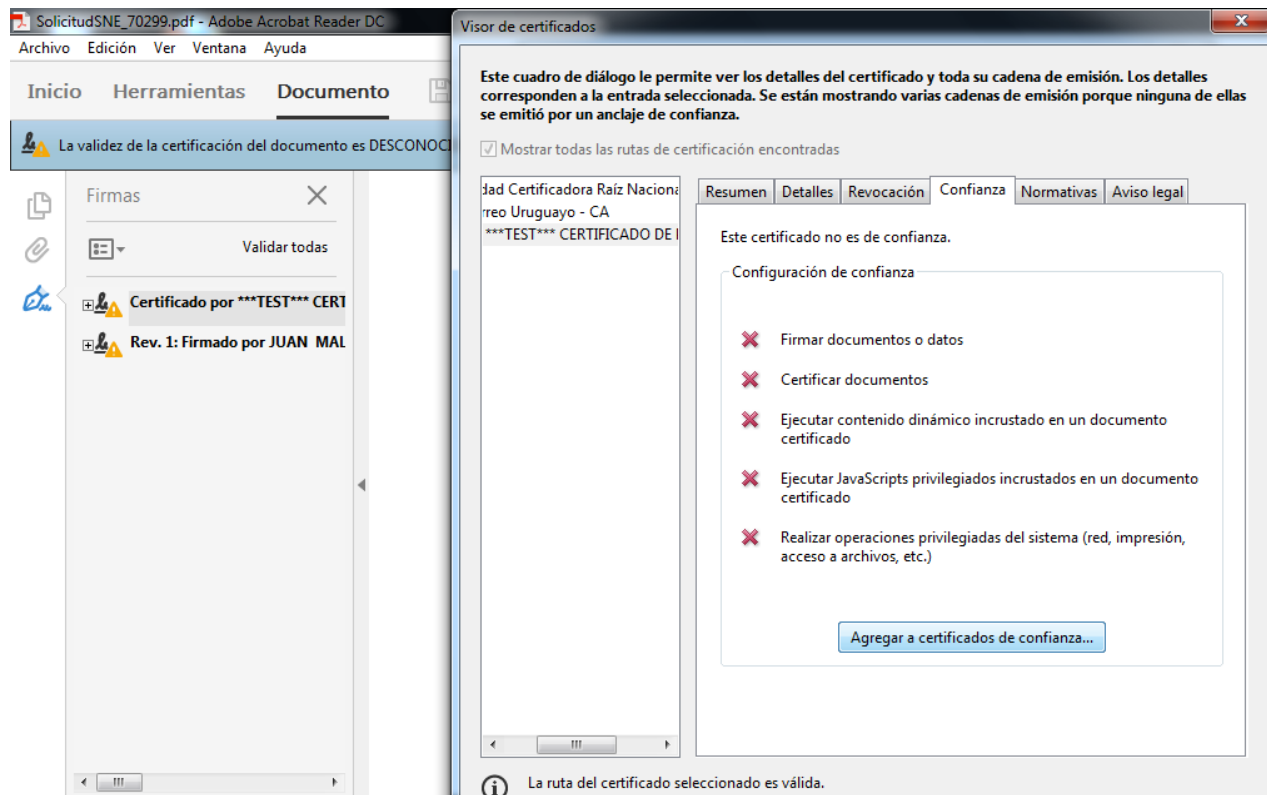
Sobre la firma del escribano hacemos click derecho >> Mostrar propiedades de firma...



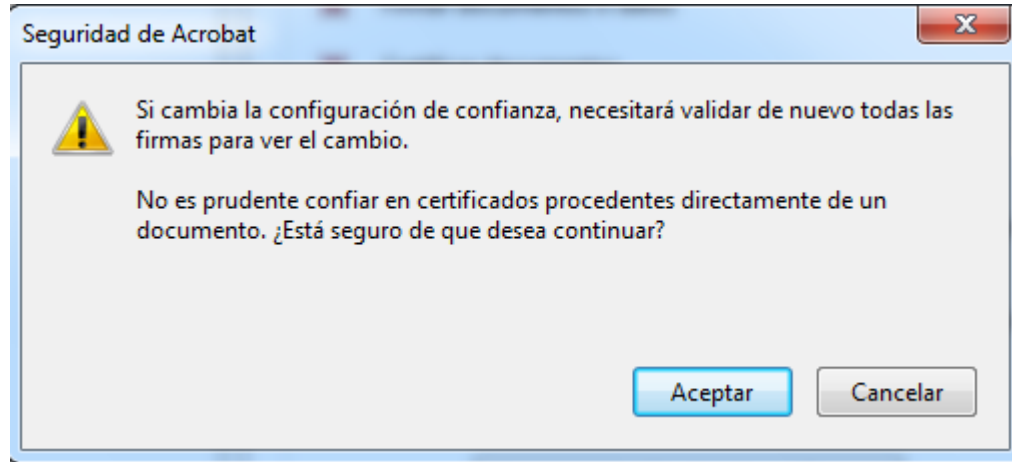
En el siguiente cuadro de diálogo hacemos click en el botón Mostrar certificado de firmante...



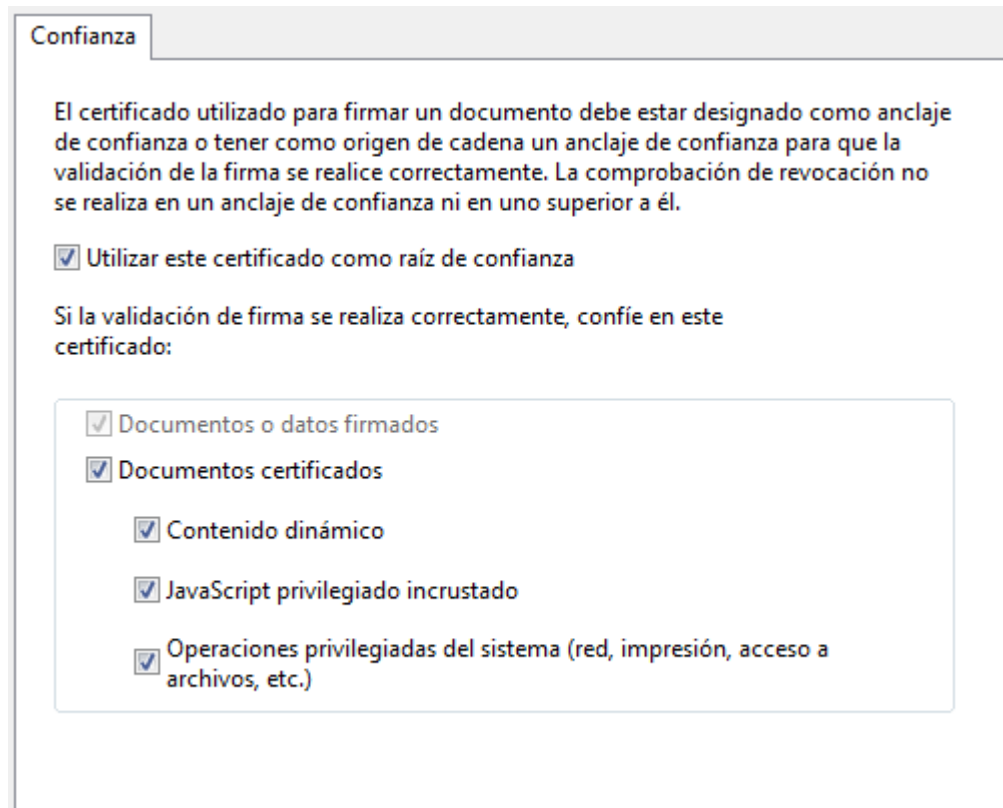
Nos posicionamos en la pestaña Confianza >> Click en Agregar a certificados de confianza



Confirmamos la advertencia de seguridad



Debemos marcar todas las opciones como muestra la siguiente captura.



The screenshot shows a dialog box titled "Confianza". It contains the following text and options:

El certificado utilizado para firmar un documento debe estar designado como anclaje de confianza o tener como origen de cadena un anclaje de confianza para que la validación de la firma se realice correctamente. La comprobación de revocación no se realiza en un anclaje de confianza ni en uno superior a él.

Utilizar este certificado como raíz de confianza

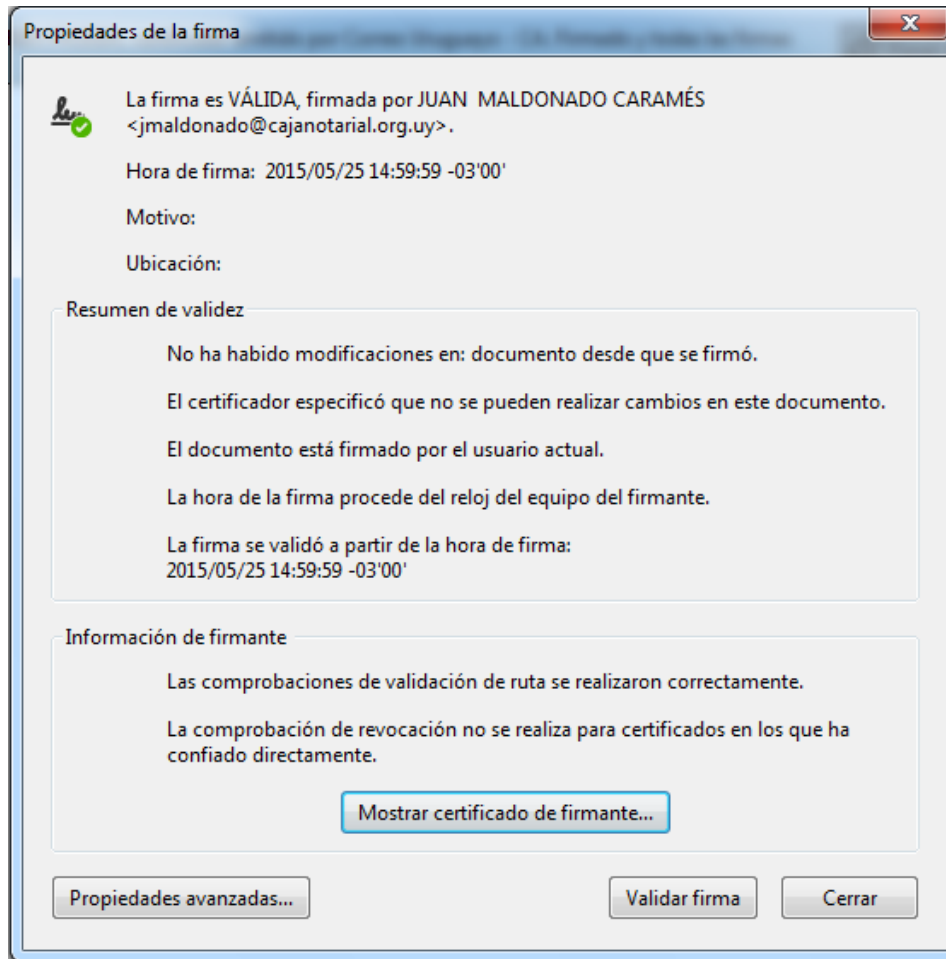
Si la validación de firma se realiza correctamente, confíe en este certificado:

- Documentos o datos firmados
- Documentos certificados
 - Contenido dinámico
 - JavaScript privilegiado incrustado
 - Operaciones privilegiadas del sistema (red, impresión, acceso a archivos, etc.)

Damos click en Aceptar para cerrar el cuadro de diálogo Confianza.

Damos click en Aceptar para cerrar el cuadro de diálogo Visor de Certificados.

En el siguiente cuadro de diálogo hacemos click en el botón Validar firma y veremos el detalle de la firma validando la identidad del firmante.



Notarán que el ícono correspondiente a la firma del escribano ha cambiado y no muestra la advertencia. También la leyenda del cabezal del documento aclara que todas las firmas son válidas.

Este procedimiento sobre la confianza de las firmas se hará solamente una vez. Al visualizar las propiedades de cada firma, se verán las mismas y la jerarquía de certificaciones, sin las advertencias de seguridad.



Certificado por ***TEST*** CERTIFICADO DE PRUEBA, ***TEST*** PRUEBA PRUEBA, certificado emitido por Correo Uruguayo - CA. Firmado y todas las firmas son válidas. Panel de firma

Firmas

Validar todas

Certificado por ***TEST*** CERTIFICAD

Rev. 1: Firmado por JUAN MALDONAI

REPUBLICA ORIENTAL DEL URUGUAY

SOPORTE NOTARIAL ELECTRÓNICO

Gh N° 000104

ESC. ADRIANA DIAZ BALPARDA - 07751/4

dsfsdfsdfsdfsdf

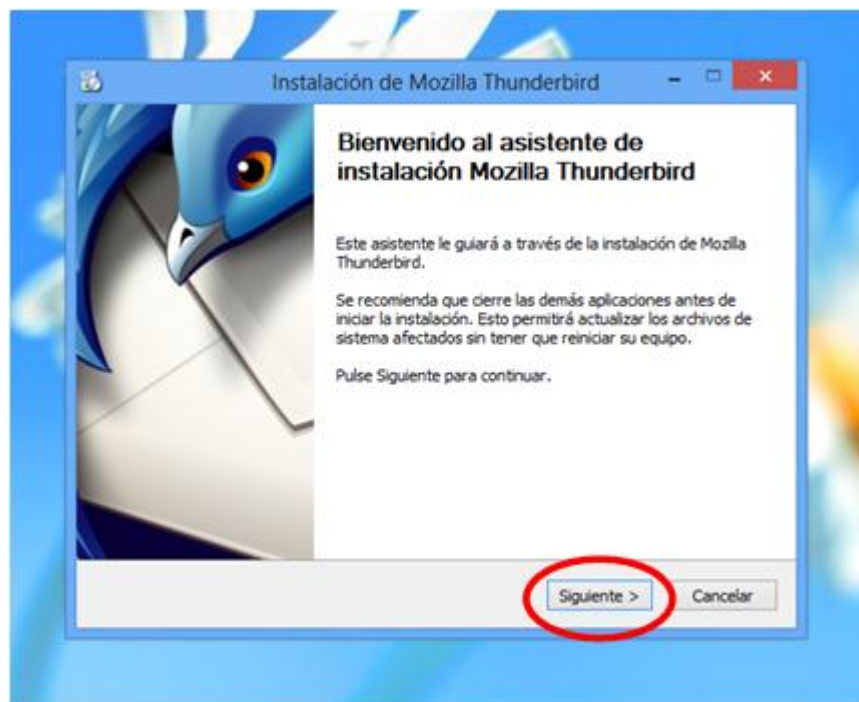
Aclaración importante

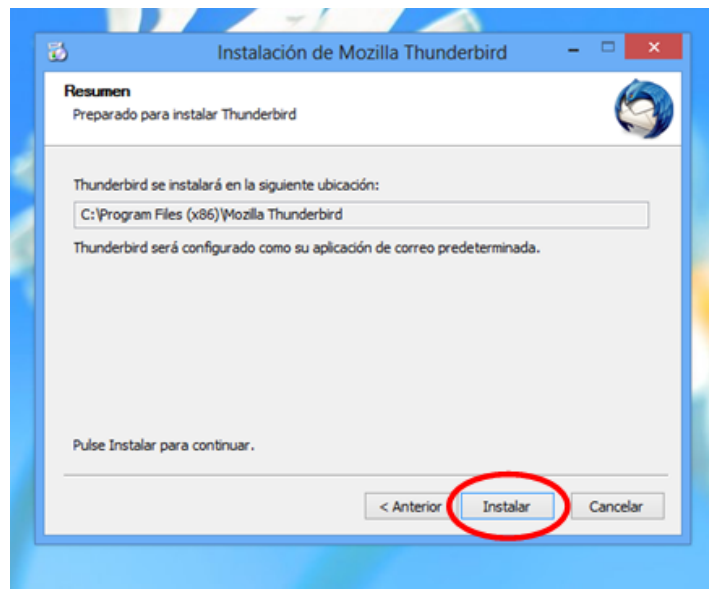
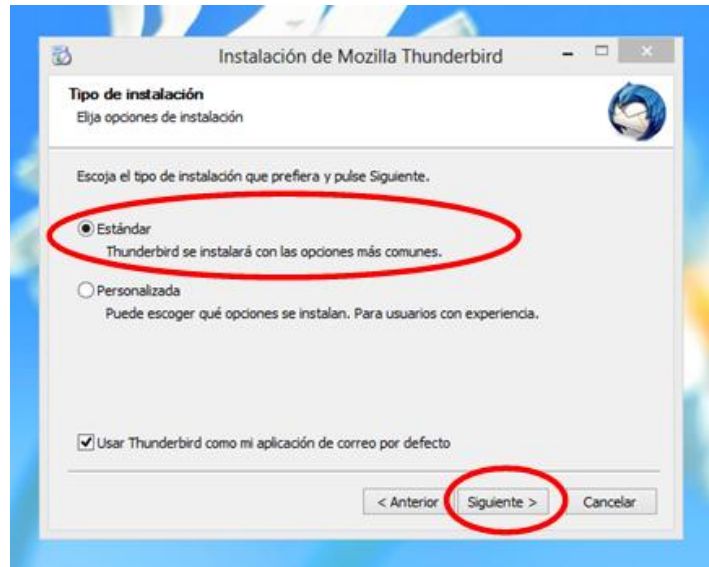
Estos pasos en la configuración de la seguridad del programa Acrobat Reader, es exclusivamente para que visualmente no figuren advertencias. Todos los chequeos de seguridad y validez de las firmas se realizan previamente antes de generar el PDF. El escribano debe tener la tranquilidad de que el documento creado es 100% válido.

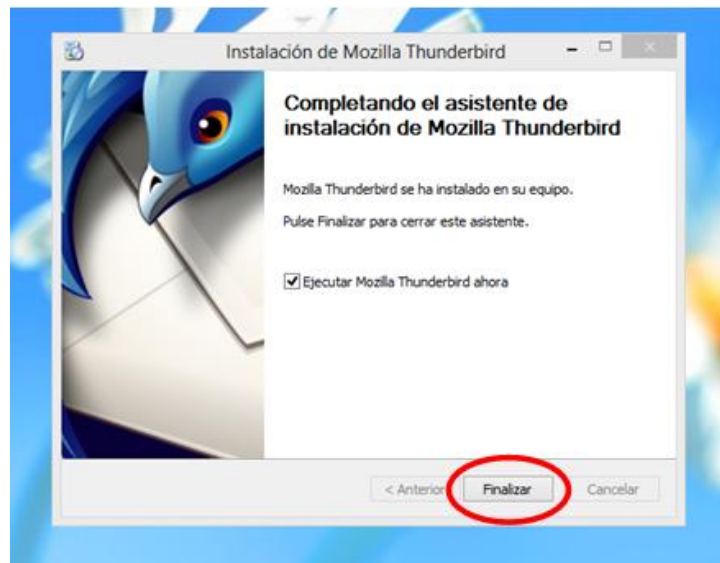
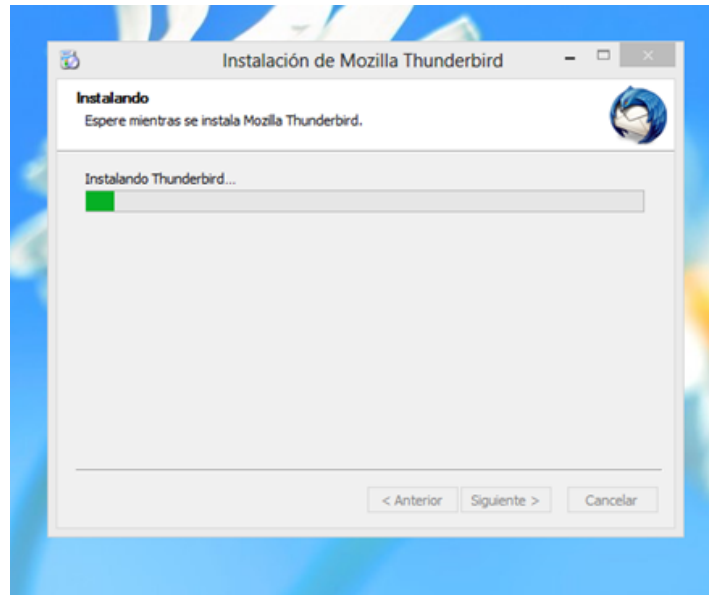
5. Configuraciones para el envío de correos firmados

5.1 Para cliente de correo Thunderbird

- 1) Descargar el instalador en <https://www.mozilla.org/es-ES/thunderbird/>
- 2) Instalación:



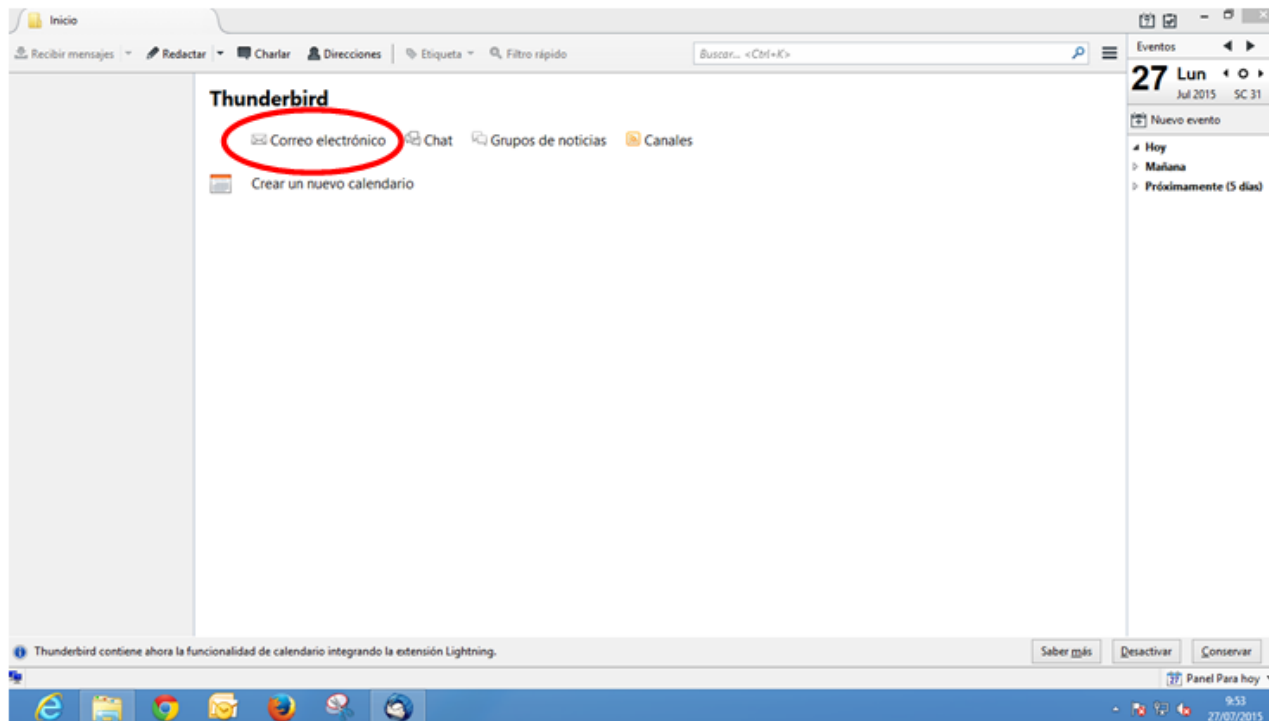




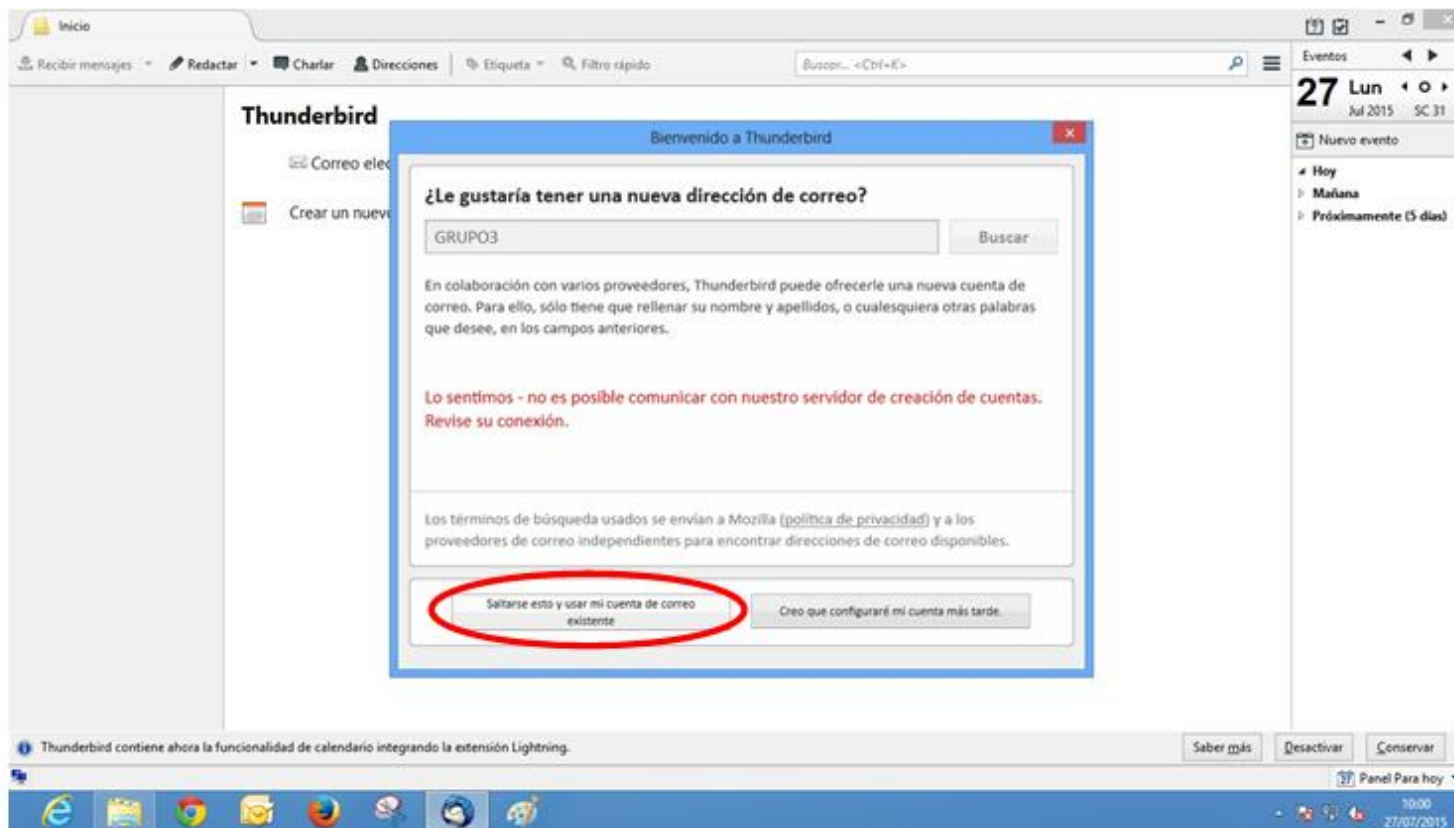
Configuración:

Una vez instalado procedemos a ejecutar el Thunderbird.

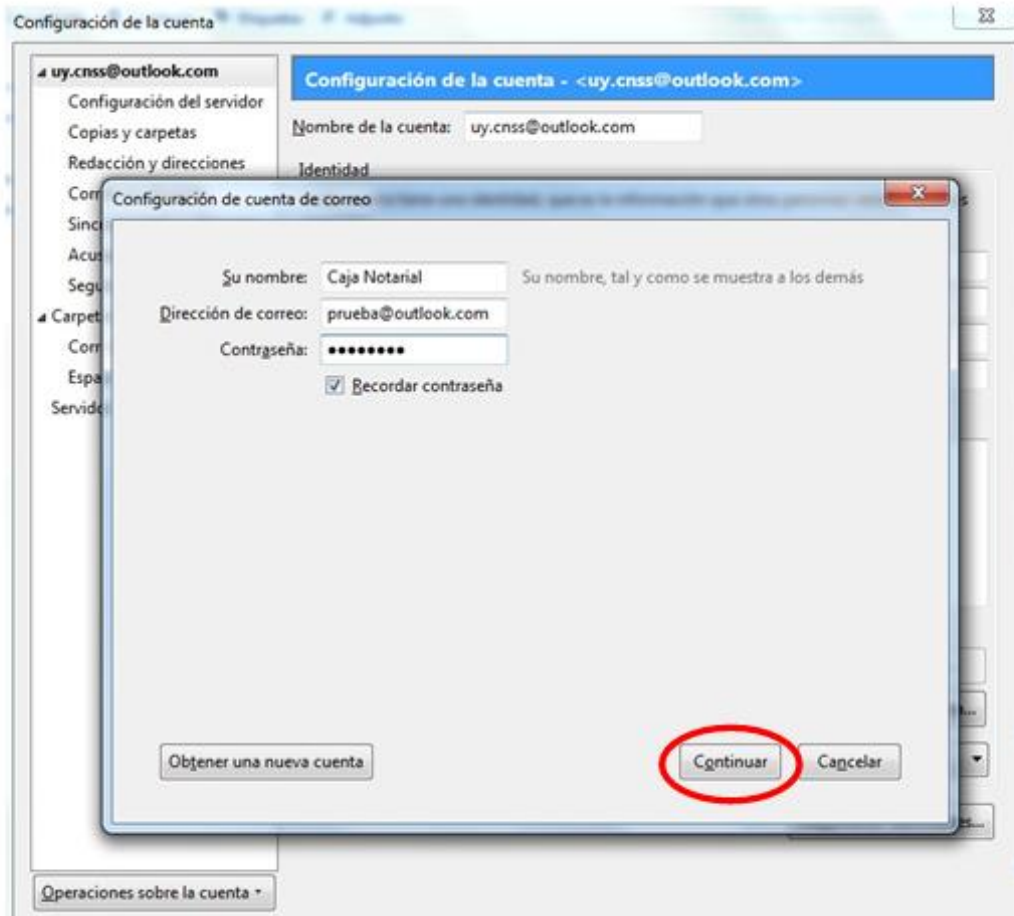
1) Vamos a : Correo electrónico



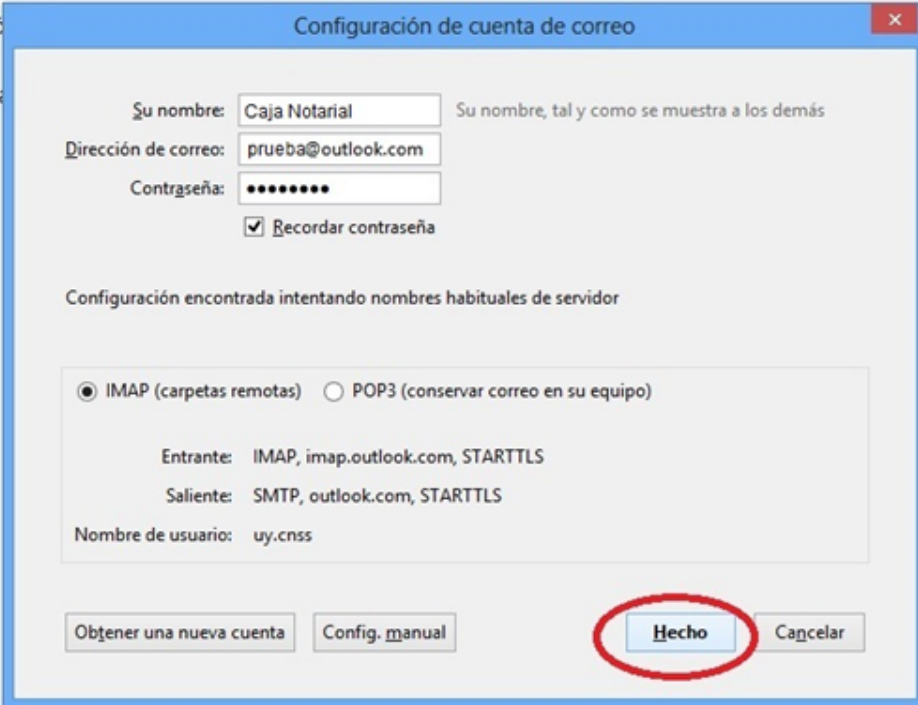
2) Damos clic en: “Saltarse esto y usar mi cuenta de correo existente”



- 3) Ingresar el correo que se desea usar, en este caso se probó con Outlook (Hotmail).
Luego damos en continuar.



4) Damos clic en “Hecho”



Configuración de cuenta de correo

Su nombre: Caja Notarial Su nombre, tal y como se muestra a los demás

Dirección de correo: prueba@outlook.com

Contraseña: ●●●●●●

Recordar contraseña

Configuración encontrada intentando nombres habituales de servidor

IMAP (carpetas remotas) POP3 (conservar correo en su equipo)

Entrante: IMAP, imap.outlook.com, STARTTLS

Saliente: SMTP, outlook.com, STARTTLS

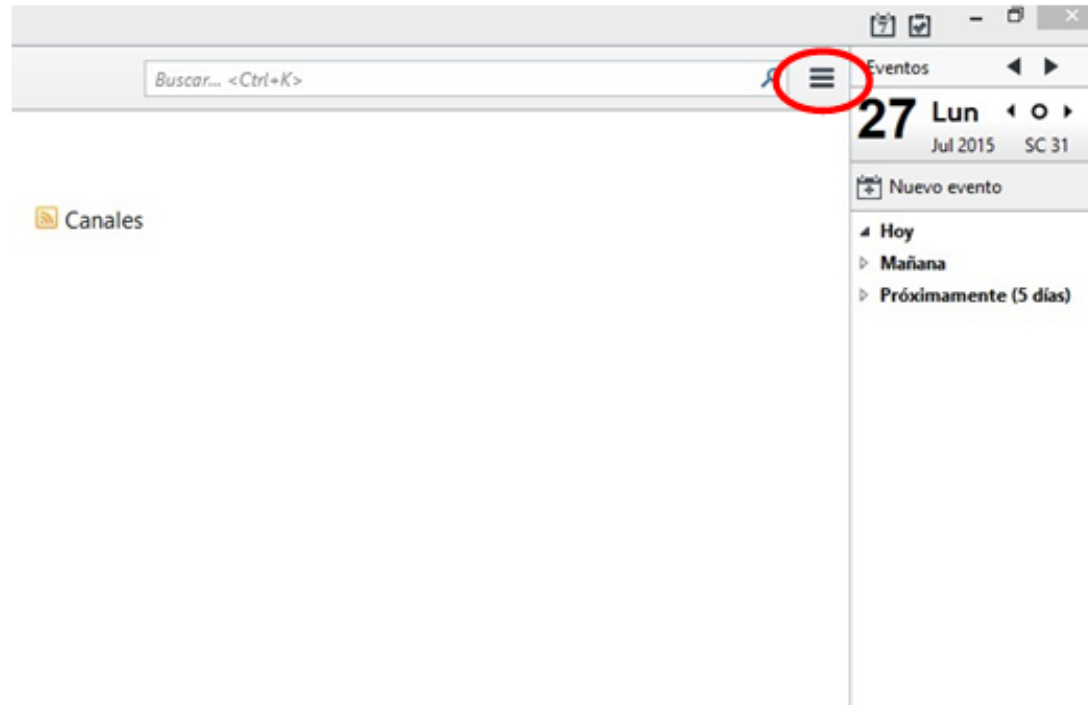
Nombre de usuario: uy.cnss

Obtener una nueva cuenta Config. manual **Hecho** Cancelar

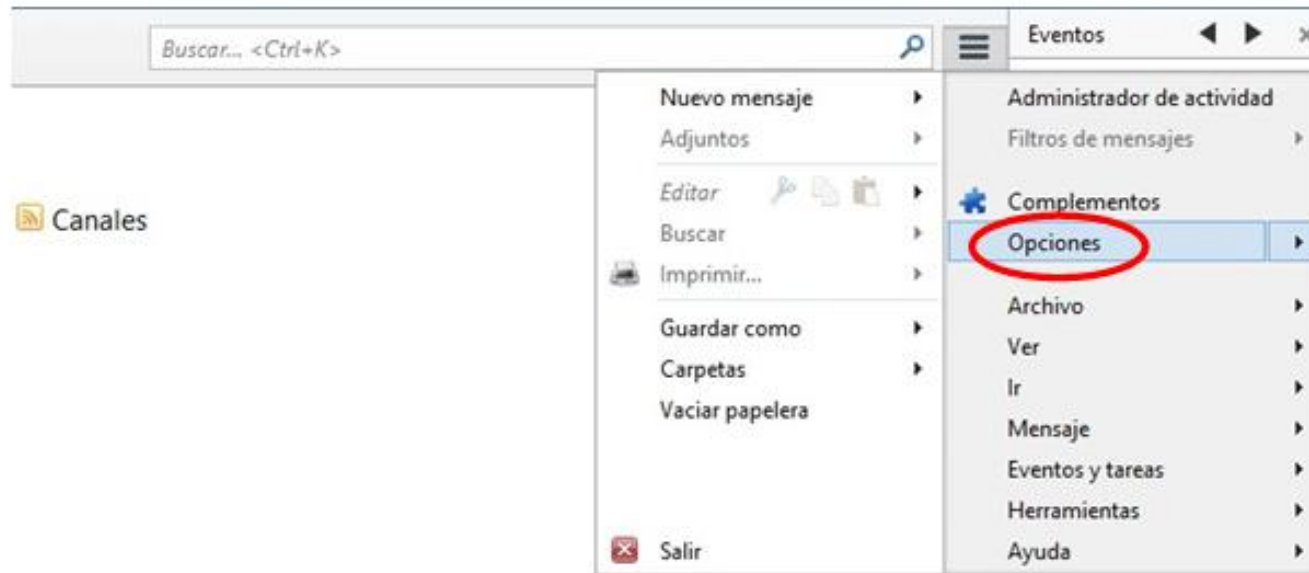
En algunos casos se deberá configurar manualmente dependiendo de cuál sea el web mail elegido. Para ellos hay que ir a “Config. manual”

Configuración para firma electrónica

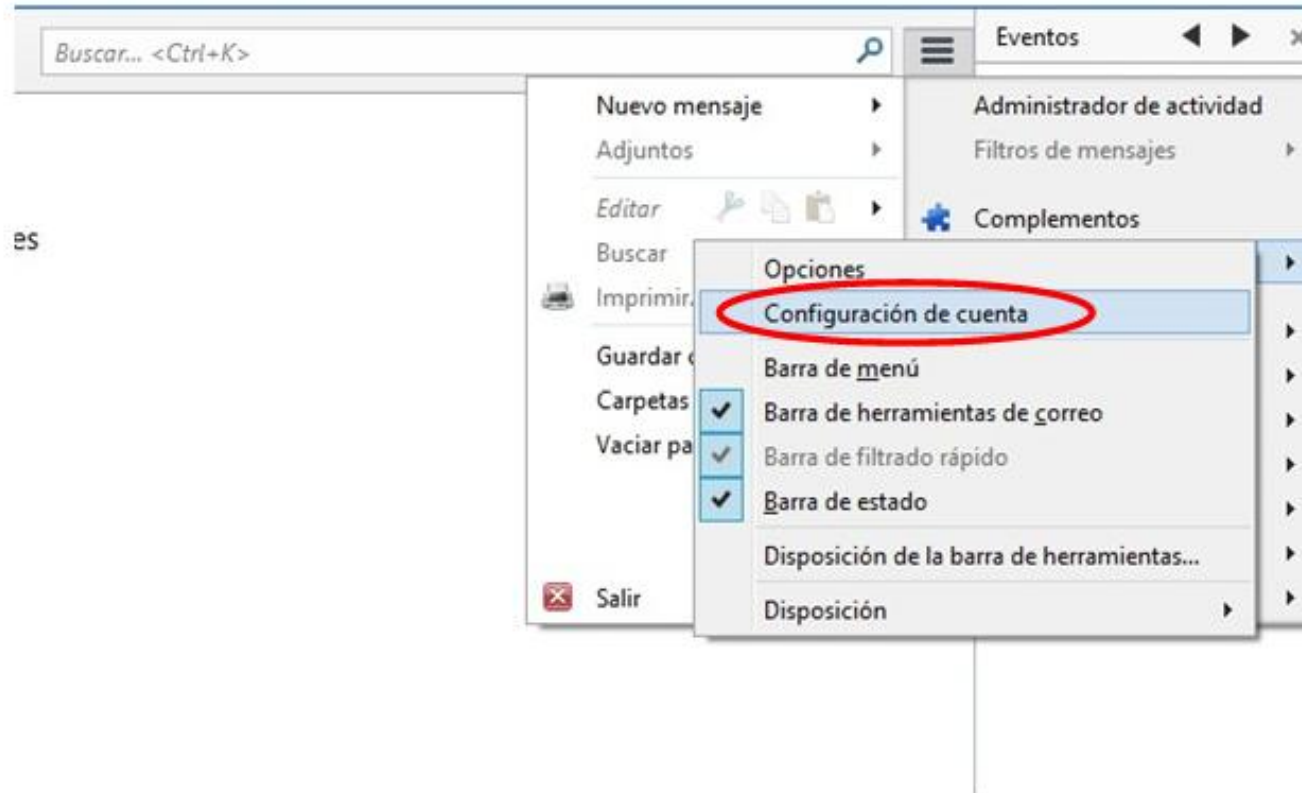
1)



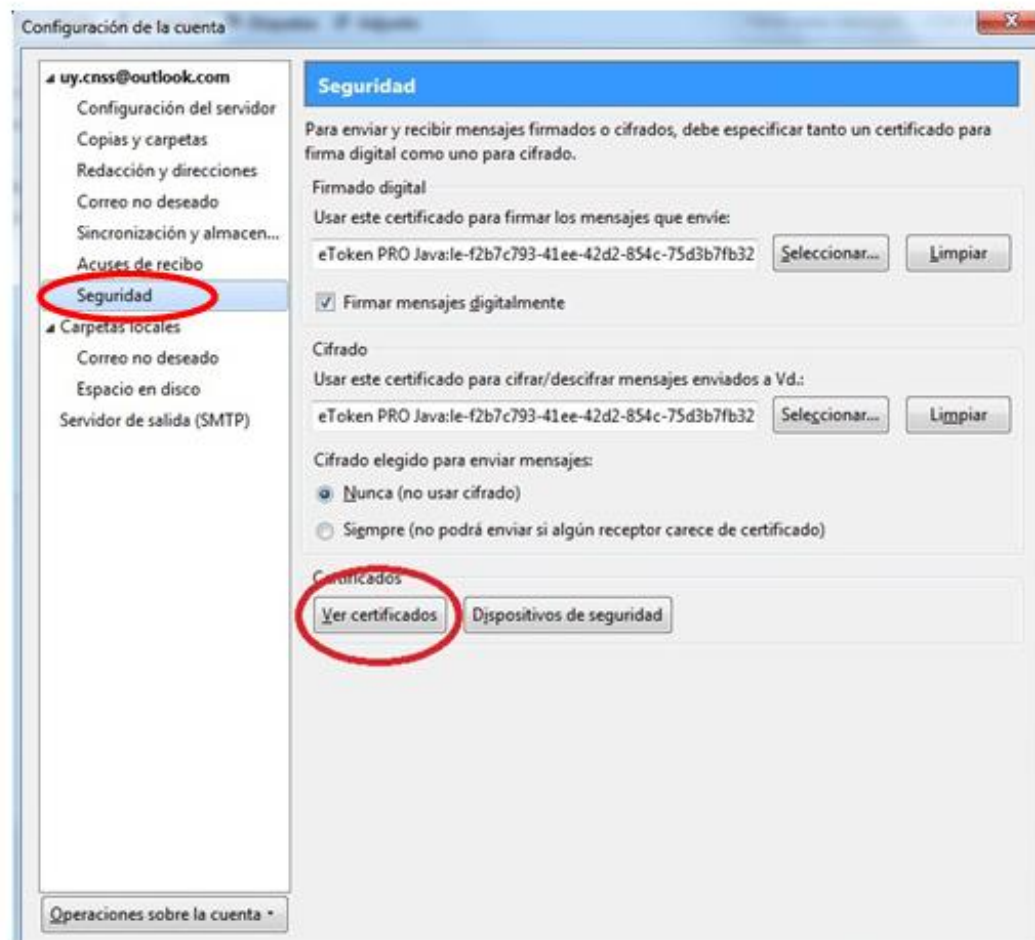
2)



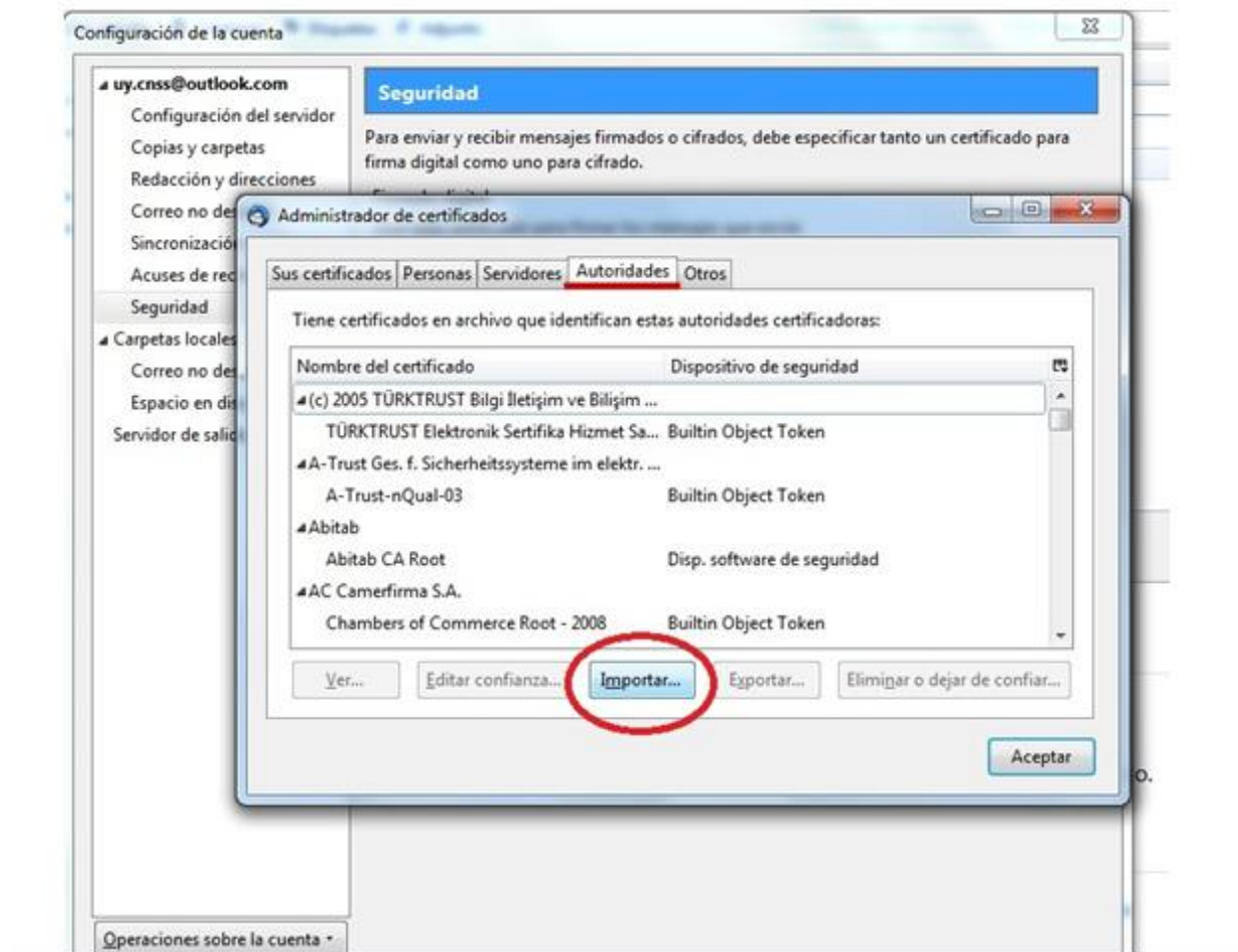
3)

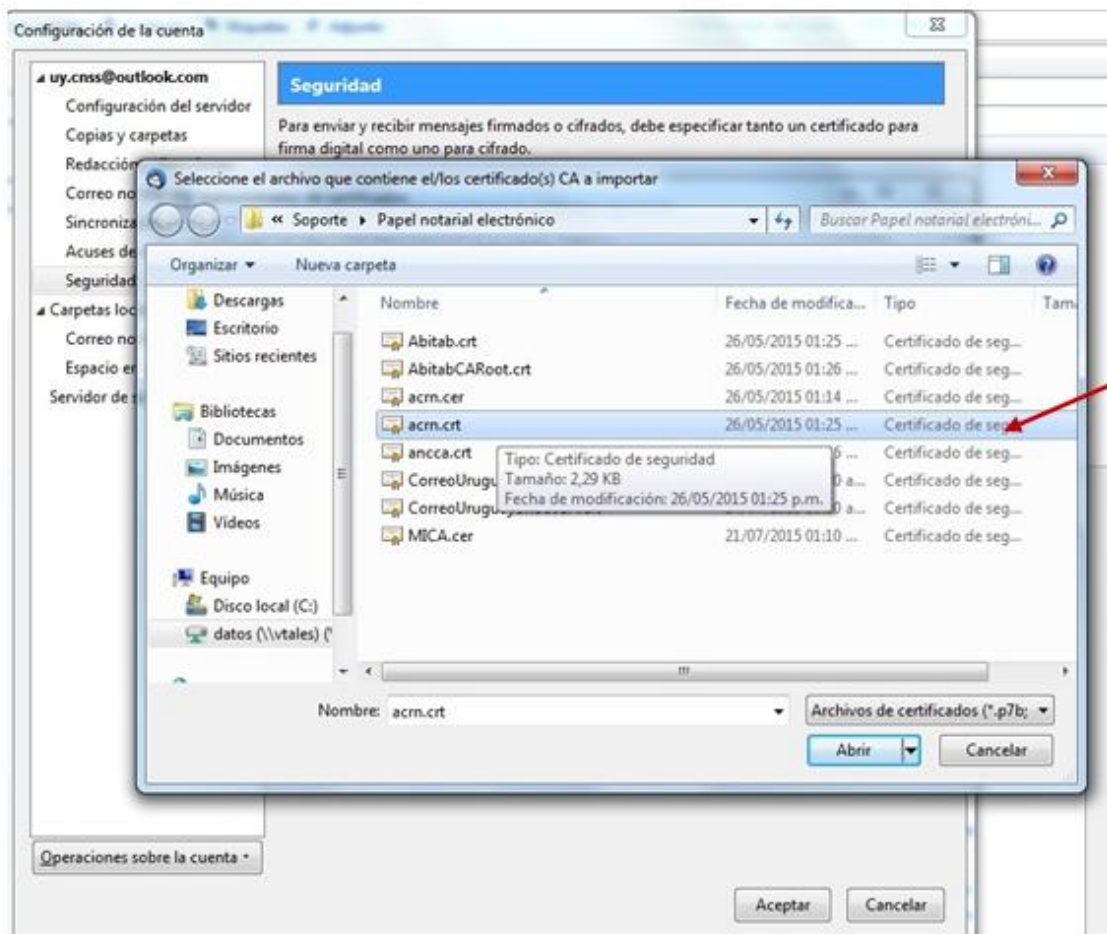


4) Ir a “Seguridad” y luego “Ver certificados”.



5) En la pestaña Autoridades Importamos los certificados Root.

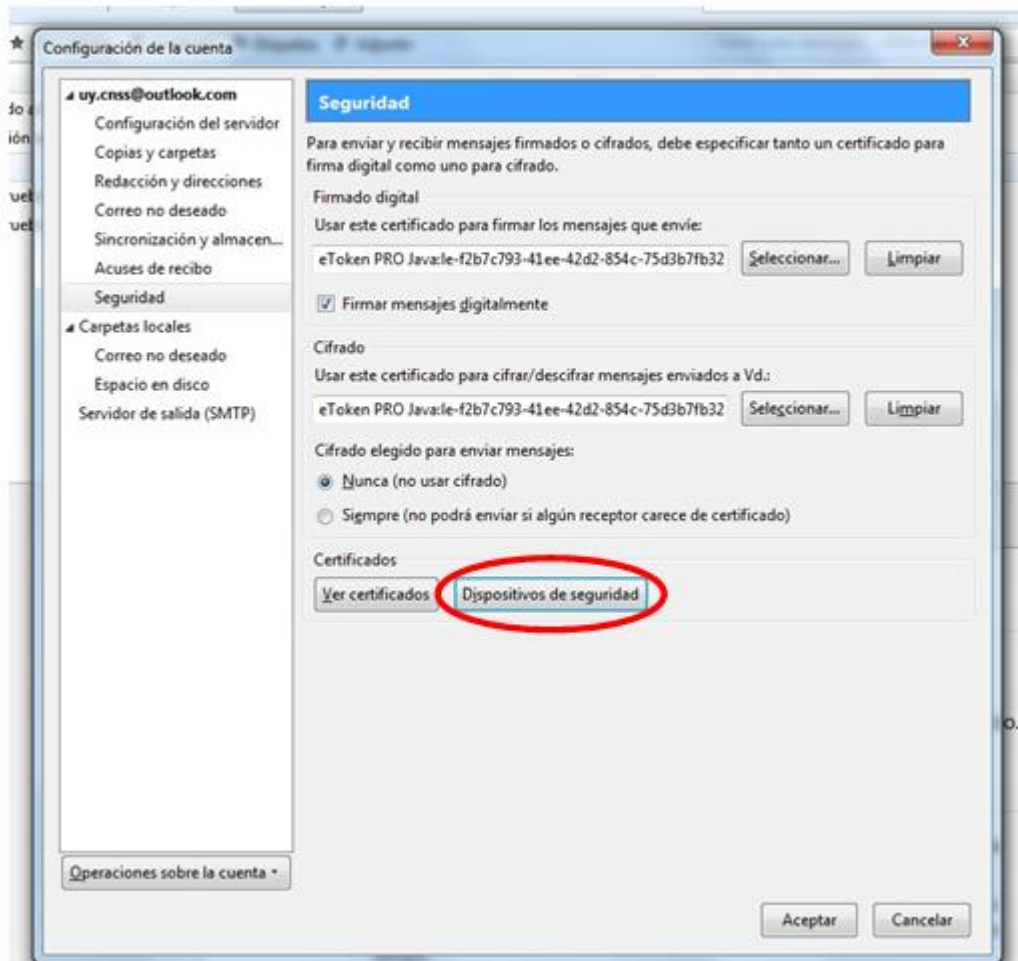




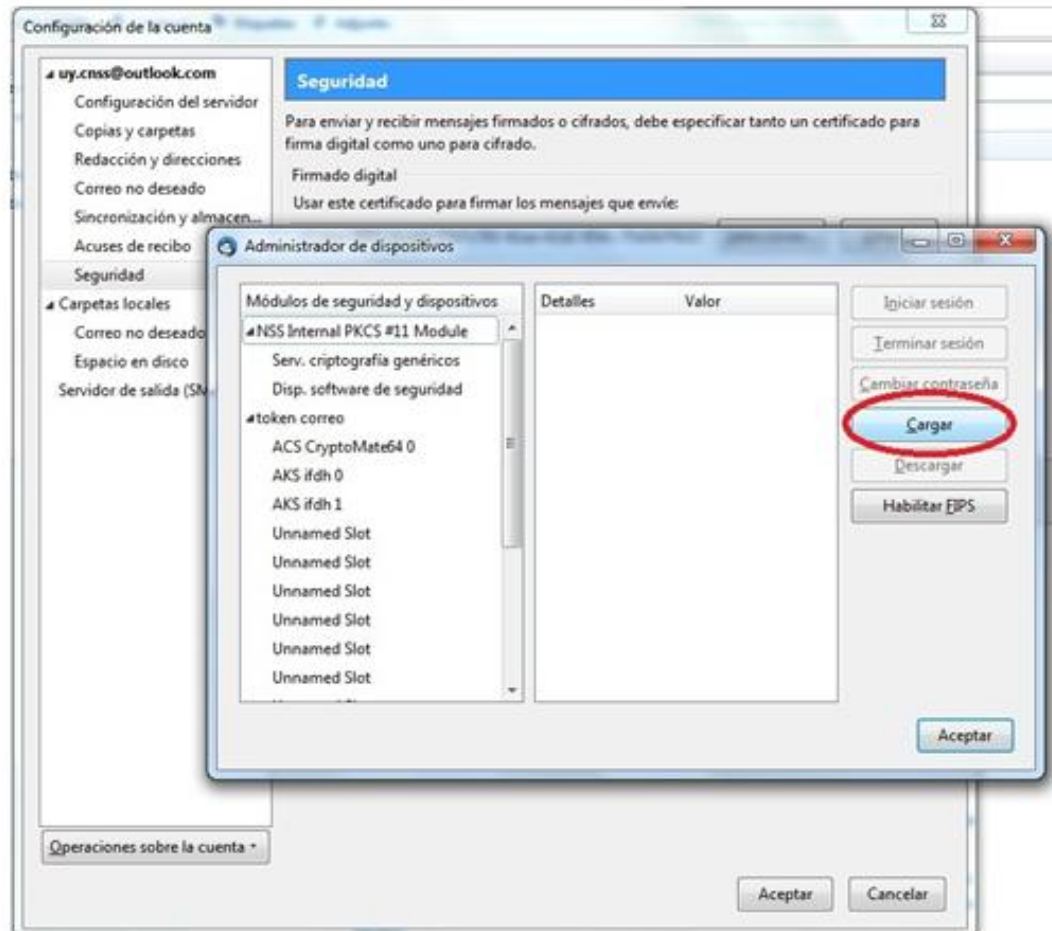
Seleccionamos el certificado correspondiente.

La ubicación dependerá de donde tengamos almacenados los certificados en la PC

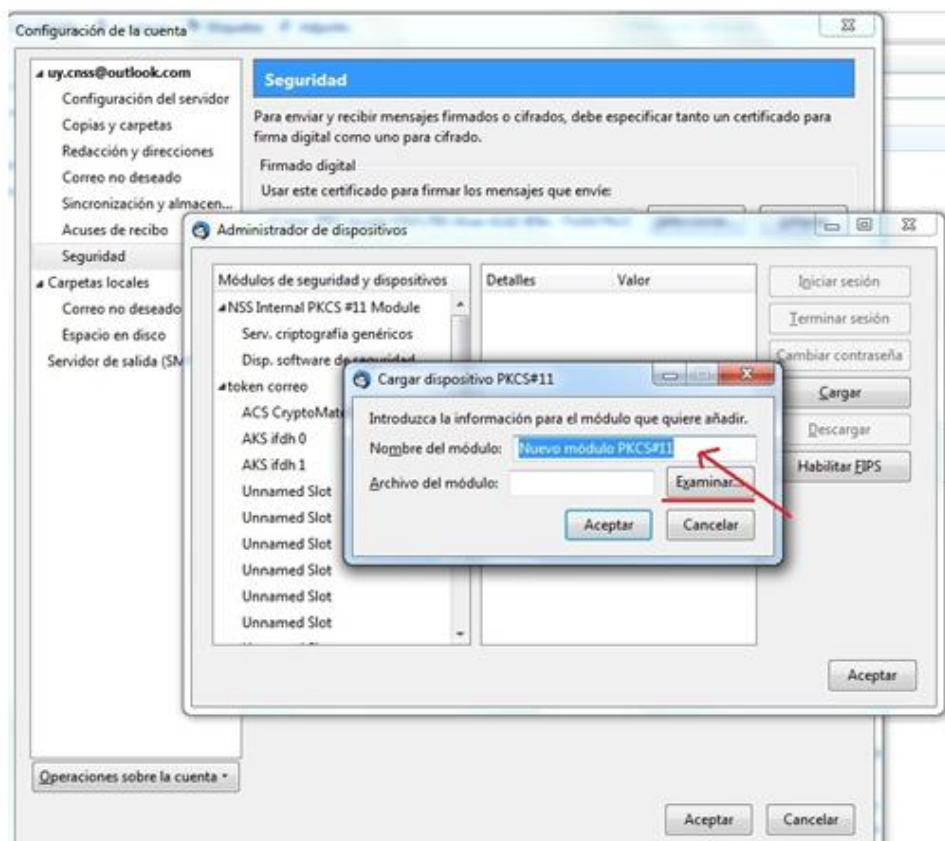
6) Para instalar el driver vamos a Dispositivos de seguridad.

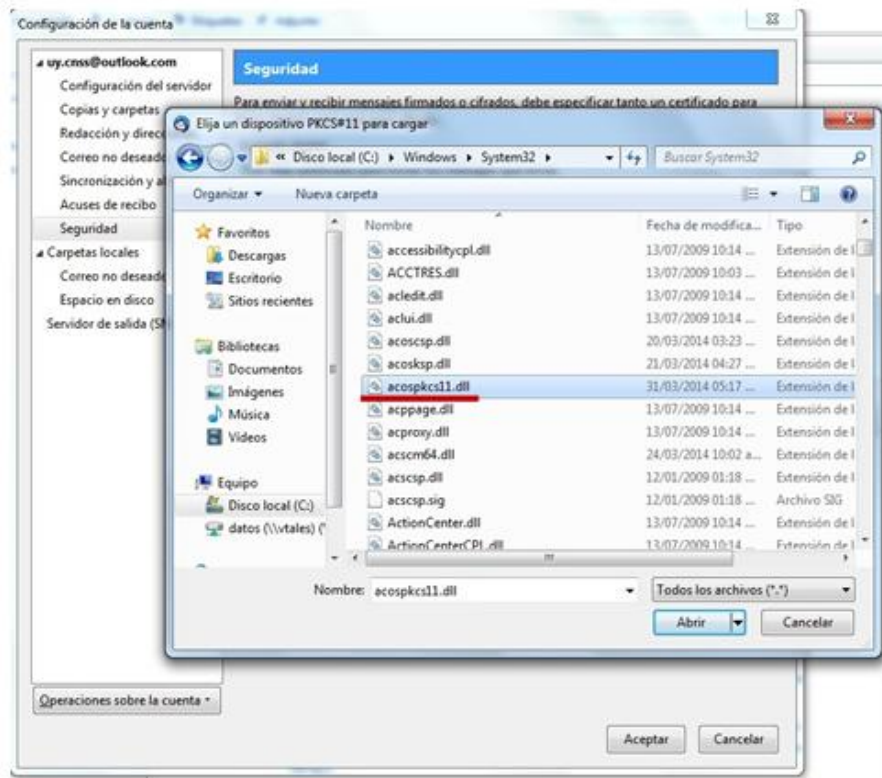


7) Clic en Cargar.



Se despliega una ventana pequeña en donde le asignamos un nombre al driver para poder identificar de qué organismo es. Por último vamos a examinar y seleccionamos el driver del token (archivo .dll).

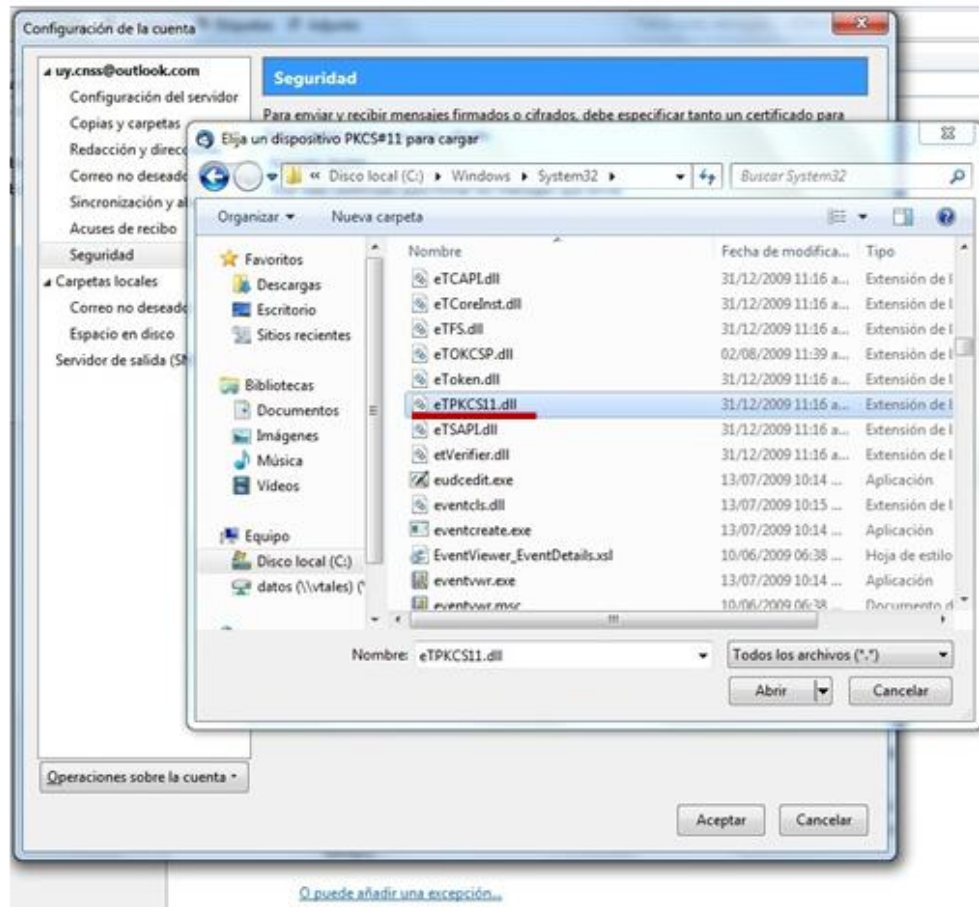




Para Abitab el driver es **acospkcs11.dll**

La ruta es:

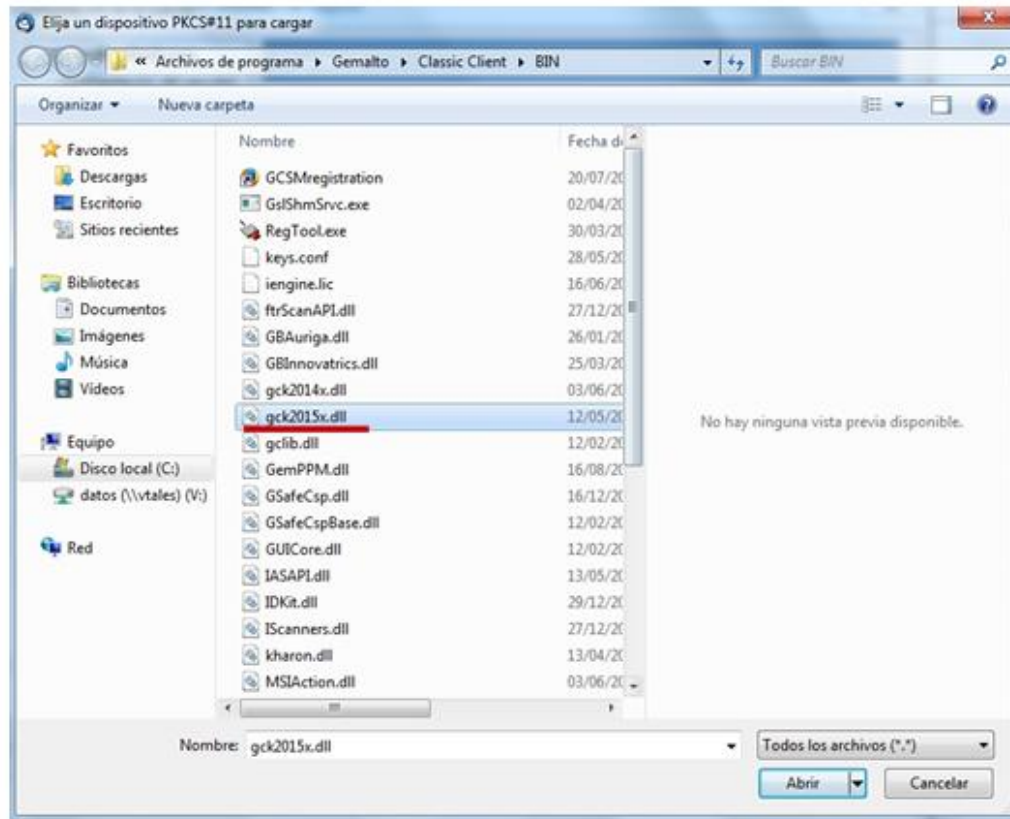
c:\Windows\System32



Para el Correo es **eTPKCS11.dll**

La ruta es:

c:\Windows\System32

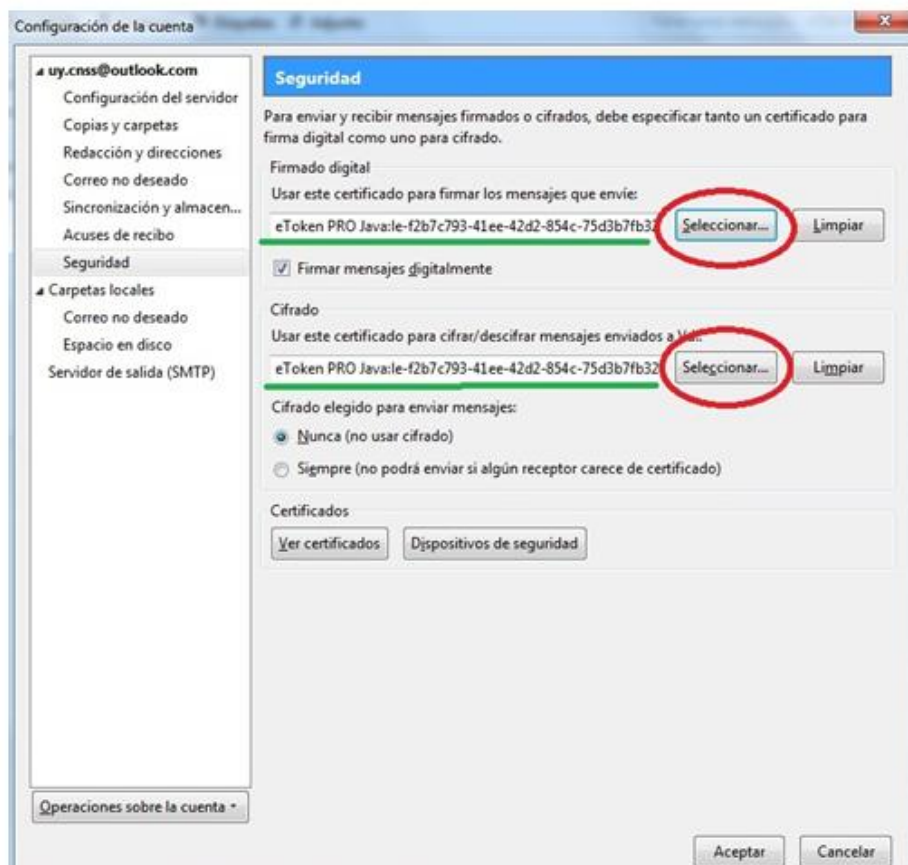


Para la Cédula Electrónica es
gck2015x.dll

La ruta es:

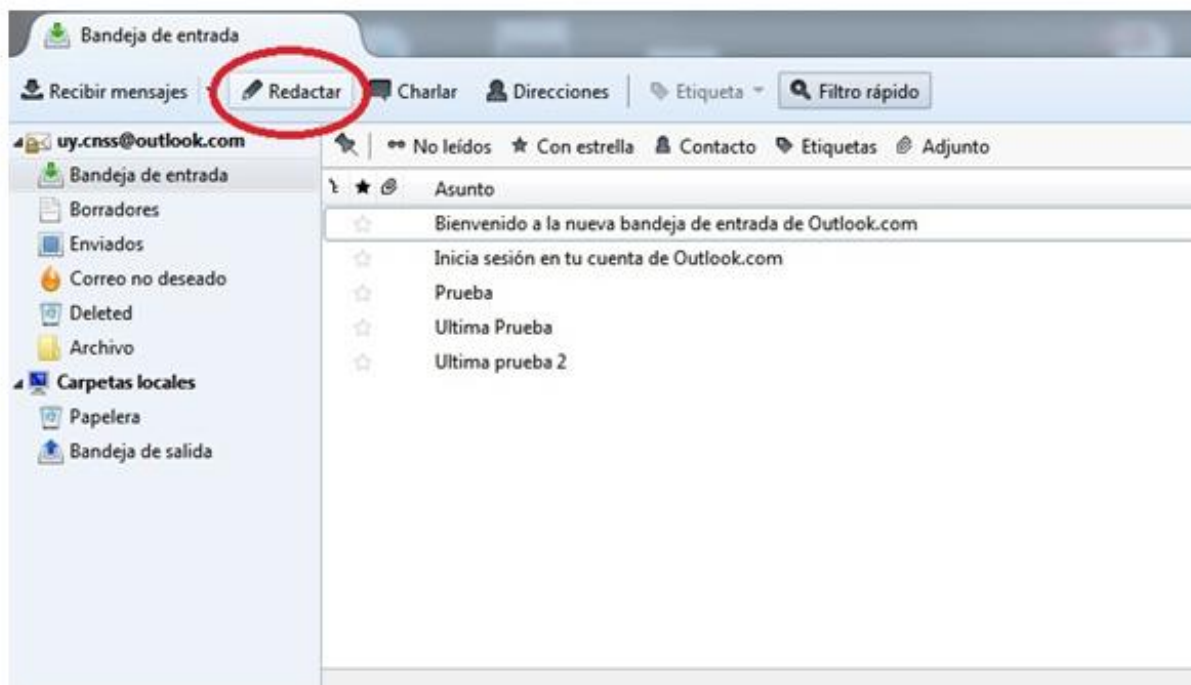
C:\Program Files\Gemalto\Classic
Client\BIN

7) Ya instalados los certificados y el driver debemos seleccionar el token en donde dice “Firma digital” y “Cifrado” como se muestra en la imagen a continuación:

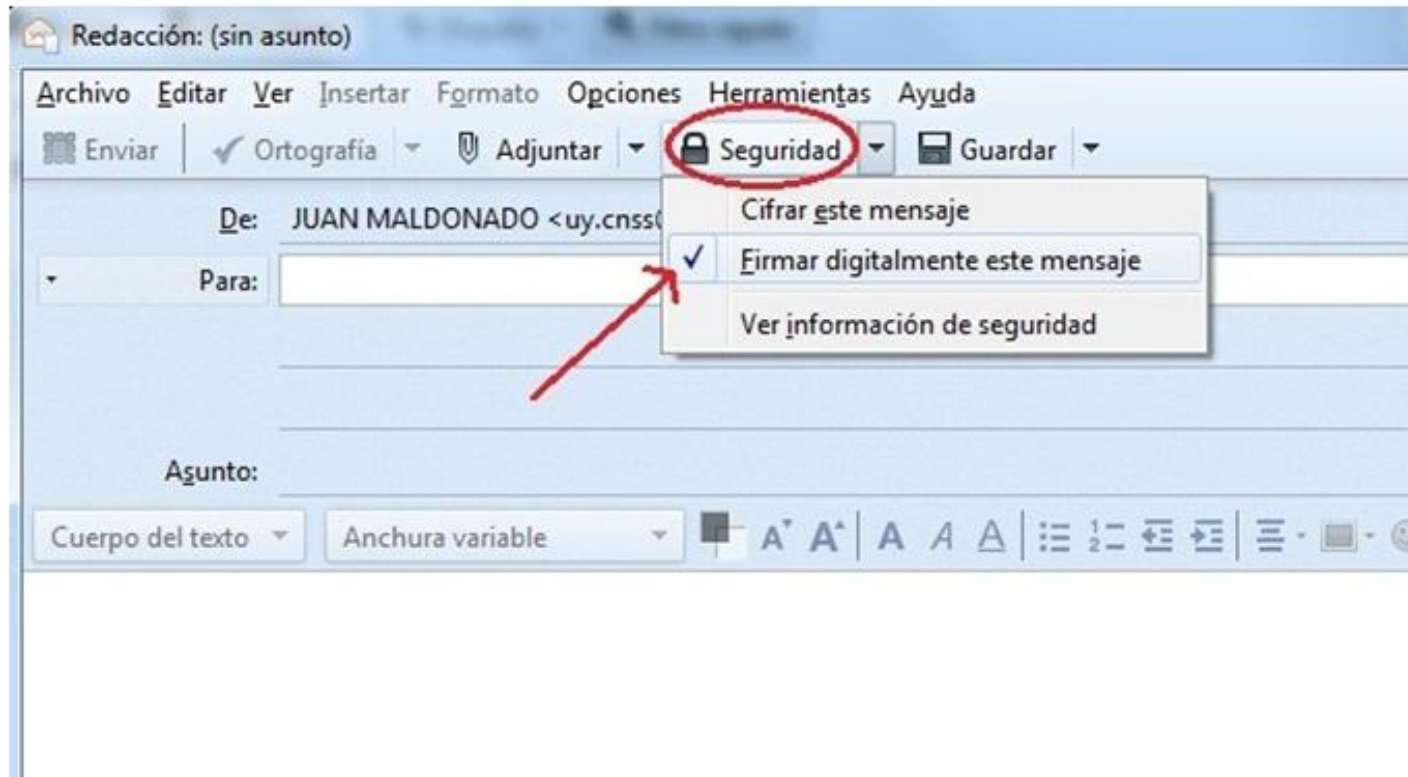


Firmar mails

1) Clic en “Redactar” para escribir nuestro mail.



2) Vamos a Seguridad y tildamos la opción “Firmar digitalmente este mensaje”.



5.2 Para cliente de correo Outlook

1) Configuración por primera vez

Outlook 2003, sobre Windows 7

Haga clic en Inicio y en Ejecutar, escriba regedit en el cuadro Abrir y, a continuación, haga clic en Aceptar.

Busque la siguiente clave del registro :

HKEY_CURRENT_USER \ SOFTWARE \ Microsoft \ Office \ 11.0 \ Outlook \ Security

Si no existe una clave del Registro de seguridad, crear una nueva clave . Para hacer esto, siga estos pasos:

Haga clic en la siguiente clave del registro :

HKEY_CURRENT_USER \ SOFTWARE \ Microsoft \ Office \ 11.0 \ Outlook

En el menú Edición , seleccione Nuevo y , a continuación, haga clic en Clave .

Escriba Seguridad y, a continuación , presione ENTRAR.

Haga clic en la clave de seguridad , haga clic en Nuevo y, a continuación, haga clic en Valor DWORD.

Escriba SuppressNameChecks , a continuación, presione ENTRAR.

En el menú Edición, haga clic en Modificar.

Escriba 1 y , a continuación, haga clic en Aceptar .

En el menú Registro, haga clic en Salir.

Outlook 2007, sobre Windows 7

Haga clic en Inicio y en Ejecutar, escriba regedit en el cuadro Abrir y, a continuación, haga clic en Aceptar.

Busque la siguiente clave del registro :

HKEY_CURRENT_USER \ SOFTWARE \ Microsoft \ Office \ 12.0 \ Outlook \ Security

Si no existe una clave del Registro de seguridad, crear una nueva clave . Para hacer esto, siga estos pasos:

Haga clic en la siguiente clave del registro :

HKEY_CURRENT_USER \ SOFTWARE \ Microsoft \ Office \ 12.0 \ Outlook

En el menú Edición , seleccione Nuevo y , a continuación, haga clic en Clave .

Escriba Seguridad y, a continuación , presione ENTRAR.

Haga clic en la clave de seguridad , haga clic en Nuevo y, a continuación, haga clic en Valor DWORD.

Escriba SupressNameChecks , a continuación, presione ENTRAR.

En el menú Edición, haga clic en Modificar.

Escriba 1 y , a continuación, haga clic en Aceptar .

En el menú Registro , haga clic en Salir .

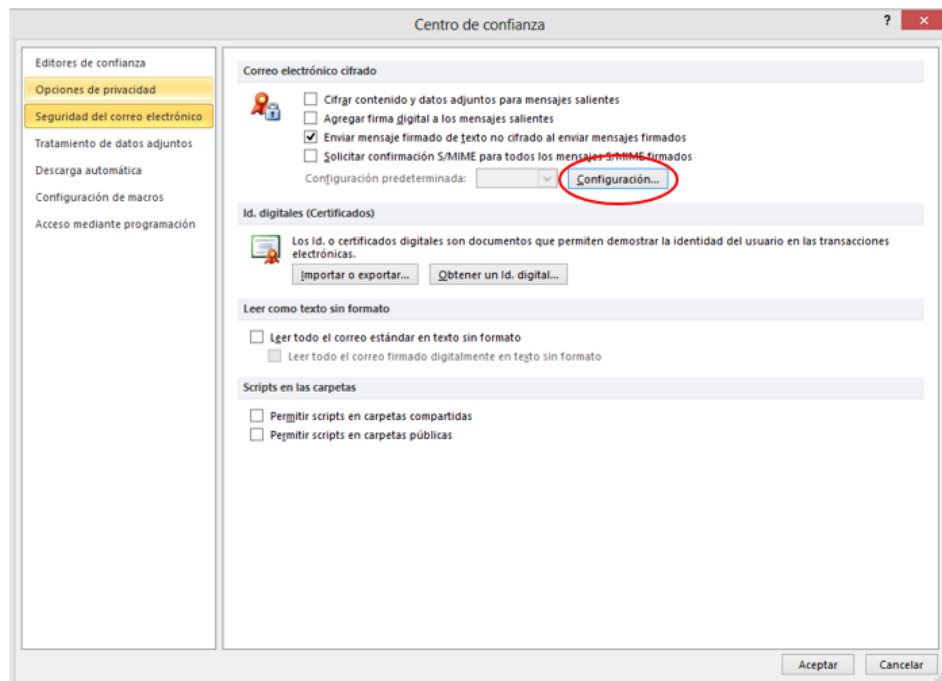
2) Para el envío de mails, según la versión de Outlook realice lo siguiente

Outlook 2007

- Menú **Herramientas>> Centro de Confianza**
- Luego, **Seguridad de Correo Electrónico**
- Seleccione **Configuración...**

Outlook 2010 y 2013

- Menú **Archivo>> Opciones**
 - Seleccione, **Centro de Confianza**
 - Presione **Configurar Centro de Confianza**
 - Luego, **Seguridad de Correo Electrónico**
 - Seleccione **Configuración...**
-



- 3) Establezca un nombre cualquiera a esta configuración. Presione ambos botones de “Elegir” y seleccione su certificado vigente en la lista que se le muestra, el resto de las opciones quedan por defecto tal cual se muestra a continuación. Presione Aceptar en todas las ventanas abiertas.

Cambiar la configuración de seguridad

Preferencias de configuración de seguridad

Nombre de configuración de seguridad:
Mi Configuración

Formato de cifrado: S/MIME

Configuración predeterminada para este formato de mensaje cifrado

Configuración predeterminada para todos los mensajes cifrados

Etiquetas de seguridad... Nueva Eliminar Contraseña...

Certificados y algoritmos

Certificado de firma: ADRIANA LUCÍA CORREA BURGOS Elegir...

Algoritmo de tipo hash: SHA1

Certificado de cifrado: ADRIANA LUCÍA CORREA BURGOS Elegir...

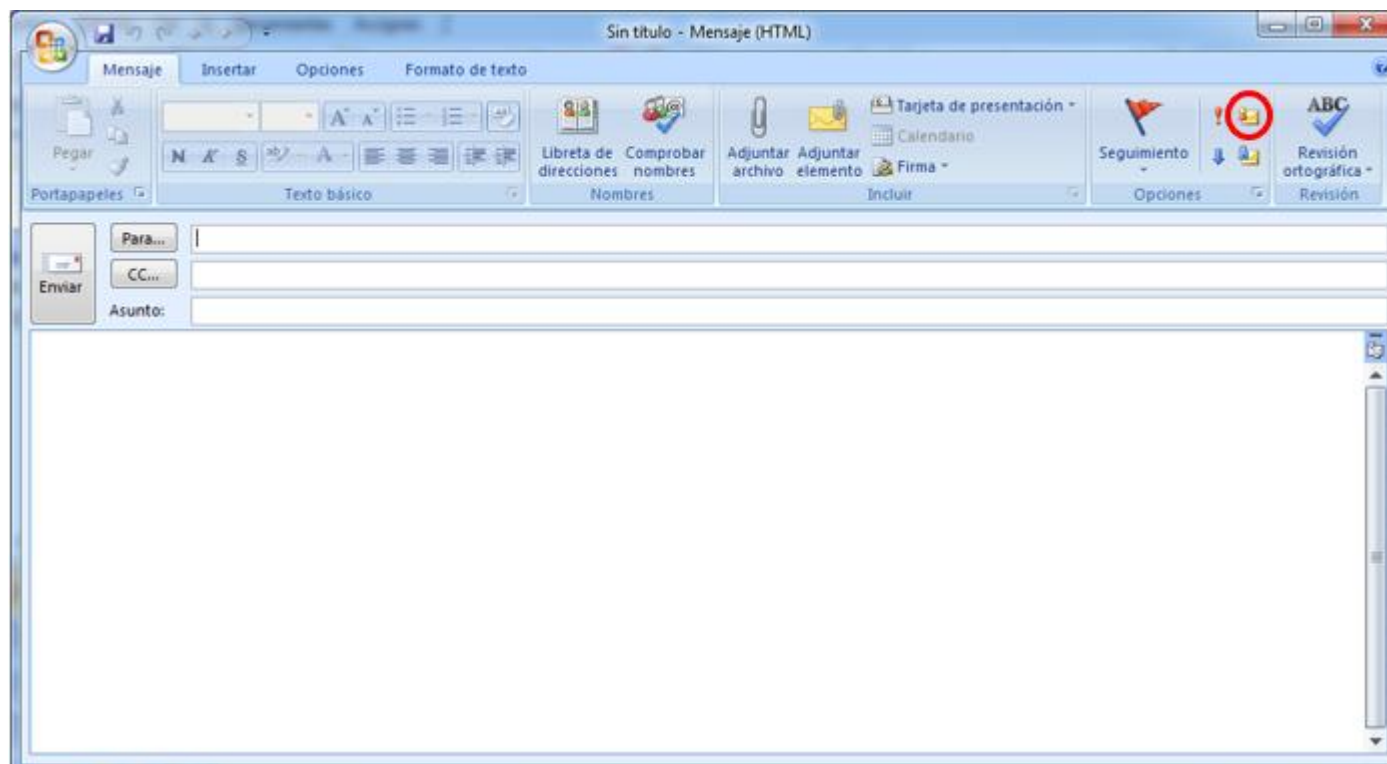
Algoritmo de cifrado: 3DES

Enviar estos certificados con mensajes firmados

Aceptar Cancelar

Firmar un correo en Outlook 2007

En la ventana de redacción de un mail, pestaña Mensaje, marcar el Icono de "Firmar Digitalmente" (seleccionado en la imagen) y enviar el mail con normalidad.



Firmar un correo en Outlook 2010 y 2013

En la ventana de redacción de un mail, pestaña Opciones, marcar el Icono de "Firmar Digitalmente" (seleccionado en la imagen) y enviar el mail con normalidad.

