CAJA COSTARRICENSE DE SEGURO SOCIAL

GERENCIA ADMINISTRATIVA

Dirección Servicios Institucionales
Área Publicaciones e Impresos

GUÍA

Firma Digital para Documentos Institucionales

GA-DSI-API- GT007

Versión 01
Febrero 2023

Firmas de Aprobación

Elaborado / modificado	Unidad	Firma
Beatriz Guzmán Meza	Área Publicaciones e Impresos	MARIA BEATRIZ GUZMAN MEZA (FIRMA) Firmado digitalmente por MARIA BEATRIZ GUZMAN MEZA (FIRMA) Fecha: 2023.02.06 17:28:17 -06'00'
Jennifer Zúñiga Ruiz	Subárea Archivo y Correspondencia	

Revisado	Unidad	Firma
Gerardo Salazar González, Jefe	Área Publicaciones e Impresos	GERARDO ANTONIO SALAZAR GONZALEZ (FIRMA) Firmado digitalmente por GERARDO ANTONIO SALAZAR GONZALEZ (FIRMA) Fecha: 2023.02.06 17:34:50 -06'00'

Aprobado	Unidad	Firma
Giorgianella Araya Araya, Directora	Dirección de Servicios Institucionales	GIORGIANELIA ARAYA ARAYA (FIRMA)

I. Introducción

Esta guía describe el proceso de firma digital y validación de esta para documentos en formato PDF, utilizando las aplicaciones recomendadas a nivel Institucional.

Estas aplicaciones permiten el firmado de documentos electrónicos de tipo PDF de forma muy fácil y dando garantía la validez de esa firma a lo largo del tiempo con todos elementos necesarios, esto último lo que se conoce como Formato Avanzado de Firma Digital, PADES LTV.

PADES LTV (long-term validación), es un estándar para añadir la Firma Digital a un documento PDF utilizando firma digital avanzada que garantiza que los documentos firmados digitalmente contienen todos los elementos que permiten validar su firma durante largos períodos de tiempo. Existen diferentes niveles de PADES, sin embargo, la guía contempla la configuración del nivel PADES-LTV, que se reconoce como el nivel oficial para Costa Rica.

PADES LTV añade estampas de tiempo, cadenas de certificados y la información de revocación a los documentos firmados digitalmente, lo que permite verificar su validez en un futuro incluso si las fuentes originales (de consulta de certificados o de listas de revocación) no estuvieran disponibles, garantizando así la robustez tecnológica que brinda validez legal a la firma digital del documento electrónico en el tiempo.

Para poder adjuntar la firma digital a los documentos electrónicos en su computadora, un requisito previo es haber realizado la instalación de los drivers de firma digital. Todos los drivers, así como la configuración necesaria de la confianza en la jerarquía nacional de certificación digital, pueden ser obtenidos en cualquier momento desde el sitio http://www.soportefirmadigital.com.

II. Objetivo

Describir los pasos que se deben seguir para la configuración de aplicativos que permitan la firma digital conforme a la normativa, esto con el fin de garantizar una correcta producción y recepción de documentos firmados digitalmente en las unidades Institucionales.

III. Alcance

Este documento es de aplicación para los funcionarios de la Institución que gestionan documentos digitales con firma digital.

IV. Marco Normativo

1. Procedimiento para la gestión de correspondencia GA-DSI-API-PR005.

V. Definiciones

Fecha oficial de la firma: Fecha en que una autoridad competente ubica la firma en el tiempo.

Firma digital: Entiéndese por firma digital cualquier conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico. Una firma digital se considerará certificada cuando sea emitida al amparo de un certificado digital vigente, expedido por un certificador registrado.” (Asamblea Legislativa, 2005, art.8).

Firmante: Persona física o jurídica que realizó la firma digital.

Garantía de integridad y autenticidad: El documento no ha sido modificado después de ser firmado. Las firmas fueron realizadas con certificados digitales de la jerarquía nacional.

Garantía de validez en el tiempo: El documento contiene todos los elementos que aseguran la validez de las firmas a través del tiempo.

SAYC: Sistema de Archivo y Correspondencia.

Validación de firmas digitales: La validación de una firma electrónica es el proceso por el que se comprueba la identidad del firmante, la integridad del documento firmado y la validez temporal del certificado utilizado. (Gobierno de España. Portal administración electrónica).

VI. Firmador de Documentos

A continuación, se describe el proceso para la instalación de los firmadores digitales que cumplen con los requisitos técnicos establecidos por el Ministerio de Ciencia Tecnología y Telecomunicaciones (MICITT); no obstante, en caso de requerir asesoría se debe solicitar a los Centros de Gestión Informática (CGI) quienes gestionarán lo correspondiente en coordinación con la Dirección de Tecnología y Comunicaciones (DTIC).

6.1. Firmador SAYC

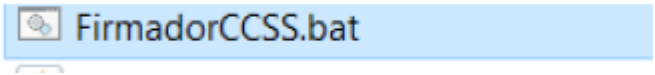
El firmador de documentos del sistema de archivo y correspondencia SAYC de la Institución, se puede utilizar tanto desde el aplicativo como fuera del mismo, a continuación, los pasos para firmar documentos dentro del SAYC:

1. Descargar la siguiente carpeta y descomprimir en la siguiente dirección: C:\Users\usuario

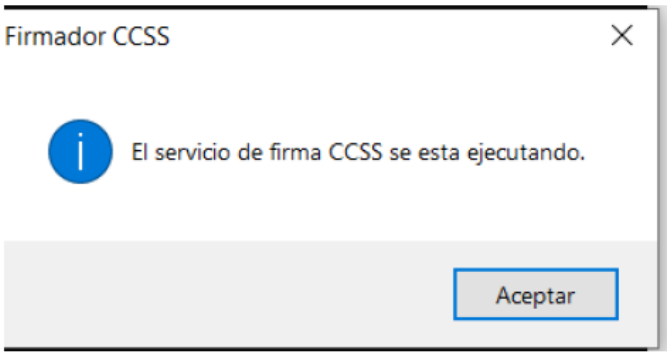
https://sayc.ccss.sa.cr/SAYC/documento/FirmadorCCSS.rar

Se debe visualizar así:

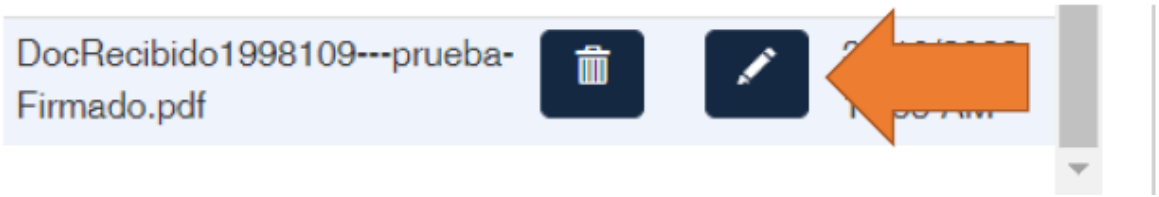
2. Ejecutar el archivo FirmadorCCSS.bat



3. Debe visualizar el siguiente mensaje:



4. Abrimos el sistema SAYC Web y seleccionamos el documento que deseamos firmar:



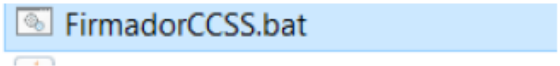
Para utilizar el firmador del SAYC fuera del sistema, se deben realizar los siguientes pasos:

1. Descargar la siguiente carpeta y descomprimir en la siguiente dirección: C:\Users\usuario

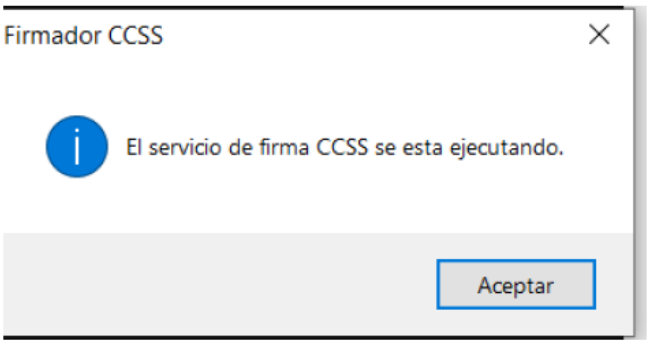
https://sayc.ccss.sa.cr/SAYC/documento/FirmadorCCSS.rar

Se debe visualizar así:

2. Ejecutar el archivo FirmadorCCSS.bat

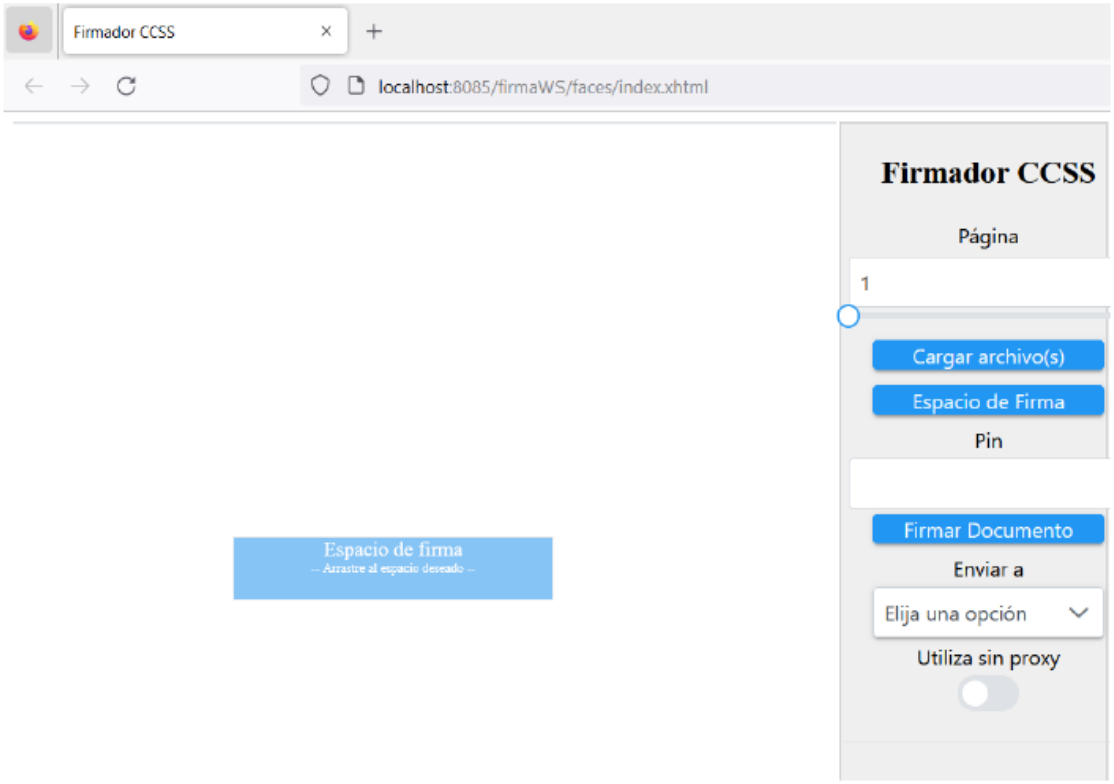


3. Debe visualizar el siguiente mensaje:



4. Se ejecuta el enlace ubicado en el escritorio con el nombre: Abrir FirmadorCCSS.url

5. Se despliega la nueva interfaz para cargar documentos y firmarlos.

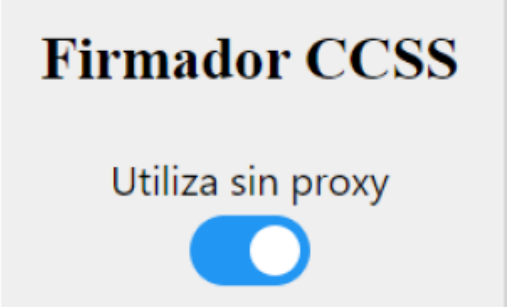


Consideraciones importantes del firmador del SAYC:

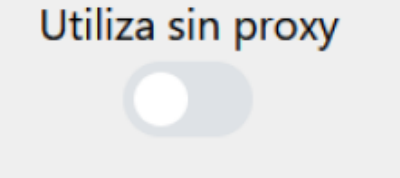
a. Los documentos firmados quedan automáticamente en el SAYC, para visualizarlo solamente se vuelve a seleccionar el oficio en el SAYC para que cargue los nuevos anexos.

b. Los documentos firmados quedan en la siguiente ubicación C:\Users\usuario\FirmaTemp

c. En modalidad teletrabajo active la opción:



d. En la oficina desactive la opción:



e. En caso de inconvenientes a la hora de abrir el firmador del SAYC, descargar y ejecutar el java que se encuentra en la siguiente carpeta:

https://cajacr-my.sharepoint.com/:u:/g/personal/ctorresa_ccss_sa_cr/EQdTe8JayTBMk9ENGFXzDAsBGcHVke3DCfYwMKrWK-NeRA?e=guYfEa

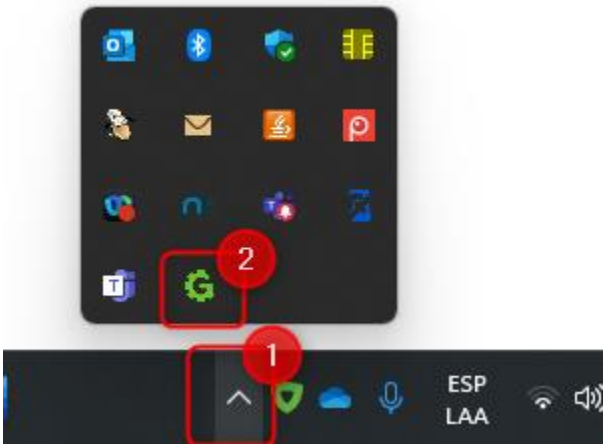
6.2. Agente GAUDI

Actualmente el Banco Central cuenta con la aplicación Agente GAUDI que realiza la autenticación y firma en las diferentes páginas web que se utilizan, con el objetivo de homologar el método de autenticación y firma, ya que en este momento las plataformas utilizan diferentes métodos por medio de complementos que en su mayoría están sin soporte o cerca de estarlo, tales como el Capicom, Hermes Digital y el Java.

Dado lo anterior, para activarlo se deben realizar los siguientes pasos:

Lo primero es verificar si la computadora tiene instalado el Agente GAUDI:

1. En la barra en la parte inferior derecha de sus equipos

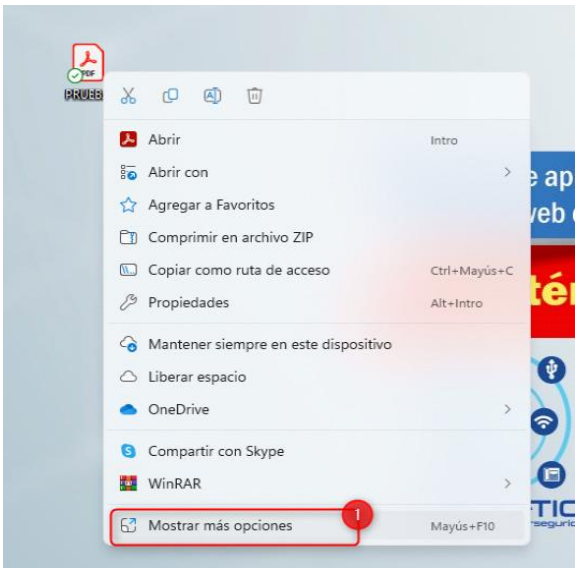


Si tienen la firma insertada en el equipo esa “G” se verá en verde (conectado), si la quita se verá en gris (desconectado), **si la tienen en rojo o no aparece la “G”** deben realizar los siguientes pasos:

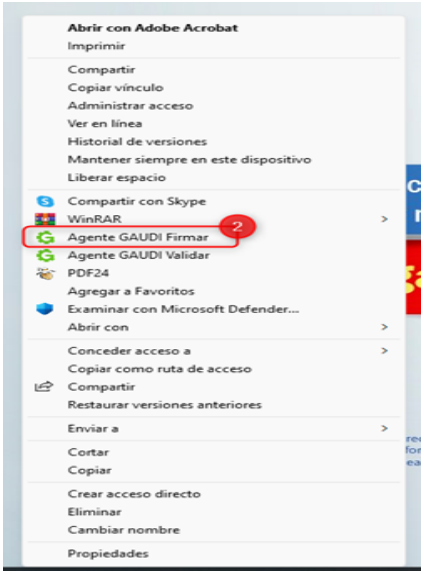
2. Volver a instalar los drivers de firma digital en el siguiente enlace https://www.soportefirmadigital.com/web/es/ y seleccionan descargar instaladores:

3. Una vez que se tiene GAUDI instalado, se puede iniciar con la firma del documento con los siguientes pasos:

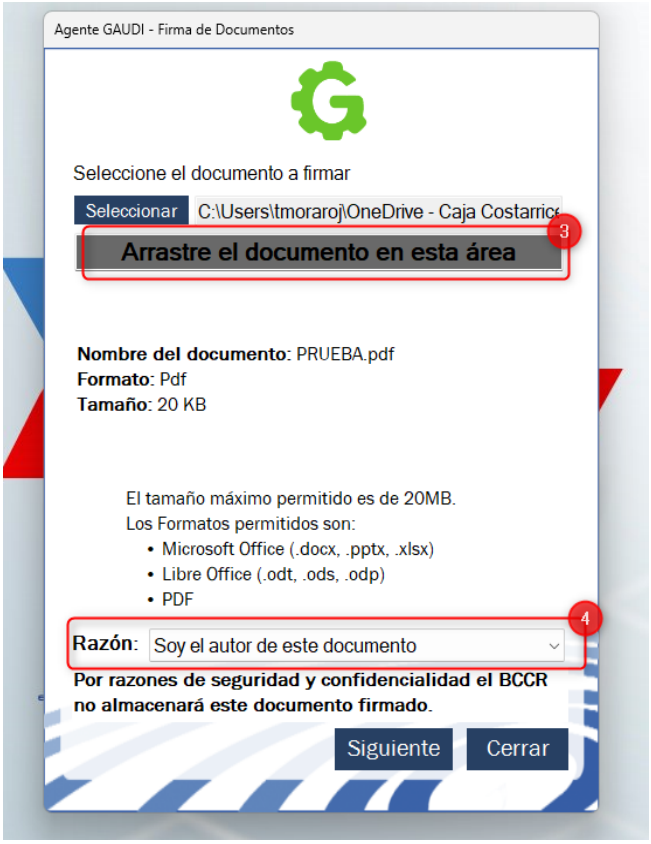
   a) Convierta el documento a PDF
   b) Inserte la firma en la computadora (la “G” tiene que estar en verde)
   c) Darle clic derecho sobre el documento que va a firmar (sin abrir) y seleccione **Mostrar más opciones**:



   d) Se desplegará un menú como este: Seleccione **Agente GAUDI Firmar**



e) Se abre una pantalla como la siguiente: donde dice “Arrastre el documento en esta área”, debe arrastrar el documento que desea firmar y seleccionar de la lista desplegable donde dice **Razón** y elegir la opción que corresponda.



f) Seguidamente se despliega una pantalla como esta, en donde se tiene que insertar el **PIN** de su firma digital y firmar:

g) Aparece una pantalla como la siguiente: si le dan **Abrir** le abre el documento, **Cerrar** elimina el cuadro con el mensaje y **Examinar** abre las carpetas.

Por lo anterior es importante recordar que, con este firmador ya no se observará el sello de agua al abrir el documento con otro software o cualquier gestor de aplicaciones (como el Adobe Acrobat Reader), lo que podría dar la impresión de que el documento está en blanco y no se firmó.

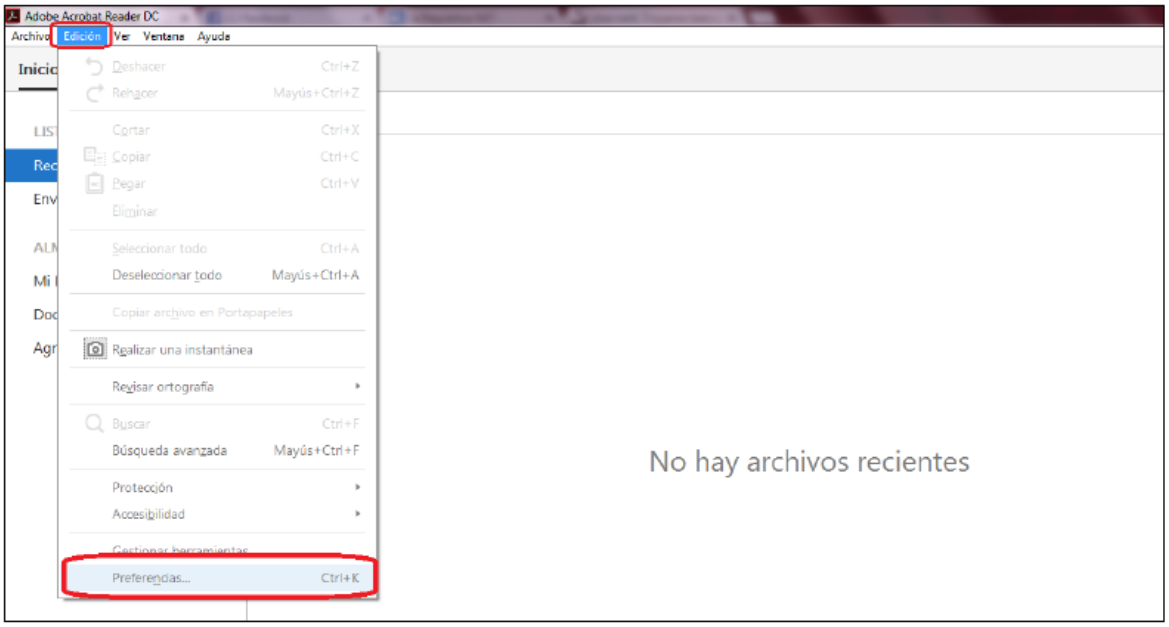
Por lo que se recomienda no dejar el espacio en blanco, dado que algunas unidades lo podrían devolver (a pesar de que es obligación del receptor verificar la firma del documento), por tanto se sugiere incluir en donde usualmente se encuentra el nombre del firmante del documento alguna imagen similar a la siguiente.

6.3. Adobe Acrobat Reader

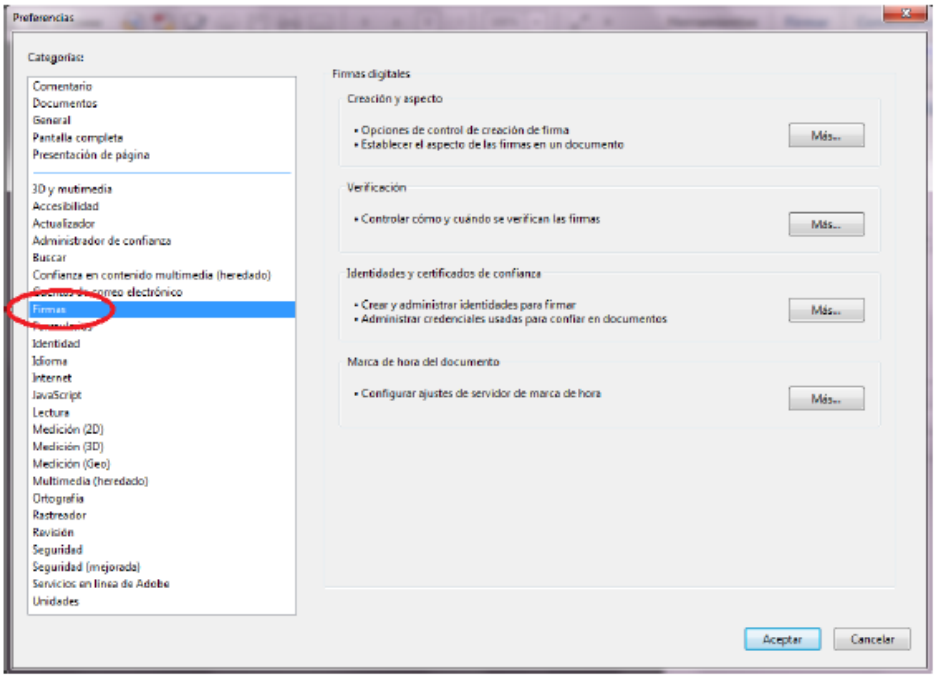
Para utilizar la Firma Digital en Adobe se debe configurar en el equipo y en la misma herramienta la confianza en la Jerarquía Nacional de Certificación Digital para que las firmas contenidas en los documentos puedan ser validadas sin ningún problema. Igualmente se debe asegurar que cuenta con la versión más actualizada de Adobe Reader DC, a continuación, se explican los pasos para configurar Adobe Reader DC para que pueda firmar y verificar documentos electrónicos de tipo PDF con los formatos oficiales de Firma Digital establecidos en Costa Rica:

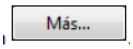
La configuración se realiza siguiendo los siguientes pasos:

1. Abrir Adobe Reader.
2. Seleccionar la opción **Edición** > **Preferencias** en el menú Principal.

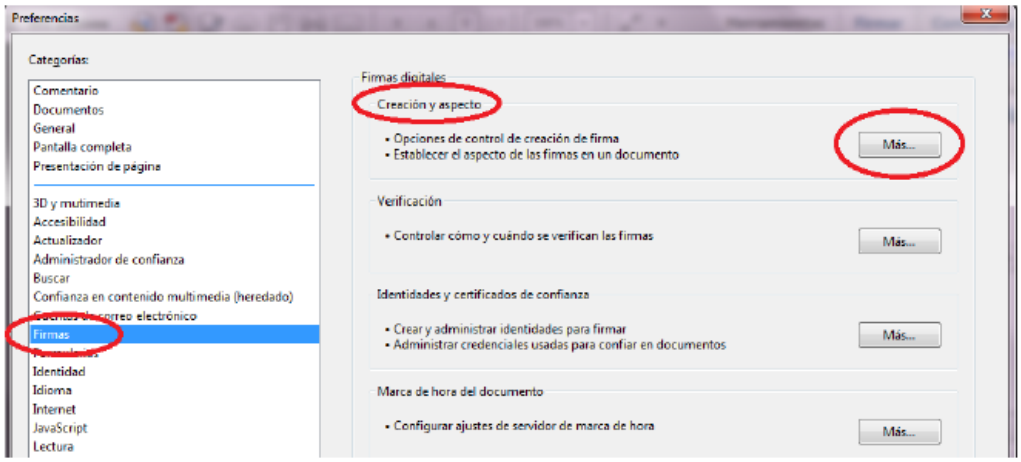


3. En la ventana de Preferencias que se muestra, elija de las Categorías que vienen en el lado izquierda la de **Firmas.** En el lado derecho se muestran las opciones de Firmas digitales que vamos a configurar.

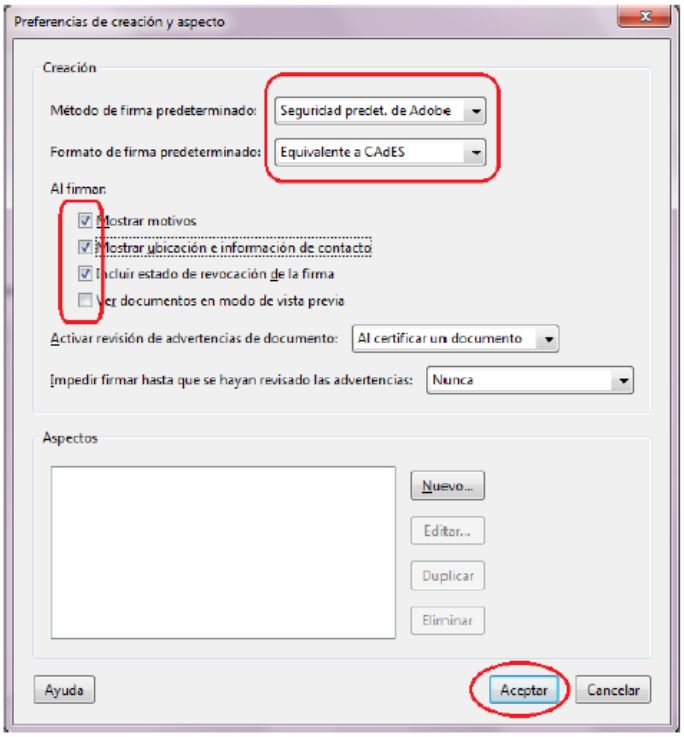


4. Elegimos la opción de la derecha **Creación y aspecto,** haciendo clic en el botón, 

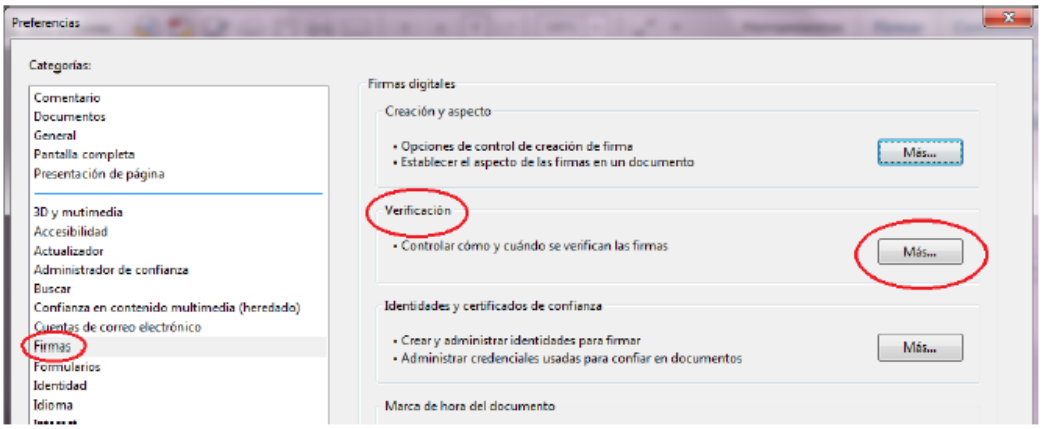
tal como lo muestra la siguiente imagen:



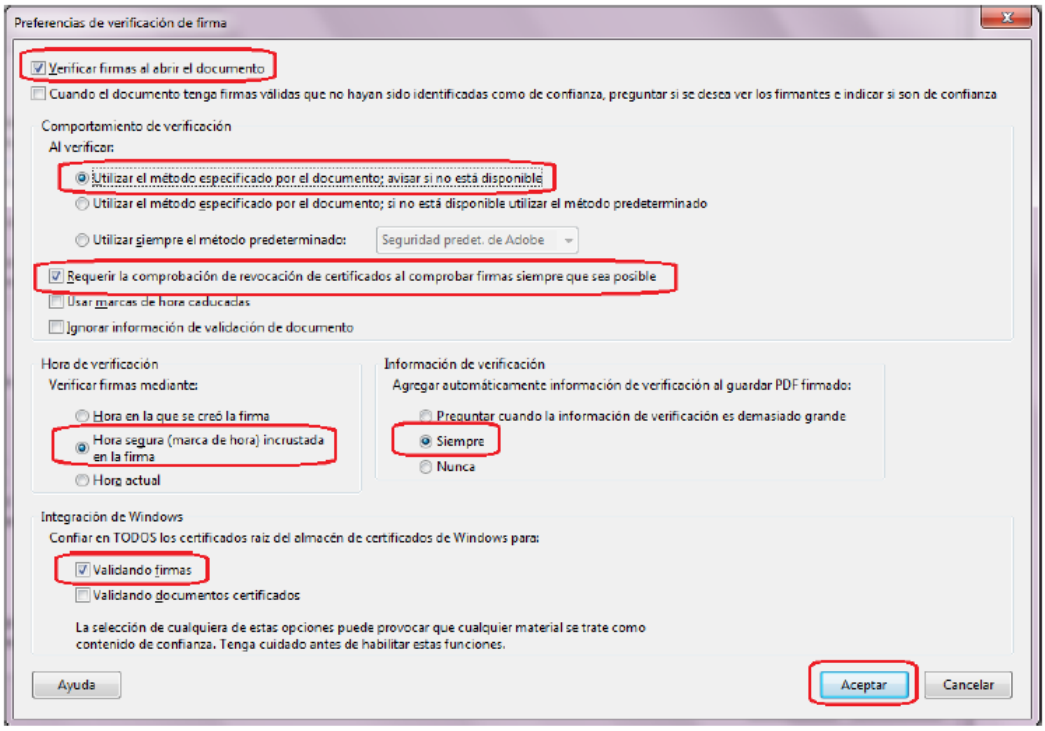
5. A continuación, se abre la ventana de Preferencias de creación y aspecto, en la misma realizamos la siguiente configuración:
    a. Método de Firma Predeterminado: **Seguridad predet. de Adobe**.
    b. Formato de Firma Predeterminado: **Equivalente a CAdES**.
    c. Marcar los 3 primeros checks.
    d. Dar clic en el botón **Aceptar**.
    e. Ver la siguiente imagen de cómo debe quedar la configuración.

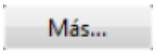


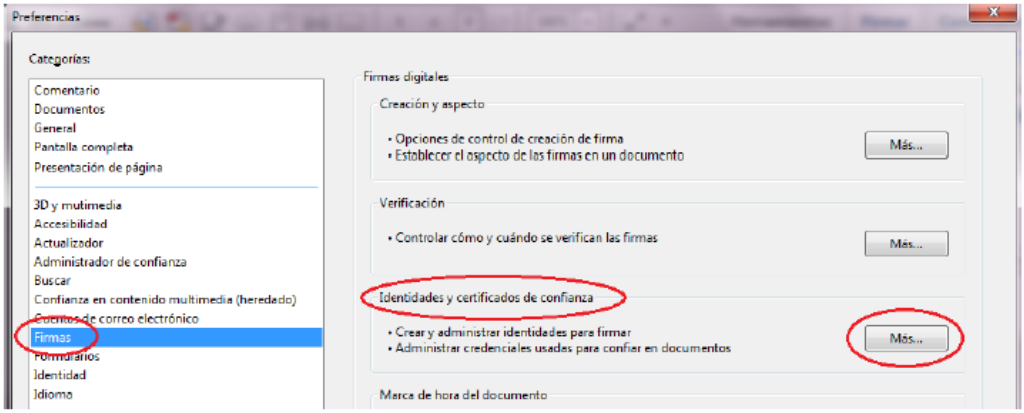
6. Elegimos la opción de la derecha **Verificación,** haciendo clic en el botón **Más**.



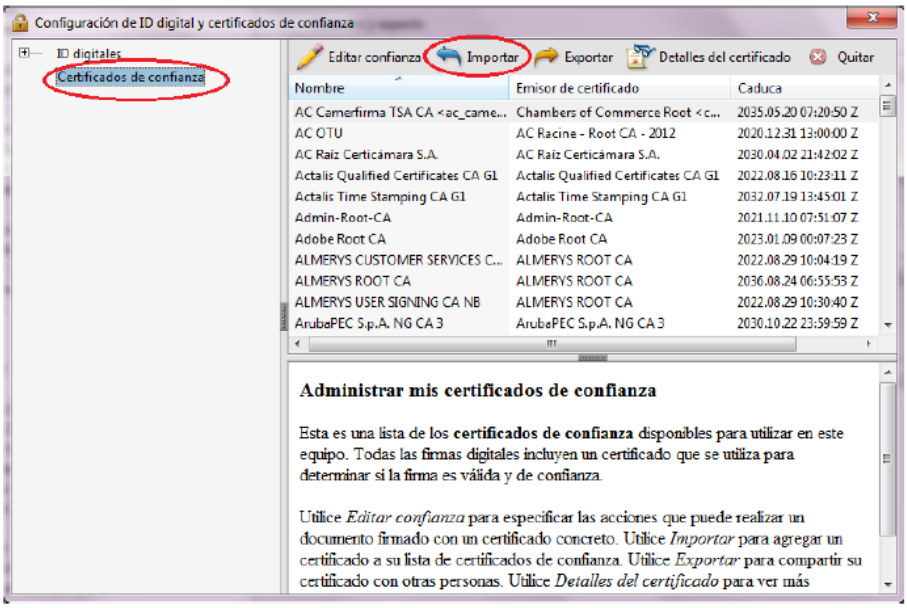
7. A continuación, se abre la ventana de **Preferencias de verificación,** en la misma realizamos la configuración tal como se muestra en la siguiente imagen, y hacemos clic en el botón **Aceptar**:



8. Elegimos la opción de la derecha **Identidades y certificados de Confianza,** haciendo clic en el botón 

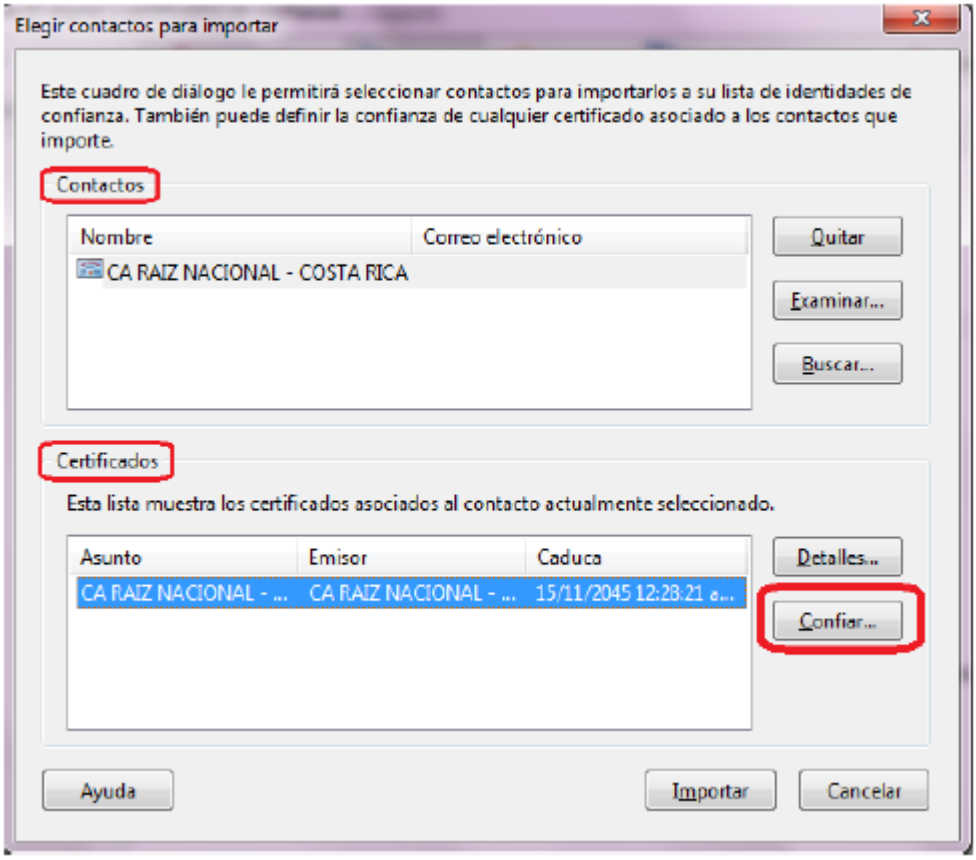


9. A continuación, se abre la ventana de **Configuración de ID digital y certificados de confianza,** en la misma elegimos de las opciones de la izquierda **Certificados de confianza** y elegimos del lado derecho la opción de arriba 

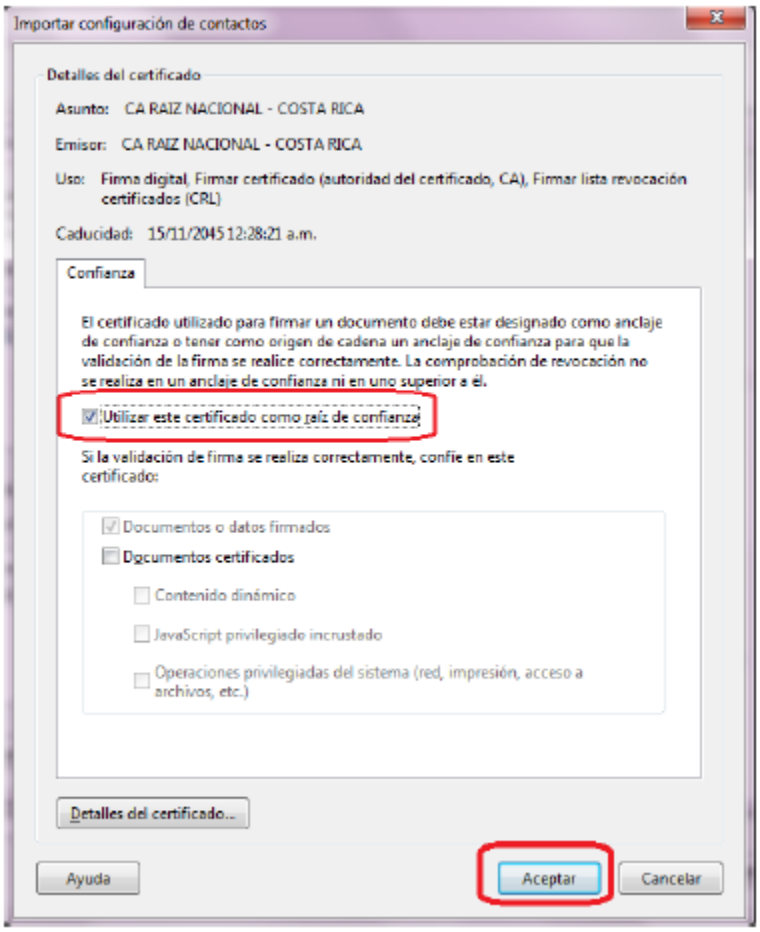


10. En la ventana que se abre, elegir contactos, escogemos la opción examinar, y posterior a esto buscamos el certificado llamado **CA RAIZ NACIONAL COSTA RICA**, ubicado en su computadora en la dirección C:\Firma Digital\certificados, o en cualquier otro apartado que haya guardado el mismo, lo elegimos y escogemos la opción **Abrir**.

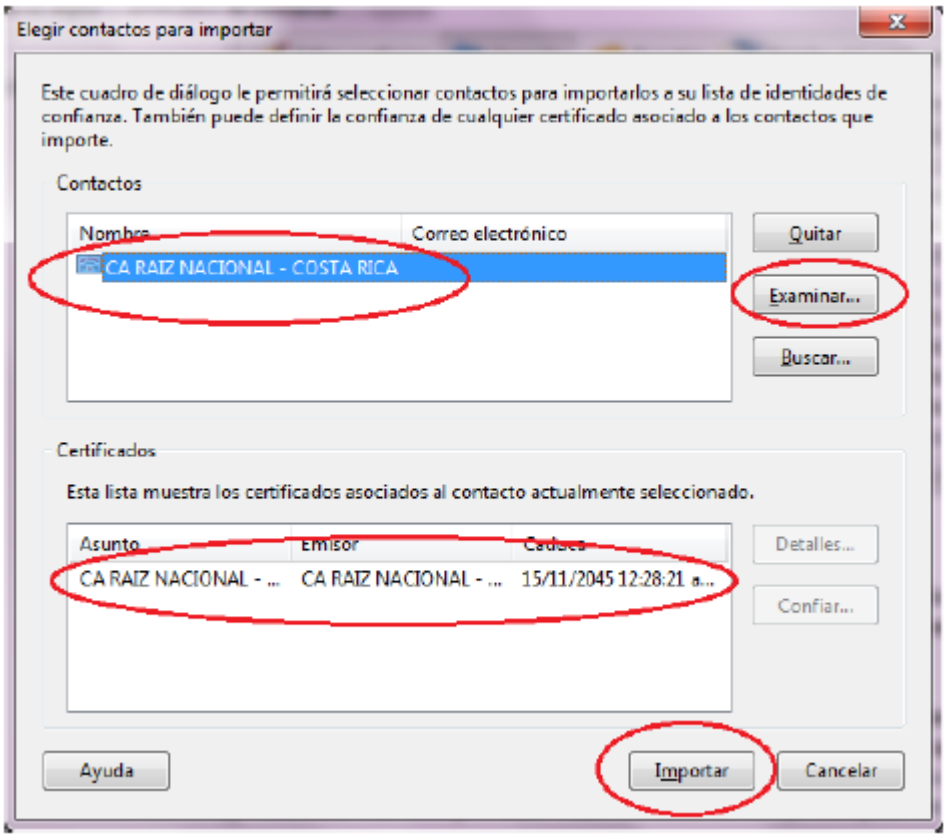
11. A continuación, nos aparece el certificado **CA RAIZ NACIONAL - COSTA RICA**, tal como lo muestra la siguiente imagen, lo marcamos en el apartado de **Contactos**, luego lo marcamos en el apartado de **Certificados** y elegimos la opción **Confiar**.



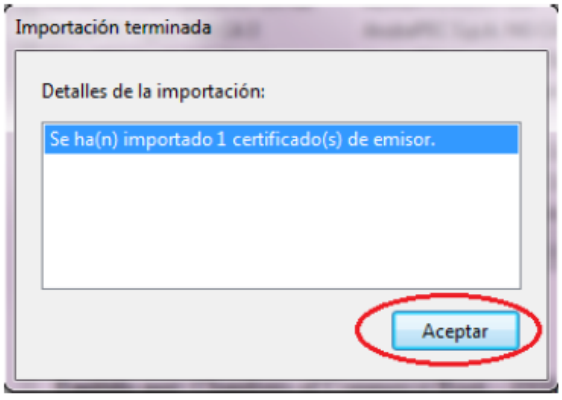
12. Luego se nos muestra la ventana de **Importar configuración de contactos,** ahí debemos marcar el check de **Utilizar este certificado como raíz de confianza** y presionamos el botón de **Aceptar.**



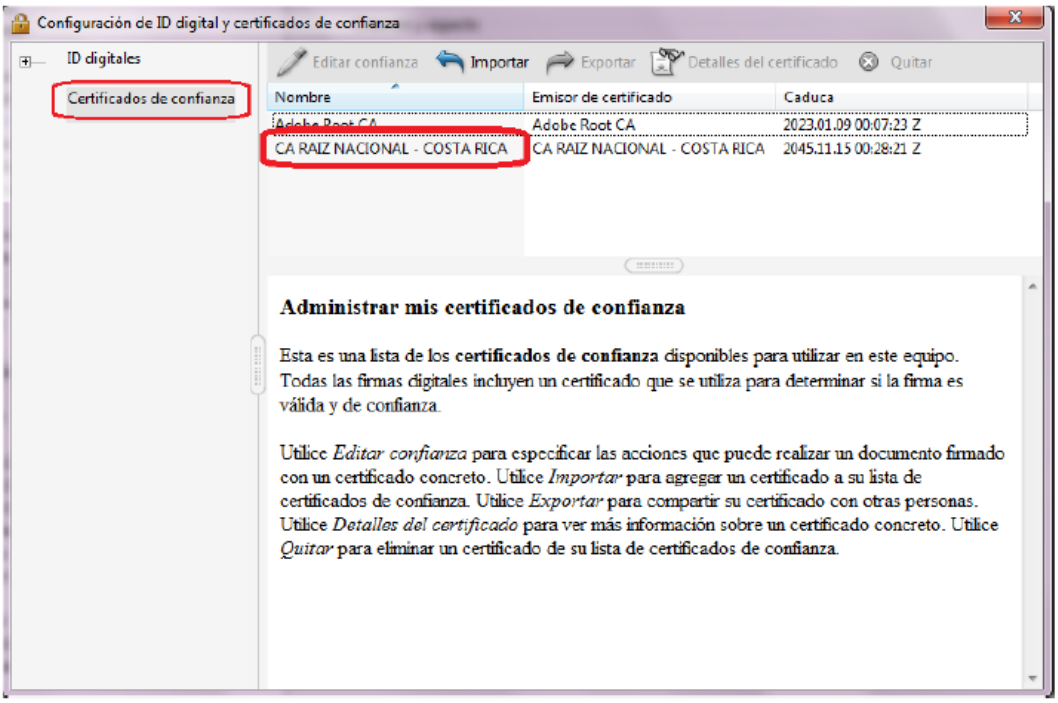
13. A continuación, volvemos a la ventana anterior ahí debemos elegir la opción de **Importar.**



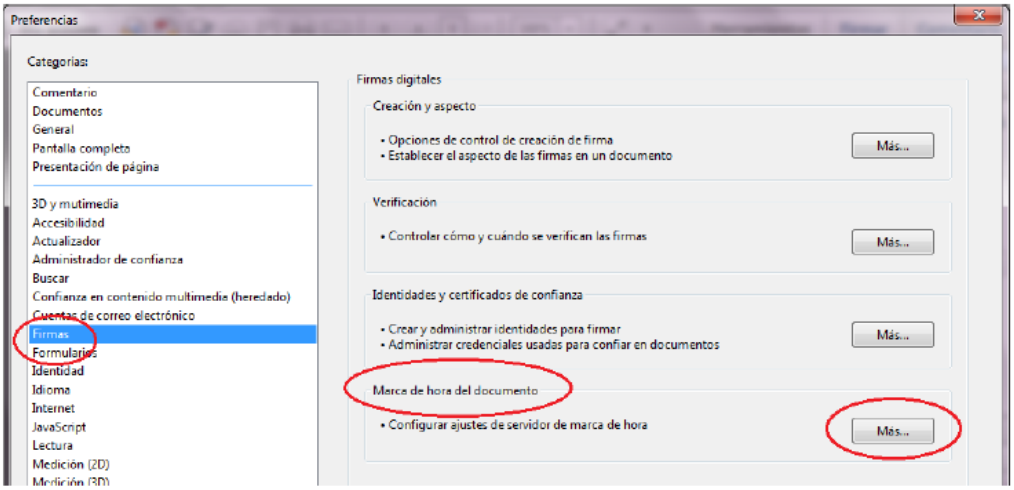
14. Luego se abre la ventana de confirmación de la importación, elegimos la opción **Aceptar.**

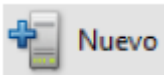


15. Con esto nos debe aparecer el certificado **Importado** en la lista de certificados de confianza. Luego cerramos la ventana.

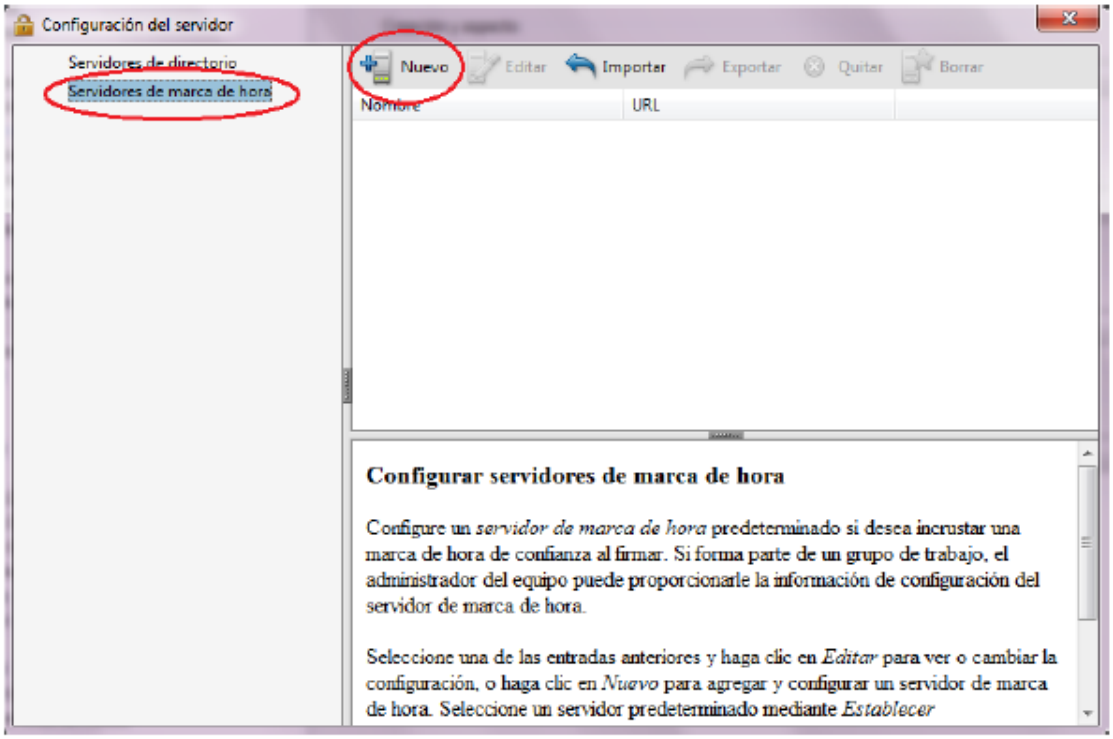


16. Elegimos la opción de la derecha **Marca de hora del documento,** haciendo clic en el botón Más...

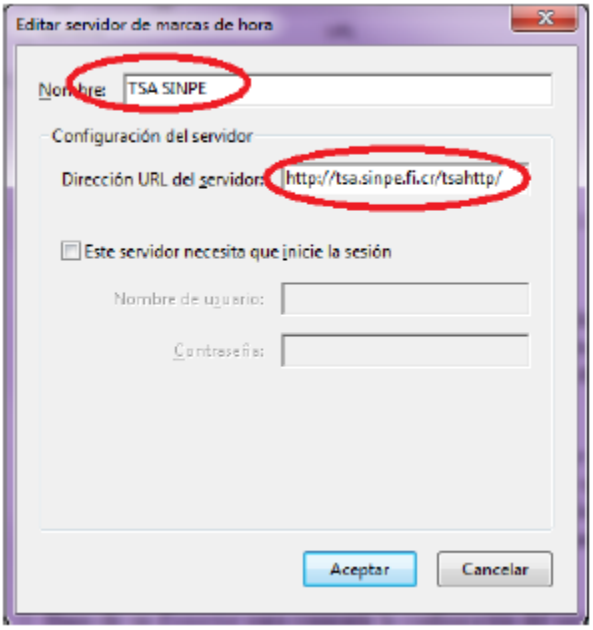


17. A continuación, se abre la ventana de **Configuración del servidor,** en la misma elegimos de las opciones de la izquierda **Servidores de marca de hora** y elegimos del lado derecho la opción de arriba 

, tal como lo muestra la siguiente imagen:

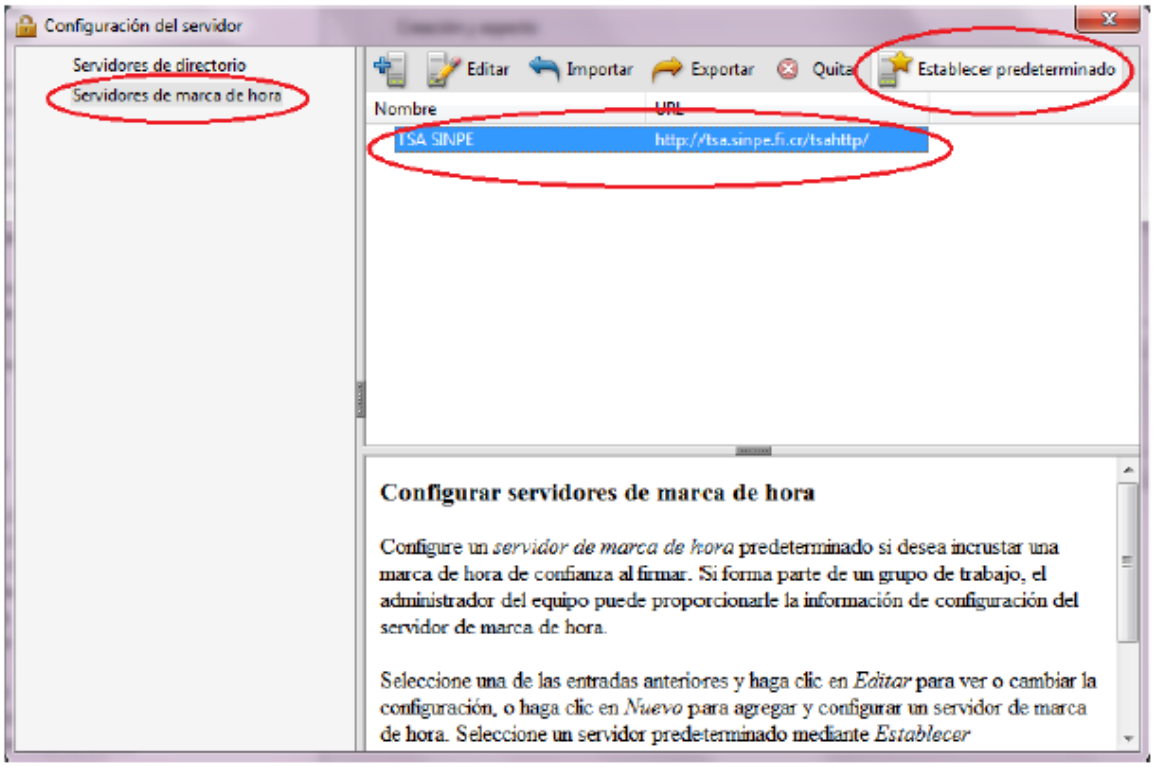


18. En la ventana que se abre procedemos a digitar la siguiente información:
    a. Nombre: **TSA SINPE**
    b. Dirección URL del servidor: **http://tsa.sinpe.fi.cr/tsahttp/**



19. Damos clic en **Aceptar**.

20. En este momento, siempre en la opción **Servidores de marca de hora** debe visualizarse el servicio de sellado de tiempo **TSA SINPE**, el cuál marcamos haciendo un clic sobre el mismo, para proceder a establecerlo como servicio predeterminado, esto haciendo un clic en el botón con una estrella **Establecer predeterminado, l**uego cerramos la ventana.



21. Con esto hemos configurado la herramienta **Adobe Reader DC** para que pueda firmar y verificar documentos electrónicos PDF con los formatos oficiales establecidos en Costa Rica y además para que confíe en la Jerarquía Nacional de Certificación Digital.

22. Elegimos la opción **Aceptar** para cerrar la ventana de Preferencias**.**

Fuentes Consultadas:

Guía de Firma Digital para Adobe Reader DC, DIRECCIÓN DE CERTIFICADORES DE FIRMA DIGITAL. MICCIT

BCCR, soporte firma digital.

Control de documentos

Código	Nombre del documento	Responsable	Soporte de Archivo	Acceso autorizado
GA-DSI-API-GT007	Guía Firma Digital para Documentos Institucionales	Área Publicaciones e Impresos	Digital	A todo el personal

Control de cambios en el documento

Referencia	Fecha	Descripción del cambio
N/A	N/A	N/A