

Manual de configuración de Adobe Reader para la validación de la firma de un documento.

Versión 1.0

Contenido

Instalar los certificados de Izenpe	3
Configurar Adobe Reader para que confíe en el certificado raíz del certificado de firma	7

Este manual describe cómo validar, con la aplicación de Adobe Reader o Adobe Acrobat, la firma de los documentos en formato PDF que IDS Ingeniería de Sistemas S.A. emite.

Aunque el manual se ha elaborado para la versión 9 de Adobe Reader, se puede utilizar para versiones anteriores, tanto de Adobe Reader como de Adobe Acrobat.

Para la validación de la firma es necesario, en primer lugar, instalar los certificados de Izenpe, y en segundo lugar configurar la aplicación para que confíe en el certificado raíz del certificado de firma.

Instalar los certificados de Izenpe

Para poder verificar correctamente la firma electrónica de los documentos PDF, debe registrar en su ordenador los certificados de Izenpe.

Estos certificados están disponibles en Izenpe y son:

- El certificado de la Autoridad de Certificación raíz (CA Raíz de Izenpe 2007).
- El certificado de la Autoridad de Certificación Intermedia (CA Ciudadanos y Entidades (reconocidos)).

1. Acceda a la siguiente web:

https://servicios.izenpe.com/jsp/download_ca/s27download_ca_c.jsp

2. Pulse en el enlace CA Raíz de Izenpe 2007

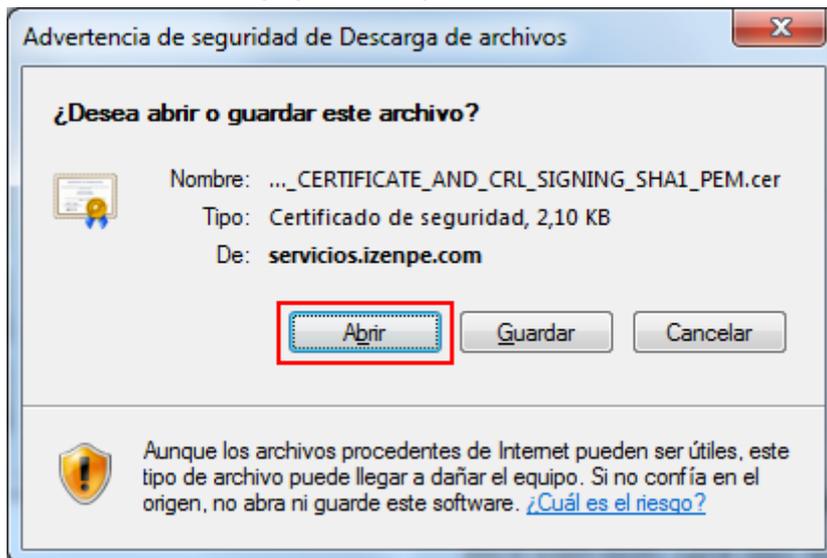


DESCARGA DE CERTIFICADOS RAÍZ - CLAVES PÚBLICAS DE IZENPE

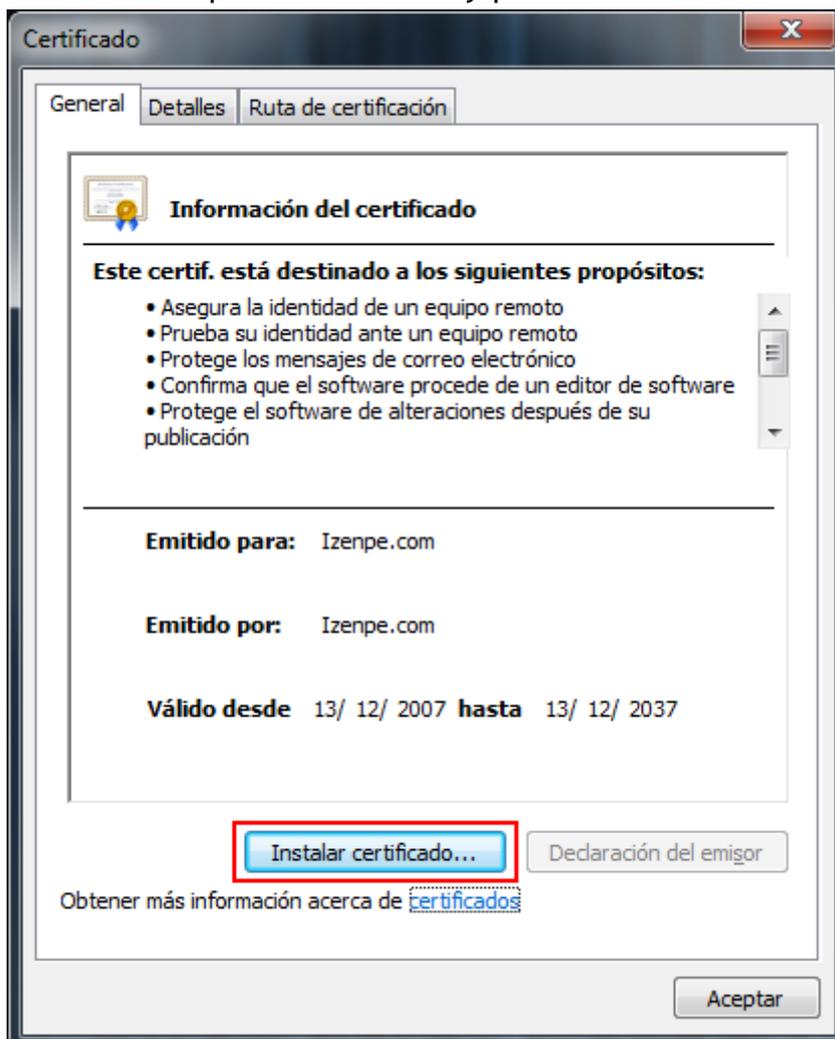
El siguiente diagrama representa la jerarquía de certificación de Izenpe con sus diferentes CA y los tipos de certificado que emite cada una de ellas. Puede descargar el certificado raíz correspondiente a cada CA pulsando sobre el bloque correspondiente.

HUELLAS DIGITALES (SHA1)	FORMATO PEM
<ul style="list-style-type: none"> • CA Raíz de Izenpe 2007 3077 9E93 1502 2E94 856A 3FF8 BCF8 1580 82F9 AEF0 	PEM
<ul style="list-style-type: none"> • CA Ciudadanos y Entidades (no reconocidos) 06FB AC35 AE18 FCBF 2229 788D D12D AC89 BE74 52AE 	PEM
<ul style="list-style-type: none"> • CA Ciudadanos y Entidades (reconocidos) 9FDC E942 9B3D 7E59 499D C3F8 3C93 6665 2269 A759 	PEM
<ul style="list-style-type: none"> • CA AAPP Vascas (no reconocidos) 7F58 BB8F 8711 C049 6128 CF71 634B 7795 0ADD D32C 	PEM
<ul style="list-style-type: none"> • CA Personal de AAPP Vascas (reconocidos) ESC8 62ED DCF1 14C8 2661 984A D648 ADF2 3F51 10FC 	PEM
<ul style="list-style-type: none"> • CA SSL con EV (no reconocidos) D2AD F838 5F63 0180 FCS1 69EC 81F8 CC33 AB88 CA33 	PEM
<ul style="list-style-type: none"> • CA Personal de Gobierno Vasco (reconocidos) 4A17 EDD4 9ED4 CC39 243A BE74 B892 DFAA 0068 6480 	PEM

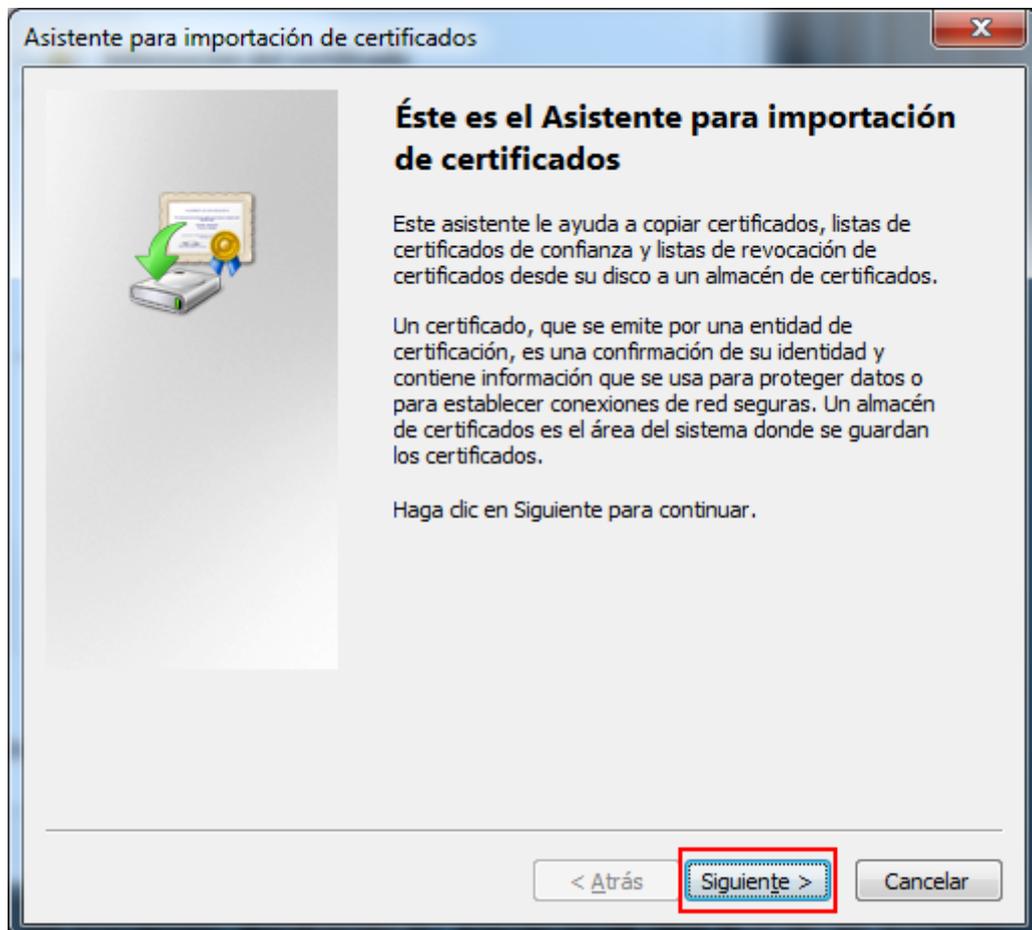
3. Se abrirá una ventana preguntando si desea abrir el archivo o guardarlo en su equipo, pulse el botón de **Abrir**.



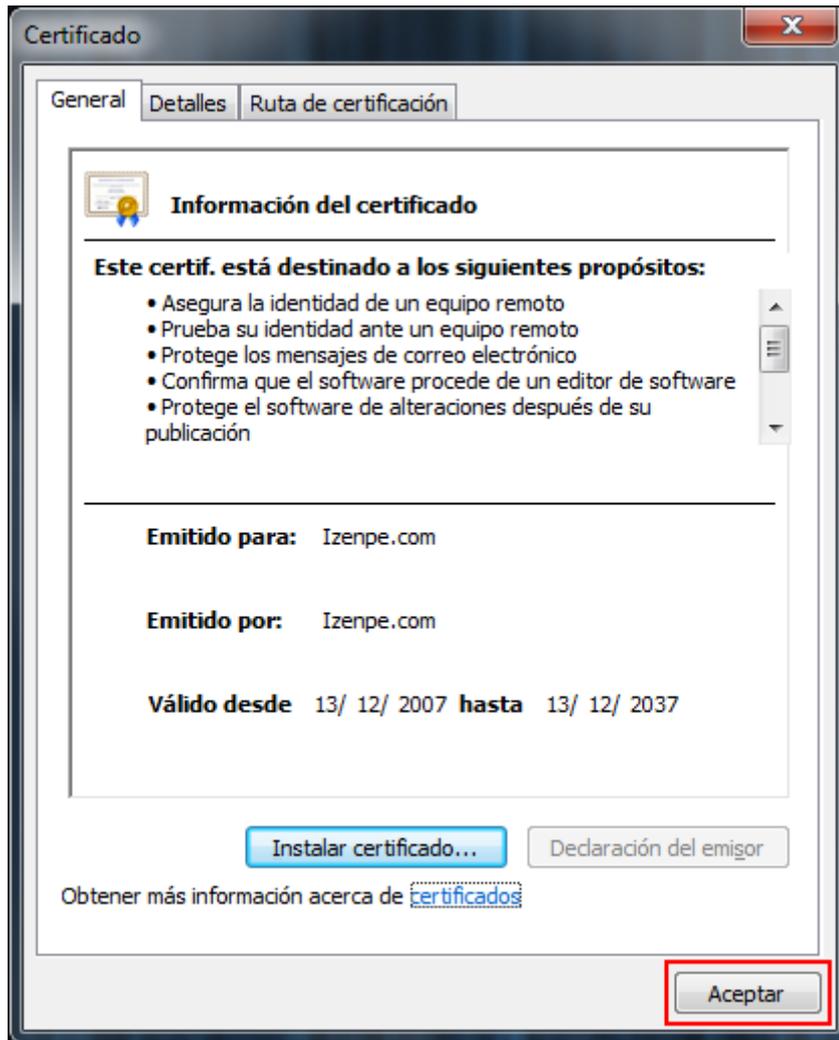
4. A continuación se mostrará una ventana con los datos del certificado, seleccione la pestaña **General** y pulse el botón **Instalar certificado ...**



5. Se abrirá una nueva ventana con el Asistente para importación de certificados, pulse el botón **Siguiente** en este paso y en el paso posterior, y finalmente el botón **Finalizar**. Tras este último paso se mostrará un mensaje indicando que la importación se realizó correctamente.



6. Pulse el botón “Aceptar” de la ventana que muestra la información del certificado para cerrarla.

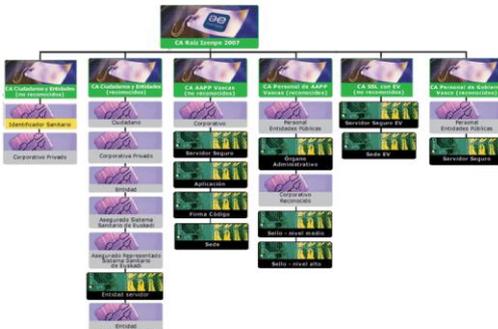


7. Pulse en el enlace CA Ciudadanos y Entidades (reconocidos) y repita los pasos del 3 al 6 para instalar este nuevo certificado.




DESCARGA DE CERTIFICADOS RAÍZ - CLAVES PÚBLICAS DE IZENPE

El siguiente diagrama representa la jerarquía de certificación de Izenpe con sus diferentes CA y los tipos de certificado que emite cada una de ellas. Puede descargar el certificado raíz correspondiente a cada CA pulsando sobre el bloque correspondiente.



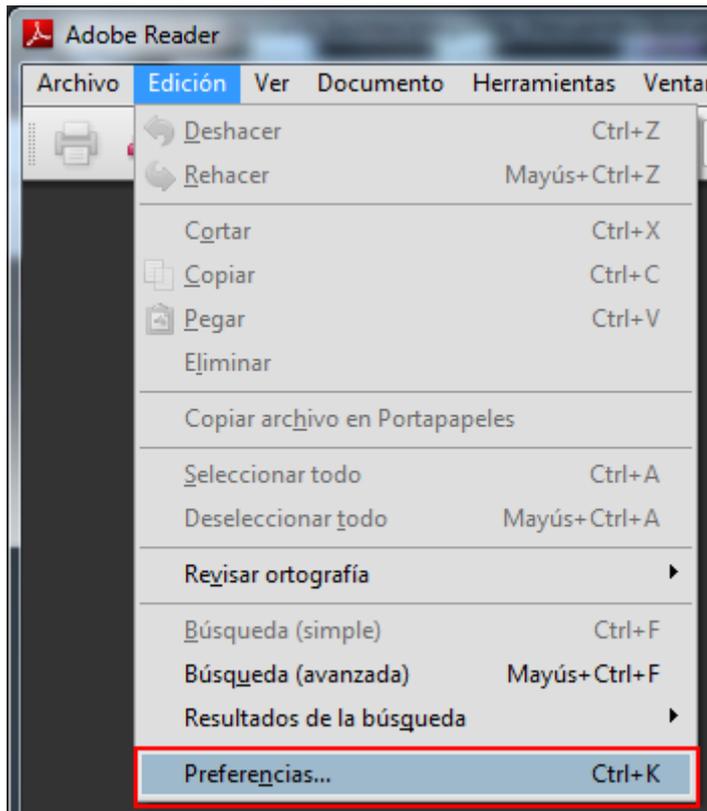
HUELLAS DIGITALES (SHA1)	FORMATO PEM
<ul style="list-style-type: none"> CA Raíz de Izenpe 2007 3077 9E93 1502 2E94 856A 3FB8 15B0 82F9 AEFO 	PEM
<ul style="list-style-type: none"> CA Ciudadanos y Entidades (no reconocidos) 06FB AC35 AE18 FC8F 2229 78BD D12D AC89 8E74 52AE 	PEM
<ul style="list-style-type: none"> CA Ciudadanos y Entidades (reconocidos) 9F0C E942 983D 7E59 499D C3F8 3C93 6665 2269 A759 	PEM
<ul style="list-style-type: none"> CA AAPP Vascas (no reconocidos) 7F58 886F 8711 C049 6128 CF71 6348 7795 0ADD D32C 	PEM
<ul style="list-style-type: none"> CA Personal de AAPP Vascas (reconocidos) ESC8 62ED DCF1 14C8 2661 984A D648 ADF2 3F51 10FC 	PEM
<ul style="list-style-type: none"> CA SSL con EV (no reconocidos) D2AD F838 5FE3 0160 FCS1 69EC 81F8 CC33 AB88 CA23 	PEM
<ul style="list-style-type: none"> CA Personal de Gobierno Vasco (reconocidos) 4417 EDD4 9ED4 CC39 243A BE74 B892 DF4A 0068 648D 	PEM

Si ha optado por guardar los certificados en su disco, haciendo doble click sobre cada uno de los archivos se mostrará la ventana del paso 4, y podrá seguir con el resto de pasos hasta importar los certificados.

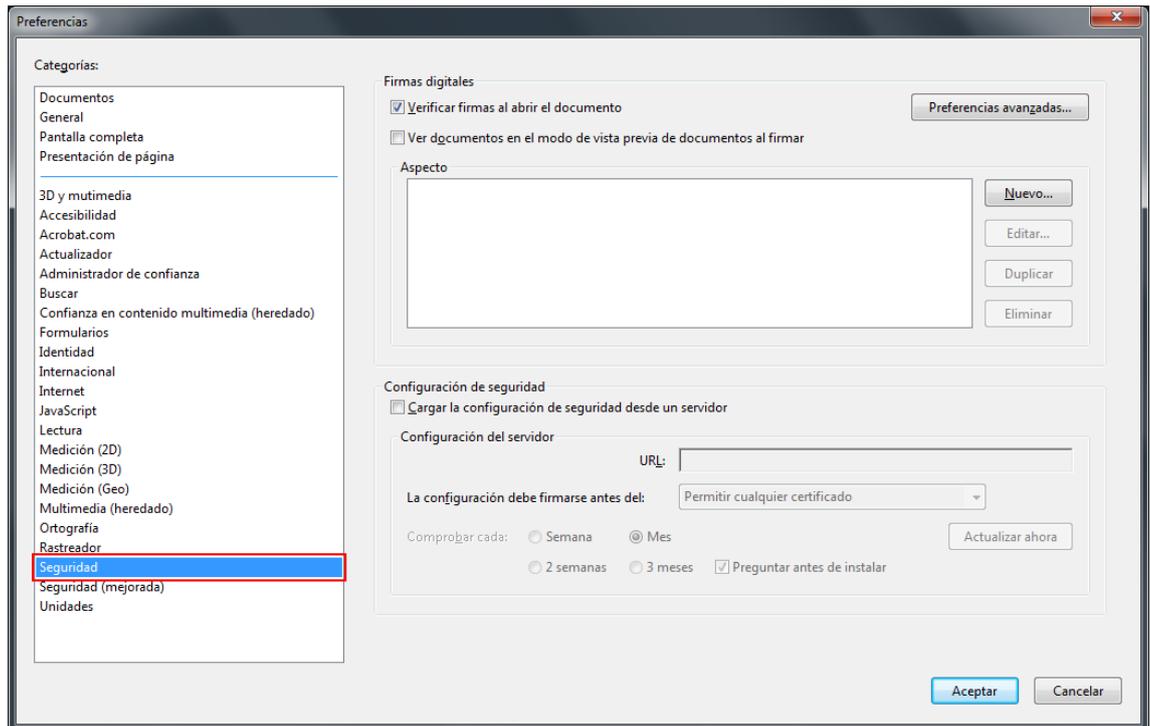
Configurar Adobe Reader para que confíe en el certificado raíz del certificado de firma

A continuación se explica el proceso para que Adobe Reader confíe en los certificados instalados anteriormente.

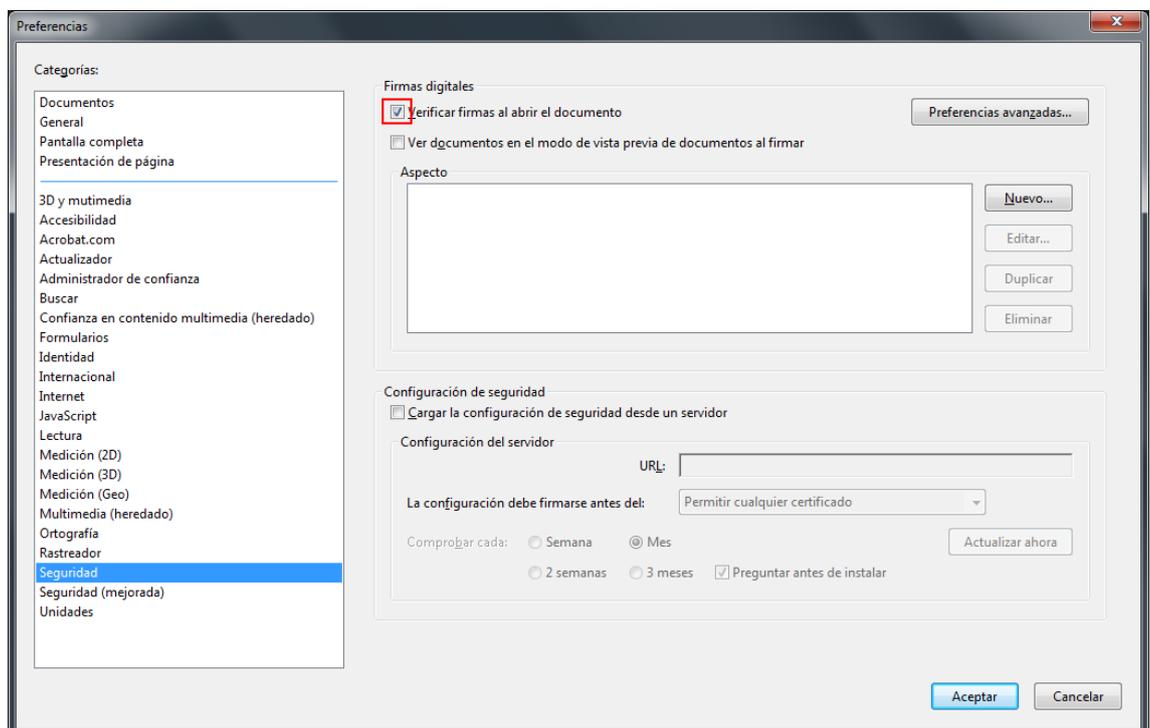
1. Abra la aplicación de Adobe Reader.
2. Seleccionar en el menú principal **Edición** > **Preferencias**.



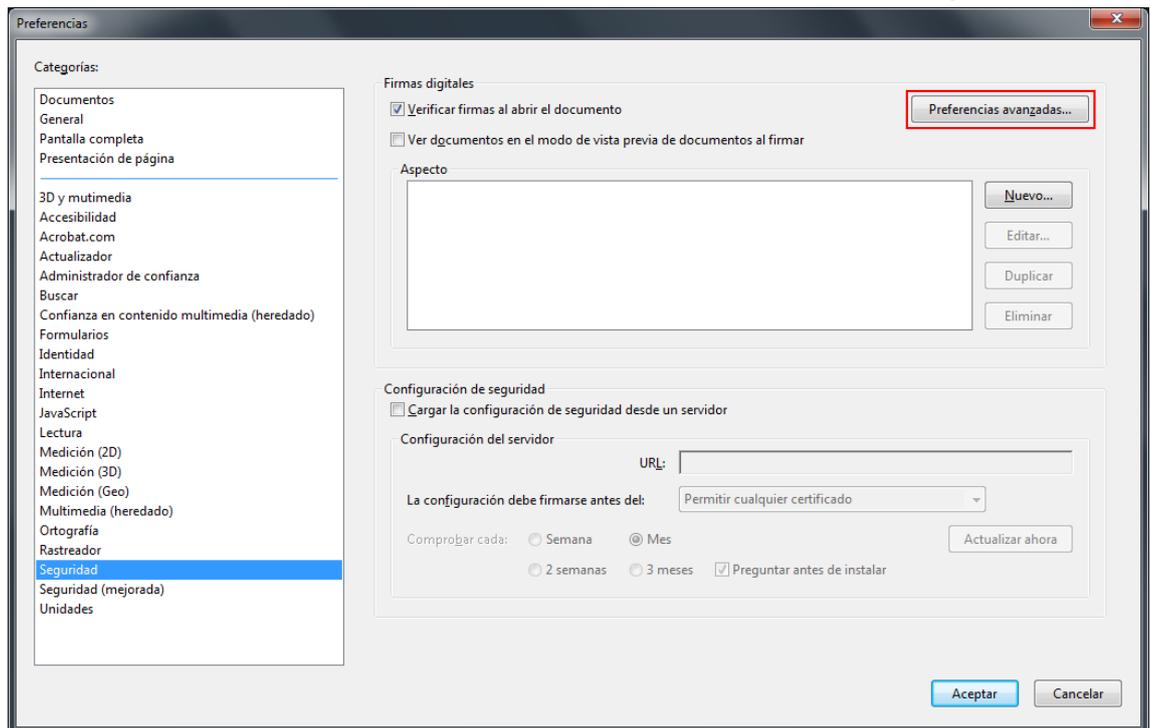
3. Seleccionar en la ventana que se muestra la opción **Seguridad** de entre todas las que hay en el panel de la izquierda.



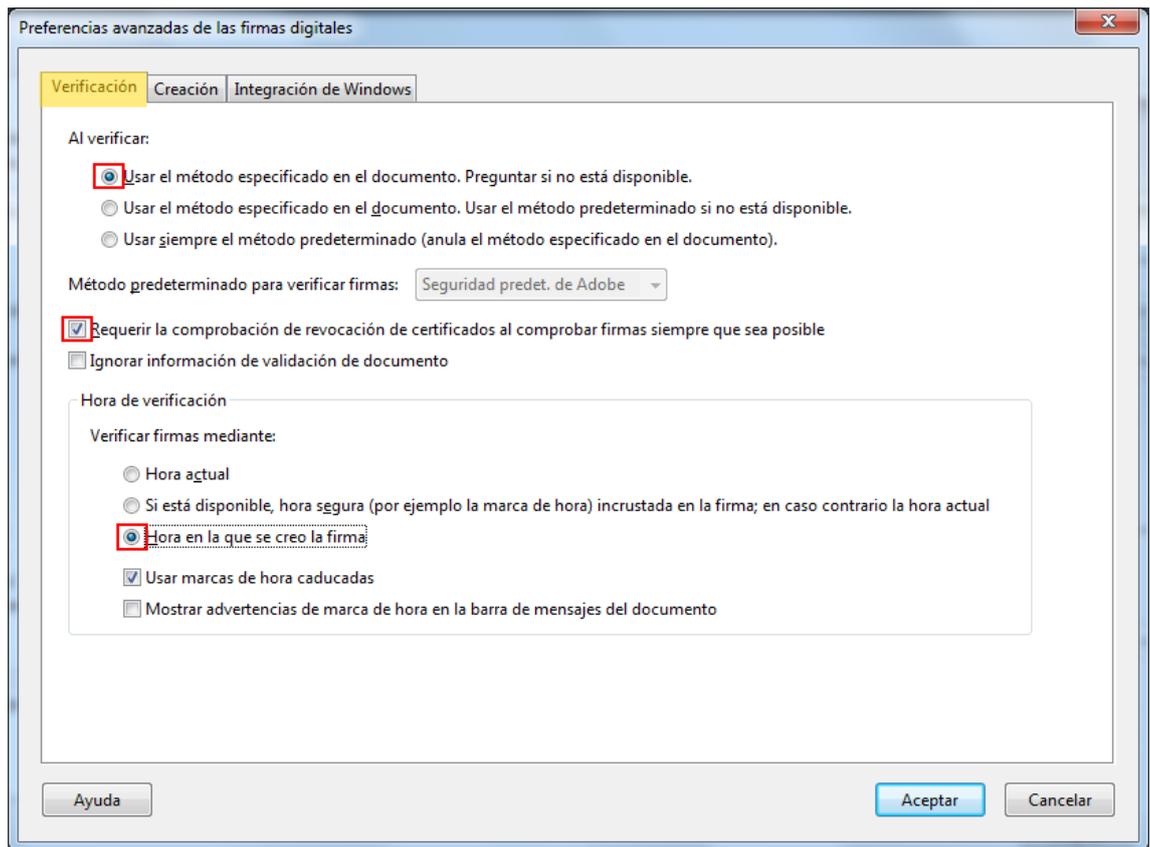
4. Marcar, si no lo está, la opción *Verificar firmas al abrir el documento*.



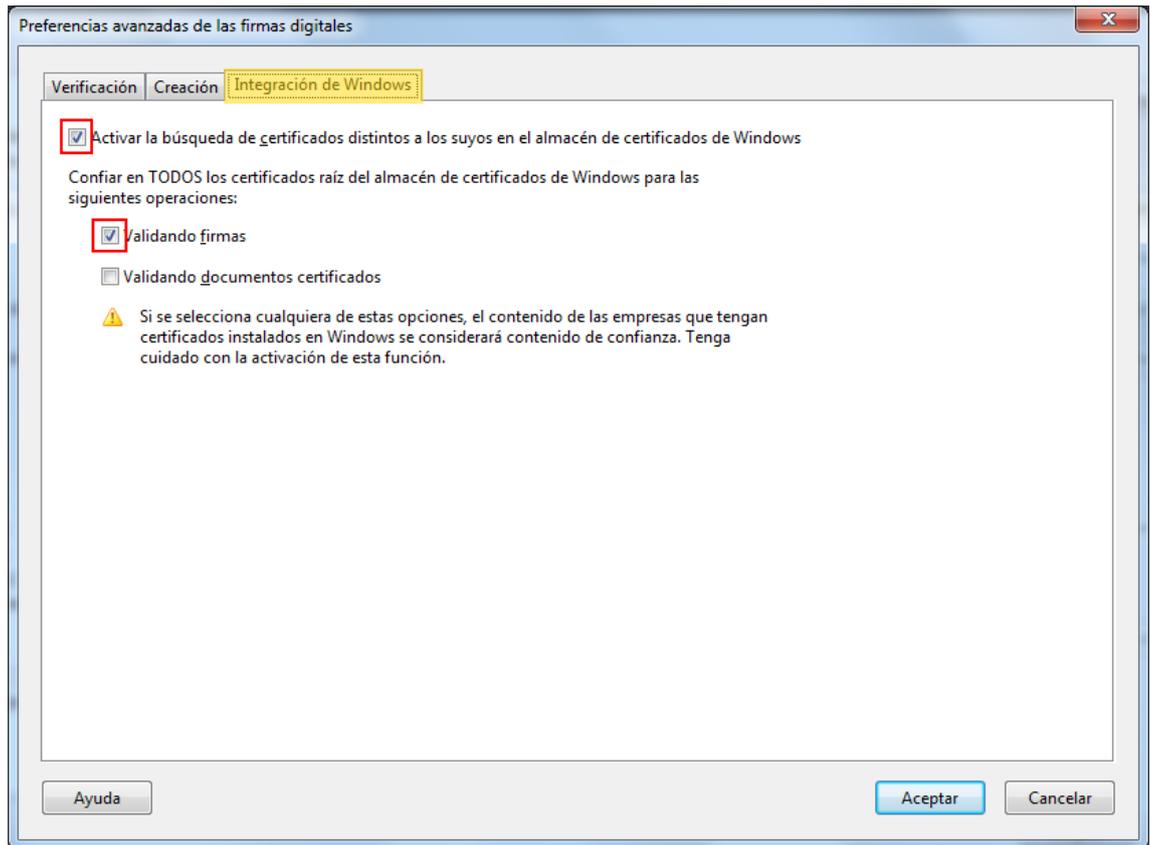
5. Pulsar el botón **Preferencias Avanzadas** para abrir la ventana Preferencias avanzadas de las firmas digitales.



6. En la ventana de Preferencias avanzadas de las firmas digitales, seleccionar la pestaña **Verificación**, y en la opción Al verificar: marcar **Usar el método especificado en el documento. Preguntar si no está disponible**.
7. Marcar la opción **Requerir la comprobación de revocación de certificados al comprobar firmas siempre que sea posible**.
8. En el recuadro Hora de verificación seleccionar la opción **Hora en la que se creó la firma**.



9. Seleccionar la pestaña *Integración de Windows*, y marcar las opciones *Activar la búsqueda de certificados distintos a los suyos en el almacén de certificados de Windows*, y *Validando firmas* de la sección “Confiar en TODOS los certificados raíz del almacén ...”.



10. Pulsar **Aceptar** para guardar los cambios y volver a la ventana Preferencias y de nuevo **Aceptar** para cerrar esta ventana.
11. La próxima vez que se abra el documento, se validará la firma automáticamente.