Instrucciones de cómo usar:

Firmar con Certificado

Ver guía visual al final del documento

Este manual detalla paso a paso cómo utilizar la herramienta de firma digital de Stirling-PDF. El proceso se centrará en el uso de un certificado digital personal (como los emitidos por la FNMT u otras autoridades de certificación) que ha sido previamente instalado en un navegador web y que exportaremos para su uso en la plataforma.

1. Fase Preparatoria: Exportar el Certificado desde el Navegador

Para firmar un documento en Stirling-PDF, necesitas tener tu certificado en un archivo físico junto con su clave privada. Si tienes el certificado instalado en tu navegador, el primer paso es exportarlo.

A continuación, se explica cómo hacerlo usando **Mozilla Firefox** (el proceso en Google Chrome o Microsoft Edge es muy similar, a través de sus opciones de Privacidad y Seguridad):

1. **Acceder a la configuración:** Abre Firefox, haz clic en el menú de las tres rayas horizontales (arriba a la derecha) y selecciona **"Ajustes"**.
2. **Ir a Privacidad:** En el menú lateral izquierdo, haz clic en **"Privacidad & Seguridad"**.
3. **Buscar Certificados:** Desplázate hacia abajo hasta encontrar la sección "Seguridad" y el apartado "Certificados". Haz clic en el botón **"Ver certificados..."**.
4. **Seleccionar tu certificado:** Se abrirá una ventana. Ve a la pestaña **"Sus certificados"**. Allí verás tu certificado personal (normalmente a tu nombre). Selecciónalo haciendo clic sobre él.
5. **Exportar:** Haz clic en el botón **"Hacer copia..."** (o "Exportar").

6. **Guardar el archivo:** Elige dónde guardar el archivo en tu ordenador. Por defecto, Firefox lo guardará en formato **PKCS12 (.p12)**. Dale un nombre reconocible (por ejemplo, `mi_certificado.p12`).
7. **Establecer contraseña (MUY IMPORTANTE):** El navegador te pedirá que introduzcas una contraseña de respaldo para proteger el archivo. **Crea una contraseña segura y recuérdala**, ya que Stirling-PDF te la pedirá obligatoriamente para poder usar la clave y firmar el documento.

2. Tipos de Certificado Soportados

La herramienta te pedirá que indiques el formato de tu certificado. Es fundamental entender las diferencias para elegir la opción correcta en el menú desplegable:

- **PFX / PKCS12 (`.pfx` o `.p12`):** Es el estándar de la industria para almacenar la clave privada y el certificado público en un solo archivo encriptado mediante una contraseña. **Esta es la opción que debes elegir** si has seguido los pasos del apartado anterior para exportar tu certificado desde el navegador.
- **PEM (`.pem`):** Es un formato de texto plano (codificado en Base64) que a menudo requiere que el certificado público y la clave privada se proporcionen en archivos separados. Es muy común en entornos de servidores web, pero menos habitual para usuarios de a pie.
- **JKS (Java KeyStore):** Es un formato de almacenamiento de claves propietario específico del entorno de programación Java. Como indica la nota de la propia aplicación, si tienes un certificado en un formato no soportado directamente en la lista, puedes usar herramientas de línea de comandos (como `keytool`) para convertirlo a `.jks` y usar esta opción.

3. Guía de Uso de la Interfaz en Stirling-PDF

Una vez tengas tu archivo `.pfx` o `.p12` y su contraseña, dirígete a la herramienta de firmado en Stirling-PDF y sigue estos pasos:

3.1. Selección de Archivos

- **Seleccione un archivo PDF para firmar:** Haz clic en el recuadro superior o arrastra desde tu explorador el documento PDF original que deseas firmar.
- **Tipo de certificado:** En el menú desplegable, selecciona **PFX** (o PKCS12, si aparece así).
- **Seleccione su archivo de almacén de claves:** Haz clic en el segundo recuadro grande o arrastra el archivo `.p12` o `.pfx` que exportaste de tu navegador.

3.2. Autenticación

- **Introduzca su almacén de claves o contraseña...:** En este campo de texto, debes escribir la misma contraseña que estableciste en el paso 7 de la Fase Preparatoria. Sin esta contraseña, Stirling-PDF no podrá desencriptar tu archivo para aplicar la firma matemática.

3.3. Configuración de la Firma Visual

Esta es una de las partes más importantes. Una firma digital es, en esencia, un código criptográfico invisible incrustado en el código del PDF. Sin embargo, Stirling-PDF te permite añadir un **sello visual** en el documento para que sea evidente a simple vista que ha sido firmado.

- Casilla "Mostrar firma":
    - **Desmarcada:** La firma será **invisible**. El documento estará criptográficamente firmado (si lo abres con Adobe Acrobat, verás un panel de firma válido), pero visualmente el PDF no cambiará en nada.
    - **Marcada:** Al activar esta opción, la herramienta imprimirá un recuadro gráfico en el PDF. Este recuadro suele incluir tu nombre (extraído automáticamente del certificado), la fecha y hora de la firma, y la razón (si la especificas).
- **Razón:** (Solo relevante si la firma es visible o si quieres que conste en los metadatos de la firma). Aquí puedes escribir el motivo por el cual firmas el documento. Ejemplos: *"Aprobado"*, *"Revisado"*, *"Doy mi*

conformidad", o *"Autorización de contrato"*. Este texto aparecerá dentro del sello visual de la firma.

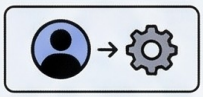
- **Número de página:** Si marcaste "Mostrar firma", debes indicar en qué página física del documento quieres que se estampe el sello. Introduce un número entero (por ejemplo, `1` para la primera página, o el número correspondiente a la última página si es allí donde están las líneas de firma del documento o un rango de páginas donde aparecerá esa firma 12-24).

3.4. Ejecución

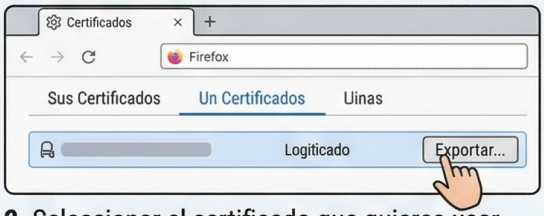
Una vez revisados todos los campos, haz clic en el botón azul **"Firmar PDF"**. La aplicación procesará la clave, aplicará el sello criptográfico (y visual, si lo elegiste) y te devolverá un nuevo archivo PDF firmado y listo para descargar, asegurando que cualquier modificación futura del documento invalidará la firma.

Stirling-PDF

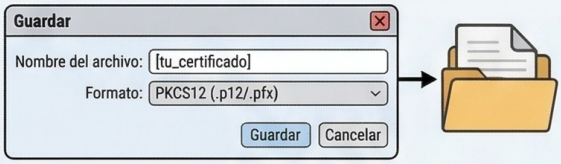
GUÍA: EXPORTAR TU .PFX DEL NAVEGADOR (Ej. Firefox)



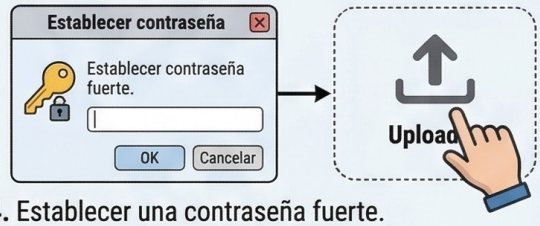
1. Ir a **Preferencias -> Privacidad y Seguridad -> Certificados -> Ver Certificados.**



2. Seleccionar el certificado que quieres usar (ej. con tu nombre) y pulsar "**Exportar...**"



3. Guardar como archivo PKCS#12 (.pfx or .p12).

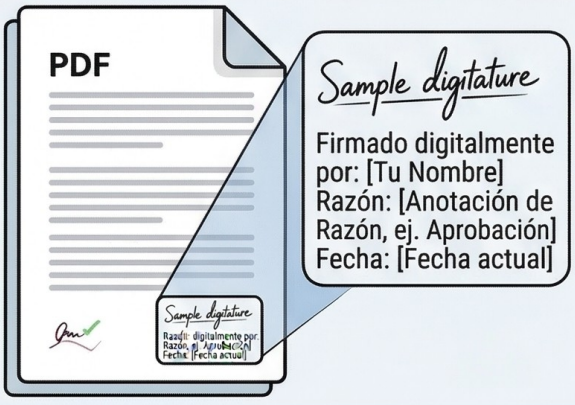


4. Establecer una contraseña fuerte. ***IMPORTANTE***: ¡No la olvides! La necesitarás más adelante.

5. Sube este archivo en Stirling-PDF.

FIRMA VISUAL Y CONFIGURACIÓN

Activar (Checked): Añade un sello de firma visual en la página especificada.
Desactivar (Unchecked): La firma es invisible (solo verificable digitalmente by software like Adobe Reader).



Seleccione un archivo PDF para firmar:

Nota: si el tipo de certificado no está enla lista de archivo almacén de claves de Java **KeyStore** la herramienta línea de comandos.

Tipo de certificado
pem
pkcs12
pfx
jks

GUÍA: TIPOS DE ARCHIVOS DE CERTIFICADO

PEM
Archivos de texto que contienen certificados codificados. A menudo requieren clave privada y certificado en archivos separados.

PFX (or PKCS#12)
Contenedor binario que incluye ***ambos*** certificado y clave privada, protegidos por una contraseña. Ideal para copias de seguridad de usuario. ***Formato del Navegador.***

JKS (Java KeyStore)
Formato propietario de Java. Más complejo, se usa para aplicaciones Java que manejan claves y certificados.

Tipo de certificado
PFX

Seleccione su archivo de almacén de claves PKCS#12 (.p12 o .pfx) (Opcional, si se proporciona, debe contener su clave privada y certificado):

Click o Arrastrar & Soltar

Introduzca su almacén de claves o contraseña de clave privada (si corresponde):

Mostrar firma

Razón

Número de página
1

Determina dónde aparecerá la firma. Escribe el número exacto (ej. 1, 5, or 'última').

Firmar PDF

Paso Final: Haz clic en 'Firmar PDF'. Si proporcionaste un **.pfx** con contraseña, el sistema la solicitará automáticamente si la contraseña es correcta y corresponde a la clave privada.