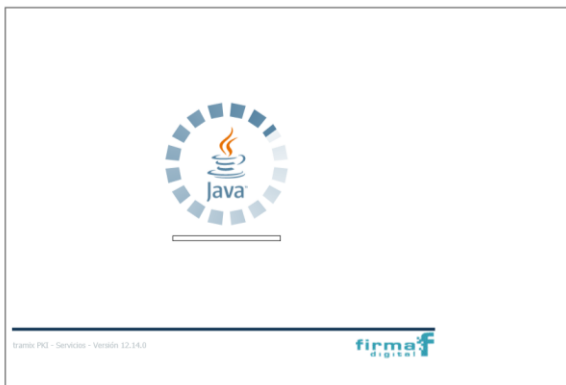


FDSL 3.0 FIRMA DIGITAL
DE SAN LUIS

MANUAL
DE USUARIO
SERVICIO JAVA
FIRMADOR
Y
VALIDADOR

Servicio de Firma y Validación de Documentos Digitales FDSL

Firmador



Validador



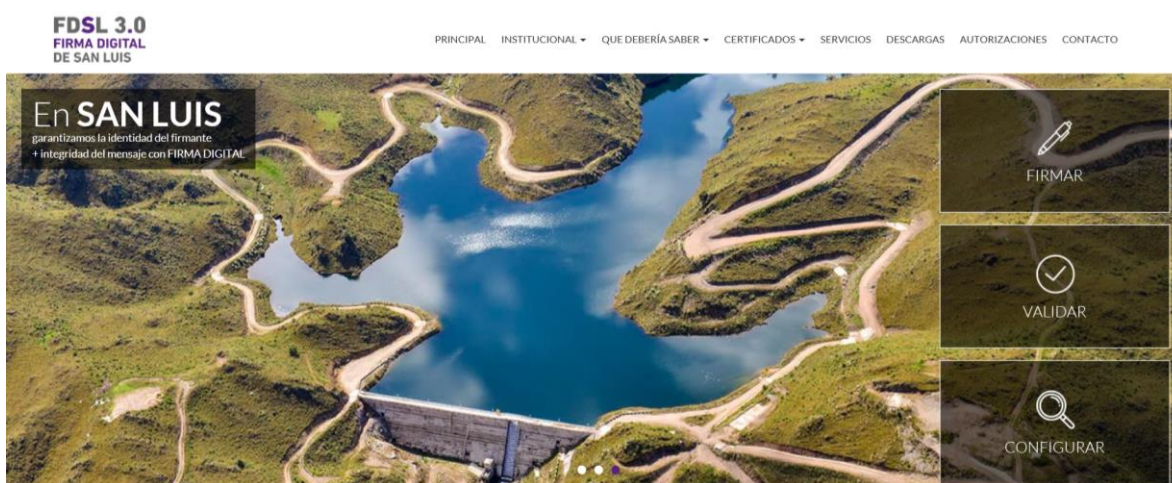
Servicio de Firma de Documentos Digitales

Antes de firmar digitalmente un documento, es necesario verificar que se cuenta con los siguientes **requisitos**:

- Poseer un certificado de *firma digital* vigente otorgado por el Instituto Firma Digital de San Luis.
- Tener instalados los drivers del dispositivo criptográfico (CIPE, Token).
- Tener instalada la última versión de Java.
- Contar con el documento a firmar en formato digital.
- Ejecutar la aplicación en navegador Internet Explorer 11 o Microsoft Edge

Los **pasos** que se deben seguir para firmar un documento digitalmente son:

- Ingresar al portal de Firma Digital ([San Luis - Firma Digital](#)) y seleccionar la opción "FIRMAR" 



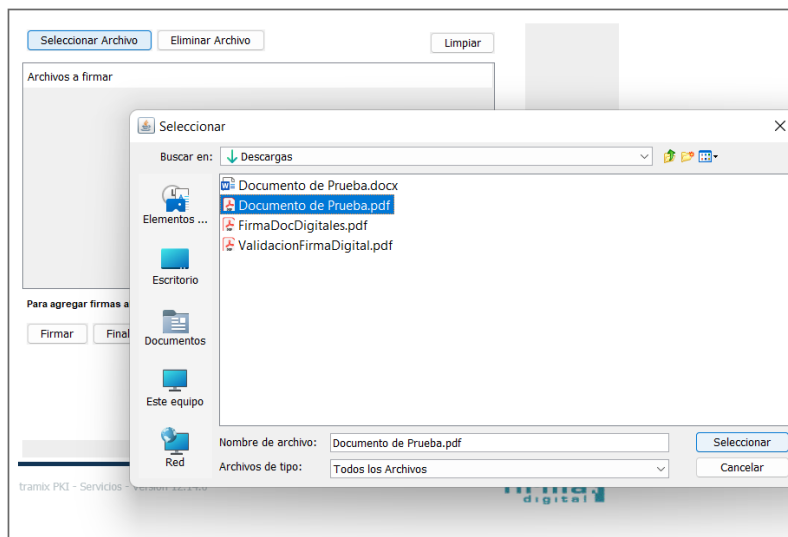
- Para navegador Microsoft Edge ver “Manual de Usuario Operativo - Modo IE en Microsoft EDGE “
 - La primera vez que se usa la aplicación, aparecerá un mensaje de seguridad, en el cual se debe hacer clic en la opción “Ejecutar”.
 - Posteriormente, comenzará a cargarse la aplicación.
2. Una vez que se cargó la aplicación, hacer clic en el botón “**Seleccionar el archivo**”.

Firmador



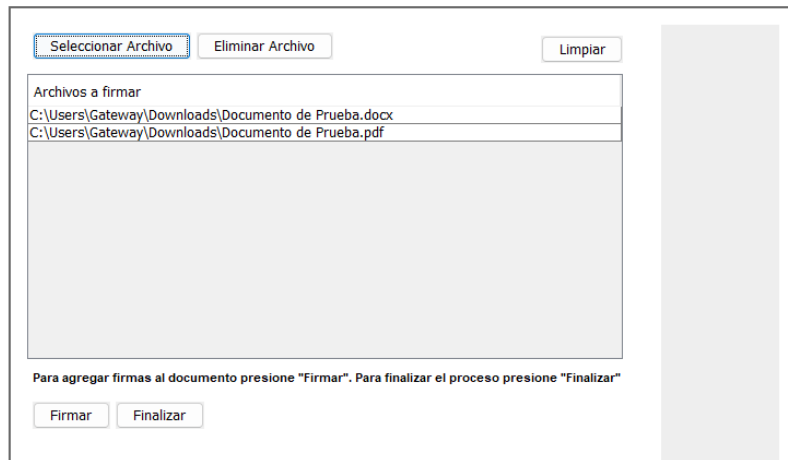
3. Luego, buscar el archivo a firmar en la carpeta donde el mismo fue guardado

Firmador



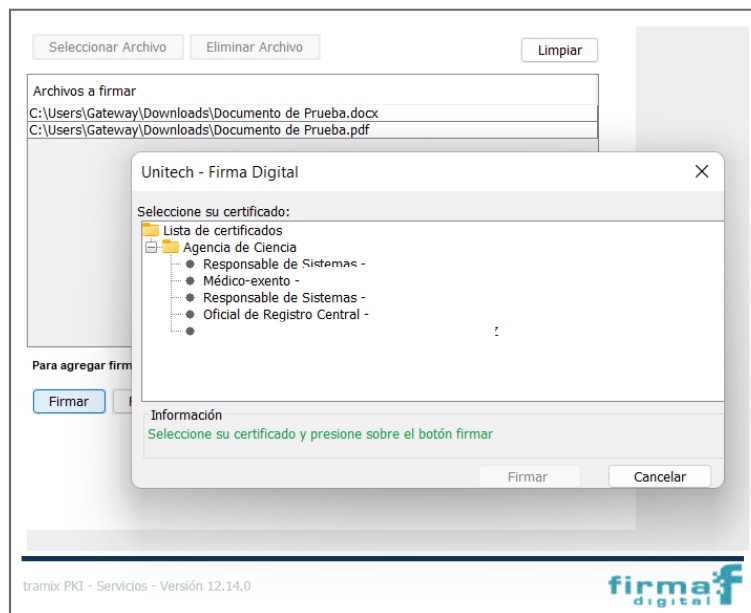
- Al seleccionar el o los archivos que se desean firmar, los mismos aparecen listados en la aplicación de Firma.

Firmador



- El o los archivos seleccionados deben encontrarse CERRADOS antes de firmarlos digitalmente
 - El dispositivo criptográfico debe estar conectado a la computadora para poder firmar. Luego hacer clic en el botón **"Firmar"**.
- Se despliega el panel de firma, buscar dentro de la lista de certificados que contiene el dispositivo criptográfico, el que se utilizará para firmar.

Firmador

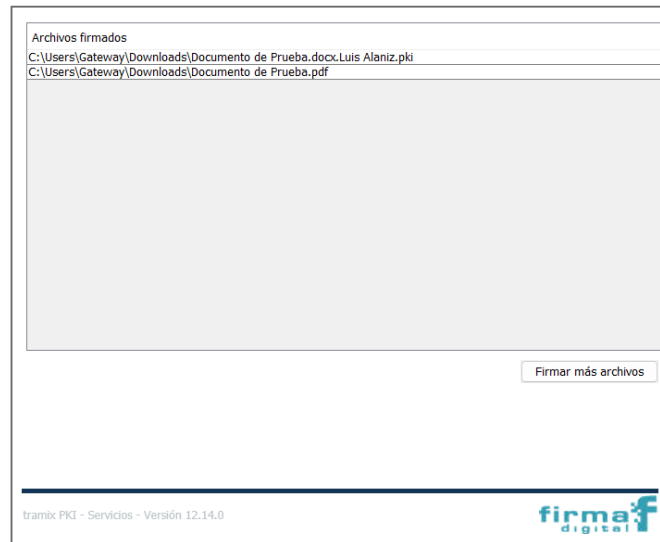


Una vez que seleccionó el certificado pulsar el botón **"Firmar"**, la aplicación pedirá la clave de seguridad del dispositivo, colocar la contraseña.

- Una vez firmado el documento, es posible seleccionar otro certificado digital para **"Firmar"** el documento nuevamente
- Luego pulsar el botón **"Finalizar"** y se concluye la tarea saliendo de la aplicación.

- Para asegurar que el documento quedo firmado correctamente, los mismos aparecen listados en **“Archivos firmados”**.

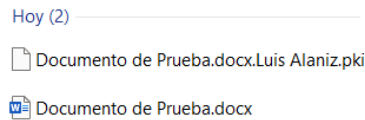
Firmador



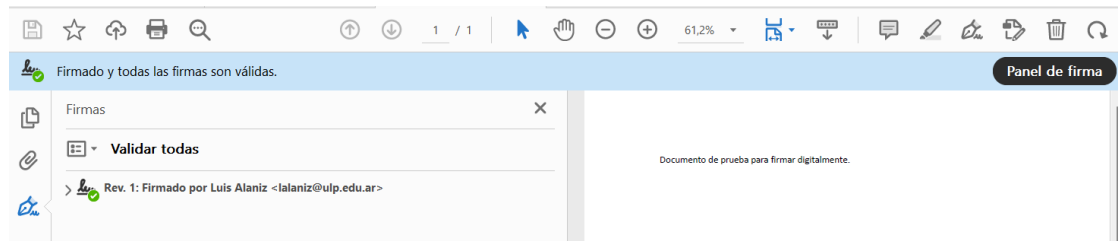
- Para iniciar una nueva tarea pulsar **“Firmar más archivos”**

IMPORTANTE:

- En caso de que el certificado seleccionado esté revocado, no se podrá firmar el documento y se mostrará el mensaje *“El certificado con el que se intenta firmar está revocado”*. Del mismo modo, si el certificado con el que se intenta firmar está vencido se mostrará un mensaje *“El certificado con el que se intenta firmar ha caducado”*.
- Para los documentos que no son en formato .pdf, el o los archivos “digesto” generados luego de firmar el documento (con extensión .pki) son guardados en la misma carpeta en la que se encuentra el archivo original, con el mismo nombre del documento + nombre del firmante.



- En el caso que se firme un archivo en formato .pdf, la firma queda incrustada dentro del mismo archivo, se puede visualizar desde el “Panel de Firma” y NO se genera un “digesto” con extensión .pki.



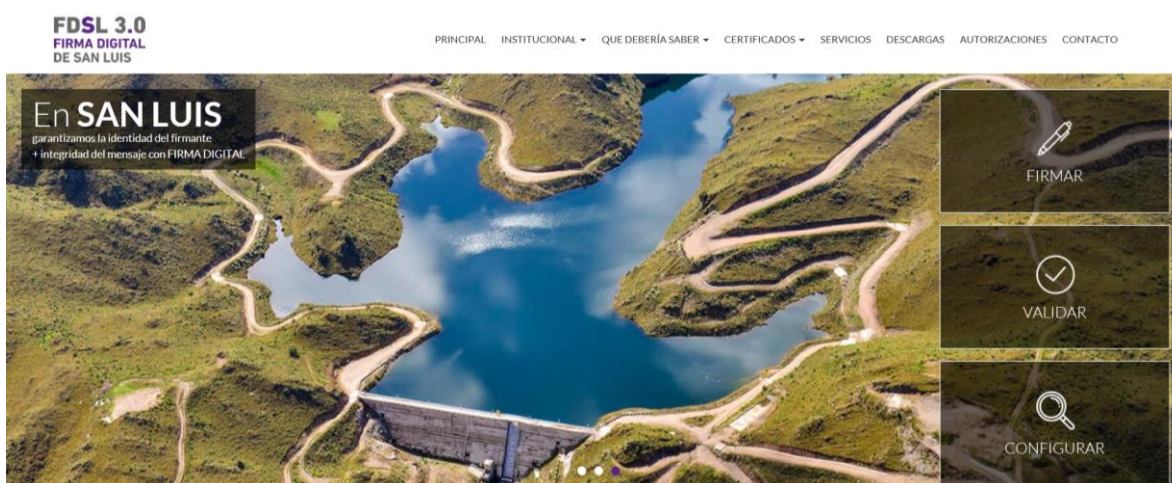
Servicio de Validación de Documentos Digitales

Antes de validar un documento firmado digitalmente, es necesario verificar que se cuenta con los siguientes **requisitos**:

- a) Tener instalada la última versión de Java.
- b) Contar con un documento firmado digitalmente.
- c) Ejecutar la aplicación en navegador Internet Explorer 11 o Microsoft Edge
- d) Para los casos en que el archivo NO es en formato .pdf, se debe tener el digesto firmado (archivo .pki) guardado en la misma carpeta que el documento original

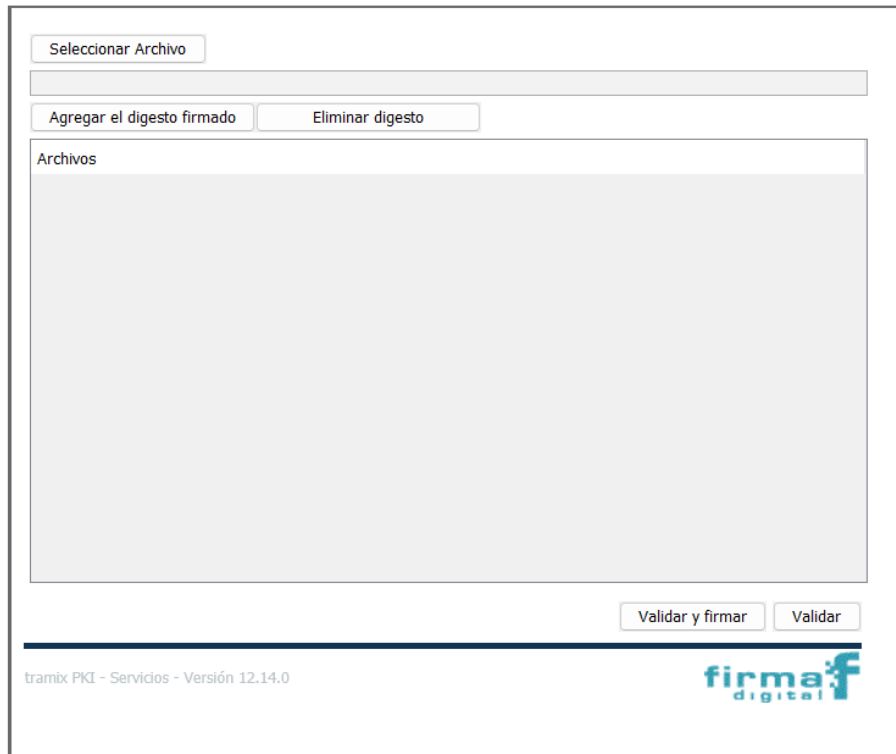
Los **pasos** que se deben seguir para validar un documento firmado digitalmente son:

1. Ingresar al portal de Firma Digital ([San Luis - Firma Digital](#)) y seleccionar la opción “VALIDAR” ✓



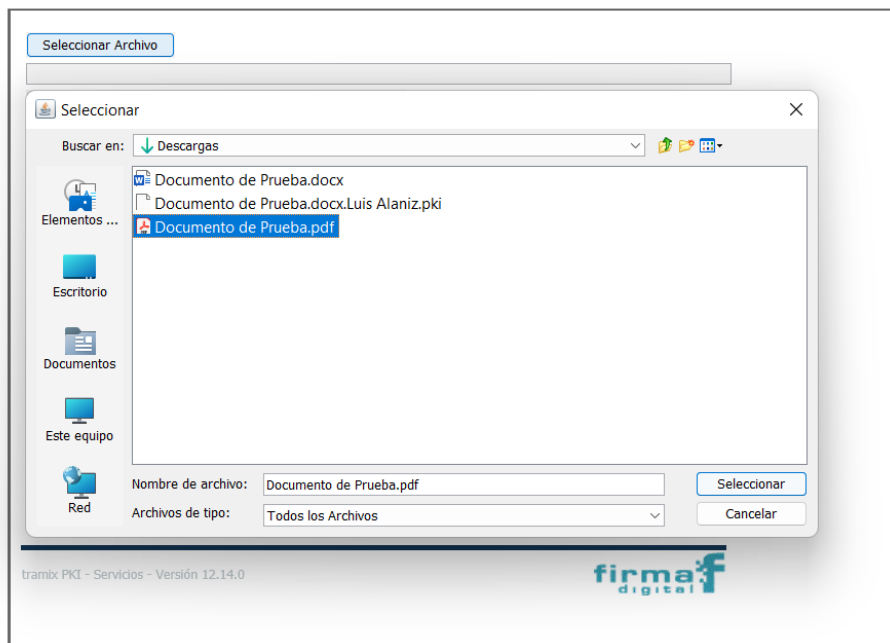
- Para navegador Microsoft Edge ver “Manual de Usuario Operativo - Modo IE en Microsoft EDGE “
 - La primera vez que se usa la aplicación, aparecerá un mensaje de seguridad, en el cual se debe hacer clic en la opción “Ejecutar”.
 - Posteriormente, comenzará a cargarse la aplicación.
2. Una vez que se cargó la aplicación, hacer clic en el botón “Seleccionar Archivo”.

Validador



3. Luego, buscar el archivo firmado en la carpeta donde el mismo fue guardado.

Validador



- Al seleccionar el archivo, el mismo aparecerá en la aplicación de validación de firma.

- Para los casos en que los archivos no son en formato .pdf, el digesto (archivo .pki) se incorporará automáticamente en la aplicación. Si el archivo a validar, no tiene el archivo digesto guardado en la misma carpeta, el mismo deberá ser buscado manualmente.

Validador

- En el caso de querer validar un archivo en formato .pdf, NO es necesario agregar un digesto (archivo .pki), porque el mismo contiene la firma incrustada en el archivo original.

Validador

4. Luego hacer click en el botón **“VALIDAR”**
 - Al momento de hacer la validación, si el documento original y/o su archivo digesto no sufrieron modificaciones, se muestra una ventana indicando que **“La firma es válida”**.
 - En caso de que la firma no es válida, ya sea porque se modificó el documento original o porque el archivo de firma no es el correcto, se muestra una ventana indicando que **“La firma no es válida”**.
 - **Seleccionando “validar más archivos”** se pueden agregar más archivos para validar.

Validador

Archivo validado
Documento de Prueba.pdf

Resultado de la validación de firmas:

Firmante	Resultado	Estado del certificado	
Luis Alaniz	✓ La firma es válida	Vigente	

Ej.1:

Validador

Archivo validado
Documento de Prueba.docx

Resultado de la validación de firmas:

Firmante	Resultado	Estado del certificado	
Luis Alaniz	✗ La firma no es válida	Vigente	

Ej.2:

- El icono ⓘ permite ver información del certificado digital que firmó el documento.

Validador

Archivo validado
Documento de Prueba.pdf

Resultado de la validación de firmas:

Firmante	Resultado	Estado del certificado
Luis Alaniz	✓ La firma es válida	Vigente

Certificado

✓ **La firma es válida.**

General Detalles

Información del certificado

Este certificado está destinado a los siguientes propósitos:

[1.3.6.1.5.5.7.3.2, 1.3.6.1.4.1.311.20.2.2, 1.3.6.1.5.5.7.3.4, 2.16.32.1.3.2.1.1.1]

Enviado a: Luis Alaniz


Emitido por PRUEBA FDSL - AC Agentes del Estado

Válido desde 15/03/2022 15:08 hasta 15/03/2026 15:08

⚠ La hora de la firma procede del reloj del equipo del firmante.

Aceptar

Validar más archivos



- En la solapa “Detalles” se muestran los datos del certificado digital con el cual se firmó el documento.

Validador

Archivo validado
Documento de Prueba.pdf

Resultado de la validación de firmas:

Firmante	Resultado	Estado del certificado
Luis Alaniz	✓ La firma es válida	Vigente

Certificado

✓ **La firma es válida.**


General Detalles

Campo	Valor
Versión	3
Número de serie	1a 00 00 01 43 63 d7 e3 64 31 29 b9 ...
Algoritmo de firma	sha256RSAENCRYPTION
Emisor	C=AR,ST=San Luis,SERIALNUMBER=...
Válido desde	15/03/2022 15:08
Válido hasta	15/03/2026 15:08
Asunto	C=AR,ST=SAN LUIS,E=lalaniz@ulp.ed...
Clave pública	30 82 01 22 30 0d 06 09 2a 86 48 86 ...
Identificador de clave entidad emisora	f7.02.3d.8c.06.f6.5a.f6.3a.e1.ea.c0.bd

C=AR
ST=SAN LUIS
E=lalaniz@ulp.edu.ar
T=Responsable de Sistemas
OU=Instituto Firma Digital de San Luis
O=Agencia de Ciencia Tecnología y Sociedad San Luis
SERIALNUMBER=CUIL
CN=Luis Alaniz

Aceptar

Validar más archivos



IMPORTANTE:

El proceso de validez de firma, Consiste en aplicar al documento original el algoritmo Hash, y por otro lado descifra el archivo firmado con la clave pública del firmante que está contenida en el digesto (archivo .pki). Luego se comparan ambos resultados y si coinciden se deduce que la firma es válida, caso contrario no se debe confiar en la integridad del documento original.