# Instructivo de Firmador

## Contenido

## Alcance

Este instructivo está dirigido a los usuarios Responsables, Segundos Responsables e Integrantes dentro de alguna unidad administrativa de la estructura organizacional de Expediente Digital.
El propósito del mismo es detallar las funciones disponibles dentro del Firmador, con Certificado Digital, de Documentos Electrónicos de la Plataforma Expediente Digital.

## ¿Quiénes pueden acceder?

Las condiciones para poder acceder a la opción:

- Tener los permisos de Responsable, 2do Responsable o integrante de alguna unidad.
- Tener CiDi nivel 2 (Ciudadano Digital).

## Cómo Acceder

1- Para acceder debe tener instalado el Firmador.

*(Consultar información sobre la instalación en https://portaltecnologico.cba.gov.ar/requerimientos-tics/servicios-tecnologicos/catalogo-de-servicios/herramientas-transversales/expediente-digital/instaladores-para-firma-digital/)*

2- Ingresar a FirmadorCBA, normalmente realizando la búsqueda por la barra de tareas de su sistema operativo.

Recomendamos siempre tener instalada solo la última versión del Firmador.

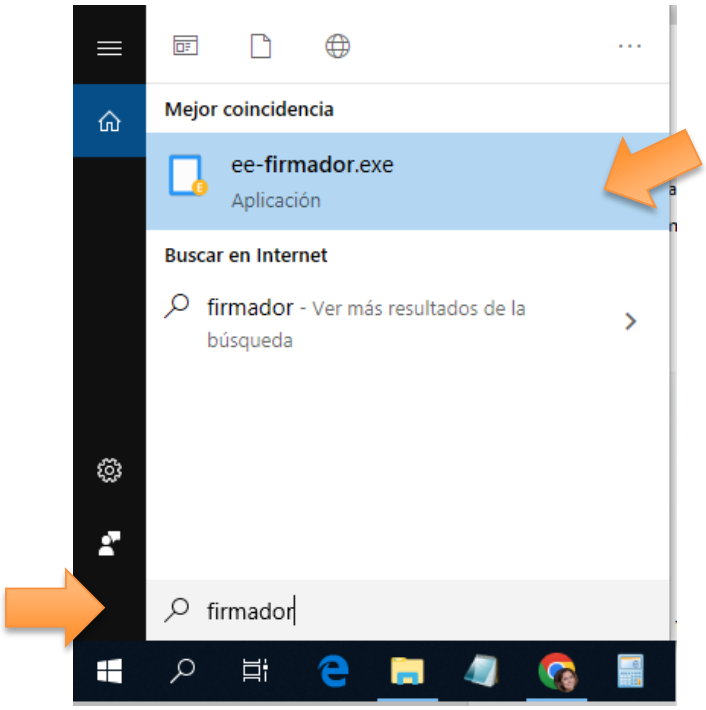


*Imagen 1: Ingreso a Firmador*

3- Al ingresar a dicho Firmador, automáticamente buscará si encuentra un Token conectado, en cuyo casi mostrará el nombre del modelo.


*Imagen 3: Pantalla principal Firmador: token detectado*

4- Caso contrario avisará que el Token no ha sido detectado.


*Imagen 4: Pantalla principal Firmador - token No Detectado*

## Validar

Esta opción permite realizar verificaciones sobre archivos externos a la plataforma Expediente Digital, ya sea que se hayan descargado de ella o que tengan otro origen.

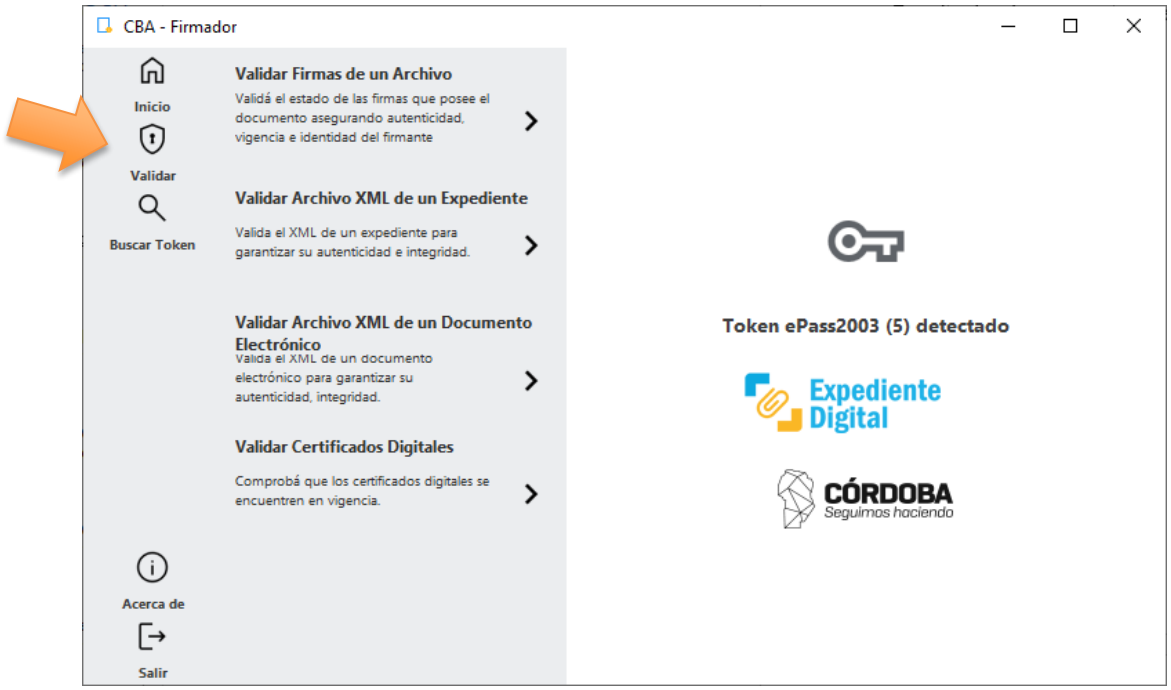


*Imagen 5: Opciones de Validación*

Al hacer clic sobre esta funcionalidad, se despliega y contrae el menú selección.

## Validar Firmas de un archivo

Al utilizar esta funcionalidad, se validará el estado de un documento en formato PDF, así como la validez de las firmas aplicadas en él.

Los puntos que se evalúan son los siguientes:

- **Formato del documento**: Se determinará si el documento está protegido, lo que impediría la posibilidad de firmarlo.
- **Autenticidad de las firmas**: Se comprobará la validez de las firmas incluidas en el archivo, verificando que sean firmas certificadas por la ONTI y confirmando la identidad del firmante.
- **Vigencia de la firma**: Se validará que la firma estaba vigente al momento de aplicarse.
- **Integridad del documento (confiabilidad)**: Se verificará que el documento no ha sido modificado desde la aplicación de la firma, y que la firma sigue siendo válida.

En resumen, este proceso sirve para asegurar que un documento contenido en el archivo PDF es confiable, válido y apto para su gestión dentro de la plataforma Expediente Digital.

### Instrucciones para su uso

Cuando ingresamos a esta opción, deberá seleccionar el archivo que desea verificar.

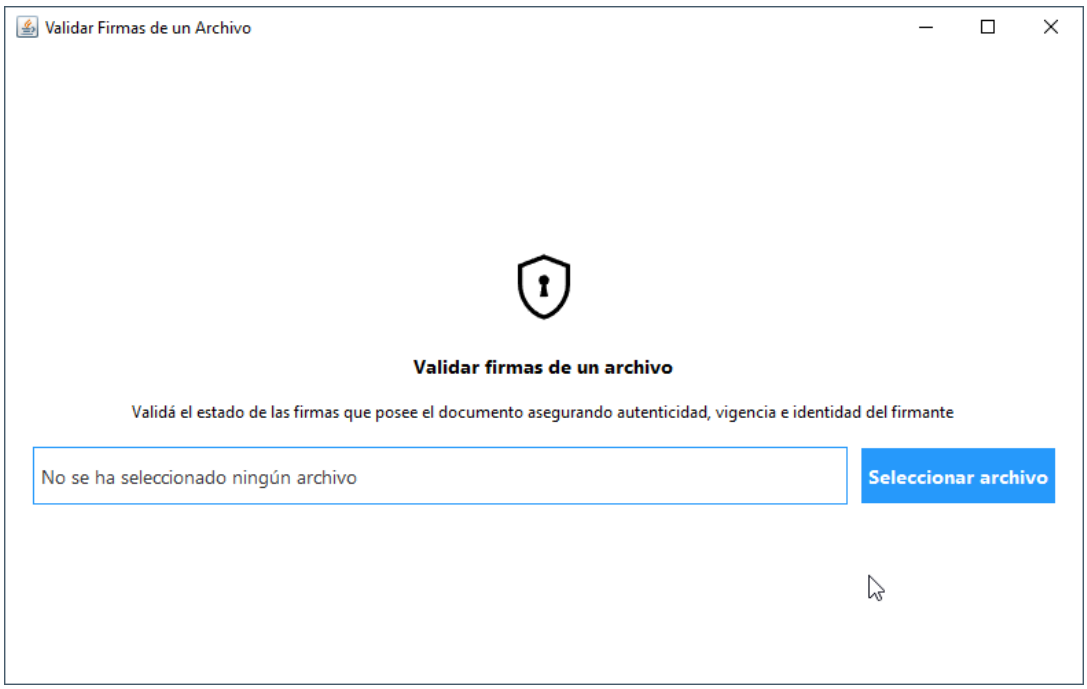


*Imagen 6: Validar firmas de un archivo: Paso 1 - Selección de Archivo*

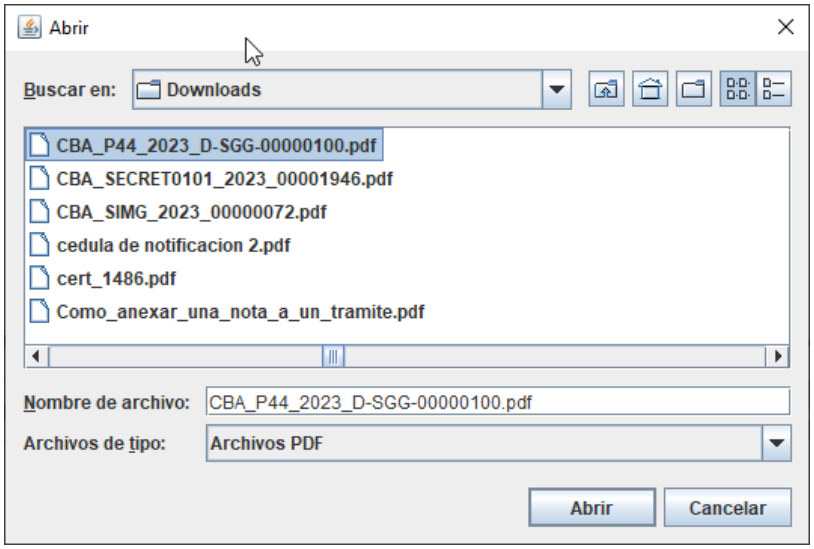


*Imagen 7: Validar firmas de un archivo: Paso 2 - Selección de Archivo*

Una vez seleccionado el archivo, presionar el botón *Validar*.

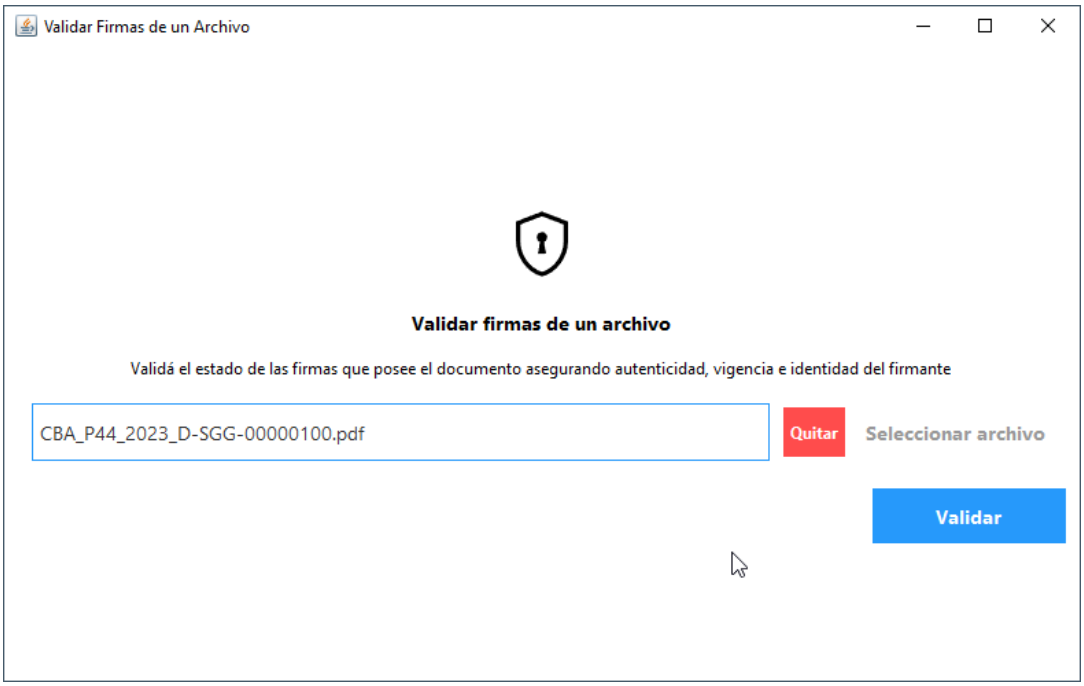


*Imagen 8: Validar firmas de un archivo: Paso 3 - Validar*

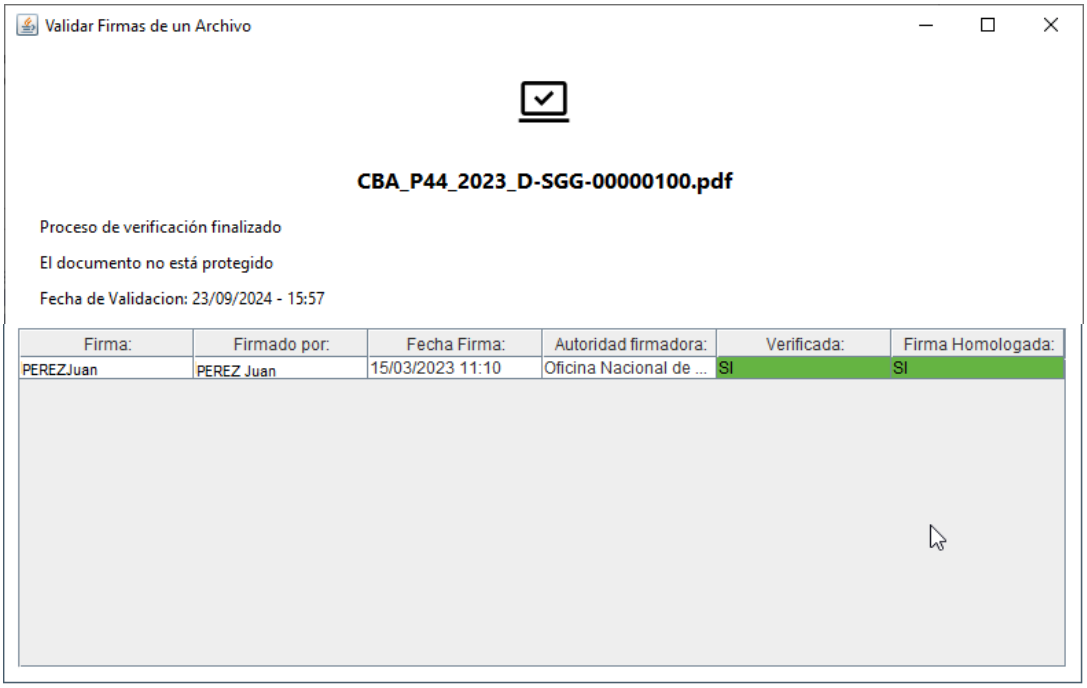


*Imagen 9: Validar firmas de un archivo: Paso 4 – Informe de Resultado*

## Información del reporte de resultado

Documento protegido

Esta comprobación se realiza, ya que cuando el documento se encuentre protegido, podrá incorporarse a la Plataforma pero no podrán solicitarse firmas sobre el mismo, ya que por su atributo no es modificable.

Firma

Es una referencia en el PDF a la firma que se analiza.

Firmado por

Es el nombre del firmante con certificado digital.

Fecha Firma

Corresponde a la fecha y hora en que fue firmado el PDF.

Autoridad firmadora

Se refiere a la autoridad emisora y garante del certificado digital que fue aplicado sobre el documento PDF.

Verificada

Indica si la firma era válida al momento de la firma.

Firma Homologada

Indica si el certificado continúa siendo válido para la entidad certificante.

## Validar Archivo XML de un Expediente

Es un procedimiento técnico que asegura que el expediente electrónico, representado en formato XML (Extensible Markup Language), cumple con una serie de requisitos fundamentales. Estos son:

- **Autenticidad**: Se verifica que el expediente es legítimo, asegurando que no ha sido alterado o manipulado por terceros. Esto garantiza que el origen del documento es confiable.
- **Integridad**: Se revisa que la estructura y el contenido del archivo XML no han sido modificados desde su creación o su última actualización. Cualquier alteración en el archivo se detecta como una posible falla en su integridad.
- **Conformidad**: Se asegura que el archivo XML cumple con las normas y especificaciones técnicas establecidas. Esto implica que el expediente sigue el esquema (estructura de datos) y los estándares requeridos por la “norma técnica del Gobierno de la Provincia de Córdoba”, lo que permite su correcta interpretación y procesamiento en los sistemas oficiales.

La opción “Validar Archivo XML de un Expediente” es una herramienta especializada que analiza el archivo XML en busca de:

- **Estructura correcta del XML**: El archivo debe seguir un esquema predefinido (generalmente en formato XSD), donde se especifica cómo deben organizarse los datos (nodos, atributos, etc.). Si hay errores en la estructura, el expediente no será conforme.
- **Firma electrónica y autenticidad**: Se comprueba que las firmas digitales aplicadas al expediente sean válidas, verificando su origen y certificación. Estas firmas son fundamentales para garantizar que el documento no ha sido alterado.
- **Contenido íntegro**: Se verifica que los datos contenidos en el XML no han sido modificados después de su firma. Cualquier cambio no autorizado en el expediente sería detectado y marcado como una falla de integridad.
- **Cumplimiento con la normativa**: Se chequea que el expediente siga todas las especificaciones técnicas definidas en la normativa del gobierno. Esto incluye el uso correcto de etiquetas y datos dentro del archivo XML.

### Instrucciones para su uso

Cuando ingresamos a esta opción, deberá seleccionar el archivo que desea verificar.

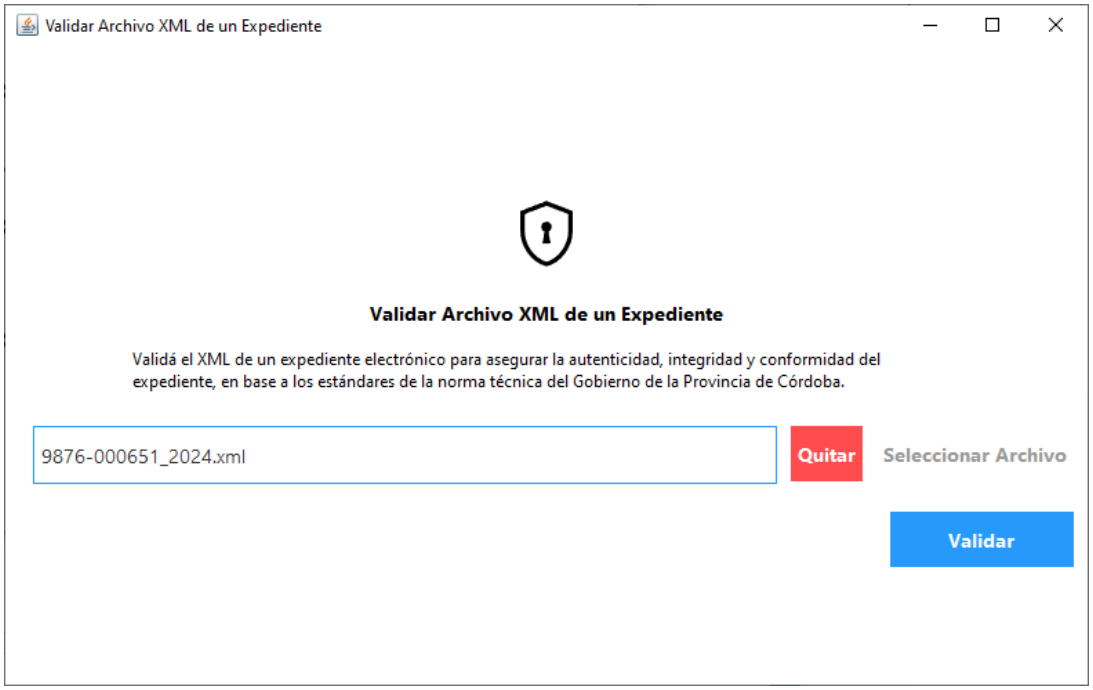


*Imagen 10: Validar Archivo XML de un Expediente: Paso 1 – Selección de archivo y confirmar*

Al finalizar la validación, se genera un reporte que indica si el expediente es válido o si presenta problemas, detallando cualquier error de autenticidad, integridad o conformidad.

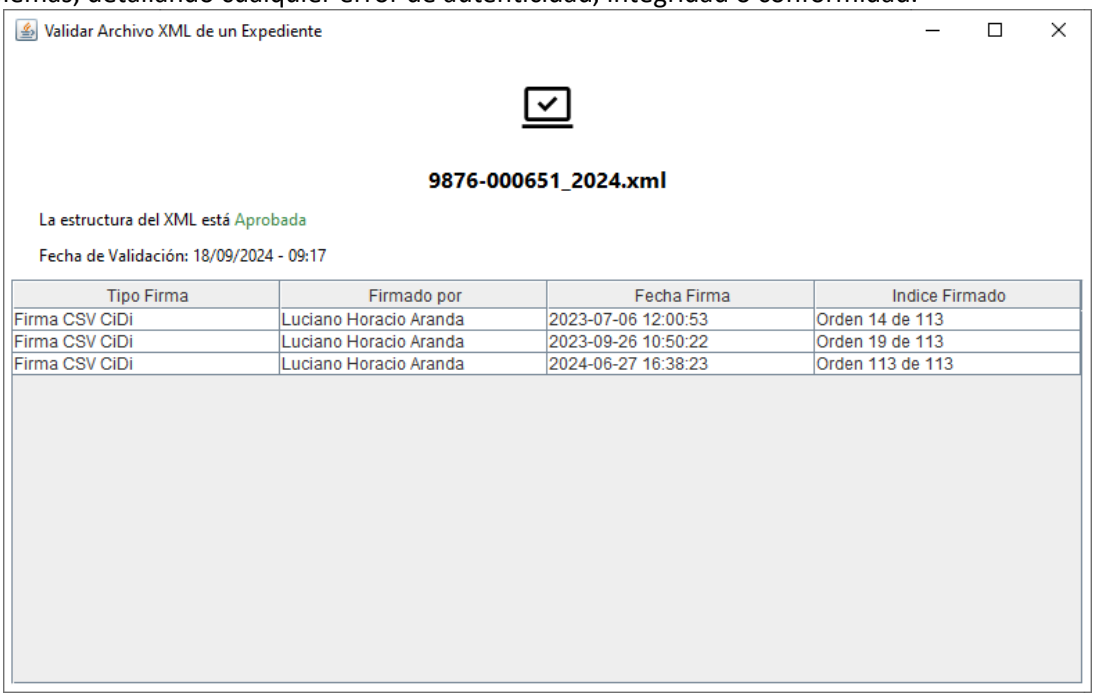


*Imagen 11: Validar Archivo XML de un Expediente: Paso 2 – Resultado de validación*

### Información del reporte de resultado

Estructura de XML

En este apartado se indica si el XML que se está analizando posee una estructura correcta y en vigencia con la especificación definida para un Expediente de acuerdo a la Norma Técnica.

Tipo de Firma

Actualmente en el XML de un Expediente podemos encontrar una "Firma CSV CiDi", cuya seguridad está dada por la Firma Electrónica del agente con Pin de Cidi.
Esta firma tiene efecto sobre el último Orden existente al momento que el agente aplique la firma, lo que implica su conformidad en todas las actuaciones hasta ese Orden del índice.
CSV o Código Seguro de Verificación (CSV), es un código que genera la aplicación a partir de SHA256 del contenido del Expediente Digital lo que permite garantizar su integridad y autenticidad.

Firmado por

Es la persona que realizó la firma sobre el Expediente.

Fecha Firma

El momento en que aplicó la firma sobre el Expediente.

Índice Firmado

Es el Orden del Índice sobre el cual efectuó la firma, y el último orden que tenía al momento de descargar el XML del Expediente desde la plataforma, es decir, el archivo que se está analizando.

## Validar Archivo XML de un Documento Electrónico

Es un procedimiento técnico que permite verificar que el Documento Electrónico representado en un formato XML, cumple con los requisitos de acuerdo con la "norma técnica" establecida por el Gobierno de la Provincia de Córdoba, asegurando los siguientes aspectos:

- **Autenticidad**: Garantiza que el documento es legítimo y no ha sido alterado por terceros.
- **Integridad**: Verifica que el archivo no ha sido modificado desde su creación o última actualización.
- **Conformidad**: Asegura que el archivo cumple con los requisitos técnicos y normativos exigidos para los expedientes.

Similar que la Validación de Expediente Electrónico, esta opción evalúa el archivo XML considerando lo siguiente:

- **Estructura correcta del XML**: El archivo debe seguir un esquema predefinido (generalmente en formato XSD), donde se especifica cómo deben organizarse los datos (nodos, atributos, etc.). Si hay errores en la estructura, el documento no será conforme.
- **Firma electrónica y autenticidad**: Se comprueba que las firmas digitales aplicadas al expediente sean válidas, verificando su origen y certificación. Estas firmas son fundamentales para garantizar que el documento no ha sido alterado.

- **Contenido íntegro**: Se verifica que los datos contenidos en el XML no han sido modificados después de su firma. Cualquier cambio no autorizado en el documento sería detectado y marcado como una falla de integridad.
- **Cumplimiento con la normativa**: Se chequea que el documento siga todas las especificaciones técnicas definidas en la normativa del gobierno. Esto incluye el uso correcto de etiquetas y datos dentro del archivo XML.

### Instrucciones para su uso

Al elegir esta opción, se deberá seleccionar el archivo que desea verificar.

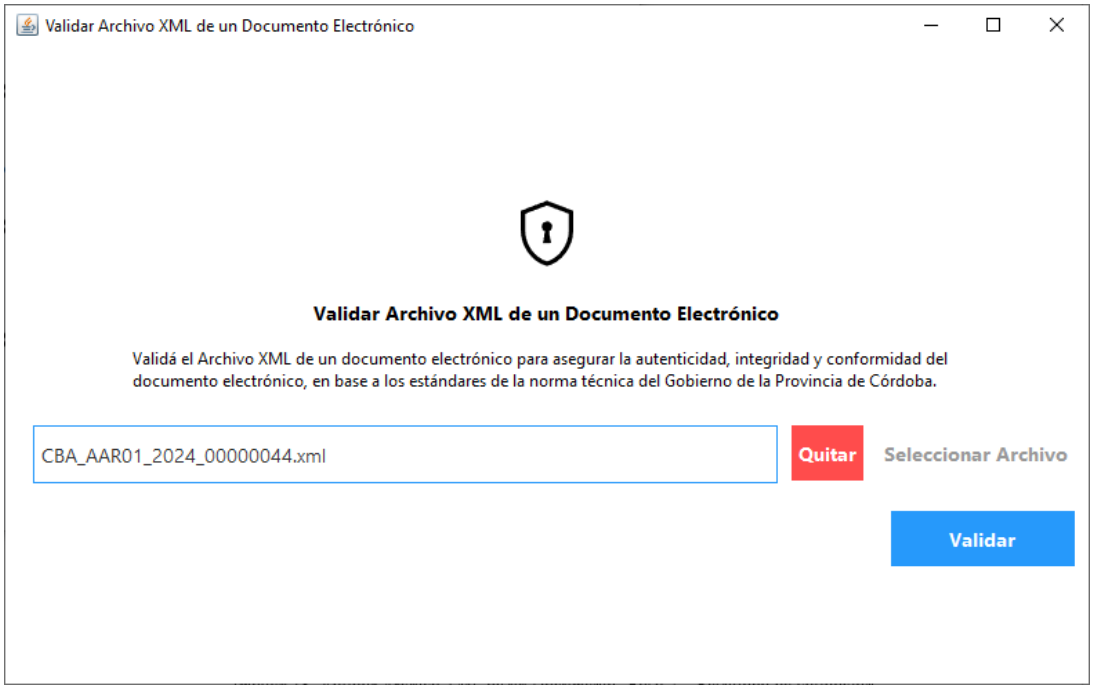


*Imagen 12: Validar Archivo XML de un Documento: Paso 1 – Selección de archivo*

Al finalizar la validación, se genera un reporte que indica si el documento es válido o si presenta problemas, detallando cualquier error de autenticidad, integridad o conformidad.

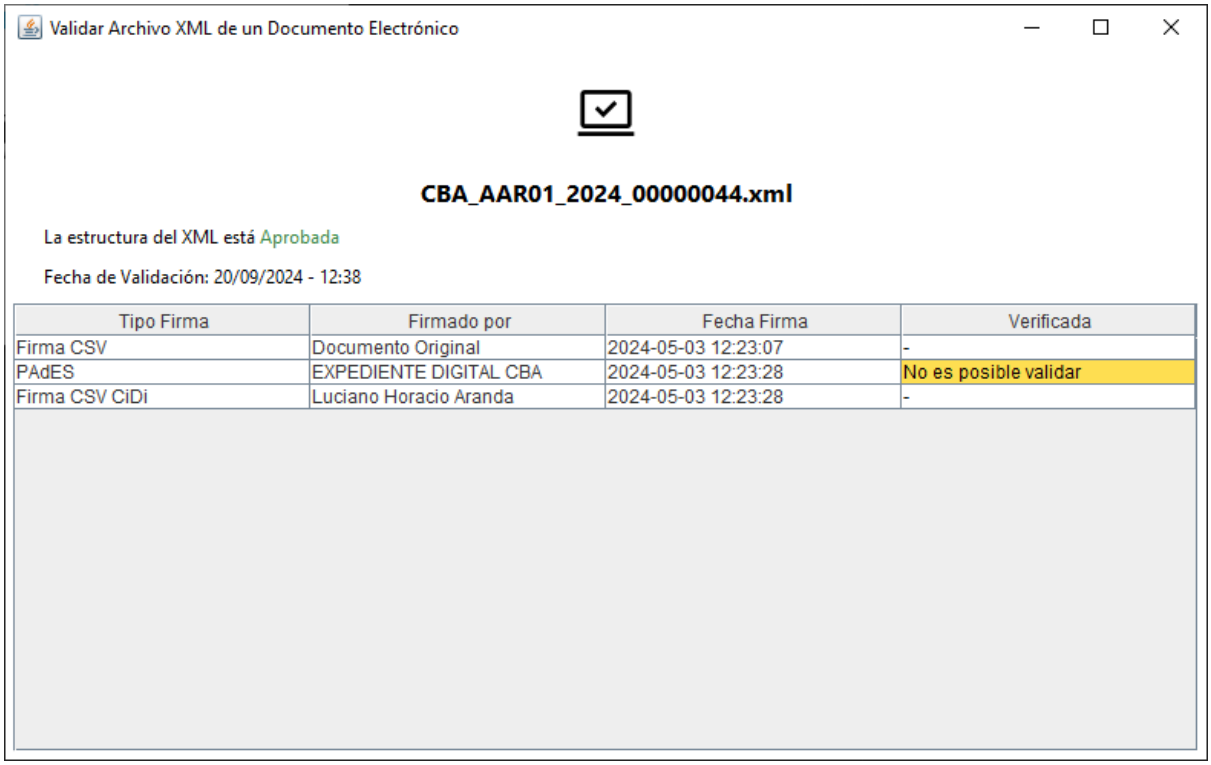


*Imagen 13: Validar Archivo XML de un Documento: Paso 2 – Resultado de validación*

## Información del reporte de resultado

Estructura de XML

En este apartado se indica si el XML que se está analizando posee una estructura correcta y en vigencia con la especificación definida para un Documento Electrónico de acuerdo a la Norma Técnica.

Tipo de Firma – Firma CSV

Se refiere a dos tipos de Seguridad, la Firma Digital de la Persona realizada sobre el PDF contenido en el Documento Electrónico, cuya seguridad está dada por el empleo del Certificado Digital.
Y la firma del CSV del contenido del Documento, utilizando SHA256 sobre los datos del Documento Electrónico lo que permite garantizar su integridad y autenticidad.

Tipo de Firma – PAdES

Se refiere la Firma Digital de la Aplicación realizada sobre el PDF contenido en el Documento Electrónico, cuya seguridad está dada por el empleo del Certificado Digital dentro de la plataforma.
Y la firma del CSV del contenido del Documento, utilizando SHA256 de los datos del Documento Electrónico lo que permite garantizar su integridad y autenticidad.

Tipo de Firma – Firma CSV CiDi

Se refiere a la Firma Electrónica de la Persona sobre contenido completo del Documento Electrónico, cuya seguridad está dada por el empleo del Pin de CiDi de la persona autenticada.

Firmado por

Es la persona o entidad que realizó la firma sobre el Expediente.

Fecha Firma

El momento en que aplicó la firma sobre el Expediente.

Verificada

Muestra el resultado de la Validación de la firma. En este punto es importante aclarar que a medida que se agregan firmas al contenido del documento, el SHA256 original ya no coincide con el contenido firmado anteriormente, pero la plataforma se encarga de realizar la validación de integridad y autenticidad antes de aplicar la siguiente firma. Por ello el resultado que tiene mayor valor en esta columna es el último registro de firma.

## Validar Certificados Digitales

Esta opción permite verificar el certificado digital existente en el token que está conectado al equipo personal. Se analizan los siguientes aspectos:

- **Identidad del firmante**: Confirma la persona o entidad a la que pertenece el certificado.
- **Vigencia del certificado**: Verifica que el certificado esté activo y no haya expirado.
- **Entidad emisora**: Comprueba qué organismo emitió el certificado digital.

### Instrucciones para su uso

Al iniciar el proceso, la aplicación visualizará una pantalla de confirmación para comenzar el proceso de validación:

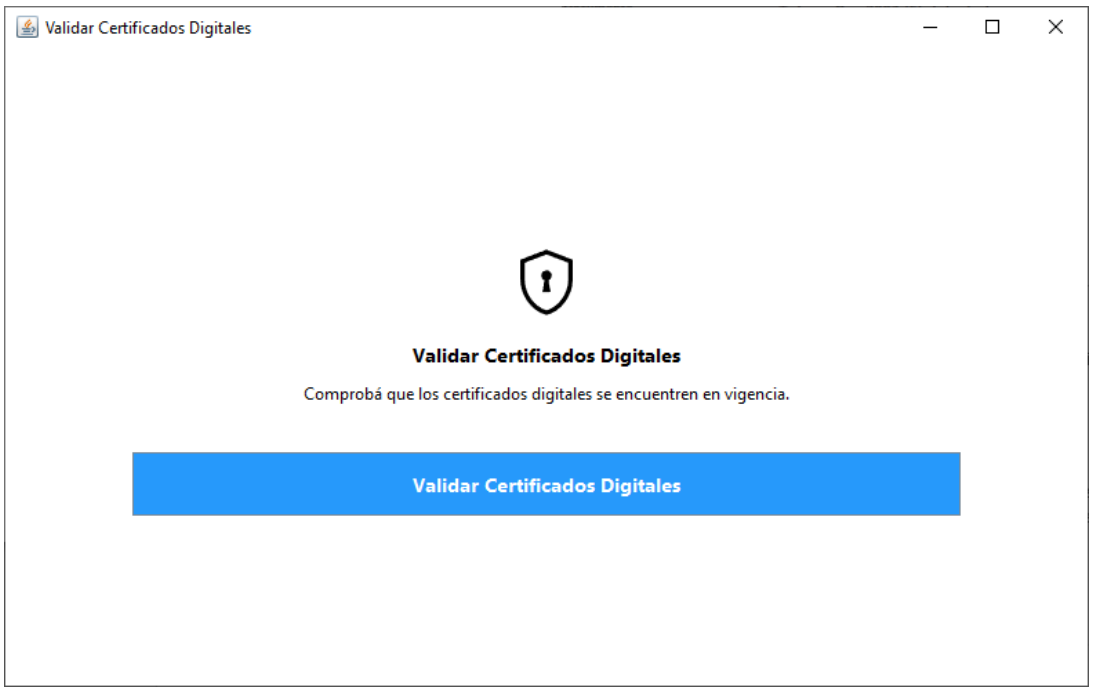


*Imagen 14: Validar Certificados Digitales: Paso 1 – Confirmar proceso de validación*

El sistema solicitará el Pin del Token para continuar.

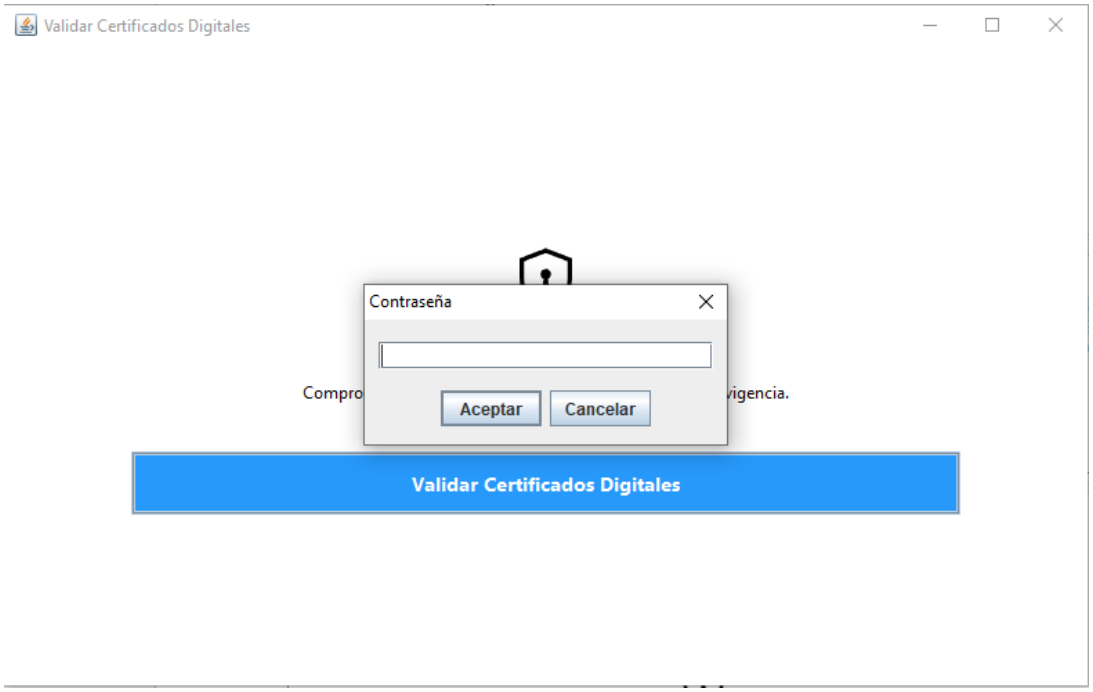


*Imagen 15: Validar Certificados Digitales: Paso 2 –Pin del Token*

Seguido de ello, la herramienta realizará el análisis de la información del Certificado y mostrará el resultado obtenido.


*Imagen 16: Validar Certificados Digitales: Paso 2 – Resultado de validación*

## Información del reporte de resultado

Autoridad Certificadora: Indica la Entidad u Organización que legitima el Certificado.
Titular del Certificado: Muestra el nombre y apellido del titular del Certificado.

Vigencia: indica si el certificado está vigente o vencido, y en caso de vigente hasta que fecha será válido.

## Buscar Token

Cuando el Token no ha sido detectado al iniciar el Firmador, no será posible firmar Documentos Electrónicos con Firma Digital o Firma Digital PDF. Por ello, esta opción es útil para forzar la detección del Token antes no encontrado.

### Instrucciones para su uso

Simplemente, conecta el dispositivo e ingresa a la opción Buscar Token. Automáticamente escaneará el hardware en búsqueda del dispositivo.

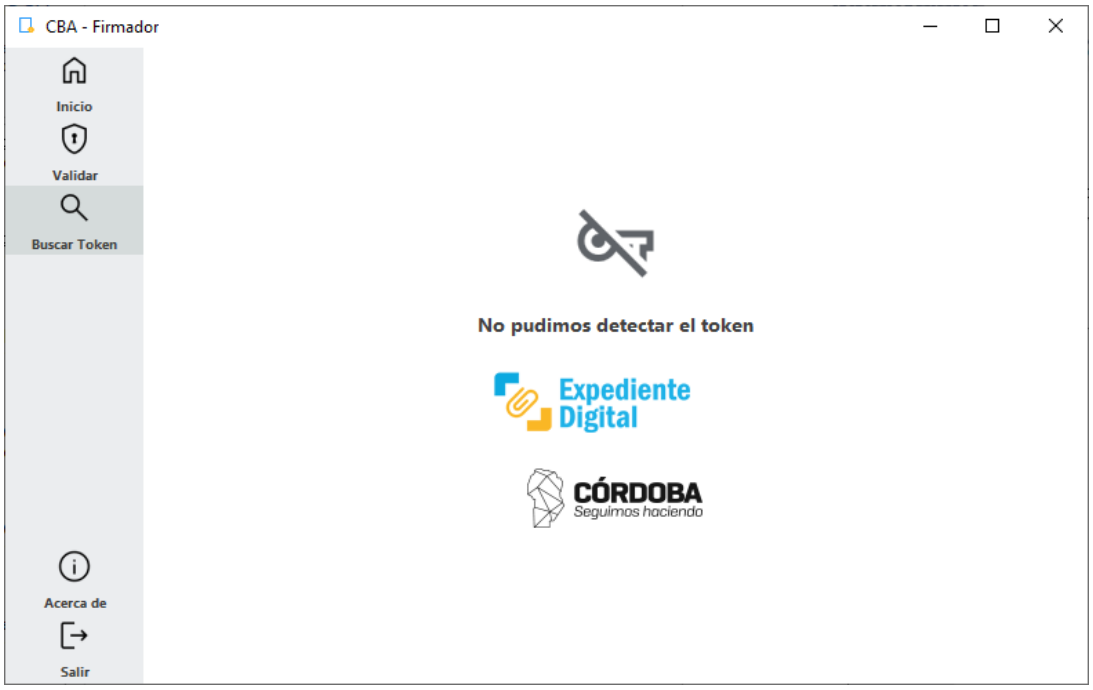


*Imagen 17: Buscar Token: Paso1- Selección de opción*

Al encontrar el token, se visualiza el modelo del mismo. Ahora sí, podrás realizar firmas sobre documentos electrónicos.


*Imagen 18: Buscar Token: Paso2- Token detectado*

## Acerca de

### Versión

Esta opción permite conocer la versión instalada de la herramienta Firmador. Adicionalmente posibilita acceder a la descarga de su instalador.

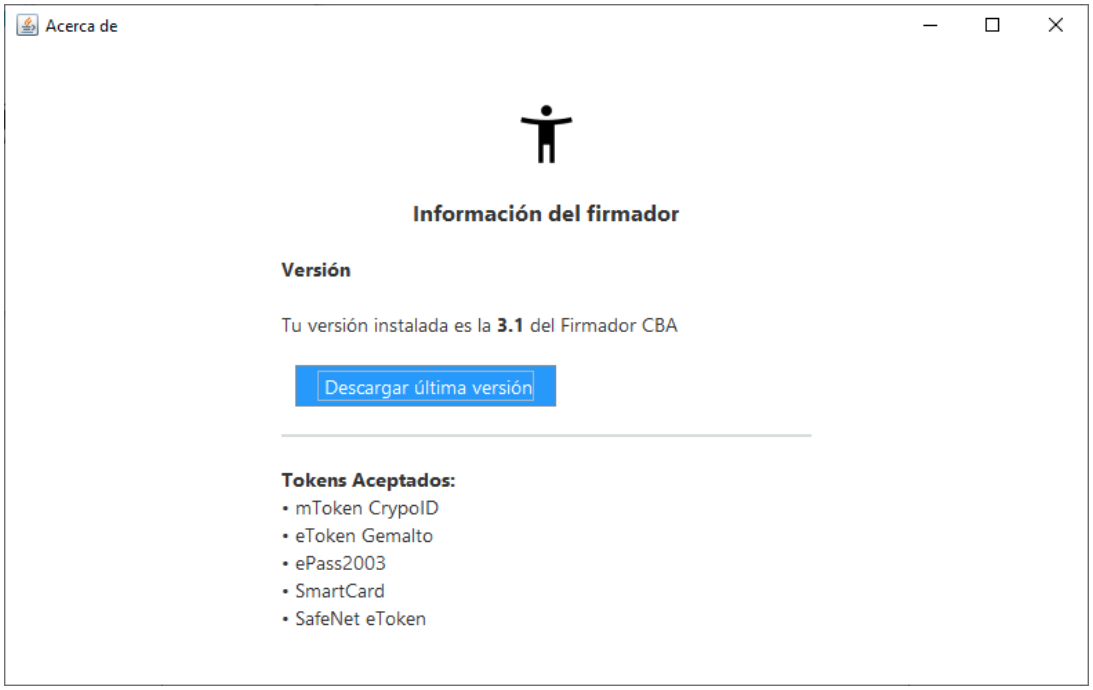


*Imagen 19: Acerca de*

## Tokens aceptados

En esta opción también se visualiza el listado de Tokens contemplados para firmar Documentos con esta herramienta.

## Salir

Simplemente cerrar Firmador.