Universidad Nacional del Noroeste de la Provincia de Buenos Aires

Integración de Firma Digital con smartcards en los Procesos Administrativos de la Universidad

Carrera: Ingeniería en Informática

Práctica Profesional Supervisada

Estudiante: Francisco Andres Berruet Marchetto

Tutor Docente: Carlos Di Cicco

Tutor de Empresa/Institución/Organización: Hugo Ramon

Fecha de presentación: 17 de Noviembre de 2025

Resumen / Abstract

El presente proyecto describe el desarrollo del “Firmador”, una aplicación multiplataforma destinada a agilizar y asegurar la firma digital de documentos PDF mediante el uso de smart cards (tokens criptográficos).

La solución se apoya en los estándares PAdES (PDF Advanced Electronic Signatures; European Telecommunications Standards Institute, 2020), X.509 (Internet X.509 Public Key Infrastructure; Cooper et al., 2008) y PKCS#11 (Cryptographic Token Interface Standard; OASIS, 2020), garantizando la validez legal, seguridad e interoperabilidad de las firmas digitales, en concordancia con el marco normativo establecido por la Ley N.º 25.506 de Firma Digital (Argentina, 2001).

Entre sus principales funcionalidades se destacan la posibilidad de que un mismo usuario firme con distintos roles (gestionando diferentes perfiles de firma asociados a cada función y/o token), la firma masiva de documentos y la integración con el sistema institucional de certificados, permitiendo una firma ágil, segura y totalmente compatible con los procesos administrativos vigentes.

El resultado fue una herramienta confiable, eficiente y de uso intuitivo, que fortalece las actividades de transformación digital de la Universidad Nacional del Noroeste de la Provincia de Buenos Aires (UNNOBA), contribuyendo a la optimización y modernización de su gestión documental.

Índice

1. Introducción

Desde su creación, la UNNOBA ha realizado aportes significativos en educación, ciencia y tecnología, potenciando un desarrollo regional equilibrado. Esta estrategia institucional está sólidamente fundamentada en los procesos de autoevaluación y planificación estratégica definidos en las Resoluciones del Consejo Superior 571/2012, 657/2013 y 1750/2019.

En este marco, la Prosecretaría de Tecnologías de la Información y Comunicación (PRO TIC), creada por la Resolución Rectoral 3698/2011, cumple la misión de fomentar la implementación de TIC para optimizar la gestión. Sus acciones se orientan en cuatro ejes estratégicos (Gestión, Servicios, Infraestructura y Consolidación), siendo el presente proyecto un pilar directo del eje de Gestión, al buscar potenciar la administración mediante el uso de TIC y asegurar la calidad de la información.

La UNNOBA impulsa la transformación digital de su gestión administrativa, incorporando la firma digital como herramienta para garantizar la autenticidad, integridad y trazabilidad de los documentos, en concordancia con la Ley N.º 25.506. En 2013 la UNNOBA cumplió los requisitos para ser Autoridad de Registro de certificados digitales de la Oficina Nacional de Tecnologías de Información (ONTI) (EXP. 2545/2013), lo que permitió la implementación de la firma con token y consolidó un ecosistema de gestión documental integrado, en el cual herramientas como Dossier, Firmador y Notificaciones interactúan para asegurar la validez jurídica de los documentos digitales.

La primera solución institucional para la firma digital de documentos PDF se basó en un applet de Java, desarrollado originalmente a partir del firmador PDF publicado por la ONTI en 2013. Este componente permitió durante varios años integrar la firma digital en los sistemas administrativos, ofreciendo funcionalidades como, la validación de certificados y OCSP, la verificación de la cadena de confianza y, cuando el navegador lo permitía, la visualización del PDF.

No obstante dicha solución se basaba en dos applets Java. La obsolescencia de esta tecnología (declarada desde 2017) y la pérdida de soporte por parte de los navegadores derivaron en problemas de compatibilidad y seguridad, fragmentando los flujos de trabajo y obligando al uso de soluciones externas o navegadores desactualizados.

En respuesta a esta situación, y en el marco de la Práctica Profesional Supervisada (PPS), a partir de octubre de 2022 se comenzó el desarrolló de “Firmador UNNOBA”. Esta aplicación multiplataforma fue diseñada para reemplazar a los obsoletos applets Java, permitiendo la firma digital de documentos PDF con smartcards de manera moderna, segura y alineada con las normativas vigentes. El proyecto busca establecer una solución estable que no solo consolide el ecosistema digital de la Universidad, optimizando la eficiencia operativa.

2. Problema y Objetivos

Problemática

La solución previa de firma digital, basada en un Applet de Java, se encuentra totalmente obsoleta y sin soporte, habiendo alcanzado su estado de End-of-Life (EoL) en 2017. Debido a la eliminación del soporte para applets en los navegadores modernos, su mantenimiento se volvió inviable tanto desde el punto de vista técnico como de seguridad.

La firma digital constituye un componente crítico dentro de los flujos administrativos de la UNNOBA: es requerida para numerosos flujos (figura 1) y resulta indispensable para garantizar la autenticidad e integridad de la documentación

En este contexto, la obsolescencia de la herramienta anterior compromete la continuidad operativa y expone a la institución a riesgos funcionales y de seguridad. Por ello, se vuelve imprescindible renovar y modernizar la solución de firma digital.

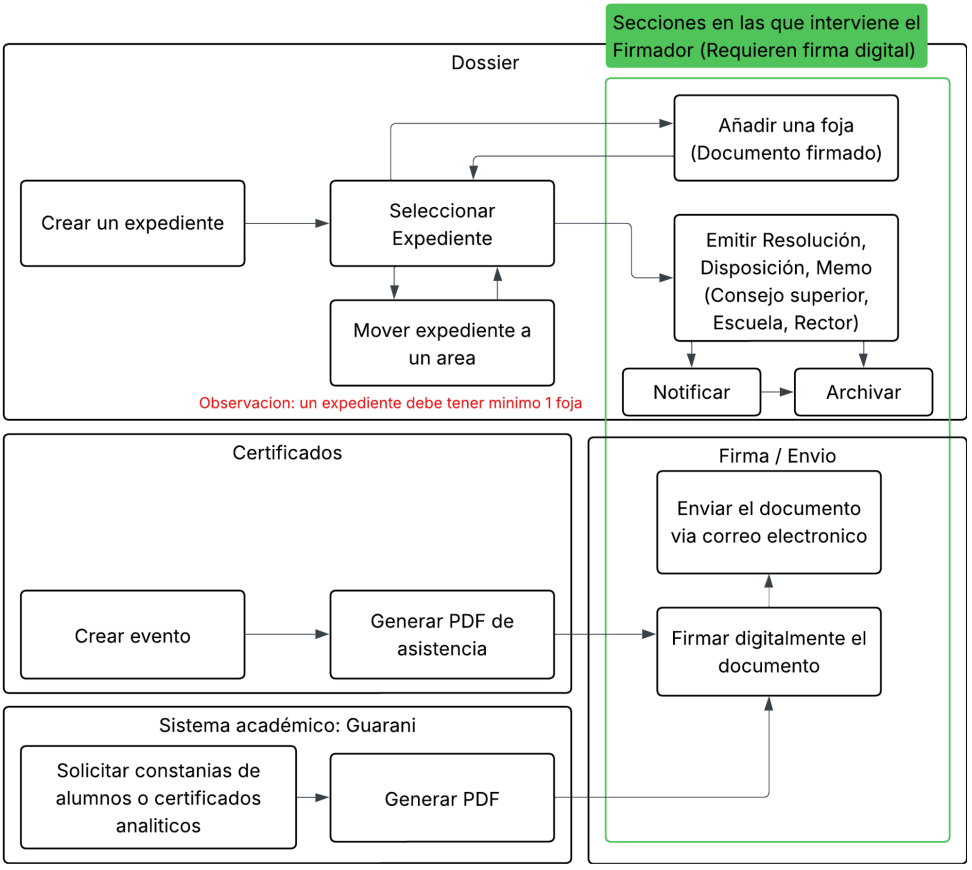


Figura 1- Diagrama de alto nivel sobre los flujos administrativos de firma digital

Este estado de obsolescencia se explica por varios factores críticos asociados al mantenimiento adaptativo y a la seguridad, que se vuelven más exigentes a medida que evoluciona la tecnología:

Riesgo de seguridad y falta de mantenimiento adaptativo: para utilizar la herramienta anterior, los usuarios debían recurrir a una versión obsoleta del navegador Firefox (52.0, 2017), sin parches de seguridad vigentes.

Problemas de rendimiento y arquitectura desactualizada: la arquitectura basada en servlets presentaba limitaciones al procesar grandes volúmenes de archivos, afectando directamente la eficiencia del proceso de firma.

Requisito institucional ineludible: la firma digital es obligatoria en múltiples flujos administrativos, por lo que no es posible retornar a procedimientos en papel o a esquemas manuales.

Necesidad de continuidad en el sistema de certificados: aunque algunos usuarios emplean herramientas alternativas para firmar, el sistema institucional de certificados aún dependía del firmador antiguo y requería una actualización urgente.

Objetivo general

Diseñar e implementar una aplicación de escritorio multiplataforma para la firma digital con smartcards, que reemplace a los sistemas obsoletos y se integre de forma segura en los flujos administrativos institucionales. Esto se realizará aprovechando el hardware existente (smartcards) y la infraestructura institucional ya disponible, como el sistema de certificados y el servicio de almacenamiento OwnCloud.

En relación con esta infraestructura, OwnCloud funciona como la plataforma institucional de gestión de archivos de la UNNOBA. Cada usuario dispone allí de una carpeta “firmador” con tres subcarpetas (*Documentos A Firmar*, *Documentos Firmados* y *Documentos Originales*) que organizan el flujo documental. El Firmador UNNOBA utiliza estas carpetas para sincronizar los archivos en red, descargando los documentos a firmar y publicando las versiones firmadas de manera centralizada.

Objetivos específicos

Desarrollar una aplicación de escritorio multiplataforma que permita firmar documentos PDF utilizando certificados digitales almacenados en smartcards.

Integrar la solución al flujo de trabajo del sistema de certificados.

3. Fundamentos técnicos

Para garantizar la validez legal y técnica de las firmas digitales, la aplicación adopta los estándares internacionales X.509 y PKCS#11. Combinados, estos estándares permiten gestionar identidades digitales, claves criptográficas y operaciones de firmado de manera segura, confiable y verificable.

¿Qué es la Firma Digital ?

La firma digital es un mecanismo criptográfico que asegura la identidad del firmante y la integridad del documento firmado. En Argentina, se encuentra regulada por la Ley N.º 25.506 de Firma Digital, que otorga a las firmas digitales la misma validez jurídica que una firma ológrafa realizada ante un escribano, siempre que se cumplan los requisitos técnicos establecidos por dicha norma.

En contextos institucionales, como la UNNOBA, la firma digital resulta esencial porque:

- permite reemplazar procesos manuales (papel, sellos, firmas presenciales),
- provee garantías técnicas verificables de autenticidad e integridad,
- habilita flujos administrativos más eficientes, auditables y automatizables,
- reduce riesgos operativos asociados a manipulaciones, pérdidas o falsificaciones de documentos.

Estas características la convierten en un componente crítico de la modernización administrativa.

Propósitos de la Firma Digital

La implementación de una firma digital garantiza tres principios fundamentales en la gestión documental:

- Integridad: Asegura que el documento no ha sufrido ninguna alteración o modificación desde el momento en que fue firmado.
- Autenticidad: Confirma que la firma está vinculada a una identidad verificable y legítima.
- No Repudio: Impide que el firmante pueda negar la autoría de la firma en el documento.

Certificados X.509
El estándar X.509 define el formato del certificado digital que vincula criptográficamente a una persona u organización con su clave pública. Este vínculo es validado mediante la firma

de una Autoridad de Certificación (CA) confiable.

Durante la firma, el certificado X.509 se incrusta dentro del PDF firmado, permitiendo que cualquier tercero valide su autenticidad, cadena de confianza y estado de revocación.

PKCS#11
Es un estándar que define una interfaz uniforme para interactuar con dispositivos criptográficos como smartcards, tokens USB o HSM.

Su principio de seguridad fundamental es que la clave privada nunca abandona el dispositivo, todo el proceso de firma se ejecuta internamente, reduciendo riesgos de filtración, mala manipulación o extracción de claves.

Proceso de firmado de un PDF con smartcard

El proceso para firmar un documento PDF utilizando un smartcard es el siguiente:

1. La aplicación inicia la sesión cargando el módulo PKCS#11 del token.
2. El usuario ingresa el PIN para desbloquear y habilitar el uso de la clave privada.
3. Se recupera el certificado X.509 y se prepara para ser incrustado en la estructura de la firma.
4. Se calcula el hash criptográfico del documento PDF y este valor se envía de forma segura al token.
5. El token utiliza internamente la clave privada para generar la firma digital del hash.
6. Finalmente, la aplicación integra la firma generada en el documento, resultando en un PDF firmado verificable por cualquier tercero.

Estándares de Firma Electrónica

Para la firma de documentos PDF, existen diversos estándares que definen cómo se incorporan y verifican las firmas digitales. Esta implementación se enfoca en la conformidad con PAdES, un estándar del ETSI (European Telecommunications Standards Institute, 2020) diseñado específicamente para documentos PDF.

PAdES define un marco robusto que permite la inclusión de firmas visibles e invisibles dentro del PDF. Una de sus ventajas más significativas es el soporte para la validez a largo plazo (Long-Term Validation, LTV). Esto se logra mediante la inclusión de elementos como marcas de tiempo confiables (timestamps) y la validación del estado de revocación de certificados (a través de CRLs u OCSP) directamente dentro del documento PDF.

4. Análisis y diseño del sistema

Cuando comenzó la PPS en la UNNOBA , se asignó al autor la tarea de resolver el problema relacionado con la firma digital de documentos PDF mediante smartcards. Tras un breve período de capacitación y de explicación acerca de cómo se integraban los sistemas existentes, comenzó con el relevamiento de requisitos.

Por consiguiente, durante las primeras semanas, se llevaron a cabo actividades de relevamiento, investigación tecnológica y diseño de la arquitectura, con el objetivo de definir una solución adecuada, multiplataforma y ajustada a las necesidades de la universidad.

Requisitos Funcionales

Los requisitos funcionales del "Firmador UNNOBA" delinean las capacidades que la aplicación debe ofrecer a sus usuarios para cumplir con su propósito principal de simplificar y asegurar la firma digital de documentos PDF. Se definieron con el objetivo de proporcionar una experiencia de usuario completa y eficiente:

- Gestión de Perfiles: La aplicación debe permitir a los usuarios configurar y gestionar perfiles de firma personalizados. (el token criptográfico, la imagen de firma visual que se incrustará en el PDF, cargo institucional y posiblemente más campos a futuro)
- Gestión y Previsualización de Documentos: Se requiere que la aplicación facilite la selección de documentos PDF desde el sistema de archivos del usuario. Una vez seleccionados, el sistema debe permitir la previsualización del documento página por página, así como la navegación fluida entre ellas, para que el usuario pueda verificar el contenido
- Firma Digital: El núcleo de la aplicación es el proceso de firma digital. Este debe ser un proceso guiado que incluye la autenticación del usuario mediante el PIN (Personal Identification Number) de su token, la selección del certificado digital deseado (si el token contiene múltiples certificados) y la capacidad de posicionar visualmente la firma en el documento PDF.
- Firma Masiva: Para optimizar la productividad en entornos con alto volumen de documentos, la aplicación debe soportar la firma de múltiples documentos simultáneamente. Este proceso debe incorporar técnicas de procesamiento paralelo para garantizar un rendimiento óptimo y eficiente. (Para los certificados principalmente)

Requisitos No Funcionales

Los requisitos no funcionales son cruciales para definir la calidad y las limitaciones del

sistema, influyendo directamente en las decisiones de diseño y la selección de tecnologías.

- Multiplataforma: La aplicación debe operar de manera consistente y fiable en los principales sistemas operativos de escritorio: Windows, Linux y macOS.
- Seguridad: La integridad y autenticidad de las firmas son primordiales. Se exige el uso de certificados digitales de entidades de confianza y librerías criptográficas robustas para asegurar la validez legal y la protección de los datos.
- Rendimiento: Especialmente en el caso de la firma masiva, la aplicación debe ser eficiente
- Experiencia del usuario (UX): La interfaz gráfica de usuario (GUI) será intuitiva y sencilla, guiando al usuario mediante instrucciones paso a paso y proporcionando retroalimentación visual efectiva.
- Mantenibilidad y Escalabilidad: La arquitectura del sistema debe ser modular y extensible, facilitando futuras actualizaciones y corrección de errores sin impacto negativo.
- Integración con Hardware Existente: La solución debe ser compatible con la infraestructura de hardware ya en uso, incluyendo los *tokens criptográficos* provistos a los firmantes.

Arquitectura propuesta

El stack tecnológico se seleccionó basándose en las tecnologías usadas en el área y en el cumplimiento de los requisitos técnicos del proyecto.

Lenguaje Base Java: Fue seleccionado estratégicamente debido a la coherencia institucional, ya que el software universitario se basa principalmente en este ecosistema.

Framework de GUI JavaFX: Para la Interfaz Gráfica de Usuario (GUI), se optó por JavaFX. Esta elección se justificó por su modernidad, su alto rendimiento de renderizado y su capacidad multiplataforma.

Principios de Diseño de Software y Arquitectura

Para garantizar la calidad, la escalabilidad y la modularidad del código, se aplican rigurosos principios de diseño y patrones de arquitectura.

Patrón Modelo-Vista-Controlador (MVC): Se implementó el patrón MVC para una clara separación de responsabilidades en capas. JavaFX se utiliza para la Vista (FXML) y provee las herramientas para actualizarla mediante los Controladores. Java se emplea para el Modelo y la Capa de Servicio. La Capa de Servicio segmenta responsabilidades específicas, como la

aplicación de la firma o la gestión de dimensiones, ubicación de firmas y manipulación de archivos PDF.

Principios SOLID: La arquitectura se diseñó aplicando los Principios SOLID para optimizar el diseño de clases y la estructura del código.

Principio de Responsabilidad Única (SRP): Este principio se cumple mediante la separación en capas (MVC + Servicio), garantizando que cada componente tenga una única razón para cambiar.

Principio Abierto/Cerrado (OCP): Se consideraron los estados claros de la aplicación, lo que permite que el software sea abierto a extensión (para nuevas funcionalidades) pero cerrado a modificación (los estados existentes se mantienen estables).

Principio de Sustitución de Liskov (LSP): Se respetó la jerarquía de herencia. Un claro ejemplo es la definición de subclases personalizadas para elementos de los componentes de JavaFX, lo que permite utilizarlas en lugar de sus tipos base adaptándolas mejor a casos de uso puntuales

La arquitectura se consolidó bajo el principio de separación de responsabilidades, quedando definidos los siguientes componentes:

- El Firmador principal, encargado de la firma de archivos locales.
- El Firmador de Certificados, que gestiona la descarga y carga de certificados vinculados a eventos institucionales.
- El sistema Certificados, responsable de la creación y envío automatizado de los documentos firmados.
- El módulo de autenticación, consumido por el Firmador de Certificados, encargado de la gestión de inicio de sesión y autorización.

Esta estructura modular asegura mantenibilidad, escalabilidad y una clara delimitación funcional entre los distintos sistemas involucrados.

Diagrama de flujo

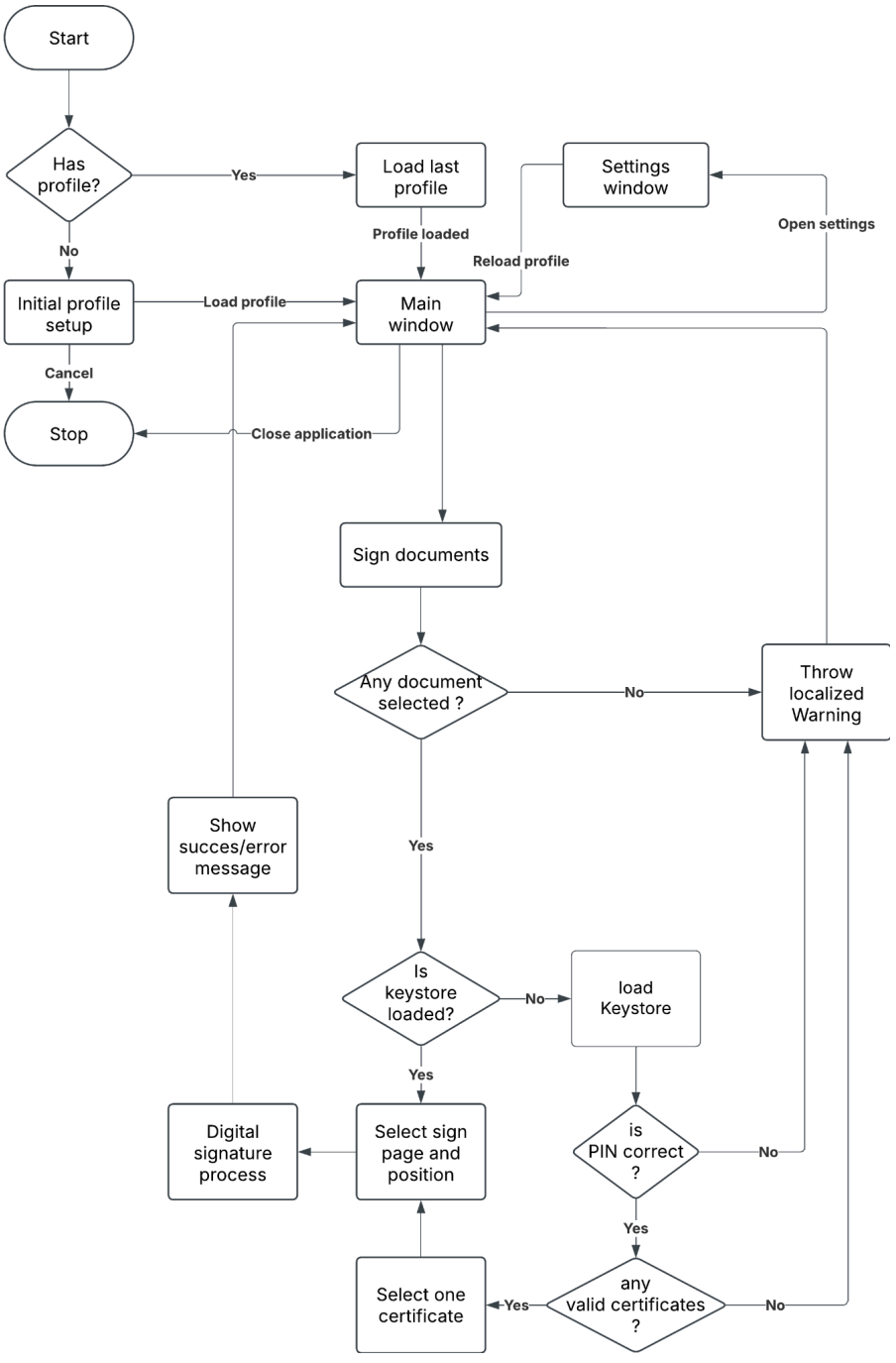


Figura 2 - Diagrama de flujo de la solución propuesta

5. Desarrollo del proyecto

Plan de Trabajo y Carga Horaria

En un estimado de 10 semanas

N°	ACTIVIDADES	TIEMPO DE DURACIÓN									
		SEMANAS									
		1	2	3	4	5	6	7	8	9	10
1	Planificación										
2	Desarrollo										
3	Optimización (pruebas cerradas)										
4	Primera entrega										
5	WS Certificados										
6	Login device Flow										
7	Integración con sistema de certificados										
8	Bug Fixes										
9	Mejoras por feedback (pruebas abiertas)										
10	Documentación										

Etapas de desarrollo

Desde el comienzo de la PPS, el enfoque fue el de crear desde cero una aplicación de escritorio para la firma digital de documentos PDF con smartcards. la idea de MVP (Producto Mínimo Viable) era una aplicación, que siguiendo el workflow actual, pudiese suplantar al firmador obsoleto

La primera etapa, fue la de relevamiento de requisitos, entender el problema y definir una estrategia. Esto incluyendo el Stack tecnológico, y cómo dividiremos el problema.

En una segunda etapa, se avanzó con el desarrollo de un prototipo inicial, que incluía la lógica de firma digital a través de librerías PKCS#11 y un flujo básico de interacción con los usuarios.

Como parte de las prácticas de desarrollo, se utilizó GitHub para el control de versiones,

garantizando trazabilidad, respaldo y un registro histórico de las decisiones técnicas tomadas a lo largo del proyecto

Una vez alcanzado el MVP, decidimos hacer algunos ajustes adicionales antes de liberarlo al público. Para esta etapa, se convocó a usuarios con Token, que firmaran regularmente.

Adicionalmente, se asignó una SmartCard al autor para realizar pruebas independientes.

En esta etapa de 'Testing Cerrado', se realizaron ajustes a los requerimientos funcionales en base al feedback recibido de los distintos actores involucrados.

A partir de este prototipo, se continuó con la implementación de las funcionalidades principales, incluyendo pruebas y validaciones en diferentes sistemas operativos (Windows, Linux y macOS), garantizando la robustez y compatibilidad del sistema.

Al cabo de un mes aproximadamente, se lanzó la versión 1.0.0, la primera versión lista para ser utilizada por los usuarios finales.

En este momento comenzó la transición de la mayoría de los usuarios.

Durante este periodo, se implementaron ajustes progresivos de acuerdo a los requerimientos de los usuarios. Por ejemplo, agregando la capacidad de previsualizar los documentos, dar información de las páginas, optimizar la firma masiva, entre otras.

Integración con sistemas existentes

Posteriormente, se inició la segunda fase del plan: el desarrollo del firmador de certificados.

Para esta nueva aplicación se realizó un fork del proyecto inicial, reutilizando gran parte de lo implementado.

Para esto es conveniente hablar sobre el sistema de certificados, y cómo esta herramienta se relaciona con el mismo.

El sistema de certificados, permite la creación de eventos, a los cuales tras su conclusión, emite certificados firmados digitalmente a sus asistentes.

Esto es utilizado para eventos como el TEC, WICC, Talleres, Cursos, Charlas, entre otros.

Un ejemplo de su uso (un caso especial), es para la emisión de certificados analíticos y de alumno regular.

Las responsabilidades de crear el documento, asignarlo a un evento/cursante, y luego enviarlo a su casilla de correo es del mismo sistema de Certificados, una vez firmado.

Será responsabilidad del firmador de Certificados, firmar los certificados confirmados a los eventos correspondientes, dejarlos en la carpeta donde funciona el Cron de envío de Certificados

La primera dificultad que enfrentamos fue la necesidad de consumir el sistema de certificados desde la aplicación de escritorio. Por lo que fue necesario :

- Ser capaces de consumir el login unnoba para autenticación.
- Consumo de documentos a través de un web service del servidor de certificados.
- Consumir LDAP para validar Servicios (Un evento se representa como un servicio)

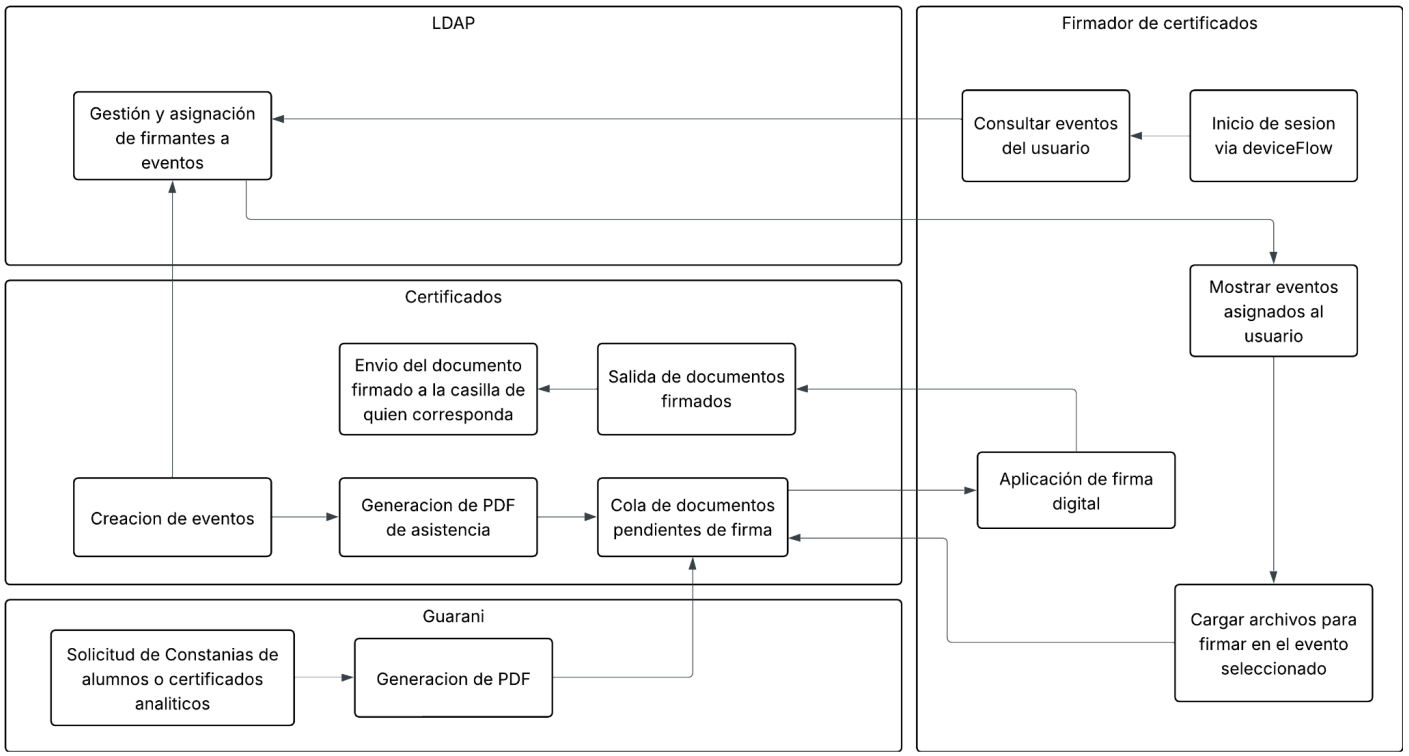


Figura 3 - Flujo propuesto entre Certificados Guaraní y la nueva aplicación

Consumir login

La principal dificultad de integración se presentó en la autenticación de la aplicación de escritorio con el sistema de *login* institucional, diseñado originalmente para flujos basados

en web. Era imperativo garantizar la seguridad de las credenciales y la compatibilidad con la infraestructura existente, gestionada bajo protocolos de Identity and Access Management (IAM) de la universidad.

Inicialmente, se evaluaron dos alternativas de diseño:

1. **Integración mediante Componente Web:** Utilizar el componente WebView de JavaFX junto con el CookieManager para incrustar la página de *login* institucional y capturar el *token* de sesión.
2. **Implementación de un Flujo Específico para Dispositivos:** Desarrollar un mecanismo de autenticación diseñado para aplicaciones cliente que carecen de la capacidad de alojar un navegador completo de forma segura.

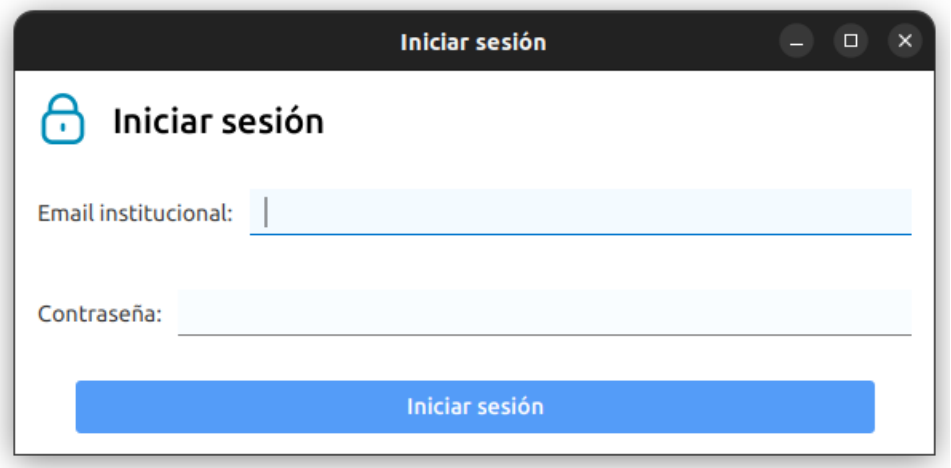


Figura 4 - Ventana de login del firmador de certificados

Se optó por la segunda opción, implementando un **Login** vía servicios web.

Este protocolo permite la autenticación segura en la aplicación de escritorio. Esta solución no sólo resolvió el desafío del "Firmador" sino que también se estandarizó para ser reutilizada por futuras aplicaciones de escritorio desarrolladas por la ProTIC.

Consumir sistema de certificados

Una vez establecida la sesión a través de servicios web, la aplicación procede a interactuar con el Sistema Institucional de Certificados para gestionar los documentos a firmar. Este

proceso se divide en tres fases principales: autorización, descarga de archivos y carga de archivos firmados.

Autorización y Listado de Eventos

La aplicación de escritorio inicia el flujo consultando un web service preexistente de LDAP, este mismo tiene como objetivo validar cuales Eventos está autorizado a firmar. Dicho web service devuelve el listado de Eventos , que son los que usaremos en este flujo.

Gestión de Archivos (Descarga y Carga)

La aplicación implementa endpoints específicos para la transferencia de archivos, desacoplando la funcionalidad de firma (que reside en el Firmador) de la gestión documental (que reside en el Sistema de Certificados). Los endpoints diseñados para este fin fueron:

Obtención de nombres de archivos: Endpoint que recibe el identificador del evento y devuelve una lista con todos los nombres de archivos en ese evento.

Obtención de archivos: Endpoint que recibe el identificador del evento y el nombre del archivo para transmitir el archivo PDF binario no firmado.

Carga de archivos firmados: Endpoint que recibe el documento firmado para su almacenamiento.

Nota: El resto de las responsabilidades funcionales del documento (como el envío automático de notificaciones o la trazabilidad del proceso) se mantienen en el Sistema de Certificados, permitiendo que el "Firmador" funcione únicamente como una capa de transmisión segura y proceso criptográfico.

Optimizaciones y ajustes específicos

Tras alcanzar un MVP funcional, se inició una etapa de pruebas con usuarios finales, específicamente usuarios de posgrado, para validar la usabilidad en flujos de trabajo reales.

Este proceso de feedback identificó un caso crucial: los certificados de alumnos.

Fue necesario implementar ajustes precisos en la aplicación para asegurar que la firma digital respetara el formato institucional preexistente para estos documentos.

Estos ajustes garantizan la coherencia visual y la validez documental de los certificados emitidos.

Diagrama de Flujo (Firmador de certificados)

Diagrama simplificado, introduciendo los microservicios de Certificados y Login.

La idea es que la aplicación tenga dos Managers, uno para la autenticación y autorización, y otro para el manejo de archivos / eventos de certificados.

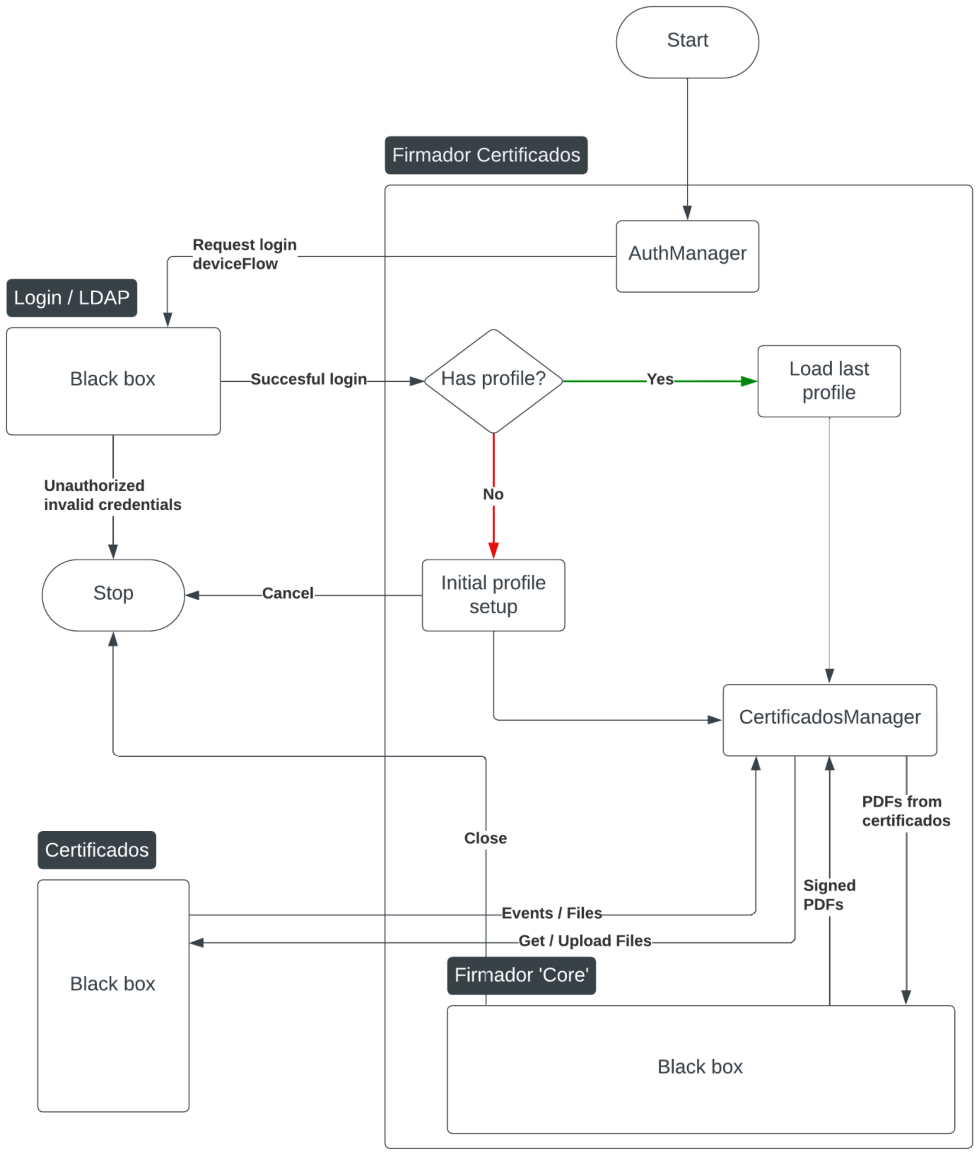


Figura 5 - Diagrama de flujo del firmador de certificados

Mantenimiento y actualización

Con el paso del tiempo, la aplicación fue ampliando sus funcionalidades para adaptarse a las necesidades reales de los usuarios. Entre las mejoras más relevantes se incorporó la gestión de múltiples perfiles de firma, lo que permite utilizar varios dispositivos criptográficos en una misma computadora o asociar diferentes identidades institucionales a una única firma digital. Esta característica resulta especialmente útil para personal que firma documentos bajo distintos cargos, como la Prosecretaría de TICs, direcciones de institutos o funciones docentes.

Asimismo, se perfeccionó el flujo de trabajo basado en OwnCloud, estructurado en tres carpetas principales: documentos por firmar, firmados y originales. Al completar la firma de un documento, se guarda una copia en la carpeta de originales y otra en la de firmados, manteniendo la trazabilidad de todo el proceso. Además, se incorporó la posibilidad de realizar firmas fuera de este flujo cuando el usuario así lo requiera, incrementando la flexibilidad del sistema.

Se añadieron también mejoras en rendimiento, seguridad y experiencia de usuario, incluyendo la posibilidad de colocar la firma en cualquier posición dentro del documento mediante una interfaz visual dinámica.

Publicación

Una vez completados los MVP de ambos firmadores, se publicaron las versiones oficiales en los sitios institucionales:

- https://firmador.unnoba.edu.ar/
- https://certificados.unnoba.edu.ar/firmador/

Tras un período de transición, las versiones web anteriores fueron discontinuadas para unificar los flujos de firma bajo la nueva plataforma:

- https://firmador.unnoba.edu.ar/masivoOld/
- https://certificados.unnoba.edu.ar/firmador/firmadorOld/

Proceso de adaptación

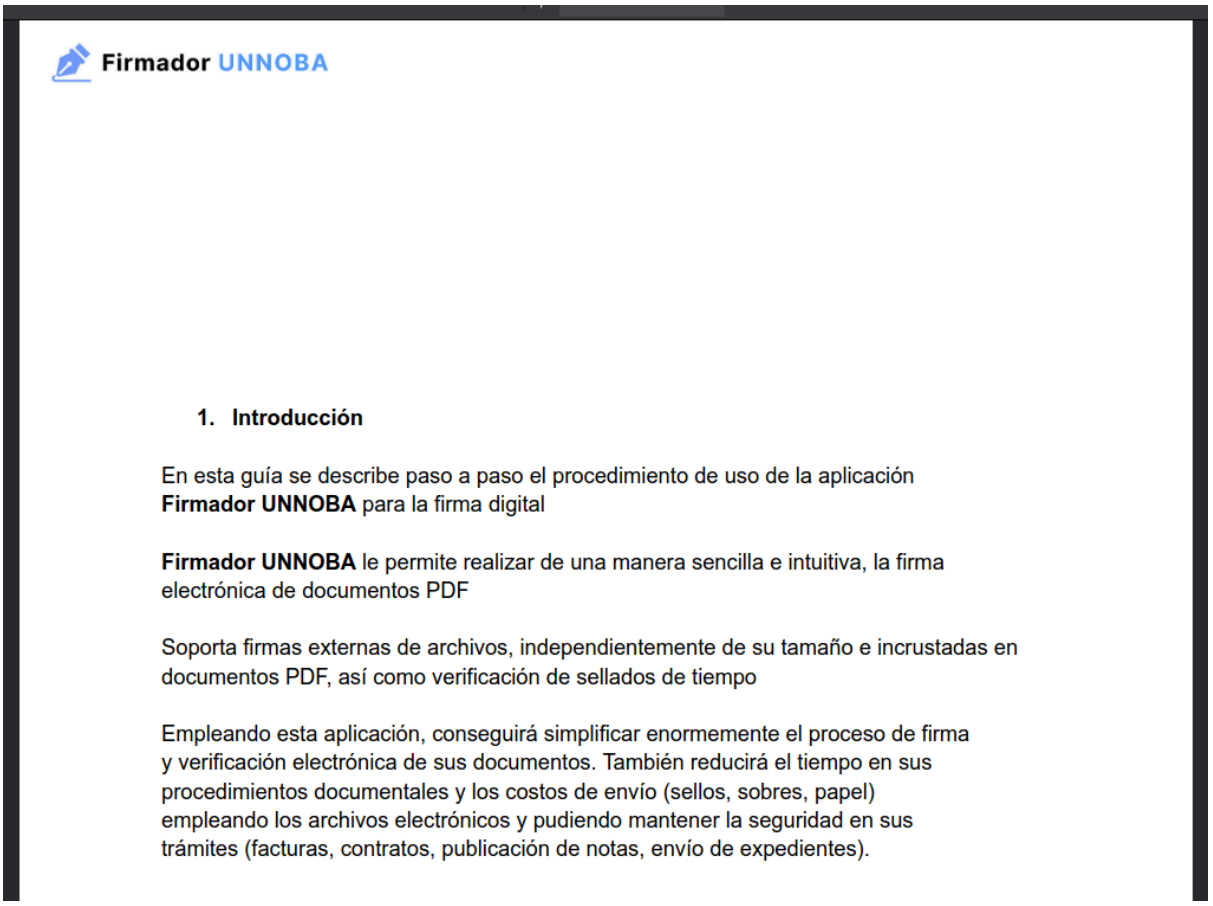
Como es lógico, cuando se genera un cambio, parte del personal puede tener dificultades al momento de utilizar la nueva herramienta. Es por esto, que desde la ProTIC realizamos procesos de capacitación y generamos documentación (manuales) para los usuarios finales. (Adicionalmente al apoyo continuo del sector de Soporte)

Dichos manuales de uso e instalación con instrucciones claras y actualizadas, se encuentran disponibles públicamente en los mismos enlaces donde funcionaban los antiguos firmadores

Figura 6 - Manuales / Guia de instalación publicados

El objetivo de estos documentos es facilitar una migración sencilla y rápida desde el sistema anterior, requiriendo únicamente la configuración previa de OwnCloud y los controladores del token criptográfico.

Describen gráficamente las funcionalidades básicas que todos los usuarios requerirán guía de Instalación, Configuración de perfiles, como Firmar documentos e información adicional. Existe una versión para Windows y otra para Linux/Mac


Firmador UNNOBA

1. Introducción

En esta guía se describe paso a paso el procedimiento de uso de la aplicación **Firmador UNNOBA** para la firma digital

Firmador UNNOBA le permite realizar de una manera sencilla e intuitiva, la firma electrónica de documentos PDF

Soporta firmas externas de archivos, independientemente de su tamaño e incrustadas en documentos PDF, así como verificación de sellados de tiempo

Empleando esta aplicación, conseguirá simplificar enormemente el proceso de firma y verificación electrónica de sus documentos. También reducirá el tiempo en sus procedimientos documentales y los costos de envío (sellos, sobres, papel) empleando los archivos electrónicos y pudiendo mantener la seguridad en sus trámites (facturas, contratos, publicación de notas, envío de expedientes).

Figura 7 - Introducción del manual de usuario

Además, la aplicación incorpora un sistema automático de verificación de versiones, que compara la instalación local con la última release disponible y notifica al usuario si se detecta una versión desactualizada.

Finalmente, el equipo de soporte técnico de la universidad asistió al personal durante el proceso de instalación, actualización y capacitación, garantizando una implementación ordenada y eficiente en toda la institución.

Flujo del programa

A continuación, vemos la ventana principal, tras seleccionar un archivo y clickear ‘Firmar’. Una vez confirmada la selección, se requiere el PIN del token, y seleccionar el certificado que utilizaremos dentro del mismo (Un token puede tener varios certificados).

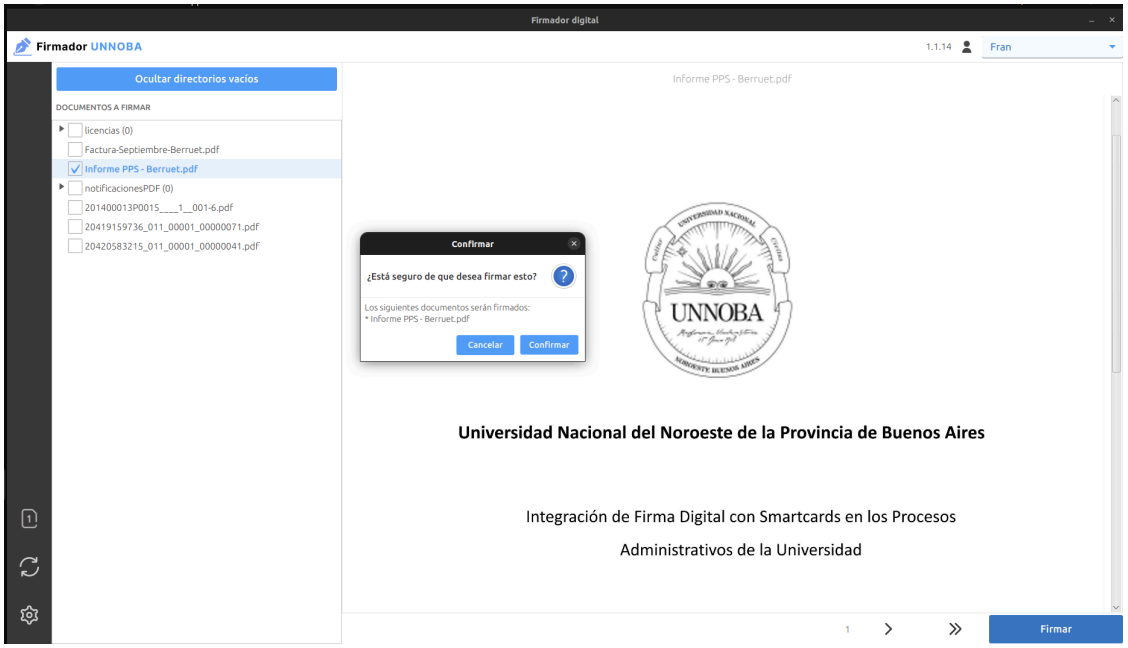


Figura 8 - Interfaz de usuario del Firmador

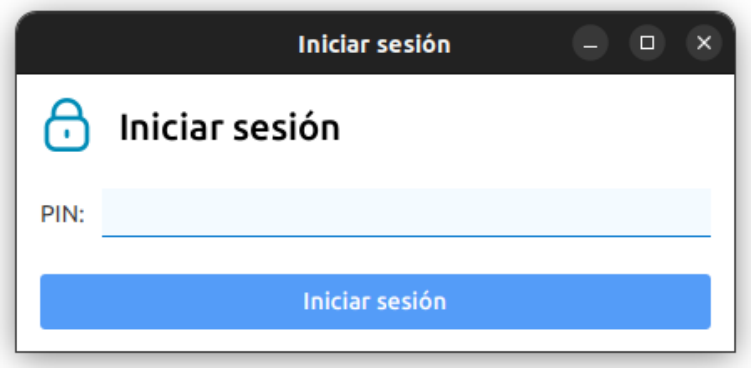


Figura 9 - Interfaz para cargar el PIN del token

Tras haber cargado el certificado, se ofrecerá la opción de seleccionar una página y posición para la firma.

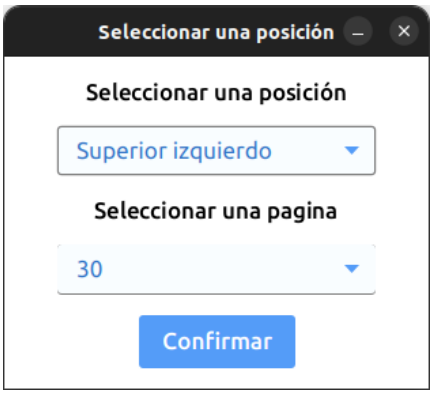


Figura 10 - Interfaz para selección de posición y página de la firma

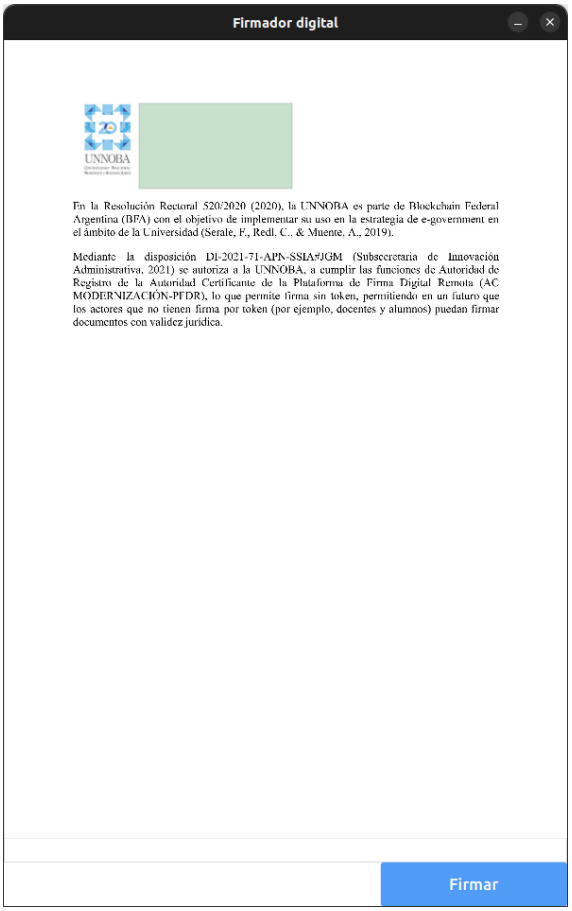


Figura 11 - Selección de posición libre

El documento seleccionado será copiado a la carpeta de ‘Documentos Originales’ y el documento firmado se guardará en ‘‘Documentos Firmados".

Si OwnCloud está configurado sobre dichas carpetas, se sincronizan con el servidor y dichos archivos quedan a disposición del resto del flujo.

Otras funciones a destacar son los perfiles, que permiten tener configurados distintas imágenes, rutas, cargos organizacionales.

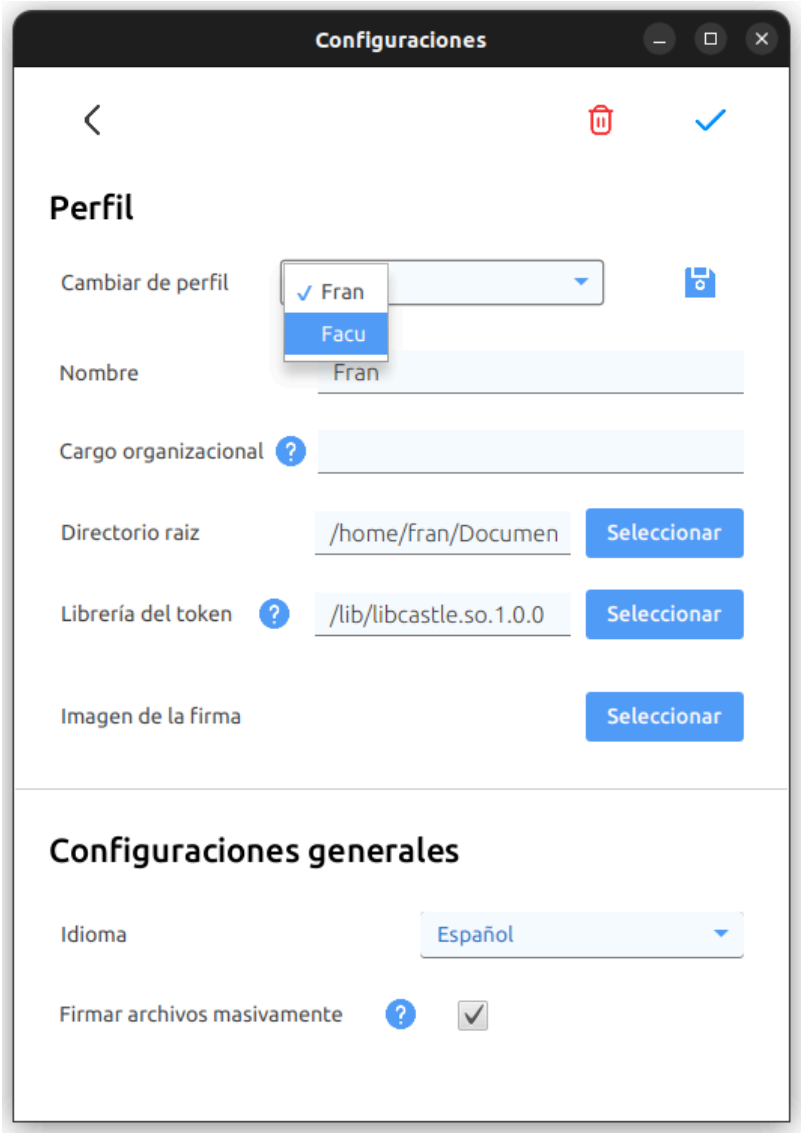


Figura 12 - Menú de configuraciones

En cuanto al Firmador de certificados, tanto su interfaz como su flujo de trabajo es similar, la única diferencia notable es el selector de eventos.

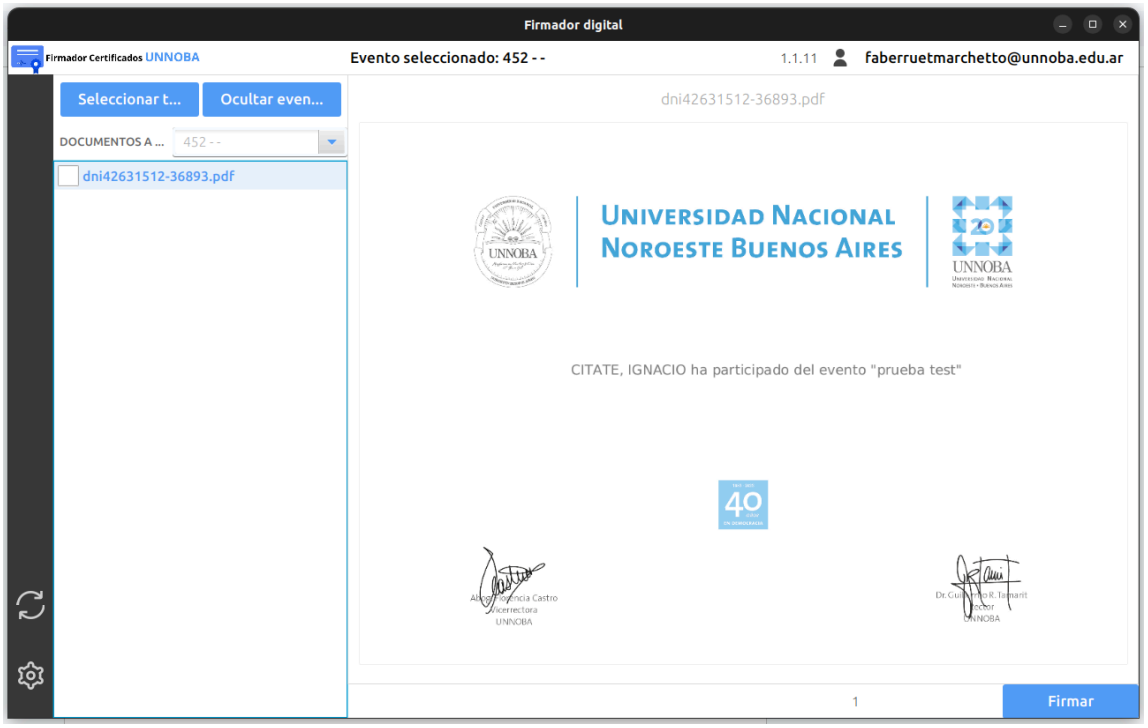


Figura 13 - Interfaz firmador de certificados

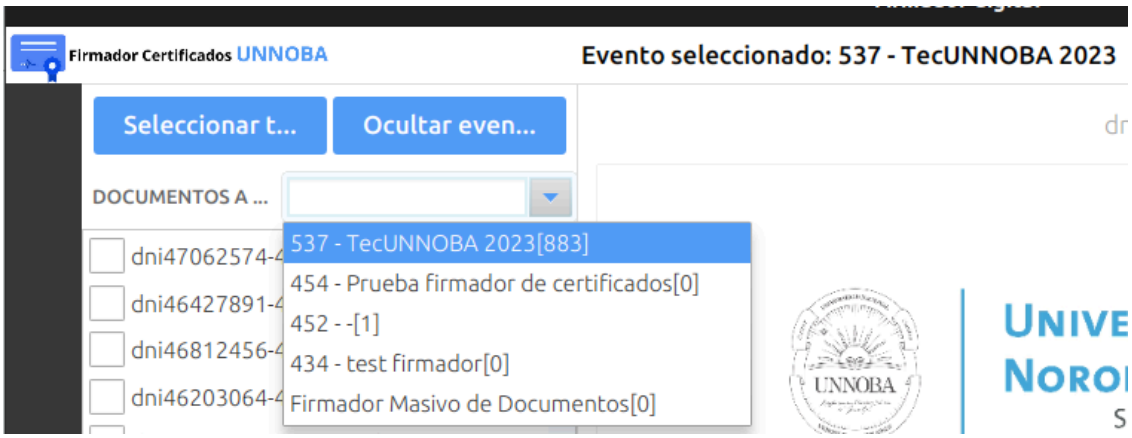


Figura 14 - Selector de eventos firmador de certificados

6. Próximos pasos

A lo largo de esta Práctica Profesional Supervisada (PPS) se desarrollaron de forma integral las etapas de análisis, diseño, implementación y mantenimiento del Firmador.

Como parte de la proyección futura del proyecto, se delinean las siguientes líneas de trabajo orientadas a su evolución y sostenibilidad:

Publicación como software de código abierto.

Desde la Prosecretaría de Tecnologías de la Información y las Comunicaciones (ProTIC) se propone liberar el código fuente del sistema bajo una licencia abierta. Esta acción busca fomentar su reutilización, auditoría colaborativa y mejora continua por parte de la comunidad académica y tecnológica.

Fortalecimiento del sistema de autenticación (Firmador de Certificados).

El flujo actual de autenticación basado en device flow no incorpora aún un mecanismo de autenticación multifactor, como contraseñas de un solo uso (One-Time Passwords, OTP). Su uso representaría un avance relevante en términos de seguridad y trazabilidad dentro del ecosistema de aplicaciones institucionales.

Investigación sobre Firma Digital Remota.

Se propone analizar la viabilidad técnica, normativa y de infraestructura para incorporar Firma Digital Remota, permitiendo firmar documentos válidos legalmente sin requerir tokens físicos. Esta funcionalidad ampliará la accesibilidad, especialmente para entornos de trabajo híbridos o distribuidos, y se alinea con las tendencias actuales en transformación digital segura.

Estudiar la Incorporar telemetría.

Se propone estudiar la posible utilidad de incorporar medición, recopilación y transmisión automática de datos al sistema de logs, para poder tener una trazabilidad de quienes y de qué manera usan la herramienta.

Centralizar las futuras aplicaciones de escritorio en una tienda

Ante la posibilidad de seguir desarrollando aplicaciones de escritorio para satisfacer necesidades puntuales, se propone analizar la viabilidad evaluar la creación de una tienda o repositorio centralizado para gestionar las futuras aplicaciones de escritorio, lo que facilita utilidades como las actualizaciones automáticas.

7. Conclusiones

Como se ha mostrado a lo largo de este informe, hemos logrado explicar cómo se afrontaron y finalmente alcanzaron los objetivos planteados para esta PPS.

La nueva herramienta no sólo reemplazó un sistema obsoleto, sino que consolidó una arquitectura sostenible basada en estándares internacionales y en prácticas de desarrollo orientadas a la mantenibilidad, la eficiencia y la seguridad. Esto permitió devolver a la institución el control total sobre un proceso crítico: la firma digital de documentos.

En el plano organizacional, el proyecto fortaleció la madurez tecnológica de la universidad, optimizando tiempos de gestión, reduciendo riesgos operativos y mejorando la trazabilidad documental. También sentó un precedente para futuras integraciones con otros sistemas institucionales, como los módulos de autenticación, certificados académicos y expedientes electrónicos.

Desde la perspectiva personal y formativa, la experiencia fue ampliamente enriquecedora. Permitió recorrer de manera completa el ciclo de vida de un sistema real, desde el análisis y el diseño hasta la implementación, el despliegue y el mantenimiento.

El impacto cuantitativo demuestra su adopción institucional: desde su puesta en funcionamiento, el Firmador UNNOBA supera los 234.891 documentos firmados por 92 usuarios, mientras que el Firmador de Certificados registra 22.558 documentos firmados por 27 usuarios. Estas cifras consolidan su rol como herramienta central en el ecosistema digital universitario.

En síntesis, el Firmador UNNOBA constituye un aporte tangible y perdurable a la infraestructura tecnológica de la Universidad, evidenciando el paso de la teoría a la práctica y reafirmando el rol del ingeniero en informática como agente activo en la innovación, la mejora continua y la modernización de las instituciones públicas.

8. Bibliografía

European Telecommunications Standards Institute. (2020). *ETSI EN 319 142-1 - Electronic Signatures and Infrastructures (ESI); PAdES Digital Signatures; Part 1: Building Blocks and PAdES Baseline Signatures* (V1.2.1). https://www.etsi.org/deliver/etsi_en/319100_319199/31914201/01.02.01_60/en_319142001v010201p.pdf

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., & Polk, W. (2008). *RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. Internet Engineering Task Force (IETF). https://www.rfc-editor.org/info/rfc5280

UNNOBA. (2012). Resolución Nº 571/2012 del Consejo Superior. https://digesto.unnoba.edu.ar/documento.frame.php?cod=939

UNNOBA. (2013). Resolución Nº 657/2013 del Consejo Superior. https://digesto.unnoba.edu.ar/documento.frame.php?cod=1032

UNNOBA. (2019). Resolución Nº 1750/2019 del Consejo Superior. https://digesto.unnoba.edu.ar/documento.frame.php?cod=3783

OASIS. (2020). *PKCS #11 v3.0 - Cryptographic Token Interface Standard*. https://docs.oasis-open.org/pkcs11/pkcs11-curr/v3.0/pkcs11-curr-v3.0.html

OpenJFX. (2025). *JavaFX SDK - Open source, next generation client application platform for desktop*. https://openjfx.io/javadoc/25/

Argentina. (2001). *Ley 25.506 - Firma Digital*. *Boletín Oficial de la República Argentina*. https://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm

Oracle. (2014). *Applet - Small program intended to be embedded inside another application*. https://docs.oracle.com/javase/8/docs/api/java/applet/Applet.html

International Organization for Standardization (ISO). (2008). *PDF 32000-1:2008, Document Management—Portable Document Format*. *Adobe Systems Incorporated*. https://opensource.adobe.com/dc-acrobat-sdk-docs/pdfstandards/PDF32000_2008.pdf

MDN Web Docs. (2023). *MVC.* Mozilla. https://developer.mozilla.org/es/docs/Glossary/MVC

Rahman, B. (2020). *SOLID Principles* https://www.baeldung.com/solid-principles

GitHub. (2025). *GitHub Documentation.* https://docs.github.com/

9. Acrónimos

Acrónimo	**Descripción**
PAdES	Estándar europeo para firmas electrónicas en documentos PDF
PKCS#11	Estándar que define una API para dispositivos criptográficos
X.509	Estándar para infraestructura de claves públicas y certificados digitales
LTV	Validación a largo plazo de firmas digitales
MVP	Producto Mínimo Viable
UX	Experiencia de Usuario
GUI	Interfaz Gráfica de Usuario
CA	Autoridad de Certificación
CRL	Lista de Revocación de Certificados
OCSP	Protocolo de Estado de Certificado en Línea
LDAP	Protocolo de Acceso a Directorios Liviano
HSM	Módulo de Seguridad de Hardware
ETSI	Instituto Europeo de Normas de Telecomunicaciones
UNNOBA	Institución educativa donde se desarrolló el proyecto
PDF	Formato de Documento Portátil
PIN	Número de Identificación Personal

10. Agradecimientos

Deseo expresar mi más sincero agradecimiento a todas las personas que hicieron posible la realización de este proyecto y enriquecieron mi experiencia durante la Práctica Profesional Supervisada.

En primer lugar, agradezco a mi familia por el apoyo incondicional en el trayecto universitario y en cada aspecto de mi vida.

A mis amigos que siempre se encuentran presentes, y fueron un gran apoyo en todo este trayecto.

A mis tutores Carlos Di Cicco y Hugo Ramon, por su tutoría y confianza al brindarme un desafío tan significativo para la universidad.

Un reconocimiento especial a mis compañeros de la ProTIC, cuya colaboración técnica y apoyo fueron fundamentales a lo largo de todo el desarrollo del proyecto.

Finalmente, quiero agradecer a la Universidad Nacional del Noroeste de la Provincia de Buenos Aires por brindarme esta oportunidad de crecimiento, que espero haber aprovechado al máximo.