COLEGIO DE ABOGADOS DEL DEPARTAMENTO JUDICIAL DE SAN ISIDRO

Firma digital remota en el sistema de presentaciones y notificaciones electrónicas de la Suprema Corte de Justicia de la Provincia de Buenos Aires

Informe técnico-jurídico y propuesta institucional

Resumen ejecutivo

El sistema de presentaciones y notificaciones electrónicas de la Suprema Corte de Justicia de la Provincia de Buenos Aires (en adelante, "SCBA") prevé, para suscribir actos procesales, la utilización de certificados de firma digital emitidos por una única Autoridad Certificante (AC-ONTI), operados mediante un dispositivo criptográfico físico (token). La dependencia de ese dispositivo constituye un reclamo concreto y sostenido de la matrícula, que este Colegio ha asumido como compromiso institucional: efectuar los pedidos pertinentes para posibilitar que los matriculados firmen sus presentaciones electrónicas sin depender de un token físico, sin reducir el estándar de seguridad ni el valor jurídico de la firma. El presente informe se estructura en torno a tres proposiciones.

Primera. La cuestión es de orden reglamentario y operativo, no de validez jurídica. La Ley 25.506 no exige que la clave privada se aloje en un dispositivo físico. La firma digital remota, modalidad en la que la clave se custodia en un módulo de seguridad gestionado por la Autoridad Certificante, constituye firma digital con idéntico valor jurídico, y se encuentra reconocida y operativa en el Estado argentino desde hace casi una década.

Segunda. La oportunidad institucional resulta particularmente propicia. Mediante el Acuerdo 4150 y la Resolución SC 1682/24, la Suprema Corte dispuso la migración progresiva de la firma electrónica a la firma digital de AC-ONTI para los operadores externos, con apagado de la infraestructura de firma electrónica previsto para el 1° de agosto de 2026. En ese contexto de universalización de la firma digital, resulta conveniente que se admita también su modalidad remota, evitando que los matriculados deban asumir el costo y las limitaciones operativas del dispositivo físico cuando existe una alternativa de igual valor jurídico.

Tercera. Existe un antecedente institucional relevante de factibilidad. El Poder Judicial de la Ciudad Autónoma de Buenos Aires, en su sistema EJE (Expediente Judicial Electrónico), admite

firma dual: token o firma digital remota desde computadora, tableta o dispositivo móvil. Dicho antecedente no tiene incidencia jurídica en relación a la SCBA ni su arquitectura resulta automáticamente trasladable, pero demuestra que un poder judicial argentino puede integrar la firma remota en un expediente judicial electrónico sin degradar el estándar jurídico de firma digital. A ello se suman la plataforma nacional de firma digital remota, operativa desde 2018, y el propio Poder Ejecutivo bonaerense, que la utiliza con sus agentes desde 2019.

La solicitud que se propone elevar se estructura de modo escalonado. En primer término, se requerirá que la SCBA aclare formalmente el texto vigente del reglamento aprobado por el Acuerdo 4013 (texto ordenado por el Acuerdo 4039) y el alcance operativo de los certificados admitidos. En segundo término, para el caso de que exista una exclusividad reglamentaria u operativa no fundada, se solicitará la adopción de una fórmula tecnológicamente neutra, que admita a todo certificador licenciado o reconocido conforme la Ley 25.506, incluida la firma digital remota, en convivencia con el régimen de token. Se formularán, además, cuatro pedidos autónomos: un dictamen de interoperabilidad, una prueba piloto en el ámbito del Departamento Judicial de San Isidro, una medida de resiliencia operativa frente a la concentración en una única autoridad certificante y un protocolo de contingencia procesal. El fundamento es la tutela judicial continua y efectiva consagrada en el artículo 15 de la Constitución de la Provincia, en cuyo marco la infraestructura técnica del proceso digital opera como condición material del derecho de defensa.

Parte I. Encuadre constitucional y convencional

1.1. El proceso digital como condición de ejercicio de derechos

La digitalización del proceso judicial bonaerense ha alcanzado una intensidad tal que la infraestructura técnica constituye el medio mismo a través del cual se ejercen derechos procesales. Un escrito no llega al expediente si no se suscribe y se presenta a través de la infraestructura prevista. Cuando la infraestructura presenta fallas, o cuando su operación depende de un dispositivo que en un momento determinado no funciona, la consecuencia no consiste en una incomodidad, sino en la imposibilidad de realizar un acto procesal, con eventual pérdida del plazo y afectación directa del derecho de defensa del justiciable.

De allí la premisa que ordena el presente informe: la accesibilidad, la disponibilidad y la seguridad de la infraestructura del proceso digital constituyen condiciones operativas de derechos constitucionales, y no meras cuestiones de implementación técnica libradas a la discrecionalidad administrativa.

1.2. Tutela judicial continua y efectiva, defensa en juicio, acceso irrestricto

El artículo 15 de la Constitución de la Provincia de Buenos Aires dispone:

> *"La Provincia asegura la tutela judicial continua y efectiva, el acceso irrestricto a la justicia, la gratuidad de los trámites y la asistencia letrada a quienes carezcan de recursos suficientes y la inviolabilidad de la defensa de la persona y de los derechos en todo procedimiento administrativo o judicial. Las causas deberán decidirse en tiempo razonable. El retardo en dictar sentencia y las dilaciones indebidas cuando sean reiteradas, constituyen falta grave."*

Cuatro garantías de esa norma se proyectan directamente sobre la cuestión. La tutela judicial continua y efectiva impone que la tecnología facilite, y no restrinja, el acceso real al proceso. El acceso irrestricto a la justicia se ve comprometido cuando la exigencia de un dispositivo físico, con su costo, su trámite presencial y sus limitaciones de compatibilidad, opera como una restricción de hecho que afecta de modo desigual a los estudios pequeños, a los profesionales del interior del Departamento Judicial, a las personas con discapacidad y a quienes presentan menor alfabetización digital. La inviolabilidad de la defensa resulta tangible cuando una imposibilidad técnica de firmar, no imputable a la conducta procesal del letrado, puede traducirse en un vencimiento. La decisión en tiempo razonable se ve afectada por las fricciones técnicas, que multiplican incidencias, reposiciones y planteos accesorios.

Estas garantías se integran con el artículo 18 de la Constitución Nacional (defensa en juicio) y con los artículos 8 y 25 de la Convención Americana sobre Derechos Humanos (garantías judiciales y protección judicial efectiva), de jerarquía constitucional (artículo 75 inciso 22 CN). En materia de acceso a la justicia de personas en condición de vulnerabilidad, resultan ilustrativas las Reglas de

Brasilia, a las que la Corte Suprema de Justicia de la Nación adhirió por Acordada 5/2009, que disponen la remoción de los obstáculos que dificulten el acceso efectivo al sistema de justicia.

1.3. La cuestión tecnológica como cuestión procesal

En un proceso digital, una exigencia tecnológica desproporcionada puede traducirse en una restricción procesal. No se postula un derecho a la última tecnología disponible. Se sostiene que, cuando el Estado dispone un único medio técnico obligatorio para ejercer un derecho, ese medio debe satisfacer estándares de accesibilidad, disponibilidad, continuidad y proporcionalidad. La existencia de una alternativa de igual valor jurídico y mayor accesibilidad torna razonable su admisión, conforme el principio de razonabilidad consagrado en el artículo 28 de la Constitución Nacional.

1.4. Neutralidad tecnológica e igualdad

La neutralidad tecnológica es un principio rector del derecho informático, en el que el régimen argentino de firma digital se encuentra enrolado. Del diseño de la Ley 25.506 y de su reglamentación surge un criterio de neutralidad tecnológica: el régimen exige estándares de seguridad, verificabilidad, control, certificación y revocación, pero no impone como única modalidad el soporte físico ni una autoridad certificante determinada. La regulación debe fijar fines y estándares de seguridad, sin atarse a una marca, a un proveedor o a un dispositivo. La admisión de múltiples certificadores licenciados y de múltiples modalidades de custodia (token y remota), exigiendo a todos el mismo estándar jurídico de firma digital, constituye la solución técnicamente neutra y armónica con el principio de igualdad ante la ley.

Parte II. Marco normativo de la firma digital

2.1. Firma digital y firma electrónica. La distinción legal

La Ley 25.506 distingue dos institutos. La firma digital (artículo 2) es el resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, bajo su absoluto control, verificable por terceros, de modo tal que permita detectar cualquier alteración posterior. Emitida por un certificador licenciado dentro de la Infraestructura de Firma Digital, goza de presunción de autoría e integridad (artículos 7 y 8), y satisface el requisito de firma con equivalencia a la manuscrita. La firma electrónica (artículo 5) constituye el género residual: el conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carece de alguno de los requisitos legales de la firma digital; no goza de las presunciones legales y, en caso de desconocimiento, traslada la carga de la prueba a quien la invoca.

El artículo 288 del Código Civil y Comercial de la Nación (Ley 26.994) consolidó esta equivalencia al disponer que, en los instrumentos generados por medios electrónicos, “el requisito de la firma de una persona queda satisfecho si se utiliza una firma digital, que asegure indubitablemente la autoría e integridad del instrumento”.

La consecuencia normativa es decisiva. La presente propuesta no plantea descender del estándar de firma digital al de firma electrónica. Propone admitir una modalidad de custodia de la firma digital distinta del token físico.

2.2. La firma digital remota es firma digital

La firma digital remota es aquella en la que la clave privada del firmante se genera y custodia de manera centralizada en un módulo de seguridad de hardware gestionado por el certificador, y el firmante la opera de forma autenticada y autorizada desde cualquier dispositivo, sin necesidad de un soporte físico propio.

Corresponde una precisión sobre el requisito de que la información de creación de firma se encuentre bajo el absoluto control del firmante (artículo 2, Ley 25.506), que constituye la objeción jurídica previsible más sensible. En la modalidad remota, ese control no se ejerce mediante la posesión física de un dispositivo, sino mediante el control funcional de cada acto de firma: autenticación robusta del firmante, autorización individual de cada operación, clave privada generada y custodiada en un módulo de seguridad del que no resulta exportable, trazabilidad completa, posibilidad de revocación inmediata y auditoría. La custodia centralizada no transfiere a un tercero el poder de firmar: el modelo exige que ninguna firma se ejecute sin la intervención actual y verificada del titular, condición auditable conforme los controles del Anexo.

El reconocimiento normativo de la modalidad es expreso y escalonado. El Decreto 892/2017 creó la Plataforma de Firma Digital Remota (PFDR) en el ámbito del entonces Ministerio de Modernización, como infraestructura estatal para la firma remota. El Decreto 182/2019 constituye la reglamentación general vigente de la Ley 25.506 (derogó el Decreto 2628/2002 y normas concordantes) y resulta el marco reglamentario de fondo de toda la firma digital, incluida la remota. La Resolución 86/2020 de la Secretaría de Innovación Pública (Resolución SIP 86/2020) autorizó a los certificadores licenciados a prestar el servicio de firma digital con custodia centralizada de claves criptográficas, esto es, la generación de las claves y la ejecución del proceso de firma mediante un sistema técnicamente confiable conforme la Ley 25.506. La tendencia reglamentaria más reciente acompaña esta orientación: el Decreto 743/2024 modificó la reglamentación y admitió mecanismos de identificación y validación de identidad a distancia para la emisión, renovación y revocación de certificados, sin exigencia de presencia física del solicitante.

En síntesis, el ordenamiento nacional prevé y regula la firma digital remota, le reconoce idéntico valor jurídico que a la firma digital con token y exige para la custodia centralizada de claves un sistema técnicamente confiable y seguro (Resolución SIP 86/2020). Los estándares internacionales de módulos criptográficos (FIPS 140-3, sucesor del FIPS 140-2, y Common Criteria) constituyen la referencia técnica de la industria para acreditar esa confiabilidad; su detalle se desarrolla en el Anexo.

2.3. La adhesión de la Provincia de Buenos Aires

La Provincia adhirió a la Ley 25.506 mediante la Ley 13.666 (Capítulos I a IV, V artículo 26, VII y IX, y Anexo), reglamentada por el Decreto 305/2012, cuya autoridad de aplicación es la Subsecretaría para la Modernización del Estado (texto según Decreto 341/16). El propio decreto asigna a la Dirección Provincial de Sistemas de Información y Tecnologías (DPSIT) el rol de Autoridad de Registro para la administración pública provincial. La adhesión no introdujo restricción alguna respecto del medio técnico de custodia de la clave privada. En el plano legislativo provincial, en consecuencia, nada obsta a la admisión de la firma digital remota.

2.4. Equivalencia jurídica y precisión sobre el alcance funcional

Las fuentes oficiales nacionales son explícitas en cuanto a que los certificados emitidos con token (AC-ONTI) y los emitidos sin token mediante la PFDR (AC-MODERNIZACIÓN) poseen la misma validez jurídica. Corresponde, no obstante, una precisión técnica. El certificado de firma digital remota de la plataforma nacional se emite hoy para personas humanas, en forma gratuita, y su firmador se encuentra orientado a la suscripción de documentos PDF. La equivalencia jurídica, por sí sola, no resuelve la integración: ese firmador no podría incorporarse de inmediato al portal de la SCBA sin desarrollo. Por ello, la propuesta no consiste en utilizar la plataforma nacional tal como hoy se encuentra disponible, sino en abrir la fórmula reglamentaria a toda modalidad de firma digital remota de certificador licenciado, y en definir, con la Subsecretaría de Tecnología Informática de la SCBA, las especificaciones de interoperabilidad correspondientes: validación del lado del servidor, manifiesto de presentación (Parte V), vinculación entre CUIT o CUIL, matrícula y domicilio electrónico, conservación de evidencia y reglas de aceptación de certificados. La equivalencia es jurídica, y la integración es un trabajo técnico acotado y verificable.

Parte III. El régimen vigente de la SCBA y la cuestión reglamentaria

3.1. El reglamento vigente y la mención a AC-ONTI

El Acuerdo 4013 (texto ordenado por el Acuerdo 4039) aprobó el “Reglamento para las presentaciones y notificaciones por medios electrónicos”, vigente desde el 1° de noviembre de 2021 (Resolución 1221/21). Su artículo 1, segundo párrafo, vincula el sistema a certificados digitales emitidos por la Autoridad Certificante AC-ONTI. Esa mención nominativa constituye el aspecto reglamentario que se propone revisar. La cuestión no se ubica en el régimen de firma digital, que ya contempla la modalidad remota, sino en la atadura del reglamento a un único certificador y, por extensión operativa, a un único soporte físico.

3.2. La universalización en curso de la firma digital

Resulta pertinente contextualizar la solicitud. Mediante el Acuerdo 4150, que reorganizó la infraestructura de gestión y control de la firma electrónica y digital y dispuso extender la firma digital a los operadores externos del sistema, y la Resolución SC 1682/24, que aprobó el cronograma de implementación, la Suprema Corte dispuso el reemplazo de la firma electrónica por la firma digital de AC-ONTI, conforme las siguientes etapas: el 1° de agosto de 2024 la vigencia de

los certificados de firma electrónica se redujo de 2 años a 3 meses; el 1° de noviembre de 2024 las renovaciones de firma electrónica pasaron a requerir presencia física; el 1° de marzo de 2025 cesó la renovación de certificados de firma electrónica y se tornó obligatoria la firma digital de AC-ONTI; y el 1° de agosto de 2026 se prevé el apagado de la infraestructura de firma electrónica, quedando únicamente la firma digital. En este contexto institucional, la presente propuesta plantea que, en el mismo movimiento en que se universaliza la firma digital, se admita también su modalidad remota.

3.3. Concentración en una única Autoridad Certificante

El modelo vigente concentra en un solo componente, AC-ONTI, la operatividad del sistema de presentaciones de la Justicia provincial. La licencia operativa de esa Autoridad se renueva por tramos semestrales, conforme la serie verificable de resoluciones nacionales: Resolución SIP 56/2023 (vigente hasta el 10/11/2025); Resolución SICyT 290/2025 (del 11/11/2025 al 11/05/2026); y Resolución SICyT 71/2026 (del 12/05/2026 al 12/11/2026). Los considerandos de las dos últimas dan cuenta, además, de una auditoría de la Sindicatura General de la Nación sobre AC-ONTI, iniciada en junio de 2025 en el marco del artículo 34 de la Ley 25.506, con informe preliminar emitido el 20 de abril de 2026: las prórrogas se otorgaron, precisamente, para evitar perjuicios a los usuarios mientras esa auditoría concluye. A su vez, la vigencia de los certificados emitidos por AC-ONTI se encuentra ligada a la expiración del certificado de la Autoridad Certificante Raíz, que cesa el 13 de noviembre de 2027 (Resolución SIP 15/2020).

Una eventual demora en una prórroga, o una interrupción en la cadena de revocación (CRL/OCSP), produciría la imposibilidad simultánea de presentar escritos electrónicamente para la totalidad de los profesionales de la Provincia. La habilitación de certificadores adicionales y de la modalidad remota constituye, además de una mejora de accesibilidad, una medida de resiliencia y continuidad operativa del servicio de justicia.

3.4. El alcance reglamentario de la propuesta

El núcleo de la propuesta es de redacción reglamentaria, no de régimen de fondo. Se plantea, en primer lugar, aclarar, interpretar o modificar, según corresponda, el artículo 1, segundo párrafo, del Acuerdo 4013 (texto ordenado por el Acuerdo 4039), reemplazando, en su caso, la referencia exclusiva a “AC-ONTI” por una fórmula tecnológicamente neutra (Parte VI). Si el texto vigente ya admitiera una lectura amplia, la cuestión sería de implementación técnica y de política operativa; si resultara restrictivo, correspondería la reforma reglamentaria expresa. En segundo lugar, adecuar en lo pertinente la implementación del Acuerdo 4150 y de la Resolución SC 1682/24, de modo que el proceso de universalización de la firma digital contemple expresamente la modalidad remota y la pluralidad de certificadores. En tercer lugar, solicitar a la Subsecretaría de Tecnología Informática de la SCBA un dictamen de interoperabilidad y un cronograma de implementación, con prueba piloto. Ninguna de estas medidas exige reformar la Ley 13.666 ni el régimen de fondo de la firma digital.

Parte IV. Antecedentes en el sistema argentino

4.1. El Poder Judicial de la Ciudad de Buenos Aires: el sistema EJE y la firma dual

El Poder Judicial de la CABA tramita sus causas a través del sistema EJE (Expediente Judicial Electrónico) y su Portal del Litigante, accesible desde computadora o desde dispositivos móviles. En materia de firma, el sistema EJE implementa una firma dual: el usuario puede suscribir con token o con firma digital remota ("Firma Cloud"), esta última desde la computadora, la tableta o el celular, sin necesidad de tener un dispositivo conectado. Token y firma remota conviven en el mismo sistema, sin que ello degrade la validez ni la seguridad de los actos.

4.2. El Consejo de la Magistratura como Autoridad de Registro de la PFDR

El soporte institucional de ese esquema resulta comparable como antecedente de factibilidad, sujeto a la evaluación técnica propia de la SCBA. Por Resolución RESOL-2019-146-APN-SECMA#JGM (6/12/2019), el Consejo de la Magistratura de la CABA fue constituido como Autoridad de Registro de la AC-MODERNIZACIÓN dentro de la Plataforma de Firma Digital Remota nacional, quedando habilitado a emitir certificados de firma digital remota, en forma gratuita, dentro de la PFDR. Por Resolución de Presidencia del Consejo de la Magistratura N° 308/2021 se instruyó el despliegue de la firma digital remota mediante la plataforma nacional, habilitando a los magistrados a firmar desde cualquier dispositivo. La Oficina de Defensa del Litigante actúa como Autoridad de Registro para los usuarios externos y abogados.

En síntesis, un órgano de un poder judicial argentino se integró a la PFDR nacional como Autoridad de Registro y habilitó la firma remota para sus jueces y para los letrados, en convivencia con el token.

4.3. Otros antecedentes

La firma digital remota no constituye una tecnología experimental. Operan bajo el mismo marco de la Ley 25.506:

Organismo	Implementación
AC-MODERNIZACIÓN (Nación)	Emite certificados de firma digital remota sin token desde 2018, con idéntica validez jurídica que los de AC-ONTI.
Provincia de Buenos Aires (DPSIT)	La Dirección Provincial de Sistemas de Información y Tecnologías se constituyó en 2019 como Autoridad de Registro de la AC-MODERNIZACIÓN dentro de la PFDR, y emite firma digital remota sin token a los agentes provinciales.
Poder Judicial de la CABA	Sistema EJE con firma dual (token y Firma Cloud) desde computadora y dispositivos móviles.
Consejos y colegios profesionales	Diversos consejos profesionales de la Provincia tramitan firma digital remota sin cargo para sus matriculados.

RENAPER; ex ANMaC (hoy RENAR); universidades nacionales	Constituidos como Autoridades de Registro de firma digital remota a nivel nacional.

4.4. La armonización con la práctica del Poder Ejecutivo provincial

El dato de mayor peso institucional dentro de la propia jurisdicción consiste en que el Poder Ejecutivo bonaerense emite y acepta firma digital remota sin token para sus propios agentes, a través de la DPSIT. Resulta institucionalmente armónico que la justicia provincial pueda contemplar, también en su régimen, esa misma modalidad operativa. Esta referencia debe tomarse con una precisión: que una modalidad opere en el ámbito del Poder Ejecutivo no significa que pueda incorporarse sin adaptación al proceso judicial. Su valor reside en demostrar que la Provincia conoce y utiliza la firma digital remota. La integración con el expediente, la matrícula, el domicilio electrónico, el cargo, los adjuntos y la validación histórica de actuaciones corresponde a la evaluación técnica propia de la SCBA.

Parte V. Arquitectura técnica y equivalencia de seguridad

(Síntesis. El desarrollo técnico se incluye en el Anexo, manteniéndose el cuerpo del informe en un plano jurídico-institucional evaluable por las áreas competentes de la SCBA.)

5.1. Defensa en profundidad

La firma digital remota no consiste en reemplazar un token por una contraseña. Opera mediante varias capas de seguridad que deben autorizarse para que la firma se ejecute: validación de identidad y matrícula; autenticación multifactor (algo que se sabe, algo que se tiene, algo que se es) con credenciales conformes al estándar WebAuthn/FIDO2; autorización por operación individual (cada firma dispara una confirmación fuera de banda en el dispositivo del profesional, con biometría y ventana temporal antirrepetición); motor de análisis de riesgo contextual; firma dentro de un módulo de seguridad de hardware (HSM) del que la clave privada no resulta exportable, con validación de revocación (CRL/OCSP) y sellado de tiempo (TSA, RFC 3161); y evidencia inmutable mediante registros de solo adición.

Corresponde una precisión técnica: WebAuthn/FIDO2 no constituye la firma digital del acto procesal ni reemplaza al certificado. Opera como capa de autenticación fuerte y de autorización por operación. La firma jurídicamente relevante sigue siendo la firma digital basada en certificado emitido por certificador licenciado, con clave no exportable en HSM, validación de revocación y evidencia auditable.

5.2. Comparación por riesgos y controles

La comparación se formula por riesgos y controles verificables, evitando afirmaciones absolutas contra el token o a favor de la firma remota: ambos modelos presentan riesgos y controles, y la propuesta preserva la coexistencia de ambas modalidades.

Vector	Riesgo en token físico	Control exigible en firma remota
Robo o pérdida	Riesgo mitigado por PIN, bloqueo y revocación; requiere reposición física.	Autenticación multifactor, revocación de credenciales y reenrolamiento controlado.
Malware local	La operación depende del equipo, el driver, el navegador, el token y el componente local de firma.	Autorización por operación, canal fuera de banda y validación del acto del lado del servidor.
Suplantación	Deben protegerse el token, el PIN y el entorno local.	Vinculación de identidad, CUIT o CUIL, matrícula, dispositivo autorizado y confirmación de cada firma.
Repudio o controversia	La firma digital presume autoría e integridad; conviene conservar evidencia de contexto.	Conservación de certificado, número de serie, emisor, sello de tiempo, estado OCSP/CRL, hash y registros auditables.
Continuidad operativa	Depende de hardware, drivers, navegador, componente local y de la infraestructura de clave pública.	Coexistencia con el token y operación bajo protocolo de contingencia y homologación de la SCBA.

5.3. El manifiesto de presentación

La principal contribución técnica de la propuesta no se limita al modo en que se firma, sino al objeto firmado. En lugar de suscribir un PDF aislado, el portal generaría un manifiesto estructurado que representa la presentación judicial completa. El manifiesto debe ser canónico, de modo de evitar controversias sobre cuál fue la representación exacta que se firmó, y debe vincular: expediente y organismo, tipo de acto, profesional, matrícula y domicilio electrónico, fecha y hora del servidor, resúmenes criptográficos (hashes) del escrito principal y de cada adjunto, la versión del esquema, el nombre, el tamaño y el tipo de cada archivo, la huella y el número de serie del certificado, el emisor, la política de certificación, el estado de revocación (OCSP o CRL) al momento de la firma, el sello de tiempo, un identificador único de transacción y el cargo electrónico.

De ese modo, la firma queda vinculada a todo el acto procesal; cualquier alteración posterior resulta detectable por comparación de hashes; y el portal conserva el control sobre validez, identidad y trazabilidad, con independencia del medio técnico de firma. Esta arquitectura permite que token y firma remota convivan sin pérdida de garantías.

5.4. Sobre la ventaja técnica del token

El token presenta una ventaja teórica, en tanto no requiere conectividad en el instante de la operación criptográfica. El portal de la SCBA, sin embargo, ya exige conexión a internet para

presentar escritos, y la presentación procesal completa requiere conectividad y validación posterior. Firmar sin conectividad un documento destinado al portal resulta una operación sin objeto práctico, por lo que la ventaja, real en abstracto, no resulta aplicable al caso. Tampoco elimina, para ninguna de las dos modalidades, la necesidad de mecanismos de contingencia y de interoperabilidad.

Parte VI. Propuesta normativa concreta

La presentación ante la Suprema Corte, por intermedio del Colegio de Abogados de la Provincia de Buenos Aires (Ley 5177, artículo 50 inciso a), contendría las siguientes solicitudes.

6.1. Aclaración del texto vigente y, en su caso, reforma del reglamento

Aclarar formalmente el alcance del artículo 1, segundo párrafo, del Reglamento aprobado por Acuerdo 4013 (texto ordenado por Acuerdo 4039), en cuanto a los certificados digitales admitidos por el sistema. Para el caso de que la referencia a "AC-ONTI" importe una exclusividad reglamentaria u operativa no fundada, modificar dicho párrafo reemplazando esa referencia por la siguiente fórmula tecnológicamente neutra:

> *"Las presentaciones y notificaciones electrónicas se suscribirán con firma digital basada en certificados emitidos por certificadores licenciados o reconocidos conforme la Ley 25.506 y su normativa reglamentaria, admitiéndose tanto la modalidad mediante dispositivo criptográfico (token) como la modalidad de firma digital remota con custodia centralizada de claves prevista en la Resolución SIP 86/2020, en las condiciones de interoperabilidad que establezca la Subsecretaría de Tecnología Informática."*

Asimismo, adecuar en lo pertinente la implementación del Acuerdo 4150 y de la Resolución SC 1682/24, de modo que el proceso de universalización de la firma digital contemple expresamente la modalidad remota y la pluralidad de certificadores.

6.2. Dictamen técnico e interoperabilidad

Peticionar a la Subsecretaría de Tecnología Informática de la SCBA para que: (a) evalúe la arquitectura de firma digital remota conforme a los estándares internacionales aplicables (FIPS 140-3, sucesor del FIPS 140-2, o Common Criteria; WebAuthn/FIDO2; RFC 3161); (b) emita dictamen sobre los requisitos de interoperabilidad que deberían satisfacer los proveedores, incluidas las especificaciones del manifiesto de presentación, la validación del lado del servidor, la verificación del estado de revocación (OCSP/CRL), el sello de tiempo y una matriz de pruebas de compatibilidad de navegadores; y (c) proponga un cronograma de implementación con hitos verificables.

6.3. Prueba piloto

Autorizar una prueba piloto, de duración no inferior a seis meses, con un grupo acotado de matriculados del Departamento Judicial de San Isidro, en convivencia con el régimen de token, a efectos de validar la interoperabilidad técnica antes de la habilitación general.

6.4. Medida de resiliencia operativa

Tomar nota de la concentración normativa y operativa en AC-ONTI (cuya licencia se renueva por tramos semestrales y se encuentra vigente hasta el 12/11/2026, conforme Resolución SICyT 71/2026), y evaluar la ampliación de la fórmula de admisión de certificadores como medida de continuidad operativa del servicio de justicia, con independencia del resultado de la solicitud principal.

6.5. Protocolo de contingencia procesal

Solicitar el dictado de un protocolo de contingencia procesal que establezca el procedimiento aplicable ante supuestos de no renovación, suspensión o caducidad de la licencia de la autoridad certificante, observación crítica de auditoría, indisponibilidad de los servicios de revocación (CRL/OCSP), falla del componente local de firma, incompatibilidad de navegadores o imposibilidad masiva de firmar. El protocolo debería prever, como mínimo, la constancia técnica del evento, una vía de presentación alternativa, el resguardo o la suspensión de los plazos afectados y el mecanismo de regularización posterior de las actuaciones.

Anexo. Arquitectura técnica de referencia

La presente arquitectura se describe como referencia de factibilidad y base para el diálogo técnico. Las especificaciones definitivas corresponden al dictamen de la Subsecretaría de Tecnología Informática de la SCBA (punto 6.2).

1. **Capa 1. Identidad.** Validación contra el padrón del Colegio y la matrícula vigente en la SCBA. Enrolamiento inicial con documento y registro biométrico, conforme los mecanismos de validación de identidad admitidos por la reglamentación vigente (incluida la validación a distancia del Decreto 743/2024). Vinculación al domicilio electrónico registrado.

2. **Capa 2. Autenticación de sesión multifactor.** Contraseña (algo que se sabe); dispositivo enrolado con clave protegida en el área segura del procesador (algo que se tiene); biometría local (algo que se es); credencial conforme WebAuthn/FIDO2, resistente a la suplantación de sitios (phishing).

3. **Capa 3. Autorización por operación.** Cada firma dispara una notificación en tiempo real al dispositivo enrolado, con el resumen criptográfico del documento, la carátula y el organismo de destino. La firma se ejecuta solo con biometría y PIN de firma (distinto al de sesión), dentro de una ventana temporal breve con identificador de un solo uso (antirrepetición).

4. **Capa 4. Análisis de riesgo contextual.** Monitoreo de patrones de uso y señales anómalas, con autenticación reforzada ante alertas (verificación adicional por canal independiente).

5. **Capa 5. Firma en módulo de seguridad de hardware (HSM).** Custodia de la clave privada en módulo certificado conforme estándares internacionales (FIPS 140-3, sucesor del FIPS 140-2, o Common Criteria). La clave se genera dentro del módulo y no resulta exportable. Validación de revocación en tiempo real (CRL/OCSP) y sellado de tiempo externo (TSA, RFC 3161).

6. **Capa 6. Evidencia inmutable.** Registro de solo adición por cada firma ejecutada: hash del documento, certificado utilizado, factores de autenticación presentados, identificación del dispositivo, sello de tiempo y referencia al expediente, disponible para auditoría del profesional y de la SCBA.

7. **Capa 7. Manifiesto de presentación.** Firma sobre un manifiesto canónico que vincula el acto procesal completo, conforme la Parte V del informe, con validación del lado del servidor por parte del portal.